sygonix®

GB **Operating Instructions**

RFID access system

Item no. 2380477

CE

Table of contents

GB

1. Introduction

Dear customer,

Thank you for purchasing this product.

This product complies with statutory, national and European regulations.

To ensure that the product remains in this state and to guarantee safe operation, always follow the instructions in this manual.

These operating instructions are part of this product. They contain important information on setting up and using the product. Do not give this product to a third party without the operating instructions. Therefore, retain these operating instructions for reference!

If there are any technical questions, please contact: www.conrad.com/contact

2. Explanation of symbols

The symbol with the lightning in the triangle is used if there is a risk to your health, e.g., due to an electric shock.

The symbol with an exclamation mark in a triangle is used to highlight important information in these operating instructions. Always read this information carefully.

The arrow symbol indicates special information and tips on how to use the product.

3. Intended use

This product is designed to prevent unauthorised access to doors (e.g. in an office) and to activate/disable alarm systems. The product enables to save up to 2000 users with different transponders.

Holding a paired transponder in front of the reading surface activates a potential-free relay changeover contact (see contact rating under “Technical data”). This can be used, for example, to control a door opener or an alarm system.

The product is intended for vertical installation on a wall and is suitable for indoor and outdoor use (IP 66).

For safety and approval purposes, do not rebuild and/or modify this product. Using the product for purposes other than those described above may damage the product. In addition, improper use can cause hazards such as a short circuit, fire or electric shock. Read the operating instructions carefully and store them in a safe place. Only make this product available to third parties together with its operating instructions.

4. Delivery content

- Access system
- Fasteners (2x special screws with matching L-key, 4x screw head stickers, mounting frame with 4x screws and 4x dowels)
- Master transponder
- 1N4004 diode (for relay changeover contact)
- IR remote control (with one CR2025 lithium battery)
- Quick guide
- Programming guide

Up-to-date operating instructions

Download the latest operating instructions at www.conrad.com/downloads or scan the QR code shown. Follow the instructions on the website.

5. Safety information

Damage caused due to failure to observe these instructions will void the warranty. We shall not be liable for any consequential damage!

We shall not be liable for damage to property or personal injury caused by incorrect handling or failure to observe the safety information! Such cases will void the warranty/guarantee.

a) General information

- This product is not a toy. Keep it out of the reach of children and pets.
- Protect the product from extreme temperatures, impacts, flammable gases, vapours and solvents. The access system is suitable for indoor and outdoor installation and use (IP66). The supplied IR remote control must be protected from moisture and humidity.
- Handle the product carefully. Jolts, impacts or a fall even from a low height may damage the product. Do not place the product under any mechanical stress.
- Do not mount or connect the product when it is connected to a power supply.
- The contact rating for the changeover contact is specified in section “Technical data” and must not be exceeded. Never switch the mains voltage, as this can cause life-threatening electric shock!
- Always observe safety information and operating instructions for the other devices (e.g. door opener, alarm system) to which the product is connected.
- If it is no longer possible to operate the product safely, stop using it and prevent unauthorised use. Safe operation of the appliance can no longer be guaranteed if it shows visible signs of damage, malfunctions, has been exposed to unfavourable storage conditions or significant transport loads.
- For installations in industrial facilities, follow the accident prevention regulations for electrical systems and equipment issued by the national safety organisation or the corresponding national authority.
- Do not leave packaging material lying around carelessly. It may become a dangerous toy for children!
- Maintenance, modifications and repairs must be carried out by a technician or a specialist repair centre.
- If you are not sure how to operate the product correctly, or if you have any questions that are not answered in these operating instructions, contact us or another specialist.

b) Battery safety information

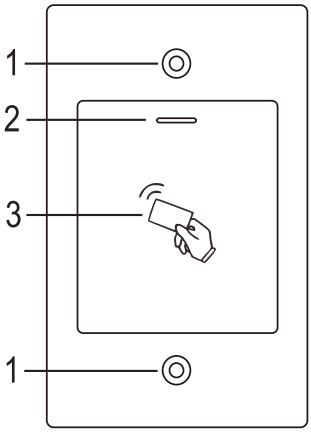
- Keep batteries out of the reach of children.
- Do not leave batteries lying around in the open; there is a risk of them being swallowed by children or pets. If swallowed, consult a doctor immediately, it could be fatal!
- Always ensure that the battery in the IR remote control is inserted with the correct polarity (observe the plus/+ and minus/- symbols).
- Batteries must not be short-circuited, opened, taken apart or thrown into a fire. This may cause a fire or explosion!
- Never attempt to recharge non-rechargeable batteries, as this may cause an explosion.
- Old or depleted batteries may emit chemical liquids that cause damage to the product. Therefore, if the device is not to be used for a long time (e.g. storage), remove the battery from the IR remote control.
- Leaking or damaged batteries can lead to caustic burning upon skin contact. Therefore, use suitable protective gloves.
- Liquids leaking from batteries are very chemically aggressive. Objects or surfaces coming into contact with these liquids could be severely damaged. Therefore, store batteries in a suitable location.
- For details on how to dispose of batteries in an environmentally friendly manner, refer to the “Disposal” section.

