

roger OSR80M-BLE Access Control System



roger OSR80M-BLE Access Control System User Manual

[Home](#) » [ROGER](#) » roger OSR80M-BLE Access Control System User Manual 

Contents

- 1 roger OSR80M-BLE Access Control System
- 2 Product Information
- 3 Product Usage Instructions
- 4 FAQs
- 5 DESIGN AND APPLICATION
- 6 Power supply
- 7 Function keys
- 8 LED indicators
- 9 INSTALLATION
- 10 OPERATION SCENARIOS
- 11 FIRMWARE UPDATE
- 12 SPECIFICATION
- 13 ORDERING INFORMATION
- 14 Contact
- 15 Documents / Resources
 - 15.1 References

roger

roger OSR80M-BLE Access Control System



Product Information

- **Specifications**
 - **Product:** Roger Access Control System OSR80M-BLE
 - **Product Version:** 1.0
 - **Firmware Version:** 1.0.8.205 or newer
 - **Document Version:** Rev.E

Product Usage Instructions

- **Power Supply**
 - The OSR80M-BLE can be powered using UTP wire pairs with varying lengths as shown in Table 1.
- **OSDP Bus**
 - The system utilizes the OSDP bus for communication.
- **Function Keys**
 - The terminal has two touch function keys that can be assigned various functions within the configuration settings.
- **LED Indicators**
 - The terminal features three LED indicators that signal different functions. Refer to Table 2 for details on LED indicator colors and meanings.
- **Buzzer**
 - The buzzer is used to signal different functions and can be programmed accordingly.
- **Tamper Detector**
 - The built-in tamper detector enables detection of unauthorized opening of the device's enclosure.
- **Identification Methods**
 - The terminal supports user identification via MIFARE cards, allowing for enhanced security through card programming.

FAQs

- **Q: How can I program MIFARE cards with custom numbers?**

- **A:** By default, the terminal reads serial numbers of MIFARE cards, but it is possible to program cards with custom numbers in selected and encrypted sectors of card memory. Refer to the AN02 application note for more information.

DESIGN AND APPLICATION

The OSR80M-BLE is an access terminal dedicated to working with an access controller that supports the OSDP v2.2 protocol. The terminal enables identification of users by 13,56 MHz Mifare® Ultralight/Classic/DESFire (EV1, EV2, EV3)/PLUS cards and by use of smartphone with NFC or Bluetooth technology. In the case of Bluetooth identification, the reading range can reach up to 10m meters while other methods offer a few centimeters of reading range. The mobile identification requires the Roger Mobile Key application installed on an Android or IOS phone. The reader is equipped with two functional keys: Door Bell and Light which can be programmed for other functions if necessary. The OSR80M-BLE can be used in the RACS 5 access control and building automation system using the additional MCI-3 interface. Because of its relatively small size, the reader can be also used as a locker/cabinet reader. OSR80M-BLE can be installed in outdoor locations without any additional protection measures. The terminal is aligned with the QUADRUS series product line.

Characteristics

- Access terminal supporting OSDP v2.2
- Read 13,56 MHz Mifare® Ultralight/Classic/Classic/DESFire (EV1, EV2, EV3)/PLUS cards
- Mobile identification using a smartphone with NFC or Bluetooth
- Door Bell and Light function keys
- 3 LEDs
- Buzzer
- RS485
- Tamper
- Outdoor operation
- Dimensions: 100x45x16 mm
- QUADRUS design-line
- CE, RoHS

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 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 a 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 employing 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 with the number of wires used for the power supply.

