Manuals+ — User Manuals Simplified.

Roger MCT84M-BK-QB Access Control System Instruction Manual

Home » ROGER » Roger MCT84M-BK-QB Access Control System Instruction Manual

Contents

roger®

Roger MCT84M-BK-QB Access Control System

Product Information

Specifications

- **Product:** Roger Access Control System
- **Model:** MCT84M-BK-QB
- **Product Version:** 1.0
- **Firmware Version:** 1.0.10.216
- **Document Version:** Rev.E

Design and Application

- **Characteristics**
  The Roger Access Control System MCT84M-BK-QB is designed for secure access control applications.
- **Power Supply**
  The system can be powered using UTP wire pairs with varying lengths as indicated in Table 2.
- **RS485 Bus**
  The system utilizes an RS485 bus for communication.
- **LED Indicators**
  The terminals are equipped with LED indicators that provide visual feedback on system status and functions. Refer to Table 3 for details on LED indicators.
- **Buzzer**
  The system includes a buzzer for audible notifications of system functions.
- **Tamper Detector**
  The terminals are equipped with tamper detectors for enhanced security.

Installation
Refer to the installation manual for detailed wiring instructions. See Figure 8 for an overview of the installation process.

Product Usage Instructions

- **MIFARE Cards**

  The system supports MIFARE cards for user identification. Refer to the AN024 application note for information on programming MIFARE cards.
- **Mobile Devices (NFC and BLE)**

  Mobile devices with NFC and BLE capabilities can be used for authentication with the system.
- **Barcodes**

  Barcodes can also be used as an authentication factor in the system.

FAQ

Q: Can I use third-party RFID cards with the system?
A: While it is possible to use RFID cards from other sources, it is recommended to conduct tests to ensure compatibility and satisfactory operation with the Roger device and software.

DESIGN AND APPLICATION

The MCT84M-BK-QB is an identification terminal dedicated to the RACS 5 access control system. Optionally, the reader can be configured to open communication protocol and used in other scenarios (e.g. in automation systems). Users can be identified by use of a QR code, BLE/NFC mobile ID, or proximity card. Reader supports encrypted QR codes that are compatible with Roger standard or non-encrypted codes. The encrypted QR codes can be generated from RACS 5 system software. They may be available in the form of printed images (labels) or displayed on a phone. BLE/NFC mobile identification requires RMK (Roger) mobile application (iOS/Android). When connected to the MC16 controller reader can operate as an access and/or Time&Attendance terminal and serve as a building automation control point. The neutral design of the enclosure matches various styles of traditional or modern interiors.

Characteristics

- RACS 5 system access terminal
- read MIFARE Ultralight/Classic/DESFire (EV1, EV2, EV3)/Plus cards
- read NFC and BLE mobile identifiers
- read encrypted QR codes
- read unencrypted bar codes 1D and 2D
- RS485 interface with EPSO 3 protocol (RACS 5 system)
- RS485 open protocol as an option
- outdoor operation
- CE, RoHS
- dimensions: 130,0 x 45,0 x 22,0 mm

Power supply
The terminal requires power supply voltage in the range of 11-15VDC. It can be supplied from the MCX2D/MCX4D expander of MC16-PAC-KIT, from the MC16 access controller (e.g. TML output), or from a dedicated power supply unit. The supply wire diameter must be selected in such a way that the voltage drop

between the supply output and the device would be lower than 1V. The proper wire diameter is especially critical when the device is located in long distance from the supply source. In such a case the use of a dedicated power supply unit located close to the device should be considered. When a separate power supply unit is used then its minus should be connected to the controller’s GND using signal wire with any diameter. It is recommended to use a UTP cable for the connection of the device to the controller. The table below shows the maximal UTP cable lengths for the number of wires used for the power supply.

Table 2. Power supply cabling	
Number of UTP wire pairs for power supply	Maximal length of power supply cable
1	150m
2	300m
3	450m
4	600m