6. Controls and connections

1 Opening for wall mounting

2 LED indicator

3 RFID sensor



→ The brightness sensor on the back serves as a tamper protection.

The IR reception LED (not visible from the outside) is located right next to the LED indicator (2).

Connection cables:

Colour	Inscription	Function
Red	12 - 18 V/DC	Power supply 12 - 18 V/DC
Black	GND	GND/ground
Blue	NO	NO (normally open) contact of relay
Brown	COM	COM (centre contact) contact of relay
Grey	NC	NC (normally closed) contact of relay
Yellow	OPEN	Door opener button
White	D1	Wiegand Data1
Green	D0	Wiegand Data0

7. Installation and connection

Ensure that the connection cables are not kinked or squashed. This can cause malfunctions, short circuits and device defects. Ensure that no cables or wires are damaged when drilling holes or tightening screws. Installation and connection may only be carried out when power supply is switched off.

Make sure that the brightness sensor on the back is not exposed to light beams after installation, as switching on the system could cause activation of tamper protection with subsequent locking of all functions.

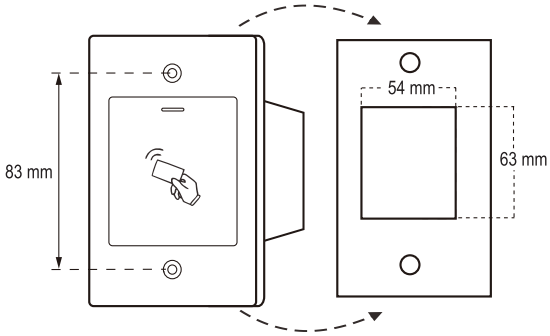
a) Installation

Use suitable screws and, if necessary, dowels to mount the mounting plate with the module on the wall (see figure on the right) depending on the type of wall.

The package includes two special screws and a matching L-key. The screw head shape provides extra protection against attempted manipulations.

The included mounting frame can be preinstalled depending on the substrate and installation position, and the access system should then be screwed tight.

Suitable screws and, if necessary, dowels should be used depending on the substrate.



A hole for the connecting cable must be drilled before fastening. Wiring should be carried out according to the wiring diagrams in the following sections.

⟶ Ensure that there is suitable insulation (e.g. heat shrink tubing).

A protective diode is included for connecting a door opener. It protects the electronics from damage caused by voltage surges. Ensure the correct polarity, as shown in the following wiring diagrams (when connected, the ring on the protective diode must face the positive pole/+).

Caution!

Never switch the mains voltage via the potential-free changeover contact! There is a risk of fatal electric shock! Observe the permissible contact rating; see “Technical data” chapter.

⟶ Use suitable cables with different colours. Note the colours and store this information together with these instructions. When connecting the cables, pay attention to the correct polarity (plus/+ and minus/-).

You can use the included stickers to cover the screw openings after cable connection and successful start-up.

b) Connecting to conventional voltage/power supply

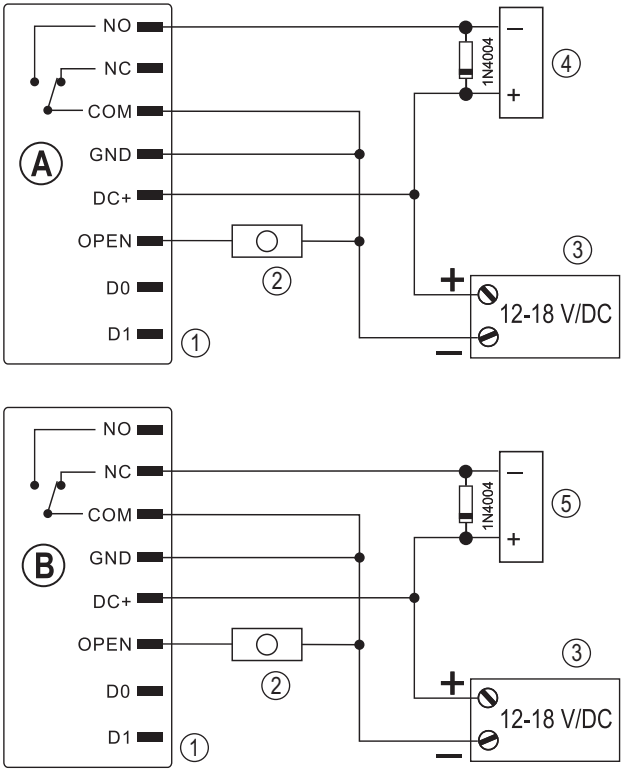
When a conventional power supply unit should be used, observe the following figures with the wiring diagram.

