

sygonix®

Ⓒ Operating Instructions
RFID code lock
Item no. 2380478

CE

Table of contents



	Page
1. Introduction	4
2. Explanation of symbols	4
3. Intended use	5
4. Delivery content	5
5. Safety information	6
6. Controls and connections	7
7. Installation and connection	8
a) Installation	8
b) Connecting to conventional voltage/power supply	9
c) Connecting to alarm system	9
d) Wiegand interface	10
8. Operation	11
9. Programming	12
a) Enabling/disabling programming mode	13
b) Changing the master code	13
c) Pairing user transponders	14
d) Deleting the user transponder	16
e) Saving a user code	17
f) Deleting the user code	19
g) Clearing all memory cells	19
h) Selecting the access mode	20
i) Saving a user PIN	21
j) Changing a user PIN	22
k) Setting the changeover contact activation time	23
l) Enabling or disabling protection against incorrect entries	24
m) Setting the alarm time for protection function	24
n) visitor transponder or visitor code	25
o) Resetting all settings to factory defaults; pairing a new master transponder	27

	Page
10. Operation	29
a) Getting started	29
b) Accessing via valid user transponder	30
c) Accessing via valid user code	30
d) Access via valid user transponder and user PIN	30
e) Accessing via door opener button	30
11. Troubleshooting	31
12. Cleaning and maintenance	33
13. Disposal	33
14. Declaration of Conformity (DOC)	33
15. Technical data	34

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. The product enables to save up to 1000 users with different transponders and user codes.

A valid access attempt activates a potential-free relay changeover contact (see contact rating under "Technical data"). In this case, for example, a door opener or an alarm system can be triggered.

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.

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

- Code lock
- 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)
- Quick start
- 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!



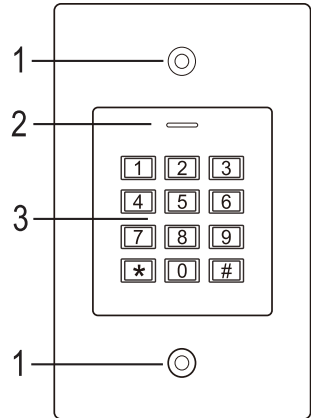
We shall not be liable for damage to property or personal injury caused by incorrect handling or failure to observe the safety information! Such cases will void the warranty/guarantee.

- 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 code lock is suitable for indoor and outdoor installation and use (IP66).
- 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.

6. Controls and connections

- 1 Opening for wall mounting
- 2 LED indicator
- 3 Keypad with an integrated RFID sensor behind it

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



Connecting cable:

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 pre-installed depending on the surface and installation position, and the code lock should then be screwed tight.

Depending on the surface, use suitable screws and, if necessary, dowels.

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/+).

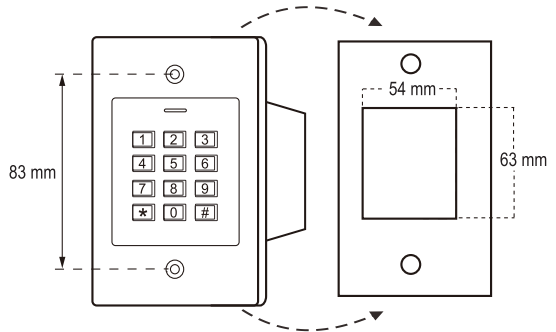


Caution!