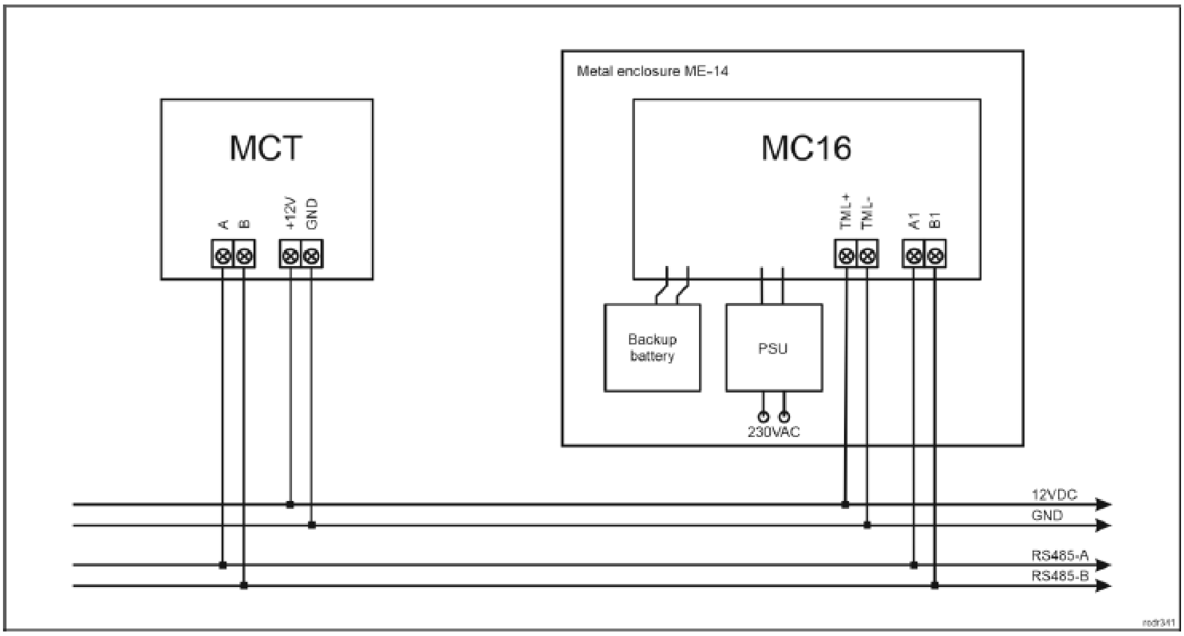


Fig. 1 MCT supply from MC16 access controller

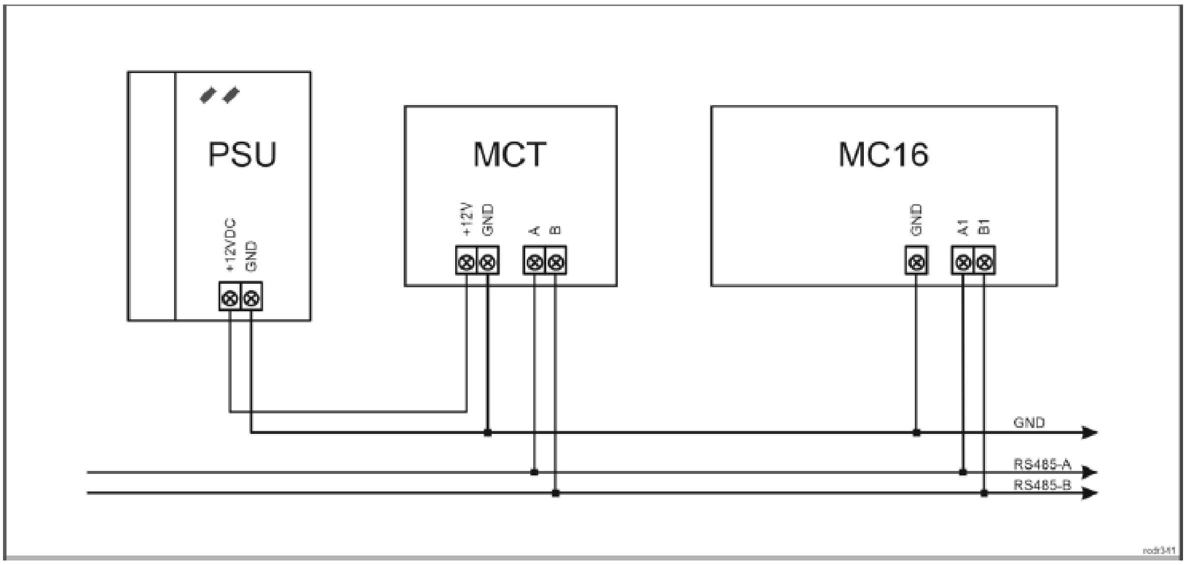


Fig. 2 MCT supply from dedicated power supply unit

RS485 bus

The communication method with the MC16 access controller is provided with an RS485 bus which can encompass up to 16 devices of the RACS 5 system, each with a unique address in the range of 100-115. The bus topology can be freely arranged as a star, tree, or any combination of them except for a loop. The matching resistors (terminators) connected at the ends of transmitting lines are not required. In most cases, communication works with any cable type (standard telephone cable, shielded or unshielded twisted pair, etc.) but the recommended cable is an unshielded twisted pair (U/UTP cat.5). Shielded cables should be limited to installations subject to strong electromagnetic interferences. The RS485 communication standard used in the RACS 5 system guarantees proper communication in a distance of up to 1200 meters as well as high resistance to interferences.

Note:
Do not use more than a single pair in UTP cable for the RS485 communication bus.

LED indicators

Terminals are equipped with three LED indicators which are used to signal integral functions and they can be additionally programmed with other available functions within high-level configuration (VISO).

Table 3. LED indicators

Indicator	Color	Integral functions
LED STATUS	Red/green	The default color of the indicator is red. If the terminal is assigned to an Alarm Zone, then the LED indicates zone arming (red) or disarming (green).
LED OPEN	Green	LED indicates access granting.
LED SYSTEM	Orange	LED indicates card reading and can signal other system functions including device malfunction.

Note: Synchronic pulsing of LED indicators signifies lost communication with the MC16 controller.

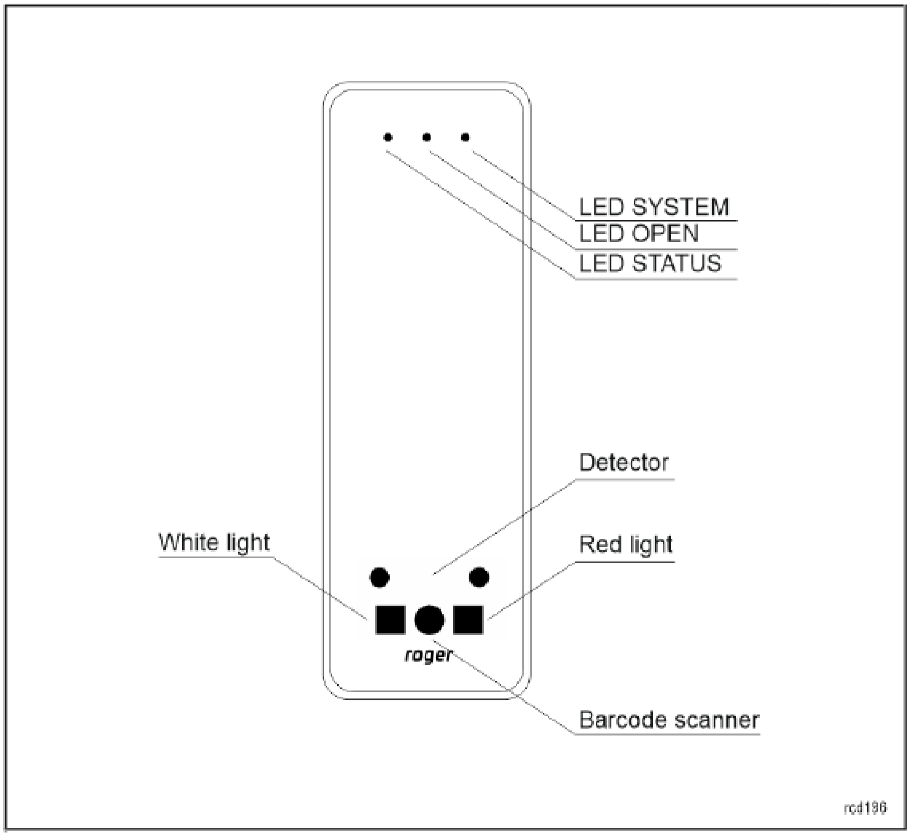


Fig. 3 LED indicators and barcode scanner

Buzzer
Terminals are equipped with a buzzer which is used to signal integral functions and it can be additionally programmed with other available functions within a high-level configuration (VISO).

Tamper detector
Built-in tamper (sabotage) detector enables detection of unauthorized opening of the device's enclosure as well as detachment of the enclosure from the wall. The detector is internally connected to the terminal's input. It does not require low-level configuration or any additional installation arrangements, but it is essential to mount the front panel in such a way that the tamper detector (fig. 4) would firmly press the back panel. The detector requires high-level configuration which consists of the assignment of the function [133] Tamper Toggle on the level of a Main Board of a controller in the VISO software navigation tree.