A) “Fail-secure” door opener: Releases the locking latch only when its operating voltage is applied (common design for front doors).

B) “Fail-safe” door opener: releases the locking latch only when the operating voltage is missing (uncommon design, e.g. used for escape route doors, which can be opened in the event of a power outage).

⟶ The included diode must be connected correctly near the door opener to protect the access system from voltage surges.

1 Access system
2 Door opener button
3 Power adapter
4 “Fail-Secure” door opener
5 “Fail-Safe” door opener



c) Connecting to alarm system

Observe the operating instructions for the alarm system used. The access system relay switches when a valid transponder is recognised. The alarm system can thus be enabled or disabled.

d) Wiegand interface

There are two application options for the Wiegand interface of the access system:

1) The access system is used as an external card reader

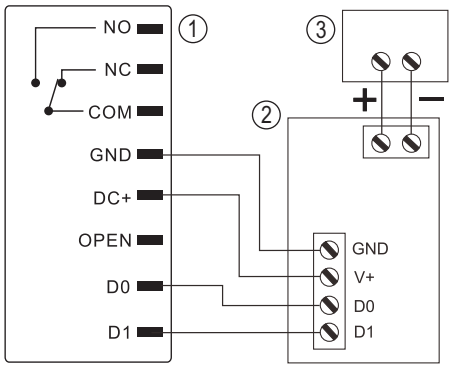
The access system can be connected to a compatible Wiegand controller and used as an external card reader. The Wiegand controller must support a 26-bit protocol that is used for the transmission of transponder data.

→ Follow the operating instructions for your Wiegand controller.

1 Access system

2 Wiegand controller

3 Power adapter



The access system has the operating voltage of 12 - 18 V/DC. If the Wiegand controller does not support this operating voltage, the access system will require a separate power supply unit. The wiring diagram will then be different from the one shown in the figure.

2) An external card reader is connected to the access system

The access system functions as a Wiegand controller and can be operated with an external card reader (with 26- or 34-bit protocol, automatic recognition).

→ Both card readers for 125 kHz transponders and card readers with MIFARE® smart card technology (13.561 MHz) are supported.

When a MIFARE® smart card reader is used, new transponders can only be paired via this card reader.

However, when a card reader for 125 kHz transponders is used, transponders can be paired both via the access system and the card reader (should you face any problems, use only the external card reader for pairing).

Make sure the two data cables D0 and D1 are not swapped; D0 must always be connected to D0 and D1 must always be connected to D1. Other connections can be carried out as shown in section 7. b). Always follow the operating instructions for the external card reader.

8. Operation

a) IR remote control

The IR remote control is factory supplied with a pre-inserted battery. Remove a small transparent protective strip that prevents early discharge of the battery and the IR remote control is ready for use.

The battery must be changed when the access system no longer responds to the IR remote control.

To do this, take out the battery holder at the lower end of the IR remote control and replace the depleted CR2025 battery with a new one. The battery's positive pole (+) must point towards the underside of the IR remote control.

Replace the battery holder of the IR remote control correctly.

Make sure you dispose of the used battery in an environmentally friendly manner (see section “Disposal”).

b) Access system

After completing the installation and connection process, switch on the operating voltage. The access system will emit a short beep and the red LED will light up. This indicates that the access system is in standby mode. You can now start programming, see next chapter.

If the access system continuously emits beeps with the LED flashing quickly, it means that the brightness sensor on the back has activated tamper protection and disabled all functions.

If this is the case, disconnect the access system from the power supply. Make sure that the brightness sensor is not exposed to light beams after installation.

If you want to briefly check the access system before installation, make sure you cover the brightness sensor on the back, for example, with a piece of non-transparent adhesive tape; if necessary, briefly disconnect the access system from the power supply to reset tamper protection.

9. Programming

Important!

We recommend that you note all settings. You will thus be able to refer to them over time and adapt them to new requirements.

You should note access data such as user name, memory cell number, transponder number, etc. to know who can access the system. These data also enable easy deletion of individual user transponders.

The access system can be reset to factory defaults, in which case all settings are lost (stored user transponders are retained in this case and may have to be deleted separately).

Programming is performed mainly with the included IR remote control. Point the LED at the end of the IR remote control towards the LED indicator (2) of the access system, where the IR reception LED is located (not visible from the outside). The IR remote control must be held close enough to the access system (approx. 1 m) for the latter to respond to it.

User transponders can also be paired and/or deleted with the included master transponder. A new master transponder can be saved if the one currently used is lost or defective.