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

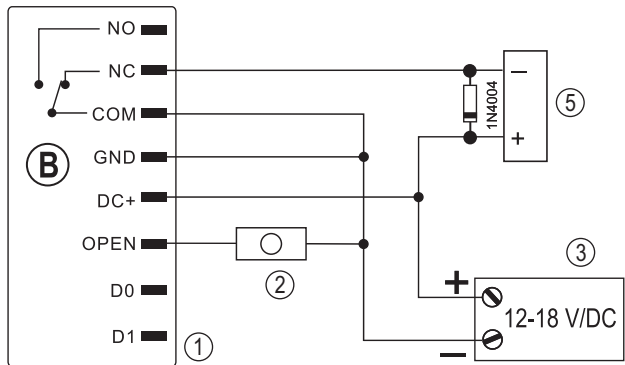
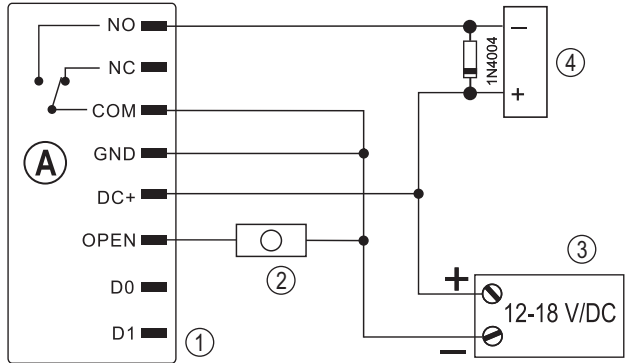
When a conventional power supply unit should be used, observe the following figures with the wiring diagram.

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 code lock from voltage surges.

- 1 Code lock
- 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 code lock relay switches when a valid transponder is recognised. An alarm system can thus be enabled or disabled.

d) Wiegand interface

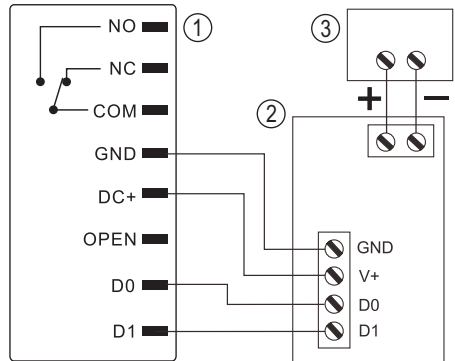
There are two application options for the Wiegand interface of the code lock:

1) The code lock is used as an external card reader

The code lock 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 Code lock
- 2 Wiegand controller
- 3 Power adapter



The code lock has the operating voltage of 12 - 18 V/DC. If the Wiegand controller does not support this operating voltage, the code lock 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 code lock

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

→ Card readers for 125 kHz transponders as well as card readers with MIFARE® chip 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 code lock and the card reader (should you face any problems, use only the external card reader for pairing).

Ensure that the two data lines D0 and D1 are not swapped; D0 must always be connected to D0 and D1 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

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



If the code lock 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 code lock from the power supply. Ensure that the brightness sensor is in the dark after installation.

If you want to briefly check the code lock 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 code lock 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, user code etc., to know who can access the system. These data also enable easy deletion of individual users or user transponders.

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

Programming is carried out using the keypad.

The RFID sensor is not visible as it is hidden right behind the keypad. The transponder must be held close enough to the code lock (no farther than 3 cm) to be recognised correctly.

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. o).

The user codes and the master code can consist of 4-6 digits.

In addition, the code lock enables to save up to 10 visitor transponders or visitor codes. Visitor transponders and visitor codes can have a pre-programmed number of access attempts (1 to 10 attempts), after which they will become invalid. For example, you can programme a visitor transponder in such a way that it only allows access once.

There are a total of 1000 memory cells:

- Memory cell number 0 - 989: user transponders or user codes
- Memory cell number 990 - 999: visitor transponders or visitor codes

The code lock has a special feature, a special access mode (see section 8. h), which requires a separate user PIN in addition to the user transponder. In this case, access is only granted after recognition of a valid user transponder and entering and confirming the user PIN. This access mode is especially secure because it requires both a physical object (transponder) and the user PIN.

a) Enabling/disabling programming mode

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

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

Each time you press a button, the code lock emits a short confirmation beep.

- The LED then flashes red (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 code lock is in standby mode.

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

b) Changing the master code

All programming operations of the code lock, with the exception of saving/changing user PINs, require 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 code lock is in normal operation.

→ The master code can consist of 4 to 6 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

The code lock has a total of 990 memory cells in which user transponders can be paired or, alternatively, user codes can be stored. You can use both the keypad and the master transponder for pairing.

→ We recommend that you create a table and fill in all access data, such as user name, memory cell number, user code, transponder number, etc. This is how you can keep track of who accessed the code lock 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 keypad

The keypad enables several pairing options:

- Quick pairing of a user transponder in the next free memory cell
- Pairing and saving a user transponder in a specific memory cell

Automatically save user transponders 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, if the transponder is lost or faulty, it cannot be deleted as the assignment between the user transponder and memory cell is unknown. In that case, all memory cells would need to be cleared.