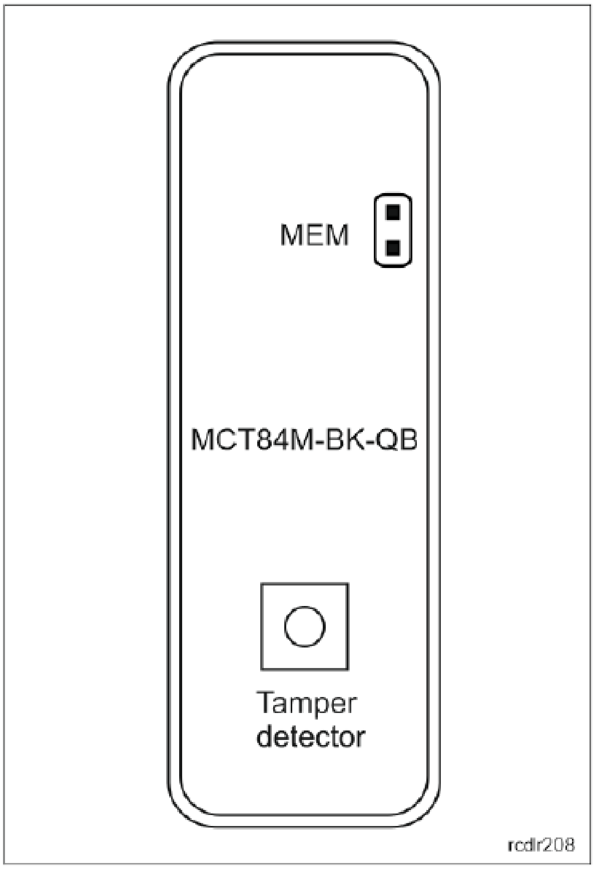


Fig. 4 Programming jumpers

Identification

Depending on the version, the following user identification methods are offered by terminals:

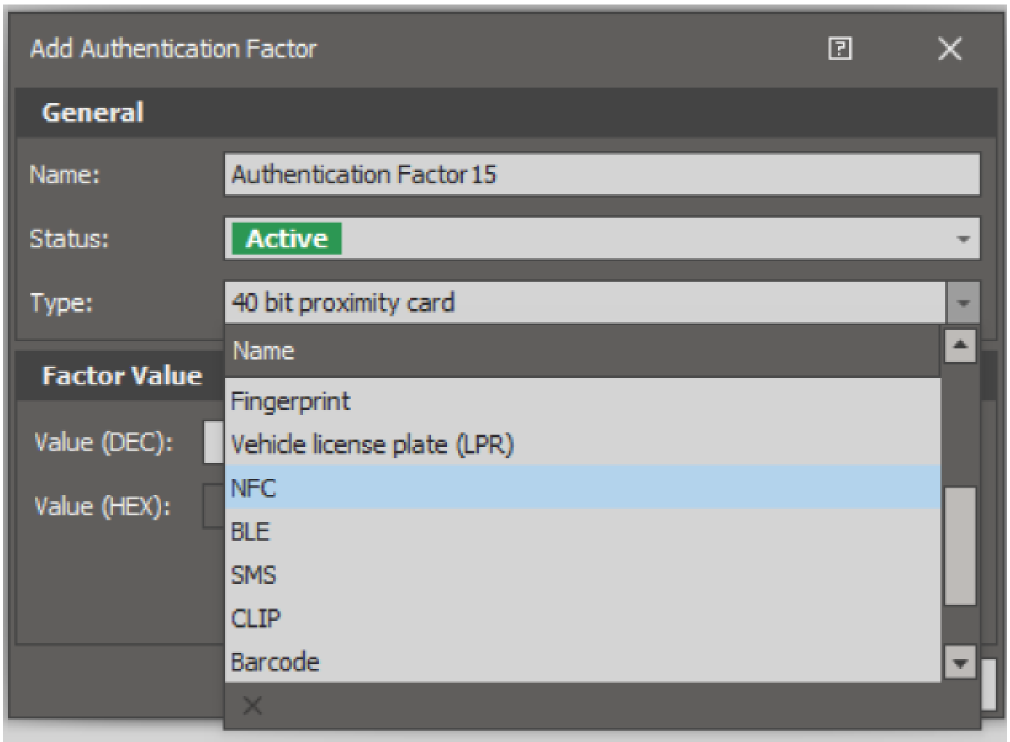
- MIFARE Ultralight/Classic proximity cards
- Mobile devices (NFC and BLE)
- 1D and 2D barcodes

MIFARE cards
By default, the terminal reads serial numbers (CSN) of MIFARE cards, but it is possible to program cards with their 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 card programming is given in the AN024 application note which is available at www.roger.pl.

The technical characteristics of the device are guaranteed for RFID cards supplied by Roger. Cards from other sources may be used, but they are not covered by the manufacturer’s warranty. Before deciding to use specific Roger products with third-party contactless cards, it is recommended to conduct tests that will confirm satisfactory operation with the specific Roger device and software in which it operates.

Mobile devices (NFC and BLE)
The MCT84M-BK-QB terminal enables the identification of users using mobile devices based on NFC (Android) and Bluetooth (Android, iOS) technology. Before starting to use BLE/NFC identification as part of the low-level configuration of the device (see point 4), define your own BLE/NFC Code Encryption Key and BLE/NFC Communication Encryption Key, and in the case of Bluetooth, additionally verify whether the BLE parameter is enabled. Install the Roger Mobile Key (RMK) application on the mobile device and set the same parameters as in the terminal. Create a key (authentication factor) in RMK by defining its type and number and then create the same authentication factor in the VISO program (fig. 5) assigning it to a user with Authorizations on the terminal. For identification, the user can select the key (authentication factor) in the RMK manually on the screen of the

mobile device.



Add Authentication Factor

General

Name: Authentication Factor 15

Status: Active

Type: 40 bit proximity card

Factor Value

Value (DEC):

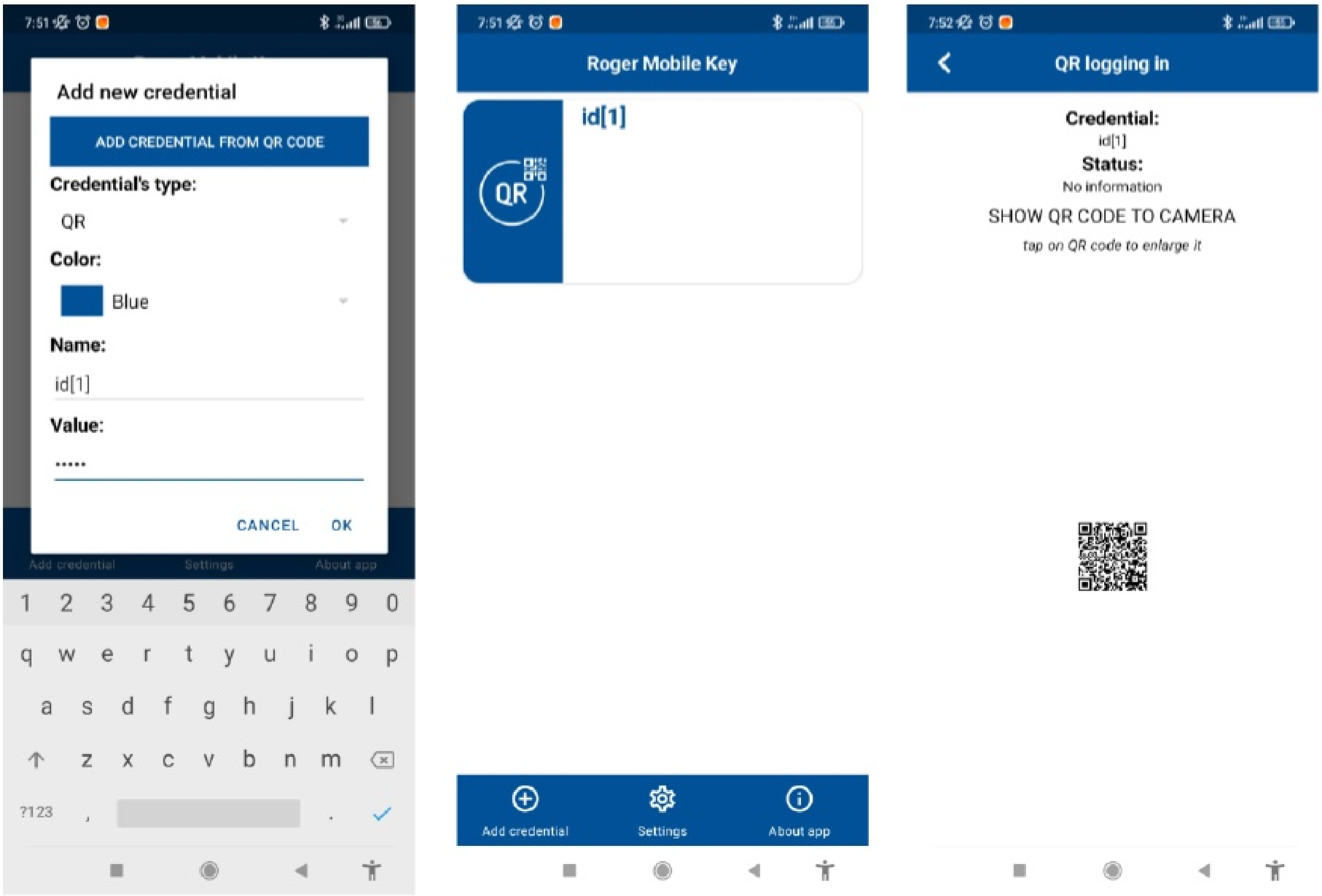
Value (HEX):