⟶ If you no longer wish to use a master transponder for security reasons, follow the procedure for resetting to factory defaults described in section 8. j).

a) Enabling/disabling programming mode

- To enable the programming mode, enter the master code with the IR remote control (factory setting = 123456):

  [*] [1][2][3][4][5][6] [#]

  Each time you press a button on the IR remote control, the access system emits a short beep.
- Flashing red LED indicates that the programming mode is active. This mode allows pairing and deleting user transponders or making various settings.
- To exit the programming mode, press the [*] button. Glowing red LED indicates that the access system is in standby mode (can be switched off as described in section 8. i).

⟶ When no button is pressed within 30 seconds after calling up the programming mode, it is exited automatically for security reasons and the access system goes back to standby mode. Previously programmed settings will be accepted.

b) Changing the master code

Access system programming always requires the master code, which should be selected accordingly.

The default master code is “123456” (the same applies after resetting the code lock to factory defaults). For security reasons, we strongly recommend that you change this master code immediately after programming when the access system is in normal operation.

⟶ The master code must always consist of six digits.

Proceed as follows:

- Enable the programming mode as described in section 8. a); the LED starts to flash red.
- Enter the programming code [0] for the master code: The yellow LED will then light up.
- Then enter the new master code, for example: [9] [8] [7] [6] [5] [4]
- Press the [#] button to confirm your entry.
- Enter the new master code once again, for example: [9] [8] [7] [6] [5] [4]
- Press the [#] button to confirm your entry.
- The LED flashes red again, which means that you can continue programming or exit the programming mode with the [*] button.

c) Pairing user transponders

Up to 2000 different user transponders can be paired with the access system. You can use both the IR remote control and the master transponder for pairing.

⟶ We recommend that you create a table and fill in all access data, including user name, memory cell number, transponder number. This is how you can keep track of who signed up for the access system and used a specific memory cell.

With these data it is also easier to delete a single user or a lost user transponder.

1) Pairing a user transponder with the IR remote control

There are several pairing options using the IR remote control:

- Quick pairing of a user transponder in the next free memory cell
- Pairing and saving a user transponder in a specific memory cell
- Saving a certain number of user transponders with consecutive 8- or 10-digit transponder numbers at a time

User transponder is automatically saved in the next free memory cell:

⟶ This pairing procedure enables quick and easy pairing of new user transponders in the next free memory cell. However, a specific user transponder that is defective or lost can only be deleted via the transponder number and not via the memory cell number, as the memory cell number to which this specific user transponder is assigned is unknown.

- Enable the programming mode as described in section 8. a); the LED starts to flash red.
- Enter the programming code [1] to pair the transponders. The yellow LED will then light up.
- Hold a transponder in front of the RFID sensor. Once a new transponder is recognised, the access system emits a short beep and the transponder is saved.

  Optionally, you can also enter the 8- or 10-digit transponder number and confirm the entry with the [#] button.

⟶ When transponder pairing is complete, the access system emits three brief beeps and the LED flashes red. The same transponder cannot be paired more than once.

- If desired, you can pair other transponders by holding them in front of the RFID sensor, one at a time (optionally, you can enter the 8- or 10-digit transponder number and confirm with the [#] button).
- Press the [#] button to exit the pairing mode. The LED flashes red again, which means that you can continue programming or exit the programming mode with the [*] button.

User transponder is assigned to a specific memory cell:

⟶ Although this pairing process takes more time, it enables to delete a specific user transponder even when it is defective or lost.

- Enable the programming mode as described in section 8. a); the LED starts to flash red.
- Enter the programming code [1] to pair the transponders. The yellow LED will then light up.
- Enter the memory cell number (1 to 2000) in which the user transponder is to be saved; you do not need to enter leading zeros.

  Example: [6] = save transponder in memory cell 6
- Press the [#] button to confirm the memory cell number.

⟶ When the memory cell number is already occupied, the access system emits three brief beeps and the LED flashes red. A memory cell cannot be overwritten. The respective memory cell should first be cleared before you can save any other user transponder in it.

- Hold a transponder in front of the RFID sensor. Once a new transponder is recognised, the access system emits a short beep and the transponder is saved.

  Optionally, you can also enter the 8- or 10-digit transponder number and confirm the entry with the [#] button.

⟶ When transponder pairing is complete, the access system emits three brief beeps and the LED flashes red. The same transponder cannot be paired more than once.

- If you wish to pair another user transponder, first enter the memory cell number as above.
- Press the [#] button to exit the pairing mode. The LED flashes red again, which means that you can continue programming or exit the programming mode with the [*] button.

Multiple user transponders with consecutive transponder numbers are saved at a time

⟶ This option enables you to save multiple transponders with consecutive transponder numbers at the same time.

Since the memory cell numbers are also consecutive, transponders can be assigned to them; moreover, it is possible to delete an individual transponder that is defective or lost via the memory cell number. However, you should first create a list of transponder numbers and memory cell numbers.