In addition, further attempts to store user transponders or user codes in a certain memory cell at a later time can cause error messages, e.g., when the memory cell is already occupied by a user transponder.

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

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

- If desired, other transponders can be paired by holding them separately in front of the RFID sensor.
- Exit the pairing mode with the (#) button. 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 (via the memory cell number) even when it is defective or lost.

This procedure is also advisable if you are planning to use the code lock with user transponders and user codes.

- Enable the programming mode as described in section 8. a); the LED starts to flash red.
- Enter the programming code **[1]** to pair user transponders. The yellow LED will then light up.
- Enter the memory cell number (**[0]** **[9]** **[8]** **[9]**) 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 code lock 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 code lock emits a short beep and the transponder is saved.

→ When transponder pairing is complete, the code lock 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.

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, if the transponder is lost or faulty, it cannot be deleted as the assignment between the user transponder and memory cell is unknown. In that case, all memory cells would need to be cleared.

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

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

- If desired, other transponders can be paired by holding them separately in front of the RFID sensor.
- Hold the master transponder once in front of the RFID sensor to finish the pairing process. The code lock will emit a short beep, the red LED will light up and the code lock will go back to standby mode.

d) Deleting the user transponder

The respective user will no longer have access once the corresponding user transponder has been deleted. Deletion is possible either via the user transponder or the memory cell number.

User transponders can also be deleted with the master transponder.

→ When the user transponder is deleted, the corresponding user PIN, if any, will be deleted as well.

1) Deleting a user transponder with the keypad

- Enable the programming mode as described in section 8. a); the LED starts to flash red.
- Enter the programming code [2] to start deletion mode. The yellow LED will then light up.
- There are 2 different ways to delete:
 - Hold the user transponder close in front of the RFID sensor. Once the transponder is recognised, the code lock emits a short beep and the transponder is deleted.
 - Enter the memory cell number of the user transponder ([0] [9] [8] [9]), 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 code lock will emit three brief beeps and the LED will flash red.

- Exit the deletion mode with the [#] button. 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 code lock 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 code lock emits a short beep and the user transponder is deleted.

→ When the user transponder is unknown and/or already deleted, the code lock emits three brief beeps and the LED flashes red.

- Other user transponders can be deleted by following the instructions above.
- Hold the master transponder once in front of the RFID sensor to finish the deletion process. The red LED will then light up and the code lock will go back to standby mode.

e) Saving a user code

The code lock has a total of 990 memory cells in which user codes can be stored or, alternatively, user transponders can be paired.

→ We recommend that you create a table and fill in all access data, such as user name, memory cell number, user code, etc. This is how you can keep track of who accessed the code lock and used a specific memory cell.

With these data it is also very easy to delete a single user.

A user code can be saved in two different ways:

- Quick saving of a user code in the next free memory cell
- Saving of a user code in a specific memory cell

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

→ This saving procedure enables quick and easy saving of new user codes in the next free memory cell. Since the memory cell number in which the user code is stored is unknown, deletion is only possible with the user code and not via the memory cell number.

In addition, further attempts to store user transponders or user codes in a certain memory cell at a later time can cause error messages, e.g., when the memory cell is already occupied by a user code.

- Enable the programming mode as described in section 8. a); the LED starts to flash red.
- Enter the programming code [1] to save user codes. The yellow LED will then light up.
- Enter the user code (consisting of 4-6 digits, [0][0][0][1] [9][9][9][9][9] is possible).

→ The code "1234" cannot be used as it has a special function (it is used for saving a user PIN, as described in section 8. i).

- Press the [#] button to confirm your entry.

→ When the user code already exists, the code lock emits three brief beeps and the LED flashes red. The same user code cannot be saved more than once.

- If necessary, you can also save other user codes (enter user code and confirm with the [#] button).
- Press the [#] button to exit the storage mode. The LED flashes red again, which means that you can continue programming or exit the programming mode with the [*] button.

