sygonix®

GB Operating Instructions

RFID/fingerprint access system

Item no. 2380479

Table of contents

Page

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!

All company and product names contained herein are trademarks of their respective owners. All rights reserved.

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. Control is possible via suitable transponders or fingerprints. A maximum of 1000 users can be stored (100 fingerprints, 890 user transponders and 10 visitor transponders).

If you hold a taught-in transponder in front of the reading area or touch the sensor with a stored finger, a floating relay changeover contact is activated (for contact rating, see ‘Technical data’). This can be used, for example, to control a door opener or an alarm system.

The product is intended for wall mounting and for indoor and outdoor use (IP66).

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.

This product complies with statutory, national and European regulations. All company and product names contained herein are trademarks of their respective owners. All rights reserved.

4. Delivery content

- Access system
- Mounting material (2x special screws with suitable L key, 4x stickers for screw heads, mounting frame with 4x screws and 4x dowels)
- Master transponder
- Diode 1N4004 (for relay changeover contact)
- IR remote control (with 1x CR2025 lithium-ion battery)
- Quick Start
- Overview sheet for programming

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 intended for installation and operation in indoor and outdoor areas (IP66). Nevertheless, the enclosed IR remote control must not be allowed to get damp or wet.
- 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.
- Never exceed the contact rating for the changeover contact specified in the 'Technical data'. 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. Seek immediate medical attention if a battery is swallowed. Risk of death!
- 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

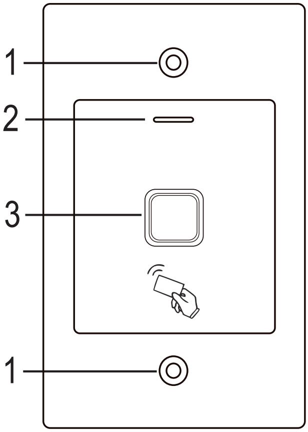
1 Opening for wall mounting

2 LED indicator

3 RFID/fingerprint sensor with LED ring

→ There is a brightness sensor on the rear, which serves as sabotage protection.

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



Connecting cable:

Colour	Inscription	Function
Red	12 - 18 V/DC	Operating voltage 12 - 18 V/DC
Black	GND	GND/ground
Blue	NO	NO contact of the relay
Brown	COM	COM contact of the relay
Grey	NC	NC contact of the 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. Do not mount or connect the product when it is connected to a power supply.

Ensure that the brightness sensor on the rear is in the dark after installation, otherwise sabotage protection will be activated after switching on the operating voltage and no function will be possible.

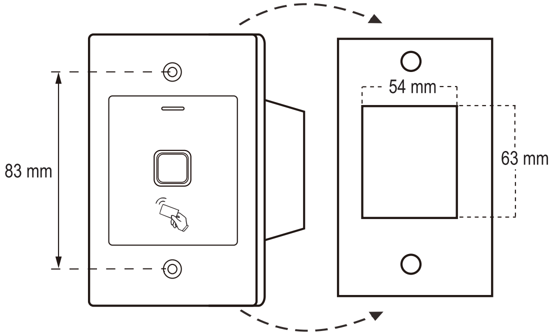
a) Installation

Attach the mounting plate to a wall using the module provided (see figure to the right) using suitable screws. Depending on the surface, dowels may also be required.

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

Depending on the surface and installation position, the enclosed mounting frame in the delivery can be mounted, into which the access system is subsequently to be screwed.

Depending on the mounting location, use appropriate screws and, if necessary, dowels.



If necessary, drill a hole for the connecting cables before mounting. Wire the cables according to the circuit examples 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, see the following circuit examples (the ring on the protective diode must point in the direction of the positive terminal/+ when connecting).

Attention!

Never switch the mains voltage via the potential-free changeover contact! There is a risk of fatal electric shock! Refer to the "Technical data" section for information on the permissible contact rating.

→ 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/-).

The screw openings can be sealed with the enclosed stickers after connection and successful commissioning.

b) Connection to conventional voltage/power supply

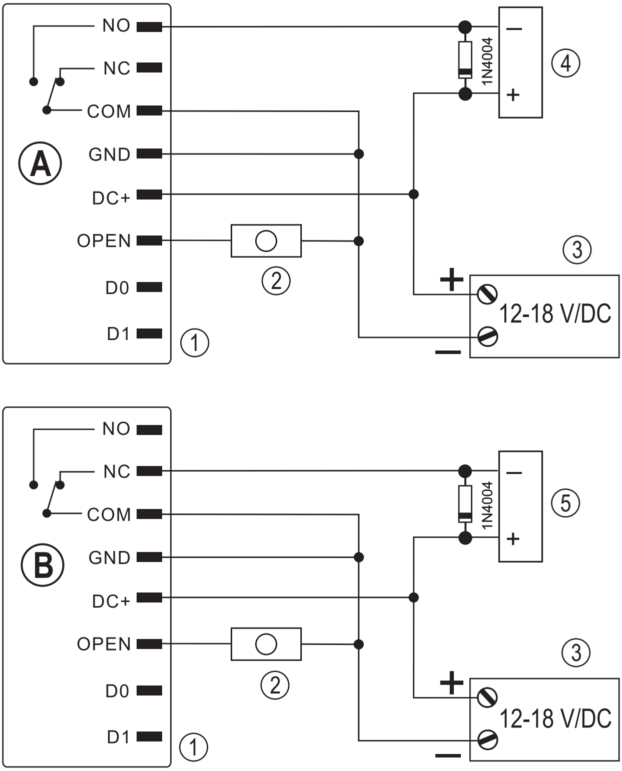
If you wish to use a conventional power adapter for operation, observe the following figures with the connection diagram.