Table 1. 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

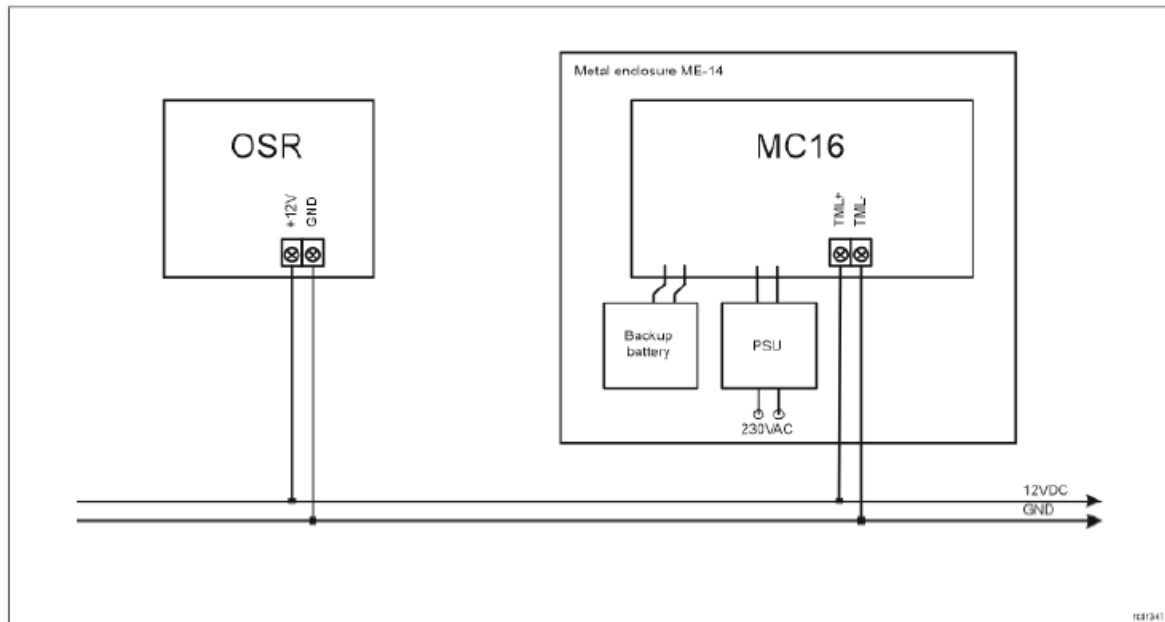


Fig. 1 OSR supply from MC16 access controller

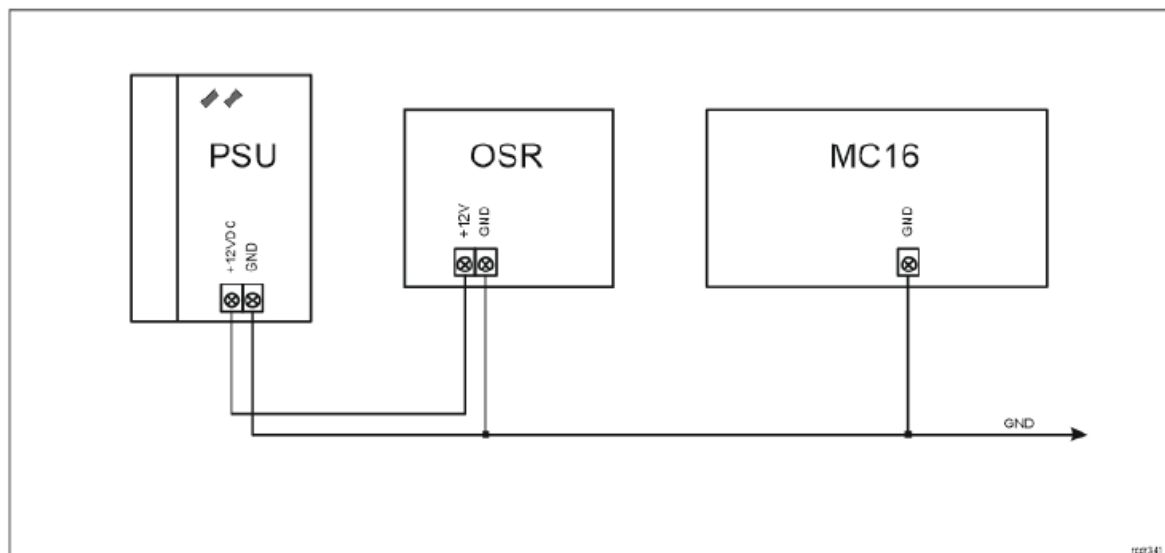


Fig. 2 OSR supply from dedicated power supply unit

OSDP bus

- The communication method with access controller is provided via the OSDP protocol on the RS485 bus.
- The device can be connected directly to access controllers supporting this bus. However, for the MC16

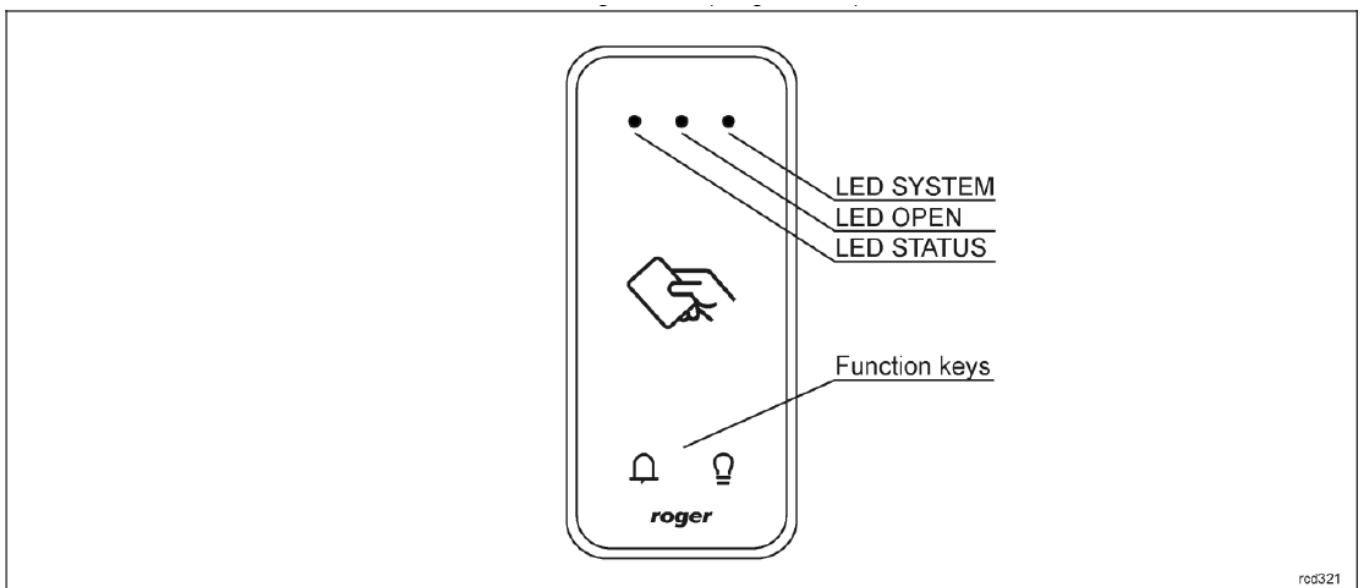
controller, it is additionally necessary to use the MCI-3 interface.

- The bus topology can be freely arranged as star, tree or any combination of them except for 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 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 single pair in UTP cable for RS485 communication bus.