User code is assigned to a specific memory cell:

→ Although this saving procedure takes more time, it enables to delete a specific user code (via the memory cell number) even when it is lost.

This procedure is also advisable if you are planning to use the code lock with user transponders and user codes.

- Enable the programming mode as described in section 8. a); the LED starts to flash red.
- Enter the programming code (1) to save user codes. The yellow LED will then light up.
- Enter the memory cell number (0 to 9 8 9) in which the user code is to be saved; you do not need to enter leading zeros.
- Press the (#) button to confirm the memory cell number.

→ When the memory cell number is already occupied, the code lock 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 a user code in it.

- Enter the user code (consisting of 4-6 digits, 0 0 0 1 9 9 9 9 9 is possible).

→ The code "1234" cannot be used as it has a special function (it is used for saving a user PIN, as described in section 8. i).

- Press the (#) button to confirm your entry.

→ When the user code already exists, the code lock emits three brief beeps and the LED flashes red. The same user code cannot be saved more than once.

- You can now save other user codes, if desired.
- Press the (#) button to exit the storage mode. The LED flashes red again, which means that you can continue programming or exit the programming mode with the (*) button.

f) Deleting the user code

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

Proceed as follows:

- Enable the programming mode as described in section 8. a); the LED starts to flash red.
- Enter the programming code **2** to start deletion mode. The yellow LED will then light up.
- There are 2 different ways to delete:
 - Enter the user code and press the **#** button to confirm.
 - Enter the memory cell number of the user code (**0** **9 8 9**), without leading zeros, e.g. **2 0**) and press the **#** button to confirm.

Other user codes can be deleted as described here above.

→ When the system does not recognise the user code and, hence, it cannot be deleted (or the entered memory cell number is already empty), the code lock will emit three 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.

g) Clearing all memory cells

This function serves to clear all 1000 memory cells (990 memory cells for user transponders/user codes and 10 memory cells for visitor transponders/visitor codes). In addition, all user transponders are deleted with their respective user PINs, if any.

Proceed as follows:

- Enable the programming mode as described in section 8. a); the LED starts to flash red.
- Enter the programming code **2** to start deletion mode. The yellow LED will then light up.
- Enter: **0 0 0 0**
- Press the **#** button to confirm the deletion. The LED flashes red again, which means that you can continue programming or exit the programming mode with the ***** button.

Example for deleting all 1000 memory cells (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 # ***

h) Selecting the access mode

The changeover contact can be activated in three different ways. The access mode can be changed for this purpose.

- **Access with user transponder or user code (default setting)**

Holding a valid user transponder in front of the RFID sensor activates the changeover contact. Alternatively, enter the stored user code and press the [#] button to confirm.

This access mode is less secure since unauthorised individuals can gain access by trying out different combinations of user codes or by chance.

- **Access with user transponder and respective user PIN**

To gain access, you must first hold a valid user transponder in front of the RFID sensor. The LED will then flash red. Then enter the user PIN (4-6 digits) assigned to the transponder and press the [#] button to confirm. Only after these actions the changeover contact is activated. This access mode is especially secure because it requires both a physical object (transponder) and the user PIN.

→ The user PIN has nothing to do with the user code. A separate user PIN must be assigned to each user transponder and it can be changed by users themselves since no master code is required for an access.

- **Access with user transponder only**

Holding a valid user transponder in front of the RFID sensor activates the changeover contact.

This access mode is less secure since a user transponder which has been found or stolen can be used for an access.

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 change the access mode. The yellow LED will then light up.
- Select the desired access mode:
 - [0] = Access with user transponder or user code (default setting)
 - [1] = Access with user transponder and respective user PIN (a separate user PIN must be assigned to each user transponder, as described in section 8. i)
 - [2] = Access with user transponder only
- Exit the setting mode with the [#] button. The LED flashes red again, which means that you can continue programming or exit the programming mode with the [*] button.

i) Saving a user PIN

When the access mode has been set to **1** as described in section 8. h), each transponder must be assigned an additional user PIN.

This access mode provides activation of the changeover contact only after recognition of a valid transponder and entering a valid user PIN and confirming with the **#** button.