A) ‘Fail Secure’ door opener: This releases the locking latch only when its operating voltage is applied (common design for front doors).

B) ‘Fail Safe’ door opener: This releases the latch when the power is removed (non-standard door opener type, used for emergency exit doors so that the door opens in the event of a power cut).

→ The enclosed diode must be connected in the vicinity of the door opener with the correct polarity 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) Alarm system connection

Observe the operating instructions for the alarm system that you are using. The relay in the access system switches when a valid transponder is detected or you touch the sensor with a stored finger. An alarm system can, therefore, be armed or disarmed.

d) Wiegand interface

The Wiegand interface of the access system can be used in 2 different ways:

1) The access system works as an external card reader

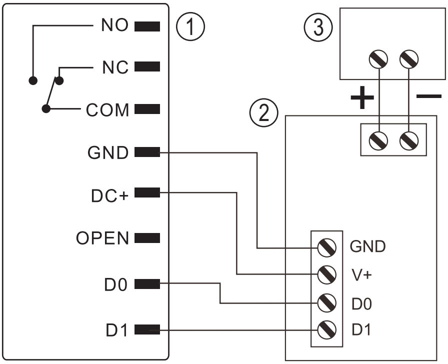
The access system can be connected to a suitable Wiegand controller and serves as an external card reader. The transponder data are transmitted via a 26-bit protocol – the Wiegand controller must, therefore, support this.

⟶ Follow the operating instructions for your Wiegand controller.

1 Access system

2 Wiegand controller

3 Power adapter



The access system works with an operating voltage of 12 - 18 V/DC. If the Wiegand controller does not provide this, you will need a separate power adapter for the access system. In that case, the wiring will be different to that shown in the figure.

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

The access system itself functions as a Wiegand controller and allows for operation of an external card reader (with 26-bit or 34-bit protocol, automatic detection).

⟶ Card readers for 125 kHz transponders as well as card readers with MIFARE® chip card technology (13.561 MHz) are permitted.

If a MIFARE® chip card reader is connected, it must be used to teach in new transponders.

When connecting a card reader for 125 kHz transponders, the teach-in process can be carried out both via the access system and via the card reader (if problems occur here, use only the external card reader for teach-in).

Ensure that the two data lines D0 and D1 are not swapped – D0 must always be connected to D0 and D1 to D1. The remaining wiring can be carried out as outlined in 7. b). Always observe the operating instructions for the external card reader.

8. Operation

a) IR remote control

The IR remote control battery is already inserted on delivery. Simply remove the small transparent protective strip (this prevents premature discharge of the battery) and the IR remote control will be ready for operation.

The battery will need to be replaced if the access system no longer responds to the IR remote control.

In that case, simply remove the battery holder at the bottom end of the IR remote control and replace the depleted battery (1x CR2025) with a new one. The positive terminal (+) of the battery must point towards the bottom of the IR remote control.

Insert the battery holder into the IR remote control, observing the correct orientation.

Dispose of batteries with respect to environmental protection; see ‘Disposal’.

b) Access system

After completing the installation and connection process, switch on the operating voltage. The access system emits a short beep and the LED lights up red. 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 and the LED flashes quickly, the brightness sensor on the rear has activated the sabotage protection; operation is not possible.

Disconnect the access system from the operating voltage immediately in this case. Ensure that the brightness sensor is in the dark after installation.

If you wish to commission the access system for testing purposes before mounting, cover the brightness sensor on the rear, e.g. use a piece of opaque adhesive tape (if necessary, briefly disconnect the access system from the operating voltage to reset the sabotage protection).

9. Programming

Important!

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

You should also enter the access data (e.g. username, memory number, transponder number) in order to maintain an overview of who is permitted access. It also makes it very easy to delete individual user transponders or user fingerprints.

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

The enclosed IR remote control is primarily used for programming. Point the LED located at one end of the IR remote control towards the position of the indicator LED (2) in the access system – this is where the IR receiver LED is located (not visible from the outside). The distance between the IR remote control and the access system must not exceed 1 m.

The enclosed master transponder can also be used to teach in or delete user transponders/fingerprints. If the master transponder is lost or faulty, a new master transponder can also be stored.

If you do not wish to have a master transponder for security reasons, this can be facilitated with a special procedure on resetting to the default settings, see 8. j).

Teach-in or deletion of user transponders/fingerprints is also possible with a master fingerprint.

The access system also allows you to store up to 10 ‘visitor’ transponders. For each of the visitor transponders, you can program the number of access attempts (1 - 10 attempts can be set) after which the transponder will become invalid. For example, you can program a visitor transponder in such a way that it only allows access once.