Fig. 5 Authentication factor type for NFC identification in VISO software

Barcodes

The MCT84M-BK-QB terminal supports encrypted QR codes and unencrypted one-dimensional (1D) and two-dimensional (2D) barcodes. By default, the terminal supports encrypted QR codes generated in the Roger Mobile Key application. The option to handle clear codes is disabled by default and can be changed via low-level configuration (RogerVDM).

Before using barcode scanner identification, you must define your own NFC/BLE Encryption Key and NFC/BLE Communication Encryption Key as part of the low-level configuration of the device (see point 4). Install the Roger Mobile Key (RMK) application on the mobile device and set the same parameters as in the terminal. Create a new identifier in RMK by defining its type as QR and value (fig. 6) Then create the same authentication factor in VISO (fig. 7) assigning it to a user with Authorizations on the terminal. For identification, the user can select the key (authentication factor) in the RMK manually on the screen of the mobile device.



Add new credential

Credential's type: QR

Color: Blue

Name: id[1]

Value: •••••

Roger Mobile Key

id[1]

QR logging in

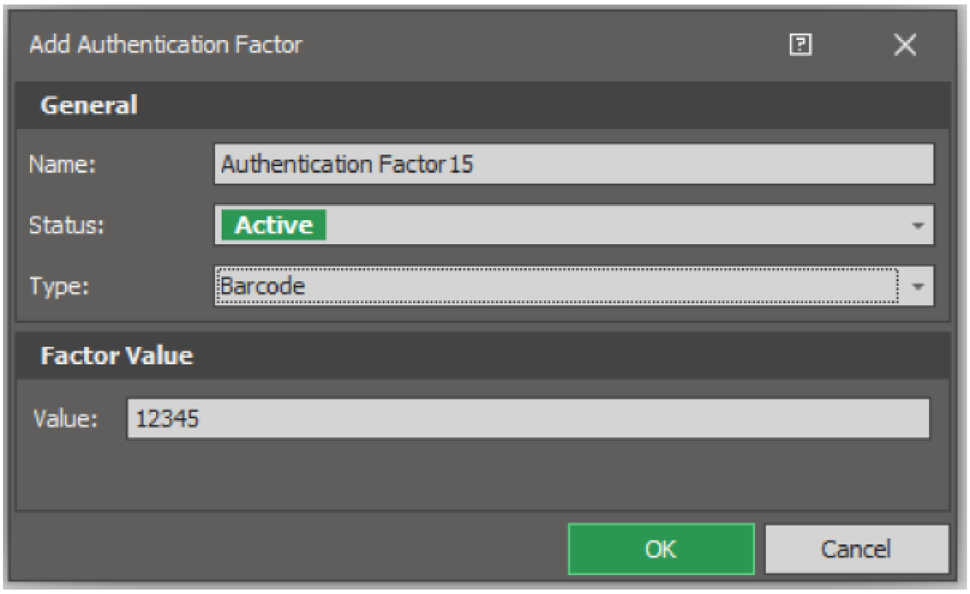
Credential: id[1]

Status: No information

SHOW QR CODE TO CAMERA

tap on QR code to enlarge it

Fig. 6 Defining a QR code in the Roger Mobile Key app.