→ It should be noted that the programming mode is not required to save a user PIN. The point is that a user can save their own secret user PIN themselves without having to know the master code.

Proceed as follows:

- Press the ***** key. The red LED flashes.
- Hold the transponder to which you want to assign a user PIN close in front of the RFID sensor. When the transponder is recognised, the code lock emits a beep.
- Enter the code **1 2 3 4**.
- Press the **#** button to confirm your entry.
- Enter the user PIN (consisting of 4-6 digits, **0 0 0 1** **9 9 9 9 9** is possible).

→ The code "1234" cannot be used as it has a special function (it is used for saving a user PIN).

- Press the **#** button to confirm your entry.
- Enter the user PIN once again for security reasons.
- After confirming your entry with the **#** button, the code lock goes back to standby mode.

j) Changing a user PIN

A user PIN can be changed in two different ways:

- User PIN can be changed by means of the user transponder (this is a perfect option for users since they do not normally know the memory cell number)
- User PIN can be changed by means of the memory cell number (this option is to be used when the user transponder is unavailable)

→ It should be noted that the programming mode is not required to change a user PIN. The point is that a user can change their own secret user PIN themselves without having to know the master code.

1) Changing a user PIN with the user transponder

- Press the **[*]** key. The red LED flashes.
- Hold the transponder for which you want to change the user PIN close in front of the RFID sensor. When the transponder is recognised, the code lock emits a beep.
- Enter the old user PIN.
- Press the **[#]** button to confirm your entry.
- Enter the new user PIN (consisting of 4-6 digits, **[0][0][0][1]** **[9][9][9][9][9]** is possible).

→ The code "1234" cannot be used as it has a special function (it is used for saving a user PIN).

- Press the **[#]** button to confirm your entry.
- Enter the new user PIN once again for security reasons.
- After confirming your entry with the **[#]** button, the code lock goes back to standby mode.

2) Changing a user PIN with the memory cell number

- Press the **[*]** key. The red LED flashes.
- Enter the memory cell number (**[0]** **[9][8][9]**) the user PIN of which is to be changed; you do not need to enter leading zeros.
- Press the **[#]** button to confirm your entry.
- Enter the old user PIN.
- Press the **[#]** button to confirm your entry.
- Enter the new user PIN (consisting of 4-6 digits, **[0][0][0][1]** **[9][9][9][9][9]** is possible).

→ The code "1234" cannot be used as it has a special function (it is used for saving a user PIN).

- Press the **[#]** button to confirm your entry.
- Enter the new user PIN once again for security reasons.
- After confirming your entry with the **[#]** button, the code lock goes back to standby mode.

k) 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 **4** to set the activation time. The yellow LED will then light up.
- Enter the desired changeover contact activation time. Possible is **1** **99** (1 to 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 an 8-second activation time (programming mode must be active, see section 8. a):

4 **8** **#**

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

4 **0** **#**

l) Enabling or disabling protection against incorrect entries

This function enables to set whether the code lock should be blocked in case of 10 or more incorrect entries in a row (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 **[6]** 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 user code; the master transponder is also inoperative)
 - [2]** = Block with alarm for 1 to 3 minutes (for setting the alarm time, see section 8. m); alarm can be disabled in advance with a valid user transponder, a user code or 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 code lock 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):

[6] **[1]** **[#]**

m) Setting the alarm time for protection function

After enabling the function **[2]** (block with alarm) as described in section 8. l), 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. Possible is **[1]** **[3]** (1 to 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]** **[#]**

n) visitor transponder or visitor code

The code lock can store up to 10 different visitor transponders or visitor codes. Memory cell numbers 990 - 999 are provided for them.

Visitor transponders or visitor codes can have a pre-programmed number of access attempts (1 to 10 attempts), after which they will become invalid. For example, you can programme a visitor transponder in such a way that it only allows access once. The visitor transponder then becomes invalid.

→ After the preprogrammed number of access attempts has been used, the code lock automatically deletes the visitor transponder or visitor code from the memory. The cleared memory cell number is now available for programming another visitor transponder or visitor code.

The visitor transponder or visitor code can also be deleted in advance (for example, when not all preprogrammed access attempts have been used), as described in paragraph 3 below.