Function keys

- The terminal is equipped with two touch function keys  and .
- Various functions can be assigned to these keys within high-level configuration (VISO) e.g. door bell, Set T&A Mode, Register Guard Tour Event, Set Automation Node On, etc.
- Within low-level configuration (RogerVDM) function buttons can be enabled.



rod321

Fig. 3 LED indicators and function keys

LED indicators

The terminal is 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 2. LED indicators		
Indicator	Colour	Integral functions
LED STATUS	Red/green	Default indicator colour is red. If the terminal is assigned to 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 MC16 controller or MCI-3 interface.

Buzzer

- The terminal is equipped with a buzzer which is used to signal integral functions and it can be additionally programmed with other available functions within high level configuration (VISO).
- **Note:** LED indicators and Speakers in high-level configuration (VISO) can only be controlled as on/off. Unlike MCT readers, flashing or cyclic activation is not supported.

Tamper detector

- Built-in tamper (sabotage) detector enables detection of unauthorized opening of device's enclosure as well as detachment of the enclosure from wall.
- The detector is internally connected to the terminal's input.
- It does not require low-level configuration (RogerVDM) or any additional installation arrangements, but it is essential to mount front panel in such way as the tamper detector (fig. 5) would firmly press the back panel.
- The detector requires high-level configuration which consists in the assignment of the function [133] Tamper Toggle on the level of a Main Board of a controller in VISO software navigation tree.

Identification

Following user identification methods are offered by the terminal:

- MIFARE Ultralight/Classic/Plus/DESFire (EV1, EV2, EV3) proximity cards.
- Mobile devices (NFC and BLE)

MIFARE cards

- By default, the terminal 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 card programming is given in 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 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 terminal OSR80M-BLE enables user identification with mobile device using NFC (Android) or Bluetooth (Android, iOS) communication.
- Prior to use of BLE/NFC identification on the terminal, within its low level configuration (see section 4) configure own NFC/BLE authentication factor encryption key and NFC/BLE communication encryption key while in case of Bluetooth additionally verify if the parameter BLE activated is enabled.
- Install Roger Mobile Key (RMK) app on mobile device and configure the same parameters as in the terminal.
- Create key (authentication factor) in RMK defining its type and number, then create the same authentication factor in VISO software (fig. 4) and assign it to the user with adequate Authorisation(s) at the terminal.
- When user wants to identify at the terminal using mobile device then key (authentication factor) can be selected from the screen or with gesture.