1000 memories are provided for the transponders and fingerprints:

- Memory number 0 - 98: user fingerprints
- Memory number 99: master fingerprint
- Memory number 100 - 989: User transponder
- Memory number 990 - 999: visitor transponder

a) Enabling/disabling programming mode

- To start programming mode, enter the master code on the IR remote control as follows (default setting = 123456):

  *   1 2 3 4 5 6   #

  The access system emits a short beep as confirmation each time a button on the IR remote control is pressed.

- The LED then flashes red (programming mode is active). You can now teach in/delete user transponders, for example, or implement different settings.
- To exit the programming mode, press the * button. The access system is in standby mode again, the LED lights up red continuously.

→ If no button is pressed within 30 seconds of calling up programming mode, the mode 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 at the latest when programming is complete and the access system is used in normal operation.

→ The master code must always consist of six digits.

Proceed as follows:

- Start programming mode as outlined in 8. a) so that the LED flashes red.
- Enter the programming code 0 for the master code. The LED lights up yellow.
- Then, enter the new master code, for example: 9 8 7 6 5 4
- Press the # key to confirm your entry.
- Enter the new master code again, for example: 9 8 7 6 5 4
- Press the # key to confirm your entry.
- The LED flashes red again. You can now carry out further programming or exit programming mode with the * button.

c) Teaching in/deleting the master fingerprint

A single master fingerprint can be taught in to the access system. This allows quick teach-in or deletion of user transponders or user fingerprints.

→ Memory number 99 is reserved for the master fingerprint.

Teaching in the master fingerprint:

- Start programming mode as outlined in 8. a) so that the LED flashes red.
- Enter programming code 1 to start the teach-in process. The LED lights up yellow.
- Enter the memory number 9 9 for the master fingerprint.
- Press the # key to confirm your entry.

→ If a master fingerprint is already assigned to memory number 99, the access system emits 3 rapid beeps and the LED flashes red. It is no longer possible to overwrite an existing master fingerprint. Start by deleting memory number 99 (see below) before storing another master fingerprint.

- To teach in the master fingerprint, touch the fingerprint sensor 3 times in succession with the same finger. An LED ring around the sensor lights up blue when the sensor is touched. The LED ring lights up green and a short beep is emitted if the fingerprint is recognised correctly. After the third correct reading, the access system emits a longer beep and the fingerprint is stored.

→ If the fingerprint cannot be read correctly, 3 beeps are emitted and the LED ring flashes red. The same happens if you try to read in a fingerprint that has already been stored.

- Exit teach-in mode with the # button. The LED flashes red again. You can now carry out further programming or exit programming mode with the * button.

Delete the master fingerprint:

- Start programming mode as outlined in 8. a) so that the LED flashes red.
- Enter programming code 2 to start deletion mode. The LED lights up yellow.
- Enter the memory number 9 9 for the master fingerprint and confirm it with the # button.

→ If the memory is already blank, the access system emits 3 quick beeps and the LED flashes red.

- Exit deletion mode with the # button. The LED flashes red again. You can now carry out further programming or exit programming mode with the * button.

d) Adding user transponders

The access system can store up to 890 different user transponders. Memory numbers 100 - 989 are provided for these transponders.

The teach-in process can be carried out via the IR remote control and with the aid of the master transponder or the master fingerprint.

→ We recommend that you create a table and fill in all access data, including username, memory number, transponder number. This is how you can keep track of who accessed the access system and used a specific memory.

It is also easier to delete a single user or a lost user transponder.

1) Teach-in of a user transponder with the IR remote control

You can teach in using the IR remote control in two different ways:

- Quick teach-in of a user transponder to the next free memory
- Teach-in of a user transponder to a specific memory

Automatically store user transponders to the next free memory:

→ This teach-in process is very fast and easy, new user transponders are taught in to the next available memory. However, if the transponder is lost or faulty, it cannot be deleted as the assignment between the user transponder and memory is unknown. In that case, all memories would need to be deleted.

- Start programming mode as outlined in 8. a) so that the LED flashes red.
- Enter programming code 1 to start the teach-in process. The LED lights up yellow.
- 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 stored.

→ If the transponder has already been taught in, the access system emits 3 quick beeps and the LED flashes red. The same transponder cannot be taught in more than once.

- If desired, other transponders can be taught in by holding them in front of the RFID sensor individually.
- Exit teach-in mode with the # button. The LED flashes red again. You can now carry out further programming or exit programming mode with the * button.

Assigning user transponders to a specific memory:

→ This teach-in process takes longer, but a certain user transponder can be deleted later (via the memory number) even if it is lost or faulty.

- Start programming mode as outlined in 8. a) so that the LED flashes red.
- Enter programming code 1 to start the teach-in process. The LED lights up yellow.
- Enter the memory number (1 0 0 ..... 9 8 9) to which the user transponder is to be stored.

  Example: 6 5 4 = Store the transponder to memory 654
- Confirm the memory number with the # button.