- Enable the programming mode as described in section 8. a); the LED starts to flash red.
- Enter the programming code [1] to pair the transponders. The yellow LED will then light up.
- Enter the memory cell number (1 to 2000) from which multiple transponders should be saved at a time. You do not need to enter leading zeros. Example: [2] [0] [0] = save transponders from memory cell 200
- Press the [#] button to confirm the memory cell number.

⟶ When the memory cell number is already occupied, the access system emits three brief beeps and the LED flashes red.

- Enter the number of transponders you want to save at the same time. Example: [3] [0] = 30 transponders with consecutive numbers are to be saved
- Press the [#] button to confirm the number of transponders.

⟶ Make sure that there are enough memory cells available from the entered memory cell number to accommodate all the transponders to be saved. For example, it is not possible to save 200 transponders starting from memory cell 1900 since the access system has a total of only 2000 memory cells. Should that be the case, the access system will emit three brief beeps and the LED will flash red.

- Enter the number of the first transponder (it should consist of 8 or 10 digits).
- Press the [#] button to confirm the transponder number.

⟶ The access system will then save the selected user transponder in the memory cell. The whole procedure lasts up to 3 minutes depending on the number of transponders.

- Press the [#] button to exit the pairing mode. The LED flashes red again, which means that you can continue programming or exit the programming mode with the [*] button.

2) Pairing a user transponder with the master transponder

⟶ This pairing procedure enables quick and easy pairing of new user transponders in the next free memory cell. However, a specific user transponder that is defective or lost can only be deleted via the transponder number and not via the memory cell number, as the memory cell number to which this specific user transponder is assigned is unknown.

- Hold the master transponder once in front of the RFID sensor. The access system will emit a short beep and the yellow LED will light up.
- Hold a user transponder once in front of the RFID sensor. Once a new transponder is recognised, the access system emits a short beep and the transponder is saved.

  Optionally, you can also enter the 8- or 10-digit transponder number and confirm the entry with the [#] button.

⟶ When user transponder pairing is complete, the access system emits three brief beeps and the LED flashes red. The same user transponder cannot be paired more than once.

- If desired, you can pair other transponders by holding them in front of the RFID sensor, one at a time (optionally, you can enter the 8- or 10-digit transponder number and confirm with the [#] button).
- Hold the master transponder in front of the RFID sensor to finish the pairing process. The access system will emit a short beep, the red LED will light up and the access system will go back to standby mode.

d) Deleting individual user transponders

The respective user will no longer have access once the corresponding user transponder has been deleted. User transponders can be deleted via the user transponder, the transponder number or the memory cell number.

User transponders can also be deleted with the master transponder.

1) Deleting a user transponder with the IR remote control

- Enable the programming mode as described in section 8. a); the LED starts to flash red.
- Enter the programming code 2 to delete the transponders. The yellow LED will then light up.
- Transponders can be deleted in three different ways:
  - Hold the user transponder once in front of the RFID sensor. Once the transponder is recognised, the access system emits a short beep and the transponder is deleted.
  - If the transponder is defective or lost, enter its 8- or 10-digit transponder number and press the # button to confirm.
  - Enter the memory cell number of the user transponder (without leading zeros, e.g. 2 0) and press the # button to confirm.

  Other user transponders can be deleted as described here above.

  → When the system does not recognise the user transponder and, hence, it cannot be deleted (or the entered memory cell number is already empty), the access system will emit 3 brief beeps and the LED will flash red.
- Press the # button to exit the delete mode. The LED flashes red again, which means that you can continue programming or exit the programming mode with the * button.

2) Deleting a user transponder with the master transponder

- Hold the master transponder twice in a row in front of the RFID sensor. The access system will emit a short beep and the yellow LED will light up.
- Hold a user transponder once in front of the RFID sensor. Once a signed up user transponder is recognised, the access system emits a short beep and the user transponder is deleted.

  Optionally, it is also possible to delete a user transponder by entering its 8- or 10-digit transponder number and pressing the # button for confirmation.

  → When the user transponder is unknown and/or already deleted, the access system emits three brief beeps and the LED flashes red.
- Other user transponders can be deleted by following the instructions above.
- Hold the master transponder in front of the RFID sensor to finish the deletion process. The red LED will then light up and the access system will go back to standby mode.

e) Deleting all user transponders

- Enable the programming mode as described in section 8. a); the LED starts to flash red.
- Enter the programming code [2] to delete the transponders. The yellow LED will then light up.
- Enter the master code again.
- Press the [#] button to exit the delete mode. The LED flashes red again, which means that you can continue programming or exit the programming mode with the [*] button.

Example for deleting all transponders (programming mode must be active, see section 8. a); the default master code "123456" is used as an example; you must use your own master code:

[*] [1][2][3][4][5][6] [#] [2] [1][2][3][4][5][6] [#] [*]

f) Setting the changeover contact activation time

This function enables to set the changeover contact activation time from 1 to 99 seconds after a valid access to the code lock (default setting is 5 seconds).