Add Authentication Factor

General

Name: Authentication Factor 15

Status: Active

Type: Barcode

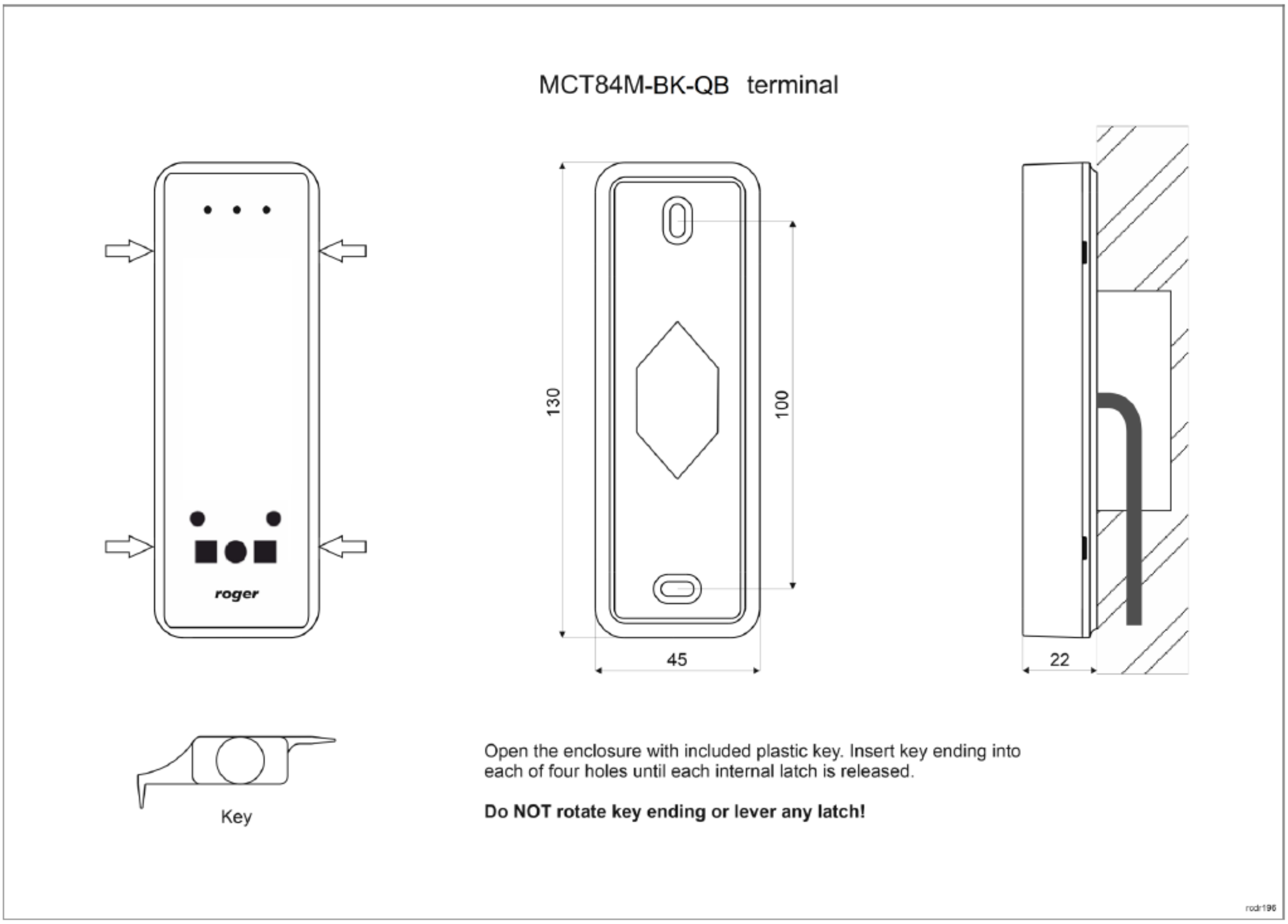
Factor Value

Value: 12345

Fig. 7 Authentication factor type for the barcode in the VISO program

INSTALLATION

Table 3. Wires		
Name	Wire colour	Description
12V	Red	12VDC power supply
GND	Black	Ground
A	Yellow	OSDP interface, line A
B	Green	OSDP interface, line B



Open the enclosure with included plastic key. Insert key ending into each of four holes until each internal latch is released.

Do NOT rotate key ending or lever any latch!

Fig. 8 MCT84M-BK-QB installation

Note:
MCT84M-BK-QB enclosure consists of a front panel and a back panel. The new device is assembled with a standard back panel, but an additional free-of-charge, extended back panel is included. This panel can be used when the connection cable has to be hidden and no flush mounting box is available.

Installation guidelines

- The terminal should be mounted on a vertical structure (wall) away from sources of heat and moisture.
- The front panel should be attached in such a way that the tamper detector (fig. 4) would firmly press the back panel.
- All electrical connections should be done with a disconnected power supply.
- If the terminal and controller are not supplied from the same PSU, then the GND terminals of both devices must

be connected with any wire.

- The device can be cleaned using a wet cloth and mild detergent without abrasive components. In particular do not clean with alcohols, solvents, petrol, disinfectants, acids, rust removers, etc. Damages resulting from improper maintenance and usage are not covered by the manufacturer’s warranty.
- If the device is installed in a place exposed to conductive dust (e.g. metal dust), the MEM/RST/FDM pins should be protected with plastic mass, e.g. silicone, after installation.
- If the reader is installed in EU countries, the BLE radio power level (parameters: BLE broadcasting power [dBm] and BLE transmission power [dBm]) should be set to 1(-18dBm).

OPERATION SCENARIOS

The terminal when connected to the MC16 access controller can be at the same time used for access control and Time&Attendance. An example of a connection diagram for such a scenario is shown in Fig. 7 where inputs and outputs from the MC16 board are used and in Fig. 8 where inputs and outputs from –the IO version terminal are used. The terminal can also operate with an MC16 controller using MCX2D/MCX4D expanders as in the case of the M16-PAC-KIT series. Various scenarios of operation with MC16 controllers are presented in the AN002 application note.

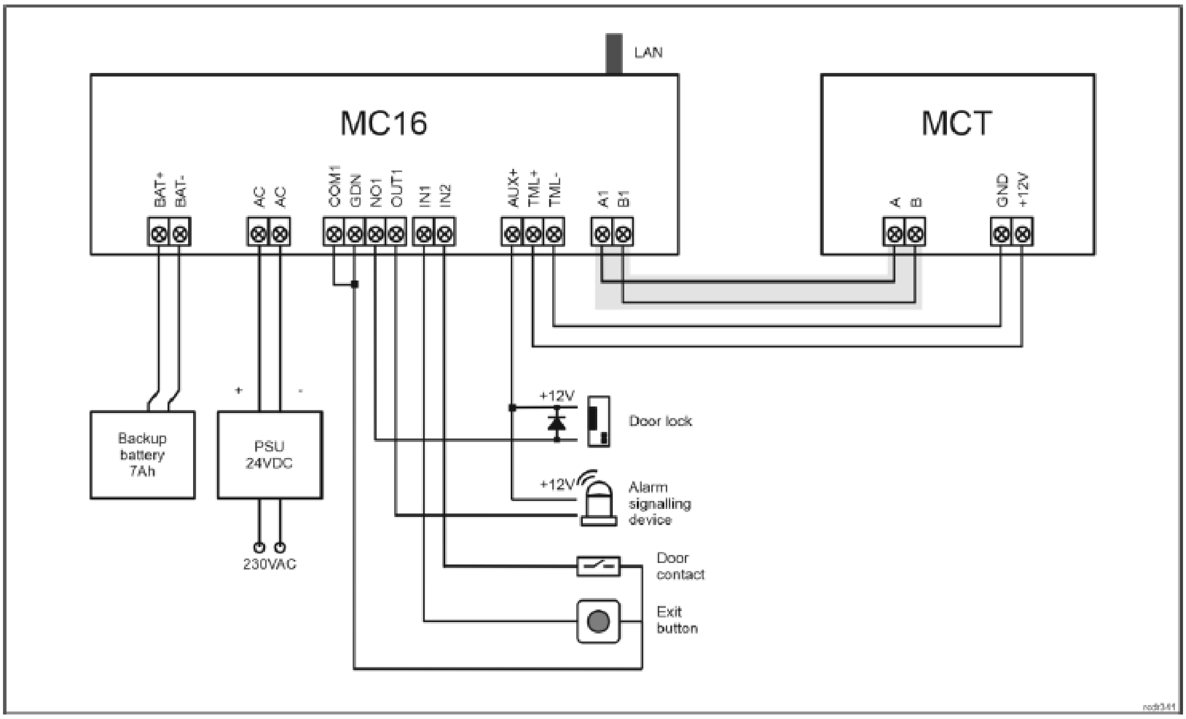


Fig. 9 Typical connection diagram for the terminal and MC16 access controller

CONFIGURATION

The purpose of low-level configuration is to prepare the device for operation in the RACS 5 system. In the case of the RACS 5 v1 system, the address of the device must be configured using RogerVDM software or by manual addressing before connection to the MC16 controller. While in the RACS v2 system, low-level configuration and addressing can be done with VISO v2 software during the final configuration of the system. Therefore in the RACS 5 v2 system, the configuration from RogerVDM software and manual addressing are optional and during installation, it is only necessary to properly connect the device to the MC16 access controller.