→ If the memory number has already been assigned, the access system emits 3 quick beeps and the LED flashes red. It is, therefore, not possible to overwrite a memory. Start by deleting the respective memory before another user transponder can be stored there.

- 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 stored.

→ If the transponder has already been taught in, the access system emits 3 quick beeps and the LED flashes red. The same transponder cannot be taught in more than once.

- If you wish to teach in another user transponder, start by entering a memory number, see above.
- Exit teach-in mode with the # button. The LED flashes red again. You can now carry out further programming or exit programming mode with the * button.

2) Teach-in of a user transponder with the master transponder or the master fingerprint

→ This teach-in process is very fast and easy, new user transponders are taught in to the next available memory. However, if the transponder is lost or faulty, it cannot be deleted as the assignment between the user transponder and memory is unknown. In that case, all memories would need to be deleted.

- Hold the master transponder 1x at a short distance in front of the RFID sensor or touch 1x with the master finger on the fingerprint sensor. The access system emits a short beep and the LED lights up yellow. Teach-in mode is active.
- Hold a user transponder a short distance in front of the RFID sensor. Once a new transponder is recognised, the access system emits a short beep and the transponder is stored.

→ If the user transponder has already been taught in, the access system emits 3 quick beeps and the LED flashes red. The same transponder cannot be taught in more than once.

- If desired, other transponders can be taught in by holding them in front of the RFID sensor individually.
- To end the teach-in process, hold the master transponder 1x in front of the RFID sensor or touch 1x with the master finger on the fingerprint sensor. The LED then lights up red and the access system is in standby mode again.

e) Deleting the user transponder

The respective user will no longer have access and the corresponding user transponder can be deleted. Deletion is possible either via the user transponder or the memory number.

The master transponder or the master fingerprint can also be used to delete a user transponder.

1) Deletion of a user transponder with the IR remote control:

- Start programming mode as outlined in 8. a) so that the LED flashes red.
- Enter programming code 2 to start deletion mode. The LED lights up yellow.
- There are 2 different ways to delete:
  - Hold the user transponder a short distance in front of the RFID sensor. If the transponder is recognised, the access system emits a short beep and the transponder is deleted.
  - Enter the memory number of the user transponder (e.g. 6 5 4) and confirm it with the # button. The transponder is then deleted.

  Another user transponder can then be deleted as described above.

→ If the user transponder is unknown (or already deleted), the access system emits 3 quick beeps and the LED flashes red.

- Exit deletion mode with the # button. The LED flashes red again. You can now carry out further programming or exit programming mode with the * button.

2) Deletion of a user transponder with the master transponder or the master fingerprint

- Hold the master transponder 2x in succession a short distance in front of the RFID sensor or touch 2x with the master finger on the fingerprint sensor. The LED indicator lights up yellow.
- Hold a user transponder a short distance in front of the RFID sensor. Once a registered user transponder is recognised, the access system emits a short beep and the user transponder is deleted.

→ If the user transponder is unknown (or already deleted), the access system emits 3 quick beeps and the LED flashes red.

- If additional user transponders are to be deleted, proceed as outlined, hold them in front of the RFID sensor.
- To end the deletion process, hold the master transponder 1x in front of the RFID sensor or touch 1x with the master finger on the fingerprint sensor. The LED then lights up red and the access system is in standby mode again.

f) Setting the user fingerprint

The access system can store up to 99 different user fingerprints. Memory numbers 0 - 98 are provided for these transponders.

The teach-in process can be carried out via the IR remote control and with the aid of the master transponder or the master fingerprint.

→ We recommend that you create a table and fill in all access data, including username, memory number. This is how you can keep track of who accessed the access system and used a specific memory.

It is also very easy to delete a single user.

1) Teach-in of a user fingerprint with the IR remote control

You can teach in using the IR remote control in two different ways:

- Quick teach-in of a user fingerprint to the next free memory
- Teach-in of a user fingerprint to a specific memory

Automatically store user fingerprints to the next free memory:

→ This teach-in process is very fast and easy, new user fingerprints are taught in to the next available memory.

In this case, however, deleting a specific user fingerprint is only possible with the fingerprint as the assignment between the user fingerprint and memory number is unknown. In that case, all memories would need to be deleted.

- Start programming mode as outlined in 8. a) so that the LED flashes red.
- Enter programming code 1 to start the teach-in process. The LED lights up yellow.
- To teach in a user fingerprint, touch the fingerprint sensor 3 times in succession with the same finger. An LED ring around the sensor lights up blue when the sensor is touched. The LED ring lights up green and a short beep is emitted if the fingerprint is recognised correctly. After the third correct reading, the access system emits a longer beep and the fingerprint is stored.

→ If the fingerprint cannot be read correctly, 3 beeps are emitted and the LED ring flashes red. The same happens if you try to read in a fingerprint that has already been stored.

- You can now teach in another user fingerprint, proceed as outlined above (touch the fingerprint sensor 3x in succession).
- Exit teach-in mode with the # button. The LED flashes red again. You can now carry out further programming or exit programming mode with the * button.

Assign a user fingerprint to a specific memory:

→ This teach-in process takes longer, but a certain user fingerprint can be deleted later (via the memory number) even if the person is no longer available for the deletion process.