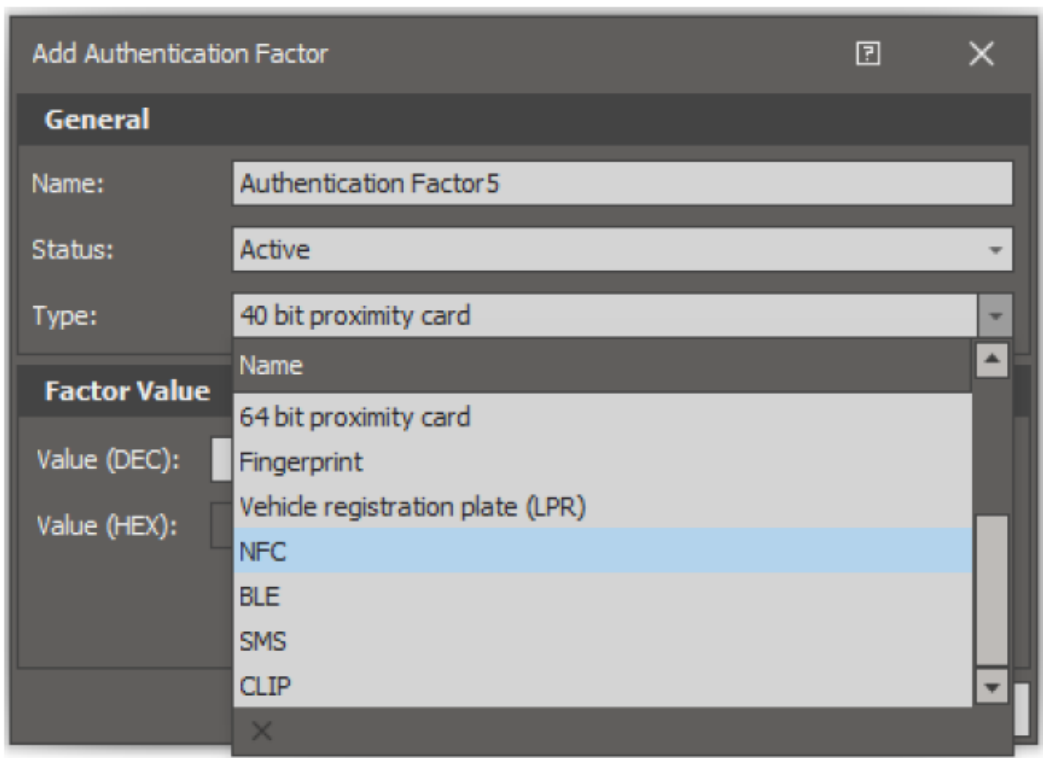


Fig. 4 Authentication factor type in VISO software

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

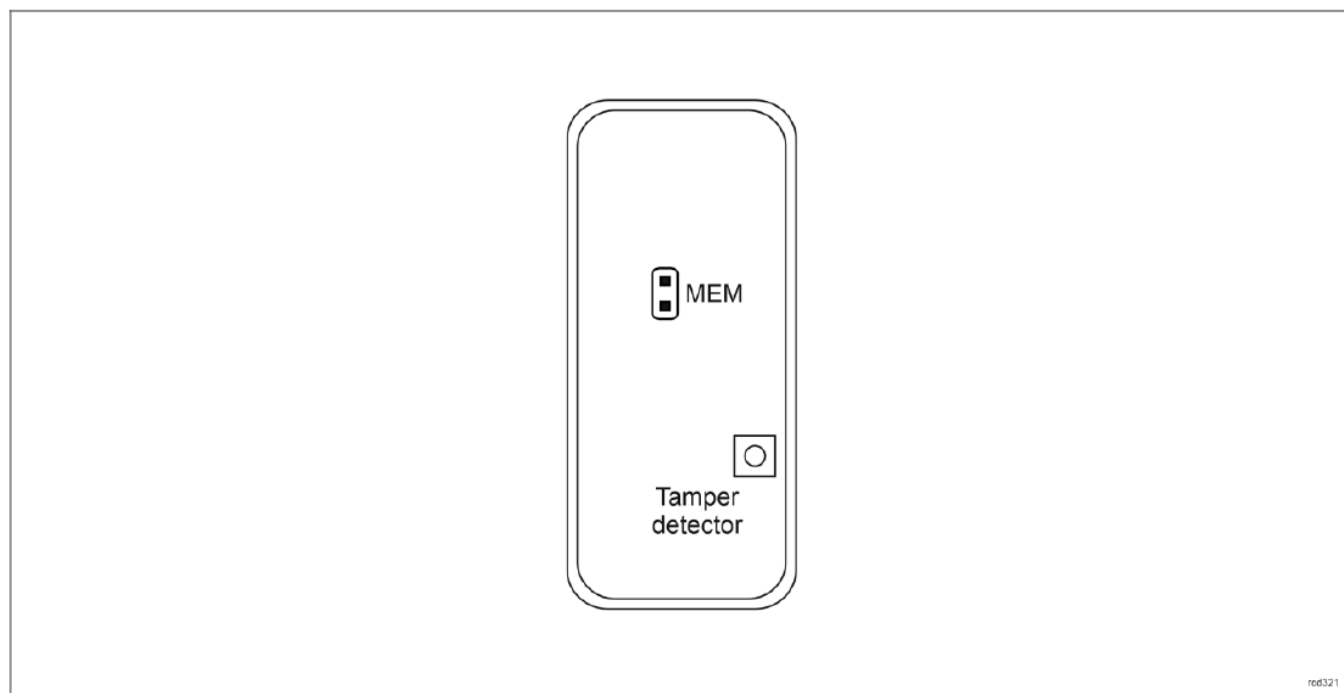
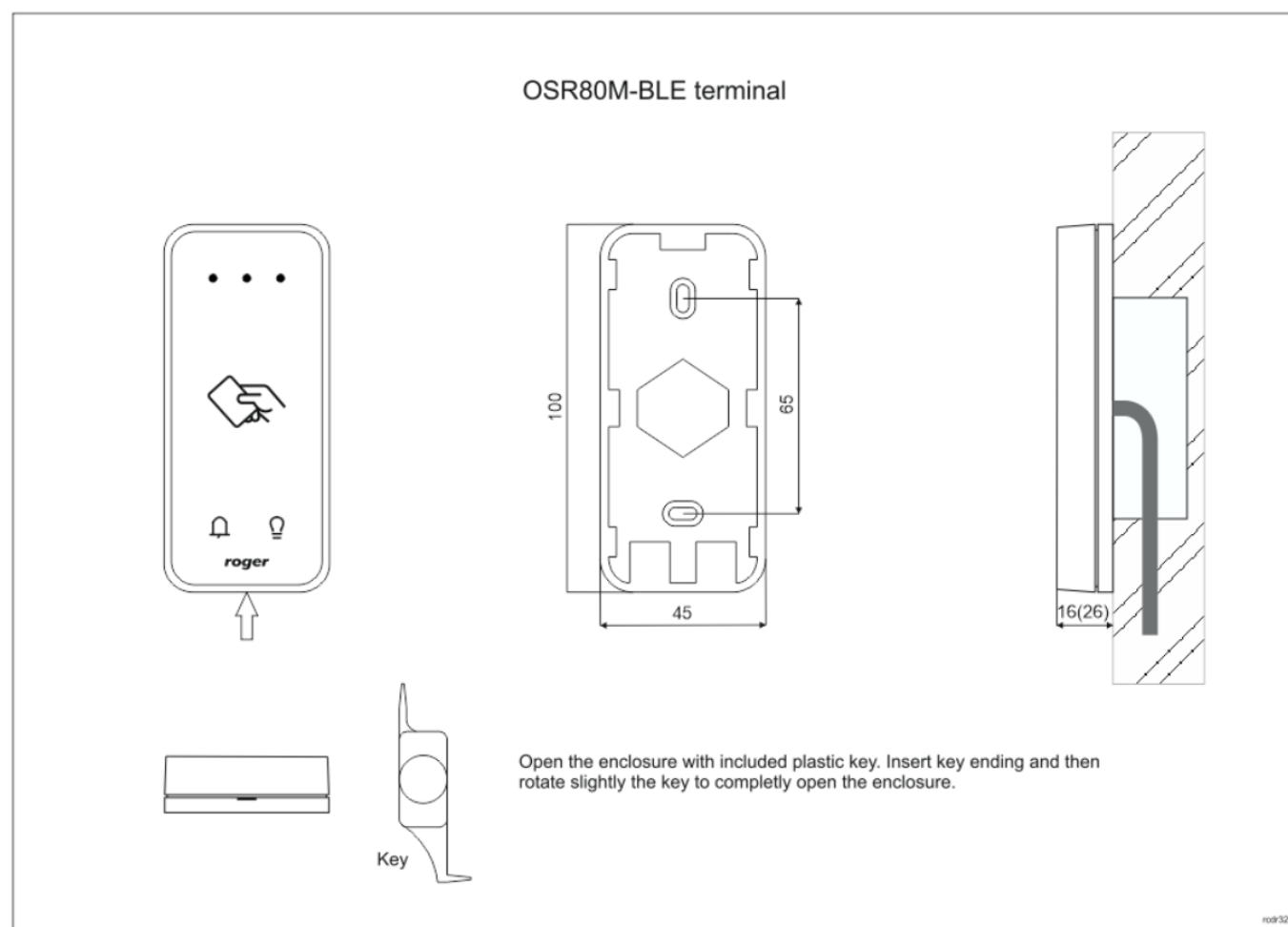