When "0" is set, the changeover contact goes to "toggle" mode. Each valid access to the code lock changes the changeover contact switch position. This can be used to enable/disable an alarm system.

Proceed as follows:

- Enable the programming mode as described in section 8. a); the LED starts to flash red.
- Enter the programming code [3] to set the activation time. The yellow LED will then light up.
- Enter the desired changeover contact activation time. You can set from [1] ..... [9][9] (1 - 99 seconds).

  Example 1: Activation time is 8 seconds: [8]

  Example 2: Toggle mode: [0]
- Press the [#] button to exit the setting mode. The LED flashes red again, which means that you can continue programming or exit the programming mode with the [*] button.

Example 1 for a 4-second activation time (programming mode must be active, see section 8. a):

[3] [4] [#]

Example 2 for toggle mode (programming mode must be active, see section 8. a):

[3] [0] [#]

g) Enabling or disabling protection against incorrect entries

This function allows you to program whether or not the access system should react to 10 or more consecutive incorrect entries with a lock (by default: disabled).

Proceed as follows:

- Enable the programming mode as described in section 8. a); the LED starts to flash red.
- Enter the programming code 4 to enable protection against incorrect entries. The yellow LED will then light up.
- Select the desired function:

  0 = Protection function is disabled (default setting)

  1 = Block for 10 minutes (during this time you cannot access with a valid user transponder or via the IR remote control; the master transponder is also inoperative)

  2 = Block with alarm for 1 to 3 minutes (for setting the alarm time, see section 8. h); alarm can be disabled ahead of time with a valid user transponder or via the IR remote control through the entry of the master code

Attention!

Many countries have specific regulations in place regarding the duration of acoustic signals. The acoustic signals generated by the access system are subject to country-specific regulations, even if they are not as loud as those of a siren or an alarm system.

- Press the # button to exit the setting mode. The LED flashes red again, which means that you can continue programming or exit the programming mode with the * button.

Example for a block for 10 minutes (programming mode must be active, see section 8. a):

4 1 #

h) Setting the alarm time for protection function

After enabling the function 2 (block with alarm) as described in section 8. g), you can set the alarm time (from 1 to 3 minutes) as described below.

Proceed as follows:

- Enable the programming mode as described in section 8. a); the LED starts to flash red.
- Enter the programming code 5 to set the alarm time. The yellow LED will then light up.
- Enter the desired alarm time. You can set from 1 ..... 3 (1 - 3 minutes).
- Press the # button to exit the setting mode. The LED flashes red again, which means that you can continue programming or exit the programming mode with the * button.

Example for a 2-minute alarm time (programming mode must be active, see section 8. a):

5 2 #

i) Enabling/disabling LED indications and beeps

Function and error messages of the access system are accompanied by LED indications and beeps. They can be enabled and disabled (default setting: LED indications and beeps are enabled)

Proceed as follows:

- Enable the programming mode as described in section 8. a); the LED starts to flash red.
- Enter the programming code 6 to set LED indications and beeps. The yellow LED will then light up.
- Select the desired function:

  1 = LED disabled

  2 = LED enabled

  3 = Beeps disabled

  4 = Beeps enabled
- Press the # button to exit the setting mode. The LED flashes red again, which means that you can continue programming or exit the programming mode with the * button.

Example 1 for disabling LED indications (programming mode must be active, see section 8. a):

6 1 #

Example 2 for disabling beeps (programming mode must be active, see section 8. a):

6 3 #

j) Resetting all settings to factory defaults; pairing new master transponder

The access system can be reprogrammed by resetting it to factory defaults. The reset procedure also allows pairing of a master transponder, if necessary.

⟶ You can use either the included master transponder marked as “Master Card” or any other suitable transponder (125 kHz type) as the master transponder.

Only one transponder can be paired as a master transponder.

Resetting to factory defaults does not delete the saved user transponders. You can delete all user transponders by referring to section 8. e).

It is possible to have no paired master transponder, for example, if, for security reasons, you wish to pair or delete user transponders only via the programming mode and not via the master transponder.

1) Resetting the access system and paring master transponder

- De-energise the access system and wait for the LED to go off.
- Press and hold down the door opener button.
- Energise the access system. The access system will emit two beeps. Now release the door opener button.
- The yellow LED will light up.
- Hold the transponder to be paired as a master transponder in front of the RFID sensor. Once the transponder is recognised, the access system emits a beep and the transponder is saved as a master transponder.

⟶ The used transponder that is already paired as the user transponder cannot be used as a master transponder. The access system will emit three brief beeps and the LED will flash red.

- When the red LED lights up, the access system is in standby mode. All the settings have been reset to factory defaults.