Low-level configuration (VISO v2)

In the RACS 5 v2 system the reader can be installed at the site without previous configuration. According to the AN006 application note, its address and other settings can be configured from VISO v2 management software, and during such configuration, access to its service contacts (fig. 4) is not required.

Low level configuration (RogerVDM)
Programming procedure with RogerVDM software:

1. Connect the device to the RUD-1 interface (fig. 9) and connect the RUD-1 to the computer's USB port.
2. Remove the jumper from MEM contacts (fig. 4) if it is placed there.
3. Restart the device (switch the power supply off and on or short RST contacts for a moment) and the orange LED SYSTEM will pulsate. Then within 5 seconds place the jumper on MEM contacts.
4. Start the RogerVDM program, select the MCT device, firmware version, RS485 communication channel, and serial port with RUD-1 interface.
5. Click Connect, and the program will establish a connection and will automatically display the Configuration tab.
6. Enter unoccupied RS485 addresses in the range of 100-115 and other settings according to the requirements of a specific installation.
7. Click Send to Device to update the configuration of the device.
8. Optionally make a backup by clicking Send to File… and saving settings to file on disk.
9. Disconnect from RUD-1 interface and leave a jumper on MEM contacts to enable further configuration of the device from VISO v2 software or remove the jumper from MEM contacts to block such remote configuration.

Note: Do not read any cards nor press the keypad when the reader is configured with RogerVDM.

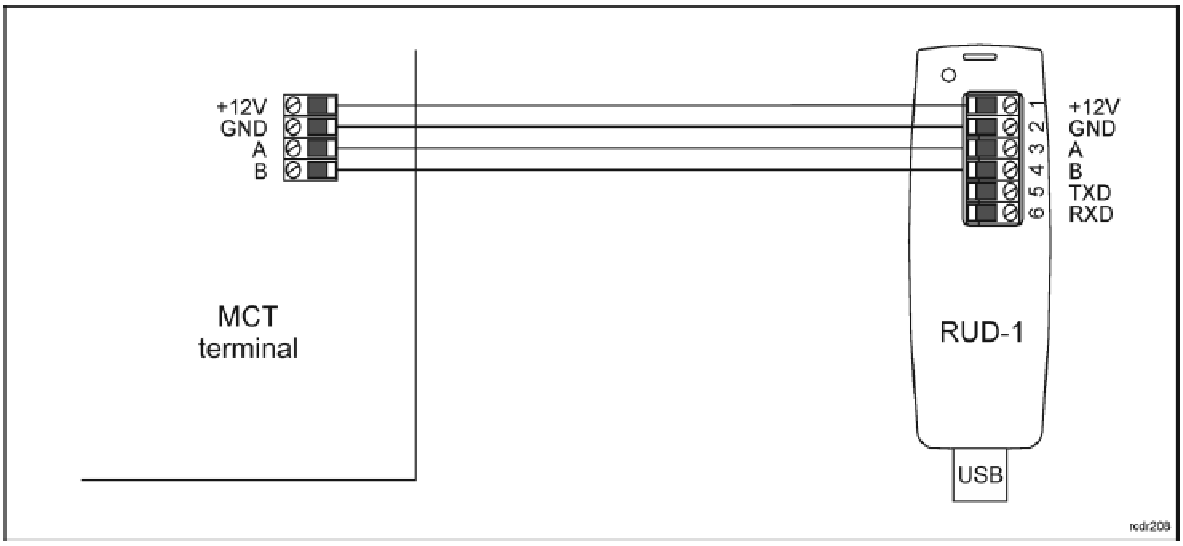


Fig. 10 Connection to RUD-1 interface (low level configuration)

Table 6. List of low-level parameters	
Communication settings	
Communication interface	The parameter defines the communication method of the device with the c ontroller.
	Range: [0]: RS485, [3] Asynchronous mode. Default value: [0]: RS485.
RS485 address	The parameter defines the device address on the RS485 bus. Range: 100 -115. Default value: 100.

RS485 encryption	The parameter enables encryption at the RS485 bus. Range: [0]: No, [1]: Yes. Default value: [0]: No.
RS485 encryption key	The parameter defines the key for the encryption of communication at the RS485 bus. Range: 4-16 ASCII characters.
Asynchronous mode type	The parameter defines a format for asynchronous mode. Range: [0]: AF type undefined, [1]: AF type defined in prefix, [2] EPSO3. Default value: [0]: AF type undefined.
Asynchronous mode rate [bps]	The parameter defines the transmission rate for asynchronous mode. Range: [2]: 1200, [4]: 2400, [8]: 4800, [16]: 9600, [24]: 14400, [32]: 19200, [48]: 28800, [96]: 57600, [192]:115200. Default value: [16]: 9600.
Mobile authentication	
NFC/BLE authentication factor encryption key	The parameter defines the key for the encryption of NFC/BLE communication. Range: 4-16 ASCII characters.
NFC/BLE communication encryption key	The parameter defines the key for the encryption of NFC/BLE communication. Range: 4-16 ASCII characters.
BLE authentication factor class	The parameter defines acceptable types of keys (authentication factors) created in the Roger Mobile Key app for Bluetooth (BLE) communication. UCE means lower security and quicker identification while REK means higher security and slower identification. It is necessary to apply classes in RMK that are acceptable for the terminal. Range: [1]: REK, [2]: UCE, [3]: UCE + REK. Default value: [3]: UCE + REK.
NFC authentication factor class	The parameter defines the acceptable type of keys (authentication factors) created in the Roger Mobile Key app for NFC communication. UCE means lower security and quicker identification while REK means higher security and slower identification. It is necessary to apply classes in RMK that are acceptable for the terminal. Range: [1]: REK, [2]: UCE, [3]: UCE + REK. Default value: [3]: UCE+REK.
Optical signalization	
RS485 communication timeout [s]	The parameter defines the delay after which the device will start signaling a lack of communication with the controller on the LED indicators. Value 0 disables signaling. Value range: 0-64 seconds. Default value 20.
LED SYSTEM pulsing when card near the reader	The parameter enables the LED SYSTEM (orange) to pulse when the card is close to the device. Range: [0]: No, [1]: Yes. Default value: [0]: No.
Backlight level [%]	The parameter defines the backlight level. When set to 0 the backlight is disabled. Range: 0-100. Default value: 100.
The backlight switches off when no activity	The parameter enables temporary backlight dimming whenever the card is read, or the key is pressed. Range: [0]: No, [1]: Yes. Default value: [1]: Yes.
LED SYSTEM flash after card read	The parameter enables a short flash of LED SYSTEM (orange) when the card is read. Range: [0]: No, [1]: Yes. Default value: [1]: Yes.
Acoustic signalisation	

Buzzer loudness level [%]	The parameter defines the buzzer’s loudness level. When set to 0 the buzzer is disabled Range: 0-100. Default value: 100.
Short sound after card read	The parameter enables a short sound (beep) generated by the buzzer when the card is read. Range: [0]: No, [1]: Yes. Default value: [1]: Yes.
Advanced settings	