Fig. 5 Programming jumpers



Note: OSR80M-BLE enclosure consists of front panel and back panel. New device is assembled with a standard back panel, but 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.
- Front panel should be attached in such way as the tamper detector (fig. 5) would firmly press the back panel.
- All electrical connections should be done with disconnected power supply.
- If the terminal and controller are not supplied from the same PSU, then GND terminals of both devices must be connected with any wire.
- Device can be cleaned using 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 manufacturer warranty.
- If the device is installed in a place exposed to conductive dust (e.g. metal dust), the MEM 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

Connection via MCI-3 interface

The terminal when connected to MC16 access controller via the MCI-3 interface, can be at the same time used for access control, Time&Attendance and to control external devices with function keys. The example of a connection diagram for such a scenario is shown in fig. 7 where the terminal is connected via the MCI-3 interface to the MC16 controller. The terminal with MCI-3 interface can also operate with MC16 controller using MCX2D/MCX4D expanders as in case of the M16-PAC-x-KIT series. To support OSDP terminals, it is necessary to run the automatic terminal detection procedure via the MCI interface. The OSDP terminal detection procedure is described in a separate manual for the MCI-3 interface.

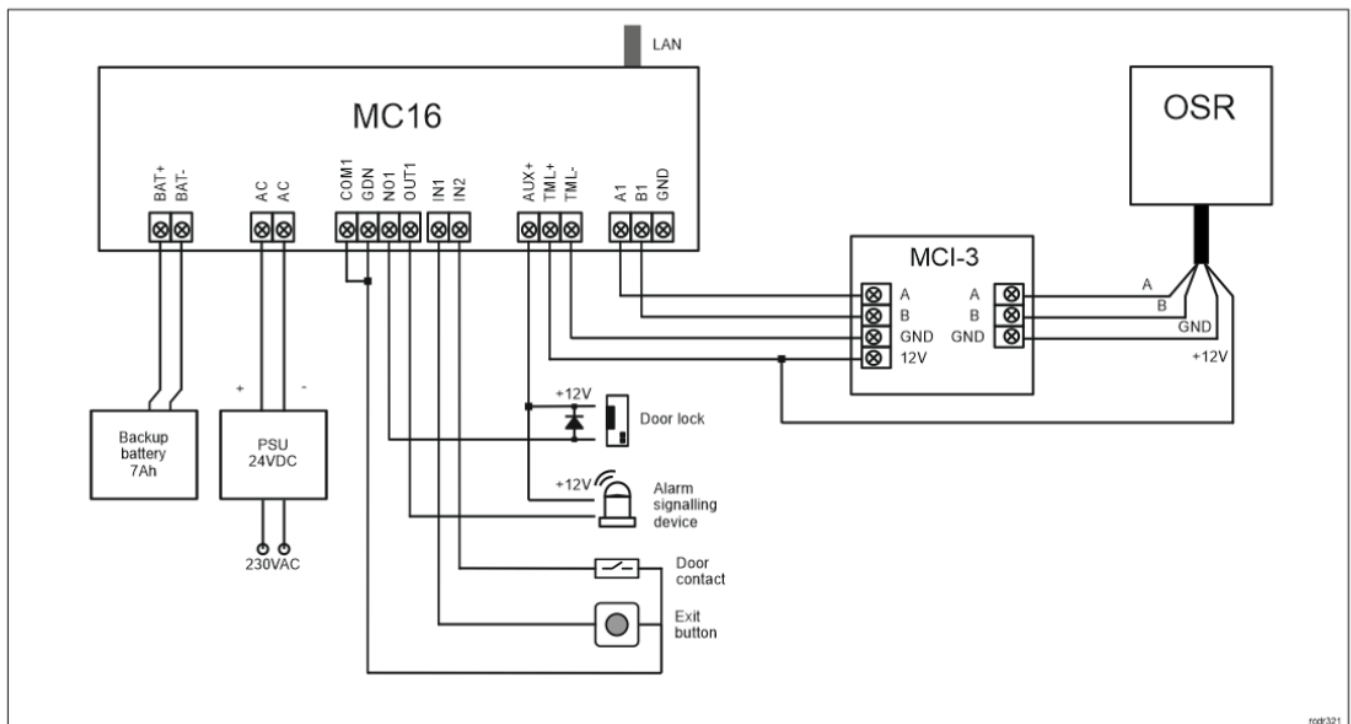


Fig. 7 Typical connection diagram for the terminal and MC16 access controller via the MCI-3 interface.

Direct connection to the OSDP controller

It is possible to make a direct connection of the OSR reader directly to the OSDP controller. An exemplary connection diagram is shown below.