- Start programming mode as outlined in 8. a) so that the LED flashes red.
- Enter programming code 1 to start the teach-in process. The LED lights up yellow.
- Enter the memory number (0 ..... 9 8) to which the user fingerprint is to be stored (without leading zero for single-digit memory numbers).

  Example 1: 6 = Store fingerprint to memory 6

  Example 2: 5 4 = Store fingerprint to memory 54
- Confirm the memory number with the # button.

→ If the memory number has already been assigned, the access system emits 3 quick beeps and the LED flashes red. It is, therefore, not possible to overwrite a memory. Start by deleting the respective memory before another user fingerprint can be stored there.

- To teach in a user fingerprint, touch the fingerprint sensor 3 times in succession with the same finger. An LED ring around the sensor lights up blue when the sensor is touched. The LED ring lights up green and a short beep is emitted if the fingerprint is recognised correctly. After the third correct reading, the access system emits a longer beep and the fingerprint is stored.

→ If the fingerprint cannot be read correctly, 3 beeps are emitted and the LED ring flashes red. The same happens if you try to read in a fingerprint that has already been stored.

- If you wish to teach in another user fingerprint, start by entering a memory number, see above.
- Exit teach-in mode with the # button. The LED flashes red again. You can now carry out further programming or exit programming mode with the * button.

2) Teach-in of a user fingerprint with the master transponder or the master fingerprint

→ This teach-in process is very fast and easy, new user fingerprints are taught in to the next available memory.

In this case, however, deleting a specific user fingerprint is only possible with the fingerprint as the assignment between the user fingerprint and memory number is unknown. In that case, all memories would need to be deleted.

- Hold the master transponder 1x at a short distance in front of the RFID sensor or touch 1x with the master finger on the fingerprint sensor. The access system emits a short beep and the LED lights up yellow. Teach-in mode is active.
- To teach in a user fingerprint, touch the fingerprint sensor 3 times in succession with the same finger. An LED ring around the sensor lights up blue when the sensor is touched. The LED ring lights up green and a short beep is emitted if the fingerprint is recognised correctly. After the third correct reading, the access system emits a longer beep and the fingerprint is stored.

→ If the fingerprint cannot be read correctly, 3 beeps are emitted and the LED ring flashes red. The same happens if you try to read in a fingerprint that has already been stored.

- You can now teach in another user fingerprint, proceed as outlined above (touch the fingerprint sensor 3x in succession).
- To end the teach-in process, hold the master transponder 1x in front of the RFID sensor or touch 1x with the master finger on the fingerprint sensor. The LED then lights up red and the access system is in standby mode again.

g) Deleting the user fingerprint

The respective user will no longer have access and the corresponding user fingerprint can be deleted. Deletion is possible either via the user fingerprint or the memory number.

The master transponder or the master fingerprint can also be used to delete a user fingerprint.

1) Deletion of a user fingerprint with the IR remote control

- Start programming mode as outlined in 8. a) so that the LED flashes red.
- Enter programming code [2] to start deletion mode. The LED lights up yellow.
- There are 2 different ways to delete:
  - Touch the fingerprint sensor with the user finger you wish to delete. If the fingerprint is recognised, the access system emits a short beep and the fingerprint is deleted.
  - Enter the memory number of the user fingerprint (without leading zero for single-digit memory numbers) and confirm it with the [#] button.

→ If the user fingerprint is not known in the system and, therefore, deletion is not possible (or the entered memory number is already blank), the access system emits 3 quick beeps and the LED flashes red.

- If you wish to delete additional user fingerprints, proceed as outlined.
- Exit deletion mode with the [#] button. The LED flashes red again. You can now carry out further programming or exit programming mode with the [*] button.

2) Deletion of a user fingerprint with the master transponder or the master fingerprint

- Hold the master transponder 2x in succession a short distance in front of the RFID sensor or touch 2x with the master finger on the fingerprint sensor. The access system emits a short beep and the LED lights up yellow.
- Touch the fingerprint sensor with the user finger you wish to delete. If the fingerprint is recognised, the access system emits a short beep and the fingerprint is deleted.

→ If the user fingerprint is unknown (or already deleted), the access system emits 3 quick beeps and the LED flashes red.

- If you wish to delete additional user fingerprints, proceed as outlined (touch the fingerprint sensor 3x in succession).
- To end the deletion process, hold the master transponder 1x in front of the RFID sensor or touch 1x with the master finger on the fingerprint sensor. The LED then lights up red and the access system is in standby mode again.
-

h) Clearing all memories

→ All 1000 memories are deleted (890 user transponders, 10 visitor transponders, 99 user fingerprints and the master fingerprint).

The master transponder and the programmed settings (e.g. the activation time for the changeover contact or the protection function) are retained.

Proceed as follows:

- Start programming mode as outlined in 8. a) so that the LED flashes red.
- Enter programming code 2 to start deletion mode. The LED lights up yellow.
- Enter: 0 0 0 0
- Exit deletion mode with the # button. The LED flashes red again. You can now carry out further programming or exit programming mode with the * button.