AF type	The parameter defines the authentication factor type returned by the terminal. Default value: [0010]: Number 40bits.
Long card read time [s]	The parameter defines long card read time. When set to 0 then a long read is disabled. Range: 0-64. Default value: 0.
Long key press time [s]	The parameter defines long press time for such key types as [*], [#], and [F1] – [F4]. When set to 0 the long press is disabled. Range: 0-64. Default value: 2.
BLE activated	The parameter enables the deactivation of Bluetooth transmission. Range: [0]: No, [1]: Yes. Default value: [1]: Yes.
BLE session timeout [s]	The parameter defines the maximal time for establishing a connection between the mobile device and the terminal in Bluetooth technology. When timeout elapses, the session is interrupted by the terminal so the mobile device can attempt to establish the connection again. When set to 0 then timeout is disabled. Range: 0-10. Default value: 5.
BLE broadcasting power [dBm]	The parameter defines the power of broadcasting radio signals for Bluetooth communication. Range: [1]: -18, [2]: -12, [3]: -6, [4]: -3, [5]: -2, [6]: -1, [7]: 0. Default value: [1]: -18.
BLE transmission power [dBm]	The parameter defines the power of the transmission radio signal for Bluetooth communication. Range: [0]: Auto; [1]: -18, [2]: -12, [3]: -6, [4]: -3, [5]: – 2, [6]: -1, [7]: 0. Default value: [0]: Auto.
Barcode scanner	
Scanner mode	The parameter defines barcode scanner mode. Range: [0]: Activated by detector, [4]: Continuous operation. Default value: [0]: Activated by the detector. For scanner mode continuous for the QR code scanner, the acceptable ambient temperature range for the reader changes to – 25°C to +40°C.
White supplementary lighting mode	The parameter defines the operation mode for white supplementary lighting. Range: [0]: Activated during scan, [2]: Always off. Default value: [2]: Always off.
Red aiming light mode	The parameter defines the operation mode for read aiming light. Range: [0]: Blinking during scan, [1] Always blinking, [2]: Always off, [16]: Activated during scan, [17]: Always on. Default value: [2]: Always off.
Time to switch to standby mode	The parameter defines the time to switch to standby mode. Range: 2-20 [s]. Default value: 6.
The time interval for a repeat of the same code [s]	The parameter defines the interval between successive scans on the same barcode. Range: 0,1-4 [s]. Default value: 2.

Plain barcodes	
Format	The parameter defines the format of the plain barcode. Range: [0]: None, [1]: HEX, [2]: ASCII, [3]: BIN. Default value: [0]: None.
First byte position (FBP)	The parameter defines the position of the first byte for the plain barcode. Range: 0-255. Default value: 0.
Maximum number of bytes	The parameter defines a maximal number of bytes for plain barcode. Range: 1-16. Default value: 8.
Comments	
DEV	The parameter defines any text or comment which corresponds to the device/object. It is later displayed in the VISO program.
KBD1	The parameter defines any text or comment which corresponds to the device/object. It is later displayed in the VISO program.
CDI1	The parameter defines any text or comment which corresponds to the device/object. It is later displayed in the VISO program or Roger Mobile Key app.
IN1 (Tamper)	The parameter defines any text or comment which corresponds to the device/object. It is later displayed in the VISO program.
Serial card number (CSN) settings	
Serial number length (CSNL) [B]	The parameter defines the number of bytes from the serial card number (CSN) which will be used to generate returned card number (RCN). RCN is the actual card number read by the reader and it is created as the sum of the serial card number (CSN) and programmable card number (PCN).
Programmable card number (PCN) settings for Mifare Classic	
Sector type	The parameter defines sector type with a programmable number (PCN). If the option [0]: None is selected, then the card returned number (RCN) will include only CSN and PCN will be discarded. Range: [0]: None, [1]: SSN, [2]: MAD. Default value: [0]: None.
Format	The parameter defines the format of PCN. Range: [0]: BIN, [1]: ASCII HEX. Default value: [0]: BIN.
First byte position (FBP)	The parameter defines the position of the first byte for PCN in the data block on the card. Range: 0-15. Default value: 0.
Last byte position (LBP)	The parameter defines the position of the last byte for PCN in the data block on the card. Range: 0-15. Default value: 7.
Sector ID	The parameter defines the sector number where PCN is stored. Range: 0-39. Default value: 1.

Application ID (AID)	The parameter defines the application ID number (AID) which indicates the sector where the PCN number is stored. Range: 0-9999. Default value: 5156.
Block ID	The parameter defines the block number where PCN is stored. Range: 0-2 for sectors 0-31 and 0-14 for sectors 32-39. Default value: 0.
Key type	The parameter defines the key type used to access the sector with PCN. Range: [0]: A, [1]: B, [2]: Roger. Default value: [0]: A.
Key	The parameter defines 6 bytes (12 HEX digits) key for accessing the sector where PCN is stored.
Programmable card number (PCN) settings for Mifare Plus	
Sector type	The parameter defines sector type with a programmable number (PCN). If the option [0]: None is selected, then the card returned number (RCN) will include only CSN and PCN will be discarded. Range: [0]: None, [1]: SSN, [2]: MAD. Default value: [0]: None.
Format	The parameter defines the format of PCN. Range: [0]: BIN, [1]: ASCII HEX. Default value: [0]: BIN.
First byte position (FBP)	The parameter defines the position of the first byte for PCN in the data block on the card. Range: 0-15. Default value: 0.
Last byte position (LBP)	The parameter defines the position of the last byte for PCN in the data block on the card. Range: 0-15. Default value: 7.
Sector ID	The parameter defines the sector number where PCN is stored. Range: 0-39. Default value: 1.
Application ID (AID)	The parameter defines the application ID number (AID) which indicates the sector where the PCN number is stored. Range: 0-9999. Default value: 5156.
Block ID	The parameter defines the block number where PCN is stored. Range: 0-2 for sectors 0-31 and 0-14 for sectors 32-39. Default value: 0.

Key type	The parameter defines the key type used to access the sector with PCN. Range: [0]: A, [1]: B. Default value: [0]: A.
Key	The parameter defines the access key for the Desfire file with PCN. 3-KTDES key is 16 bytes (32 HEX digits), and TDES and AES keys are 16 bytes (32 HEX digits).
Programmable card number (PCN) settings for Mifare Desfire	
Sector type	The parameter defines sector type with a programmable number (PCN). If the option [0]: None is selected, then card returned number (RCN) will include only CSN and PCN will be discarded. Range: [0]: None, [1]: Desfire file. Default value: [0]: None.
Format	The parameter defines the format of PCN. Range: [0]: BIN, [1]: ASCII HEX. Default value: [0]: BIN.
First byte position (FBP)	The parameter defines the position of the first byte for PCN in the data block on the card. Range: 0-15. Default value: 0.
Last byte position (LBP)	The parameter defines the position of the last byte for PCN in the data block on the card. Range: 0-15. Default value: 7.
Application ID (AID)	The parameter defines application ID number (AID) which indicates the sector where the PCN number is stored. Range: 0-9999. Default value: F51560.
File ID (FID)	The parameter defines the file identifier in AID. Range: 0-32 for Desfire EV1 and 0-16 for Desfire EV0. Default value: 0.
Communication protection level	The parameter defines the encryption method for communication between the card and the reader. Range: [0]: Plain, [1]: Data authentication by MAC, [2]: Full encryption. Default value: [0]: Plain.
Key number	The parameter defines the application key number used for file read. Range: 0-13. Default value: 0.
Key type	The parameter defines the encryption key type for the Desfire file. Range: [0]: TDES Native, [1]: TDES Standard, [2]: 3-KTDES, [3]: AES128. Default value: [0]: TDES Native.
Key	The parameter defines the access key for the Desfire file with PCN. 3-KTDES key is 24 bytes (48 HEX digits), and TDES and AES keys are 16 bytes (32 HEX digits).