2) Resetting the access system without paring master transponder

- De-energise the access system and wait for the LED to go off.
- Press and hold down the door opener button.
- Energise the access system. The access system will emit two beeps.
- Wait about 10 seconds, keep the door opener button pressed and do not release it.
- The access system will emit a beep and the red LED will light up.
- You can now release the door opener button for the access system to go back to standby mode. All settings have been reset to factory defaults and there are no master transponders for pairing or deleting user transponders.

Table with default settings:

Function	See chapter	Factory setting
Master code	8. b)	123456
Changeover contact activation time	8. f)	5 seconds
Protection against incorrect entries	8. g)	switched off
Alarm time for protection function	8 h)	1 minute
LED indicator	8. i)	enabled
Beep	8. i)	enabled

10. Operation

a) Getting started

Power on the access system once it has been connected and installed. After powering on, the access system will emit a beep and the red LED will glow steadily (standby).

The access system is now ready for use and can be programmed.

If the access system continuously emits beeps with the LED flashing quickly, it means that the brightness sensor on the back has activated tamper protection and disabled all functions.

If this is the case, disconnect the access system from the power supply. Make sure that the brightness sensor is not exposed to light beams after installation.

If you want to briefly check the access system before installation, make sure you cover the brightness sensor on the back, for example, with a piece of non-transparent adhesive tape; if necessary, briefly disconnect the access system from the power supply to reset tamper protection.

You should take the following steps:

- Create a table and fill in all settings and user/transponder numbers.
- Switch on the IR remote control by first removing the protective strip from the battery holder or inserting the battery.
- Think of a master code (consisting of 6 digits) and programme it (see section 8. b). The default master code is “123456” (the same applies after resetting the access system to factory defaults).
- The included master transponder (e.g. marked as “Master Card”) is used only for quick saving or deletion of user transponders. The IR remote control serves for all other programming operations.
- If you no longer wish to use the master transponder, for example, for security reasons, you can reset the access system accordingly, as described in section 8. j). In this case, user transponders can only be paired or deleted via the IR remote control.
- Pair user transponders with the access system (see section 8. e).
- Set the changeover contact activation time (see section 8. f) to be used e.g. for switching a door lock (default setting is 5 seconds).
- Check whether the saved user transponders can unlock the door lock.
- You can programme other functions, for example, enable protection against incorrect entries (section 8. g/h) or enable/disable LED indications or beeps (section 8. i).

b) Accessing via valid user transponder

Once the access system has recognised a valid user transponder, the changeover contact and door opener are activated for a preset time and the green LED lights up. When the time is up, the red LED lights up (standby).

⟶ After enabling the toggle mode (as described in section 8. f), each valid user transponder permanently switches the changeover contact to the other position.

c) Accessing via door opener button

Briefly pressing the door opener button activates the changeover contact and the door opener for a preset time and the LED lights up green.

⟶ After enabling the toggle mode (as described in section 8. f), each press of the door opener button permanently switches the changeover contact to the other position.

11. Troubleshooting

The access system retains its settings and is ready for operation after a power outage. However, the access system will not work during a power failure.

⟶ For safety reasons, we recommend that you connect the access system to an uninterruptible power supply (as in case of an alarm system) depending on the application.

After powering on the access system for the first time, it continuously emits beeps and the LED flashes red

- The brightness sensor on the back of the access system has activated tamper protection and locked all functions. If this is the case, disconnect the access system from the power supply. Make sure that the brightness sensor is not exposed to light beams after installation.
- If you want to briefly check the access system before installation, make sure you cover the brightness sensor on the back, for example, with a piece of non-transparent adhesive tape; if necessary, briefly disconnect the access system from the power supply to reset tamper protection.

The IR remote control does not work

- Point the small LED at the end of the IR remote control towards the LED indicator of the access system. The IR reception LED is located right next to it.
- The IR remote control must be held close enough to the access system (approx. 1 m) for the latter to respond to it.
- The front panel of the access system is exposed to direct sunlight (or any other IR light source such as IR spotlight of a surveillance camera) and its proper functioning is disturbed. Hold the IR remote control closer to the access system.
- The IR remote control battery is weak or depleted and must be replaced with a new one. Dispose of batteries with respect to environmental protection; see section “Disposal”.
- The battery was inserted incorrectly. Observe the correct polarity (the battery's positive pole (+) must point towards the underside of the IR remote control).

The door opener does not work

- The changeover contact is potential-free. This means that you must arrange the external wiring accordingly since the access system does not power the door opener.
- If the door opener has corresponding polarity markings (plus/+ and minus/-), ensure it is correctly connected to the access system and power supply.
- Check the polarity of the protective diode connected to the door opener.
- The used transponder is not paired.
- The changeover contact cannot be enabled with the master transponder.
- The NO/NC contacts should be wired correctly according to the door opener used (fail-safe or fail-secure door opener).