Example for deleting all 1000 memories (the default master code 123456 is used as an example; you must use your own master code):

* 1 2 3 4 5 6 # 2 0 0 0 0 # *

i) Select access mode

The changeover contact can be activated in 3 different ways:

- With a transponder <u>or</u> fingerprint (default setting)
- Only with a fingerprint
- Only with a transponder

→ The changeover contact cannot be activated with the master transponder or the master fingerprint.

Proceed as follows:

- Start programming mode as outlined in 8. a) so that the LED flashes red.
- Enter the programming code 3 for the access mode: The LED lights up yellow.
- Select the desired access mode:

  0 = with a transponder or fingerprint (default setting)

  1 = only with a fingerprint

  2 = only with a transponder

- Exit setting mode with the # button. The LED flashes red again. You can now carry out further programming or exit programming mode with the * button.

Example for access via a transponder only (programming mode must be active, see 8. a):

3 2 #

j) Setting the changeover contact activation time

This program setting allows you to define how long the changeover contact is activated during a valid access attempt (default setting: 5 seconds); an interval of 1 - 99 seconds can be set.

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:

- Start programming mode as outlined in 8. a) so that the LED flashes red.
- Enter the programming code 4 to set the activation time. The LED lights up yellow.
- Enter the desired changeover contact activation time. Possible is 1 ..... 9 9 (= 1 - 99 seconds; without leading zero for single-digit memory numbers).

  Example 1: Activation time is 8 seconds: 8

  Example 2: Toggle mode: 0
- Exit setting mode with the # button. The LED flashes red again. You can now carry out further programming or exit programming mode with the * button.

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

4 8 #

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

4 0 #

k) Selecting or switching off protection against incorrect entries

This function allows you to set whether the access system should be blocked in case of 10 or more incorrect entries in succession (default setting: disabled).

Proceed as follows:

- Start programming mode as outlined in 8. a) so that the LED flashes red.
- Enter the programming code 6 to enable protection against incorrect entries. The LED lights up yellow.
- Select the desired function:

  0 = Protection function is deactivated (default setting)

  1 = Block for 10 minutes (during this time, neither access via valid transponder/fingerprint nor operation via IR remote control is possible, the master transponder or master fingerprint is also without function)

  2 = Block with alarm for 1 - 3 minutes (for information on setting the alarm duration, see 8. l); the block and alarm can be terminated prematurely with a valid transponder or fingerprint

Attention!

There are regulations in many countries governing the duration of alarm tones. Even if the tone signal of the access system is not as loud as the siren of an alarm system, it may nevertheless fall under country-specific regulations.

- Exit setting mode with the # button. The LED flashes red again. You can now carry out further programming or exit programming mode with the * button.

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

6 1 #

l) Setting the alarm duration for the protection function

If you selected the 2 function (= block with alarm) in 8. j), you can set the alarm duration as outlined below (1 - 3 minutes, default setting: 1 minute).

Proceed as follows:

- Start programming mode as outlined in 8. a) so that the LED flashes red.
- Enter the programming code 5 to set the alarm duration. The LED lights up yellow.
- Enter the desired time for the alarm duration. Possible is 1 ..... 3 (= 1 - 3 minutes).
- Exit setting mode with the # button. The LED flashes red again. You can now carry out further programming or exit programming mode with the * button.

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

5 2 #

m)Teaching in visitor transponders

The access system can store up to 10 different visitor transponders. Memory numbers 990 - 999 are provided for these transponders.

For each of the visitor transponders, you can program the number of access attempts (1 - 10 attempts can be set) after which the transponder will become invalid. For example, you can program a visitor transponder in such a way that it only allows access once. The visitor transponder then becomes invalid.

→ Once the number of access attempts programmed for the visitor transponder has been used, the access system automatically deletes the transponder from the memory. The memory number is then free for programming another visitor transponder.

For information on deleting the visitor transponder prematurely (for example, if the complete number of access attempts was not used), see 8. e).

We recommend that you create a table and fill in all access data, including visitor name, number of access attempts, memory number, transponder number. For visitor transponders, you should also use transponders with a different colour or shape.

Proceed as follows:

- Start programming mode as outlined in 8. a) so that the LED flashes red.
- Enter the programming code 8 to teach in visitor transponders. The LED lights up yellow.
- Enter the number of times the visitor transponder may be used (0 ..... 9, where ‘0’ stands for 10x use).

  Example 1: 2 = the visitor can use the transponder 2x, it then becomes invalid

  Example 2: 0 = the visitor can use the transponder 10x, it then becomes invalid
- Confirm the number with the # button.
- Enter the memory number (990 ..... 999) to which the visitor transponder is to be stored.

  Example: 9 9 5 = Store the transponder to memory 995
- Confirm the memory number with the # button.

→ If the memory number has already been assigned, the access system emits 3 quick beeps and the LED flashes red. It is, therefore, not possible to overwrite a memory. Start by deleting the respective memory (see 8. e) before another visitor transponder can be stored there.

- 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 stored.

→ If the transponder has already been taught in, the access system emits 3 quick beeps and the LED flashes red. The same transponder cannot be taught in more than once.