Manual addressing

Manual addressing procedure enables configuration of new RS485 address with all other settings unchanged.

Manual addressing procedure:

1. Remove all connections from the A and B lines.
2. Remove the jumper from MEM contacts (fig. 4) if it is placed there.
3. Restart the device (switch the power supply off and on or short RST contacts for a moment) and the orange

LED SYSTEM will pulsate. Then within 5 seconds place the jumper on MEM contacts.

4. Enter 3 digits of the RS485 address in the range of 100-115 with any MIFARE card.
5. Leave a jumper on MEM contacts to enable further configuration of the device from VISO v2 software or remove the jumper from MEM contacts to block such remote configuration.
6. Restart the device.

Readers without a keypad can be addressed with multiple card readings where the N number of readings emulates the digit of the address. Three series of readings with any MIFARE proximity card are necessary to set the address. After each series wait for two beeps and proceed with the next digit. Zero digit is emulated with 10 readings.

Example:
Programming of ID=101 address with card readings:

1. Read the card 1 time and wait for two beeps.
2. Read the card 10 times and wait for two beeps.
3. Read the card 1 time and wait for two beeps.
4. Wait till the reader is restarted with the new address.

Memory reset
Memory reset procedure resets all settings to factory default ones including ID=100 address.

Memory reset procedure:

1. Remove all connections from the A and B lines.
2. Remove the jumper from MEM contacts (fig. 4) if it is placed there.
3. Restart the device (switch the power supply off and on or short RST contacts for a moment) and the orange LED SYSTEM will pulsate. Then within 5 seconds place the jumper on MEM contacts.
4. Read any MIFARE card 11 times.
5. Wait till the device confirms reset with a long acoustic signal.
6. Leave the jumper on MEM contacts to enable further configuration of the device from VISO software and disconnect the device from the RUD-1 interface.
7. Restart the device.

High-level configuration (VISO)
The purpose of high-level configuration is to define the logical functioning of the terminal which communicates with the MC16 access controller, and it depends on the applied scenario of operation. The example of access control system configuration is given in the AN006 application note which is available at www.roger.pl.

FIRMWARE UPDATE

The firmware of the device can be changed to a newer or older version. The update requires a connection to the computer with the RUD-1 interface and starting RogerVDM software. The latest firmware file is available at www.roger.pl.

Note:
Backup configuration with RogerVDM software before firmware update because the update will restore factory default settings.

Firmware update procedure:

1. Connect the reader to the RUD-1 interface (fig. 10) and connect the RUD-1 to the computer’s USB port.
2. Place jumper on MEM contacts (fig. 5).
3. Restart the device (switch the power supply off and on).
4. Start the RogerVDM program and in the top menu select Tools and then Update firmware.
5. In the opened window select a device type, serial port with RUD-1 interface, and path to main firmware file (*.frg), and in case of a device with a keypad also path to additional firmware file (*.cyacd).
6. Click Update to start firmware upload with the progress bar at the bottom.
7. When the update is finished, disconnect from the RUD-1 interface and remove the jumper from MEM contacts. Additionally, it is recommended to start the memory reset procedure.

SPECIFICATION

Table 7. Specification	
Supply voltage	Nominal 12VDC, min./max. range 10-15VDC
Current consumption (average)	~80 mA (additional 120 mA if the barcode scanner is set to read continuously).
Tamper protection	Enclosure opening reported to access controller
Identification methods	13.56MHz MIFARE Ultralight, Classic, Plus, and DESFire (EV1, EV2, EV3) proximity cards Mobile devices (Android) with NFC Mobile devices (Android, iOS) with BLE (Bluetooth Low Energy) v4.1 Barcodes (1D): UPC A, UPC E, EAN 8, Interleaved 2 of 5, EAN 13, GS1-128,

	Code 128 Barcodes (2D): QR, PDF417, Data Matrix
Reading range	Up to 7 cm for MIFARE cards and NFC Up to 10 m for BLE – depends on ambient conditions and particular mobile devices. The terminal’s radio power can be increased within the low-level configuration. 2-20 cm for the proximity sensor of the QR scanner (for scanner operating mode [0]: Reading triggered by the sensor) – depends on ambient conditions and type of code applied. 4-25 cm for a QR code scanner for a 10x10mm code. Note: As the size of the code increases, minimum and maximum reading distances increase
Distance	1200m maximal cable length for RS485 bus between controller and reader
IP Code	IP65
Environmental class (according to EN 50133-1)	Class IV, outdoor general conditions, temperature: -25°C to +60°C, relative humidity: 10 to 95% (no condensation) Operating temperature: -25°C- +60°C (for scanner mode [0]: Sensor-triggered reading), Operating temperature: -25°C- +40°C (for scanner mode [4]: Continuous reading)
Dimensions H x W x D	130 x 45 x 22 mm
Weight	~100g
Certificates	CE, RoHS

ORDERING INFORMATION

Table 8. Ordering information	
MCT84M-BK-QB	Access Terminal
RUD-1	Portable USB-RS485 communication interface dedicated to ROGER access control devices

PRODUCT HISTORY

Table 9. Product History

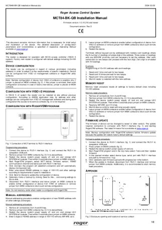
Version	Date	Description
MCT84M-BK-QB v1.0	07/2022	The first commercial version of the product

This symbol placed on a product or packaging indicates that the product should not be disposed of with other wastes as this may hurt the environment and health. The user is obliged to deliver equipment to the designated collection points for 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 natural resources and is safe for health and the environment. The 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.

Documents / Resources

 Roger Access Control System MCT84M-BK-QB Operating Manual Product version: 1.0 Firmware version: 1.0.10.216 Document version: Rev.E	Roger MCT84M-BK-QB Access Control System [pdf] Instruction Manual MCT84M-BK-QB Access Control System, MCT84M-BK-QB, Access Control System, Control System, System
 Roger Access Control System MCT84-BK-QB Installation Manual	Roger MCT84M-BK-QB Access Control System [pdf] Installation Guide MCT84M-BK-QB Access Control System, MCT84M-BK-QB, Access Control System, Control System, System

References

- Kontrola Dostępu i Automatyka Budynkowa - Roger
- Kontrola Dostępu i Automatyka Budynkowa - Roger
- User Manual