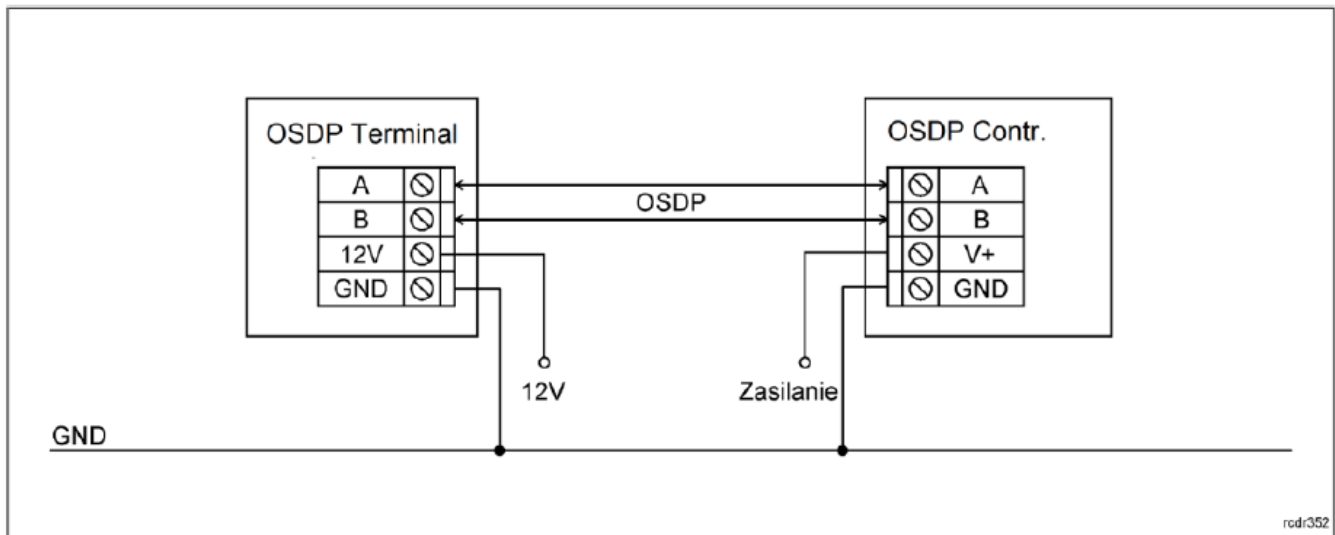


Fig. 8 Connecting the OSR reader directly to the OSDP controller.

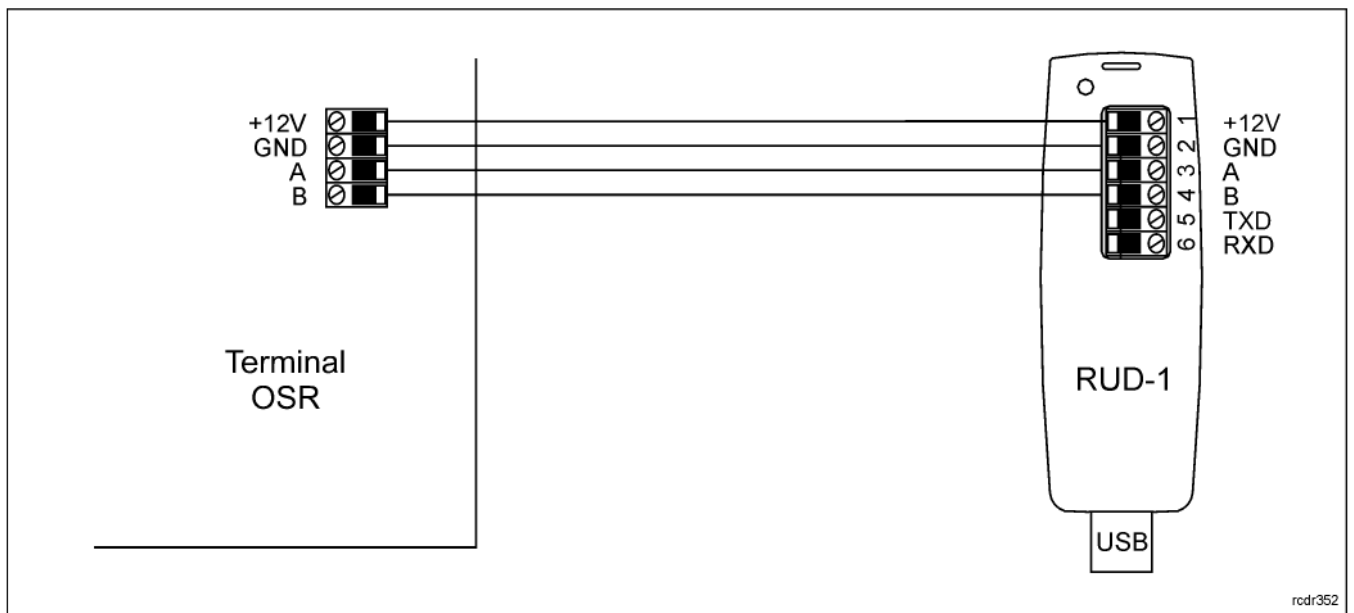
CONFIGURATION

The purpose of low level configuration is to prepare device for operation in RACS 5 system. In case of RACS 5 v1 or RACS5 v2 system the address of device must be configured using RogerVDM software or by manual addressing before connection to MC16 controller.

Low level configuration (RogerVDM)

Programming procedure with RogerVDM software:

1. Connect the device to RUD-1 interface (fig. 9) and connect the RUD-1 to computer's USB port.
2. Remove jumper from MEM contacts (fig. 5) if it is placed there.
3. Restart the device (switch power supply off and on) and orange LED SYSTEM will pulsate. Then within 5 seconds place jumper on MEM contacts.
4. Start RogerVDM program, select OSR device, v1.0 firmware version, RS485 communication channel and serial port with RUD-1 interface.
5. Click Connect, the program will establish connection and will automatically display the Configuration tab.
6. Enter unoccupied OSDP address in range of 0-126 and other settings according to requirements of specific installation.
7. Click Send to Device to update the configuration of 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 jumper on MEM contacts.



rodr352

Fig. 9 Connection to RUD-1 interface.