- If you wish to teach in another visitor transponder, start by entering the number of access attempts.
- Exit teach-in mode with the # button. The LED flashes red again. You can now carry out further programming or exit programming mode with the * button.

n) Resetting all settings to the default settings; teaching in a new master transponder

If you wish to reprogram the access system, you can reset the access system to the default settings. During the reset process, it is also possible to teach in a master transponder and a master fingerprint, if desired.

→ The transponder labelled with ‘master card’ can be used as the master transponder or any other suitable transponder (125 kHz type).

Only one master transponder can be taught in.

The stored user/visitor transponders and user fingerprints are not deleted when resetting to the default settings. If you wish to delete all transponders and fingerprints, see 8. h).

It is also possible for no master transponder to be taught in (e.g. if you wish to teach in/delete the user transponders exclusively via programming mode and not via the master transponder for security reasons).

1) Reset of the access system + teach-in of master transponder + master fingerprint

- De-energise the access system and wait for the LED to go out.
- Press the door opener button and hold it down.
- Reconnect the access system to the voltage/power supply. The access system emits two beeps. Now release the door opener button.
- The access system emits a beep and the LED lights up yellow.
- Hold the transponder to be taught in as a master transponder in front of the RFID sensor. If the transponder is recognised, the access system emits a beep and the transponder is stored as a master transponder.

→ If the transponder used has already been taught in as a user transponder, it cannot be used as a master transponder. The access system emits 3 quick beeps and the LED flashes red.

- To teach in the master fingerprint, touch the fingerprint sensor 3 times in succession with the same finger. An LED ring around the sensor lights up blue when the sensor is touched. The LED ring lights up green and a short beep is emitted if the fingerprint is recognised correctly. After the third correct reading, the access system emits a longer beep and the fingerprint is stored.

→ If the fingerprint cannot be read correctly, 3 beeps are emitted and the LED ring flashes red. The same happens if you try to read in a stored user fingerprint as a master fingerprint.

- The LED lights up red, the access system is in standby mode. All the settings are reset to the default settings

2) Reset of the access system without teaching in a master transponder

→ If a master fingerprint is stored, it is retained and is not deleted.

- De-energise the access system and wait for the LED to go out.
- Press the door opener button and hold it down.
- Reconnect the access system to the voltage/power supply. The access system emits two beeps.
- Wait for around 5 seconds, keep the door opener button pressed and do not release it.
- The access system emits a beep and the LED lights up red.
- Now release the door opener button; the access system is now in standby mode again. All settings have been reset to the default settings; however, there is no master transponder for teach-in/deletion of user transponders.

Table for default settings:

Function	See chapter	Default setting
Master code	8. b)	123456
Access mode	8. i)	Transponder or fingerprint
Changeover contact activation time	8. j)	5 seconds
Protection against incorrect entries	8. k)	switched off
Alarm duration for protection function	8. l)	1 minute

10. Operation

a) Getting started

Power on the access system once it has been connected and installed. After switching on the operating voltage, the access system emits a beep and the LED lights up red continuously (standby).

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

> If the access system continuously emits beeps and the LED flashes quickly, the brightness sensor on the rear has activated the sabotage protection; operation is not possible.
>
> Disconnect the access system from the operating voltage immediately in this case. Ensure that the brightness sensor is in the dark after installation.
>
> If you wish to commission the access system for testing purposes before mounting, cover the brightness sensor on the rear, e.g. use a piece of opaque adhesive tape (if necessary, briefly disconnect the access system from the operating voltage to reset the sabotage protection).

You should take the following steps:

- Create a table and enter all settings and user/transponder numbers.
- Put the IR remote control into operation (remove the protective strip from the battery compartment or insert the battery).
- Think of a master code (consisting of 6 digits) and program it (see 8. b). The default master code is 123456 (or after resetting the access system).
- The supplied master transponder (e.g. labelled with ‘master card’) is only used for the quick storage or deletion of user transponders (or user fingerprints). All other programming must be carried out via the IR remote control.
- If you do not wish to have a master transponder for security reasons, for example, the access system can be reset accordingly, see 8. n). In that case, the teach-in or deletion of user transponders is only possible via the IR remote control (or via a master fingerprint, if stored).
- If desired, teach in a master fingerprint, see 8. c).
- Teach in the user transponders to the access system, see 8. d).
- Teach in the user fingerprints to the access system, see 8. f).
- Select the access mode, see 8. i).
- Program the changeover contact activation time (see 8. j) to be used e.g. for switching a door lock (the default setting is 5 seconds).
- Switch on protection against incorrect entries (if desired), see 8. k) and 8. l).
- Now, check whether the door lock can be opened with the stored user transponders or user fingerprints.

b) Access using a valid user transponder/fingerprint

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

→ If toggle mode has been programmed (see 8. j), each valid user transponder or user fingerprint switches the changeover contact permanently 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.

→ If toggle mode has been programmed (see 8. j), each time the door opener button is pressed, the changeover contact switches permanently to the other position.

11. Troubleshooting

Preprogrammed settings are not affected by a power cut to the access system. However, the access system will be non-operational during a power cut.