Transponder is not recognised

- Make sure you hold one transponder in front of the RFID sensor at a time (see section 6, clause 3).
- Ensure the transponder is close enough (approx. 3 cm) to the access system.
- Only EM transponders with a frequency of 125 kHz can be used.
- Metal objects can adversely affect a transponder's functionality (for example, if you keep the transponder in a wallet with metal coins).

New user transponder cannot be paired

- Make sure you hold one transponder in front of the RFID sensor at a time (see section 6, clause 3).
- Ensure the transponder is close enough (approx. 3 cm) to the access system.
- Only EM transponders with a frequency of 125 kHz can be used.
- The memory is already occupied. Use another memory cell or clear the existing one before pairing another transponder on the same memory cell.
- To save the transponder in a specific memory cell, enter the memory cell number without leading zeros (for example: for memory cell number 16, enter “16” instead of “0016”).
- When the Wiegand controller uses a MIFARE® smart card reader, new transponders can only be paired via this card reader.
- When the Wiegand controller uses a card reader for 125 kHz transponders, pairing can be performed both via the access system and the external card reader. Use an external card reader to check the functionality.

Changeover contact is permanently active (and cannot be switched back)

- The changeover contact activation time has been set to “0” and is in toggle mode. Each valid access attempt via the user transponder changes the changeover contact switch position.

Resetting to factory defaults does not delete any user transponders

- This is normal. All user transponders can be deleted by following the instructions described in section 8. e).

Wiegand connection does not work

- Make sure the two data cables D0 and D1 are not swapped; D0 must always be connected to D0 and D1 must always be connected to D1. Other connections can be carried out as shown in section 7. b). Always follow the operating instructions for the external card reader.
- Both card readers for 125 kHz transponders and card readers with MIFARE® smart card technology (13.561 MHz) are supported.

Power is supplied, but the LED does not light up in standby

- Switch on LED indications as described in section 8. i).

Access system emits no beeps

- Switch on beeps as described in section 8. i).

12. Cleaning and maintenance

This product does not require maintenance. Use a dry, lint-free cloth for occasional cleaning. In case of heavy soiling, lightly moisten the cloth with water.

Never use aggressive detergents, rubbing alcohol or other chemical solutions, as they can cause discolouration or erase button inscriptions.

13. Disposal

a) Product

Electronic devices are recyclable waste and must not be placed in household waste. At the end of its service life, dispose of the product in accordance with applicable regulatory guidelines.

If a battery is inserted, remove it and dispose of it separately from the product.

b) (Rechargeable) batteries

You as the end user are required by law (Battery Ordinance) to return all used batteries/rechargeable batteries. Disposing of them in the household waste is prohibited.

Contaminated (rechargeable) batteries are labelled with this symbol to indicate that disposal in the domestic waste is forbidden. The abbreviations for heavy metals in batteries are: Cd = Cadmium, Hg = Mercury, Pb = Lead (name on (rechargeable) batteries, e.g. below the trash icon on the left).

Used (rechargeable) batteries can be returned to collection points in your municipality, our stores or wherever (rechargeable) batteries are sold. You thus fulfil your statutory obligations and contribute to environmental protection.

Batteries/rechargeable batteries that are disposed of should be protected against short circuit and their exposed terminals should be covered completely with insulating tape before disposal. Even empty batteries/rechargeable batteries can contain residual energy that may cause them to swell, burst, catch fire or explode in the event of a short circuit.

14. Declaration of Conformity (DOC)

Conrad Electronic SE, Klaus-Conrad-Straße 1, D-92240 Hirschau, hereby declares that this product conforms to Directive 2014/53/EU.

→ Click on the following link to read the full text of the EU Declaration of Conformity:

www.conrad.com/downloads

Enter the product item number in the search box. You can then download the EU declaration of conformity in the available languages.

15. Technical data

a) Access system

Power supply	12 - 18 V/DC
Power consumption	Standby <50 mA
Frequency band	124.6 - 125.4 kHz
Transmission power	11.62 dBm
Max. reading distance	approx. 3 cm
Data retention in case of a power cut	yes
Suitable transponders	Commercially available EM transponders for frequency 125 kHz
Output	Potential-free single-pole changeover contact (relay)
	Max. contact rating 24 V/DC, 2 A
	Adjustable switching time (1 - 99 seconds or toggle mode; default setting: 5 seconds)
Wiegand connection	yes (output = 26-bit protocol, input = 26/34-bit protocol with automatic recognition)
Transponder memory cells	2000
Mounting location	indoors/outdoors
Protection class	IP66
Ambient conditions	Temperature -40 °C to +60 °C
Cable length	approx. 25 cm
Dimensions	115 x 70 x 25 mm (H x W x D)
Weight	approx. 185 g

b) IR remote control

Operating voltage	3 V/DC via 1x CR2025 battery (lithium coin cell)
Max. IR range	approx. 1 m

2380477_V3_1021_02_VTP_m_en