Note: Do not read any cards when the device is configured with RogerVDM.

Table 4. List of low level parameters

Communication settings	
OSDP address	Parameter defines device address on OSDP bus. Range: 0-126. Default value: 0.
Factor conversion	Parameter defines method of converting the read factor. Value range: [0]: RS485 (EPSO3), [1]: Media only. Default value: [0]: RS485 (EPSO3)
LED control	Parameter defines method of controlling the terminal's LED indicators. Range of values: [0]: 4 monochrome indicators [1]: RGB tricolour indicator. Default value: [0]: 4 monochrome indicators
Communication encryption	Parameter defines the encryption conditions for communication between the controller (CP) and the reader (PD). Encryption can be unconditional at all times or managed by a controller. Range of values: [0]: Controller initiated, [1]: Constant. Default value: [0]: Controller initiated.
OSDP password	Password for encrypting communication on the OSDP bus. Value range: 4-16 ASCII characters.
Mobile authentication	
NFC/BLE authentication factor encryption key	Parameter defines key for encryption of NFC/BLE communication. Range: 4-16 ASCII characters.
NFC/BLE communication encryption key	Parameter defines key for encryption of NFC/BLE communication. Range: 4-16 ASCII characters.
BLE authentication factor class	Parameter defines acceptable type of keys (authentication factors) created in 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 which are acceptable for terminal. Range: [1]: REK, [2]: UCE, [3]: UCE + REK. Default value: [3]: UCE + REK.
NFC authentication factor class	Parameter defines acceptable type of keys (authentication factors) created in 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 which are acceptable for terminal. Range: [1]: REK, [2]: UCE, [3]: UCE + REK. Default value: [2]: UCE.
Optical signalisation	
RS485 communication timeout [s]	Parameter defines the delay after which the device will start signaling 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 reader	Parameter enables LED SYSTEM (orange) pulsing when card is close to the device. Range: [0]: No, [1]: Yes. Default value: [0]: No.
Backlight level [%]	Parameter defines backlight level. When set to 0 then backlight is disabled. Range: 0-100. Default value: 100.
Backlight switching off when no activity	Parameter enables temporary backlight dimming whenever card is read, or key is pressed. Range: [0]: No, [1]: Yes. Default value: [0]: No.
LED SYSTEM flash after card read	Parameter enables short flash of LED SYSTEM (orange) when card is read. Range: [0]: No, [1]: Yes. Default value: [1]: Yes.
LED SYSTEM flash after key press	Parameter enables short flash of LED SYSTEM (orange) when key is pressed. Range: [0]: No, [1]: Yes. Default value: [1]: Yes.
Acoustic signalisation	
Buzzer loudness level [%]	Parameter defines buzzer loudness level. When set to 0 then buzzer is disabled. Range: 0-100. Default value: 100.
Short sound after card read	Parameter enables short sound (beep) generating by buzzer when card is read. Range: [0]: No, [1]: Yes. Default value: [1]: Yes.
Short sound after key press	Parameter enables short sound (beep) generating by buzzer when key is pressed. Range: [0]: No, [1]: Yes. Default value: [1]: Yes.
Keypad settings	
Keypad activated	Parameter enables deactivation of keypad. Range: [0]: No, [1]: Yes. Default value: [1]: Yes.
Advanced settings	
Card/PIN buffer timeout [s]	Parameter defines the time of keeping the card number or PIN code in the reader's buffer. After exceeding this time, the identifier will be deleted even though it has not been sent to the controller. Range: 1-64. Default value: 10.
BLE activated	Parameter enables deactivation of Bluetooth transmission. Range: [0]: No, [1]: Yes. Default value: [1]: Yes.
BLE session timeout [s]	Parameter defines maximal time for establishing connection between mobile device and terminal in Bluetooth technology. When timeout elapses, the session is interrupted by terminal so mobile device could attempt to establish connection again. When set to 0 then timeout is disabled. Range: 0-10. Default value: 5.

BLE broadcasting power [dBm]	Parameter defines power of broadcasting radio signal 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]	Parameter defines power of 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.
Serial card number (CSN) settings	
Serial number length (CSNL) [B]	Parameter defines the number of bytes from serial card number (CSN)

	which will be used to generate returned card number (RCN). RCN is the actual card number read by reader and it is created as sum of serial card number (CSN) and programmable card number (PCN). Default value: 8.
--	--

Programmable card number (PCN) settings for Mifare Ultralight

Sector type	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]: SSN. Default value: [0]: None.
SSN first page number	Parameter defines location of SSN in card memory. Range: 4-12. Default value: 4.

Programmable card number (PCN) settings for Mifare Classic

Sector type	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]: SSN, [2]: MAD. Default value: [0]: None.
Format	Parameter defines format of PCN. Range: [0]: BIN, [1]: ASCII HEX. Default value: [0]: BIN.
First byte position (FBP)	Parameter defines the position of the first byte for PCN in data block on card. Range: 0-15. Default value: 0.
Last byte position (LBP)	Parameter defines the position of the last byte for PCN in data block on card. Range: 0-15. Default value: 7.
Sector ID	Parameter defines sector number where PCN is stored. Range: 0-39. Default value: 1.
Application ID (AID)	Parameter defines application ID number (AID) which indicates sector where PCN number is stored. Range: 0-9999. Default value: 5156.