→ For security reasons, we recommend that you use an uninterruptible power supply for the access system (as in case of an alarm system), depending on the intended use.

After switching on the operating voltage at initial start-up, the access system emits continuous beeps and the LED flashes red

- The brightness sensor on the rear of the access system has activated the sabotage protection; operation is not possible. Disconnect the access system from the operating voltage immediately in this case. Ensure that the brightness sensor is in the dark after installation.
- If you wish to commission the access system for testing purposes before mounting, cover the brightness sensor on the rear, e.g. use a piece of opaque adhesive tape (if necessary, briefly disconnect the access system from the operating voltage to reset the sabotage protection).

The IR remote control does not work

- Point the small LED at one end of the IR remote control at roughly the position of the LED on the access system. The IR receiver LED is located directly adjacent to it.
- The distance between the IR remote control and the access system must not exceed 1 m.
- Sunlight on the front of the access system (or other IR light, e.g. from an IR spotlight for a surveillance camera) will interfere with its function. Reduce the distance between the IR remote control and the access system.
- The battery of the IR remote control is low or depleted, replace the battery with a new one. Dispose of batteries with respect to environmental protection; see ‘Disposal’.
- The battery has been inserted incorrectly. Ensure the correct polarity (the positive terminal/+ of the battery must point towards the bottom of the IR remote control).

The door opener doesn't work

- The changeover contact is potential-free. This means that you must use the appropriate external wiring because the access system does not supply voltage/power to the door opener.
- If the door opener has corresponding polarity markings (positive/+ and negative/-), ensure that it is correctly connected to the access system and the voltage/power supply.
- Check the polarity of the protective diode connected to the door opener.
- The transponder or fingerprint has not been taught in.
- The changeover contact cannot be activated with the master transponder or master fingerprint.
- 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

- Ensure to hold only one transponder in front of the RFID, (see Section 6, point 3).
- The distance between the transponder and the access system should not exceed 3 cm.
- 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).

Teaching in a new user transponder does not work

- Ensure to hold only one transponder in front of the RFID, (see Section 6, point 3).
- The distance between the transponder and the access system should not exceed 3 cm.
- Only EM transponders with a frequency of 125 kHz can be used.
- The memory is already occupied. Use another memory or clear the existing one before teaching in another transponder to the same memory.
- If a MIFARE® chip card reader is connected to the Wiegand connection, it must be used to teach in new transponders.
- If a card reader for 125 kHz transponders is connected to the Wiegand connection, the teach-in process should be possible both via the access system and via the external card reader. For test purposes, use the external card reader.

Teach-in of user fingerprints does not work or does not work properly

- If required, use another finger to test it. The fingerprint sensor must detect enough papillary strips for the fingerprint to be valid.
- Place your finger in the centre and over the entire surface. The detected area of the skin surface must have a minimum size for it to be valid. It does not matter which way around the finger is oriented. It is therefore possible to teach in the finger ‘vertically’ at any time and later place it on the surface rotated by 90° to gain access.
- Do not wear gloves.

The changeover contact is permanently active (and does not switch back)

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

The changeover contact cannot be activated despite a correctly taught-in user transponder or user fingerprint

- Check the access mode setting, see 8. i).

After resetting to the default settings, the user transponders, user fingerprints and the master fingerprint are not deleted

- This is normal. If you wish to delete all memories, proceed as outlined in 8. h).

The visitor transponder does not work

- A visitor transponder can only be used for a certain number of access attempts (1 - 10 are programmable, see 8. m). The visitor transponder is then automatically invalid and is also removed from the memory of the access system.

  In order for the same transponder to become valid again so that it can be given to the next visitor, it must be taught in again with a certain number of access attempts, see 8. m).

The Wiegand connection does not work

- Ensure that the two data lines D0 and D1 are not swapped – D0 must always be connected to D0 and D1 to D1. The remaining wiring can be carried out as outlined in 7. b). Always observe the operating instructions for the external card reader.
- Card readers for 125 kHz transponders as well as card readers with MIFARE® chip card technology (13.561 MHz) are permitted.

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 disposed of in the 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.

Before disposal, the exposed contacts of batteries must be fully covered with a piece of adhesive tape to prevent short-circuits. Even if batteries are depleted, the remaining energy can become dangerous in the event of a short-circuit (bursting, severe heating, fire, explosion).

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’s item number in the search field; 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
Current consumption	standby < 30 mA
Frequency range	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 detection)
Memory for transponders	900 (of which 890 user transponders and 10 visitor transponders)
Memory for fingerprints	100 (of which 99 user fingerprints and 1 master fingerprint)
Mounting location	indoors/outdoors
Protection class	IP66
Ambient conditions	temperature -25 °C to +60 °C
Cable length	approx. 25 cm
Dimensions	115 x 70 x 25 mm (H x W x D)
Weight	approx. 190 g

b) IR remote control

Operating voltage	3 V/DC via 1x battery of type CR2025 (lithium button cell)
IR range	max. approx. 1 m

GB This is a publication by Conrad Electronic SE, Klaus-Conrad-Str. 1, D-92240 Hirschau (www.conrad.com).