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

1) Pairing the visitor transponder

- Enable the programming mode as described in section 8. a); the LED starts to flash red.
- Enter the programming code **[8]**. The yellow LED will then light up.
- Enter the number of times the visitor transponder may be used (**[0]** **[9]**, where "0" stands for 10 uses).

Example 1: **[2]** = visitor can use the transponder two times, after which it becomes invalid

Example 2: **[0]** = visitor can use the transponder ten times, after which it becomes invalid

- Confirm the number with the **[#]** button.
- Enter the memory cell number (**[9]** **[9]** **[0]** **[9]** **[9]** **[9]**) in which the visitor transponder is to be stored.
Example: **[9]** **[9]** **[5]** = Save the transponder to memory cell 995
- Press the **[#]** button to confirm the memory cell number.

→ When the memory cell number is already occupied, the code lock 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 visitor transponder in it.

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

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

- If you wish to pair another visitor transponder, first enter the number of access attempts.
- 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) Saving the visitor code

- Enable the programming mode as described in section 8. a); the LED starts to flash red.
- Enter the programming code **[8]**. The yellow LED will then light up.
- Enter the number of times the visitor code may be used (**[0]** **[9]**, where "0" stands for 10 uses).
Example 1: **[2]** = visitor can use the visitor code two times, after which it becomes invalid
Example 2: **[0]** = visitor can use the visitor code ten times, after which it becomes invalid
- Confirm the number with the **[#]** button.
- Enter the memory cell number (990 - 999) in which the visitor code is to be stored.
Example: **[9][9][5]** = Save visitor code in memory cell 995
- Press the **[#]** button to confirm the memory cell number.
→ When the memory cell number is already occupied, the code lock 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 visitor code in it.
- Enter the visitor code (consisting of 4-6 digits, **[0][0][0][1]** **[9][9][9][9][9]** is possible).
→ The code "1234" cannot be used as it has a special function (it is used for changing a user code of the user transponder).
- Press the **[#]** button to confirm your entry.
→ When the visitor code already exists, the code lock emits three brief beeps and the LED flashes red. The same visitor code cannot be saved more than once.
- Before saving another visitor code, first enter the number of access attempts.
- Press the **[#]** button to exit the storage mode. The LED flashes red again, which means that you can continue programming or exit the programming mode with the **[*]** button.

3) Deleting the visitor transponder or visitor code

After the preprogrammed number of access attempts has been used, the code lock automatically deletes the visitor transponder or visitor code from the memory. The cleared memory cell number is now available for programming another visitor transponder or visitor code.

The visitor transponder or visitor code can also be deleted in advance (for example, when not all preprogrammed access attempts have been used).

Proceed as follows:

- Enable the programming mode as described in section 8. a); the LED starts to flash red.
- Enter the programming code **[2]** to start deletion mode. The yellow LED will then light up.
- Enter the memory cell number (**[9] [9] [0] [9] [9] [9]**) of the visitor transponder or visitor code that you want to clear and press the **[#]** button to confirm.

Other memory cells can be cleared as described here above.

→ When the memory cell is already empty, the code lock emits three brief beeps and the LED flashes 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.

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

The code lock can be reprogrammed by resetting it to factory defaults. The reset procedure also allows pairing of master transponders, 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 transponders, 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 code lock and pairing master transponders

- De-energise the code lock and wait for the LED to go off.
 - Keep the  button pressed.
 - Reconnect the code lock to the voltage/power supply. The code lock will emit two beeps. Now release the  button.
 - The LED indicator lights up yellow.
 - Hold the transponder to be paired as a master transponder in front of the RFID sensor. Once the transponder is recognised, the code lock 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 code lock will emit three brief beeps and the LED will flash red.
- When the red LED lights up, the code lock is in standby mode. All settings have been reset to factory defaults.

2) Resetting the code lock without pairing master transponders




- De-energise the code lock and wait for the LED to go off.
- Keep the  button pressed.
- Reconnect the code lock to the voltage/power supply. The code lock will emit two beeps.
- Wait about 10 seconds, keep the  button pressed and do not release it.
- The code lock will emit a beep and the red LED will light up.
- You can now release the  button for the code lock to go back to standby mode. All settings have been reset to factory defaults; however, there is no master transponder for pairing/deletion of user transponders.