Block ID	Parameter defines block number where PCN is stored. Range: 0-2 to for s ectors 0-31 and 0-14 for sectors 32-39. Default value: 0.
Key type	Parameter defines key type used to access sector with PCN. Range: [0]: A, [1]: B, [2]: Roger. Default value: [0]: A.
Key	Parameter defines 6 bytes (12 HEX digits) key for accessing sector where PCN is stored.
Programmable card number (PCN) settings for Mifare Plus	
Sector type	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]: SSN, [2]: MA D. Default value: [0]: None.
Format	Parameter defines format of PCN. Range: [0]: BIN, [1]: ASCII HEX. Defaul t value: [0]: BIN.
First byte position (FBP)	Parameter defines the position of the first byte for PCN in data block on ca rd. Range: 0-15. Default value: 0.
Last byte position (LBP)	Parameter defines the position of the last byte for PCN in data block on ca rd. Range: 0-15. Default value: 7.
Sector ID	Parameter defines sector number where PCN is stored. Range: 0-39. Def ault value: 1.
Application ID (AID)	Parameter defines application ID number (AID) which indicates sector wh ere PCN number is stored. Range: 0-9999. Default value: 5156.
Block ID	Parameter defines block number where PCN is stored. Range: 0-2 to

	for sectors 0-31 and 0-14 for sectors 32-39. Default value: 0.
Key type	Parameter defines key type used to access sector with PCN. Range: [0]: A, [1]: B. Default value: [0]: A.
Programmable card number (PCN) settings for Mifare Desfire	
Sector type	Parameter defines sector type with 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	Parameter defines format of PCN. Range: [0]: BIN, [1]: ASCII HEX. Default value: [0]: BIN.
First byte position (FBP)	Parameter defines the position of the first byte for PCN in data block on card. Range: 0-15. Default value: 0.
Last byte position (LBP)	Parameter defines the position of the last byte for PCN in data block on card. Range: 0-15. Default value: 7.
Application ID (AID)	Parameter defines application ID number (AID) which indicates sector where PCN number is stored. Range: 0-9999. Default value: F51560.
File ID (FID)	Parameter defines file identifier in AID. Range: 0-32 for Desfire EV1 and 0-16 for Desfire EV0. Default value: 0.
Communication protection level	Parameter defines the encryption method for communication between card and reader. Range: [0]: Plain, [1]: Data authentication by MAC, [2]: Full encryption. Default value: [0]: Plain.
Key number	Parameter defines application key number used for file read. Range: 0-13. Default value: 0.
Key type	Parameter defines encryption key type for Desfire file. Range: [0]: TDES Native, [1]: TDES Standard, [2]: 3-KTDES, [3]: AES128. Default value: [0]: TDES Native.
Key	Parameter defines access key for Desfire file with PCN. 3-KTDES key is 24 bytes (48 HEX digits), 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 A and B lines.
2. Remove jumper from MEM contacts (fig. 5) if it is placed there.
3. Restart the device (switch power supply off and on) and orange LED SYSTEM will pulsate. Then within 5 seconds place jumper on MEM contacts.
4. Enter 3 digits of OSDP address in range of 0-126 with any MIFARE card.
5. Leave jumper on MEM contacts.
6. Restart the device.

Readers without keypad can be addressed with multiple card readings where the N number of readings emulates

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

Memory reset

Memory reset procedure resets all settings to factory default ones including ID=0 address.

Memory reset procedure:

1. Remove all connections from A and B lines.
2. Remove jumper from MEM contacts (fig. 5) if it is placed there.
3. Restart the device (switch power supply off and on) and the orange LED SYSTEM will pulsate. Then within 5 seconds place jumper on MEM contacts.
4. Read any MIFARE card 11 times.
5. Wait till device confirms reset with long acoustic signal.
6. Leave jumper on MEM contacts.
7. Restart the device.

High level configuration (VISO)

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

FIRMWARE UPDATE

The firmware of device can be changed to newer or older version. The update requires 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.

Note: If MCI-3 interface is connected to the terminal, it must be disconnected during a firmware update.

Firmware update procedure:

1. Connect the device to RUD-1 interface (fig. 9) and connect the RUD-1 to the computer's USB port.
2. Place jumper on MEM contacts (fig. 5).
3. Restart the device (switch 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 device type, serial port with RUD-1 interface and path to firmware file (*.frg).
6. Click Update to start firmware upload with the progress bar in 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 5. Specification	
Supply voltage	Nominal 12VDC, min./max. range 10-15VDC
Current consumption (average)	~70 mA
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
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.
Distance	1200 m maximal cable length for RS485 bus between controller and terminal
ZIP 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)
Dimensions H x W x D	100 x 45 x 16(26) mm
Weight	~100g
Certificates	CE, RoHS

ORDERING INFORMATION

Table 6. Ordering information	
OSR80M-BLE	Outdoor MIFARE DESFire (EV1, EV2, EV3)/Plus/NFC/Bluetooth access terminal; OSDP v2.2; 2 function keys
MCI-3	The interface enables the connection of a reader that uses OSDP protocol to the MC 16 series access controller (RACS 5 system).
RUD-1	Portable USB-RS485 communication interface dedicated to ROGER access control devices

PRODUCT HISTORY

Table 7. Product History		
Version	Date	Description
OSR80M-BLE v1.0	03/2022	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 hurt 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 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 OSR80M-BLE Access Control System [pdf] User Manual OSR80M-BLE Access Control System, OSR80M-BLE, Access Control System, Control System, System
---	---

References

- [🔗 Kontrola Dostępu i Automatyka Budynkowa - Roger](#)
- [User Manual](#)

Manuals+, Privacy Policy

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.