Table with default settings:

Function	See chapter	Factory setting
Master code	8. b)	123456
Access mode	8. h)	Transponder or user code
Changeover contact activation time	8. k)	5 seconds
Protection against incorrect entries	8. l)	switched off
Alarm time for protection function	8. m)	1 minute

10. Operation

a) Getting started

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

The code lock is now ready for use and can be programmed.



If the code lock 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 code lock 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 code lock 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 code lock 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, user codes, etc.
- Think of a master code (consisting of 6 digits) and programme it (see 8. b). The default master code is "123456" (the same applies after resetting the code lock 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 keypad 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 code lock accordingly, as described in section 8. o). In this case, user transponders can only be paired or deleted via the keypad.
- Select the desired access mode (see section 8. h).
- Pair the user transponders with the code lock (see section 8. c) and/or save user codes (see section 8. e). In the access mode **1** entered by means of the user transponder and user PIN, as described in section 8. h), you can programme a separate user PIN for each user transponder.
- Set the changeover contact activation time (see section 8. k) to be used e.g. for switching a door lock (default setting is 5 seconds).
- You can now check whether the door lock can be opened with the stored user transponders (or whether the user transponder and user PIN are required for the access mode **1**).
- You can programme other functions, for example, enable protection against incorrect entries (section 8. l/m)

b) Accessing via valid user transponder

- Access with a user transponder only is possible if setting **0** or **2** has been selected for access mode (see section 8. h).

Make sure you hold the user transponder in front of the code lock (no farther than 3 cm). Once the code lock has recognised the transponder, the changeover contact and door opener are activated for a preset time and the green LED lights up. Once the time has elapsed, the LED lights up red again (standby).

- After enabling the toggle mode (as described in section 8. k), each valid access attempt permanently switches the changeover contact to the other position.

c) Accessing via valid user code

- Access with a user code only is possible if setting **0** has been selected for access mode (see section 8. h).

Enter the user code and press the **#** button to confirm. After the correct entry, 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. k), each valid access attempt permanently switches the changeover contact to the other position.

d) Access via valid user transponder and user PIN

- Access via a combination of user transponder and user PIN is possible if setting **1** has been selected for access mode (see section 8. h).

Hold the user transponder in front of the code lock (no farther than 3 cm). When the code lock recognises the transponder, the LED flashes red. Now enter the corresponding user PIN within 10 seconds and then press the **#** button to confirm. After the correct entry, 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. k), each valid access attempt permanently switches the changeover contact to the other position.

e) 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

Preprogrammed settings are not affected by a power cut. However, the code lock will be non-operational during a power cut.

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

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

- The brightness sensor on the back of the code lock has activated tamper protection and locked all functions. If this is the case, disconnect the code lock 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 code lock 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 code lock from the power supply to reset tamper protection.

The door opener doesn't work

- The changeover contact is potential-free. This means that you must use the appropriate external wiring because the code lock does not supply voltage/power to the door opener.
- If the door opener has corresponding polarity markings (plus/+ and minus/-), ensure it is correctly connected to the code lock 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).

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 to the code lock changes the changeover contact switch position.

Resetting to factory defaults does not delete any user transponders, user codes or user PINs

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

Transponder is not recognised

- Make sure you hold one transponder in front of the RFID sensor at a time (see section 6, clause 3).
- The distance between the transponder and the code lock 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).

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).
- The distance between the transponder and the code lock 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 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 code lock and the external card reader. Use an external card reader to check the functionality.

A user code cannot be saved

- The code "1234" cannot be used as it has a special function (it is used for changing a user code of the user transponder).
- The user code already exists.

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.

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



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.

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

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 recognition)
Memory cells	990 user transponders or user codes 10 visitor transponders or visitor codes
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. 209 g

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

All rights including translation reserved. Reproduction by any method, e.g. photocopy, microfilming, or the capture in electronic data processing systems require the prior written approval by the editor. Reprinting, also in part, is prohibited. This publication represent the technical status at the time of printing.

Copyright 2021 by Conrad Electronic SE.