sygonix®

CE

Table of contents

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 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 a triangle indicates that 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 either via suitable transponders or the integrated fingerprint sensor.

If you hold a tuned-in transponder in front of the code lock or place a finger that is stored in the system on the fingerprint sensor, a potential-free changeover contact will be activated (for contact rating, see chapter "Technical data"). This can be used, for example, to trigger a door opener or an alarm system.

The product is designed for operation indoors and outdoors (IP66).

For safety purposes, do not convert 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 instructions carefully and store them in a safe place. If you pass the product on to a third party, please hand over these operating instructions as well.

4. Package contents

- Code lock
- IR remote control with CR2025 battery
- 1x transponder card for adding user transponders
- 1x transponder card for deleting user transponders
- Mounting material (2x screws, 2x dowels)
- 1x L-key
- 3x 1N4004 diodes
- Operating instructions

Up-to-Date Operating Instructions

Download the up-to-date operating instructions at www.conrad.com/downloads or scan the QR code shown. Follow the instructions on the website.

5. Safety instructions

Read the operating instructions and safety information carefully. If you do not follow the safety instructions and information on proper handling in these operating instructions, we assume no liability for any resulting personal injury or damage to property. Such cases will invalidate the warranty/guarantee.

- The unauthorised conversion and/or modification of the product is prohibited for safety and approval reasons.

- The device is not a toy. Keep out of the reach of children and pets.

- The product is designed for operation indoors and outdoors (IP66). However, it must never be used in or under water, as this will destroy it.

- Protect the product from extreme temperatures, impacts, flammable gases, vapours and solvents.

- Never exceed the contact rating for the potential-free changeover contact specified in chapter "Technical data". Never attempt to connect the code lock to a mains voltage, as this may cause a fatal electric shock.

- Please 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.

- Always observe the safety and operating instructions of any other devices which are connected to the product (e.g. door openers and alarm systems).

- Always comply with the accident prevention regulations for electrical equipment when using the product in commercial facilities.

- If it is no longer possible to operate the product safely, take it out of operation and protect it from any accidental use. Safe operation can no longer be guaranteed if the product:

  - is visibly damaged,

  - is no longer working properly,

  - has been stored for extended periods in poor ambient conditions or

  - has been subjected to any serious transport-related stresses.

- 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. Battery safety information

Keep batteries out of the reach of children.

Do not leave batteries lying around in the open; there is a risk of them being swallowed by children or pets. If swallowed, consult a doctor immediately, it could be fatal!

Always ensure that the battery in the IR remote control is inserted with the correct polarity (observe the plus/+ and minus/- symbols).

Batteries must not be short-circuited, opened, taken apart or thrown into a fire. This may cause a fire or explosion!

Never attempt to recharge non-rechargeable batteries, as this may cause an explosion.

Old or depleted batteries may emit chemical liquids that cause damage to the product. Therefore, if the device is not to be used for a long time (e.g. storage), remove the battery from the IR remote control.

Leaking or damaged batteries can lead to caustic burning upon skin contact. Therefore, use suitable protective gloves.

Liquids leaking from batteries are very chemically aggressive. Objects or surfaces coming into contact with these liquids could be severely damaged. Therefore, store batteries in a suitable location.

To dispose of batteries in an environmentally friendly manner, see "Disposal" chapter.

7. Connections and control elements
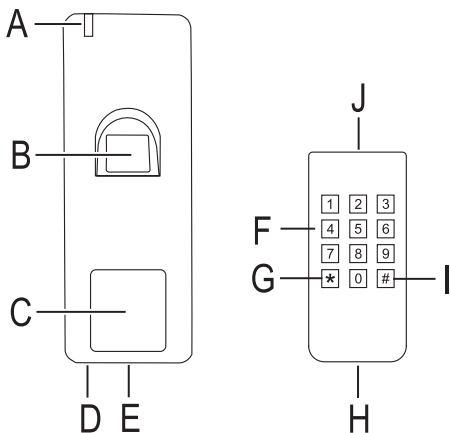
A   Control LED

B   Fingerprint sensor

C   Transponder sensor surface

D   IR receiver

E   Fastening screw

F   Keypad for buttons 0 to 9

G $*$ button

H   Clip for battery compartment

I $\#$ button

J   IR transmission LED

→   The wall mounting bracket and the connection cable are located on the back of the code lock.

Connecting cable:

Colour	Function
Red	12 V/DC
Black	GND
Blue	NO contact of the relay
Purple	COM contact of the relay
Orange	NC contact of the relay
Yellow	Input for door opener button (NO contact / normally open contact)
Green	Wiegand connection, Data 0, D0
White	Wiegand connection, Data 1, D1
Grey	Alarm output (minus/-)
Brown	Input for door sensor (NC contact / normally closed contact)

Connection for operating voltage (cable: red + black)

The power supply (12 V/DC) must be connected here. Pay attention to the correct polarity. The code lock requires a current of max. 150 mA. It also requires power for the alarm output siren (up to 2 A).

Potential-free changeover contact (cable: blue + purple + orange)

The potential-free changeover contact (for contact rating, see "Technical data" chapter) is activated in the event of a successful access attempt (correct transponder card or fingerprint). The switching time can be programmed (1 – 99 seconds). Toggle operation is also possible.

Input for separate door opener button (cable: yellow)

By pressing a button (NO contact, normally open contact), the potential-free changeover contact can be activated. For example, it can be used for manual activation of a door opener. If you need to connect more than one button, connect them in parallel.

Wiegand data cables (cable: green + white)

You can connect to other devices to the Wiegand interface.

Alarm output (cable: grey)

This can be used to control an alarm siren (12 V/DC, max. 2 A).

Input for door sensor (cable: brown)

The code lock uses a door sensor to emit an alarm when the door is opened without a valid access attempt having been made previously using a transponder or fingerprint.

8. Mounting and connection

⚠️ Do not mount or connect the product when it is connected to a power supply.

• Unscrew the screw (see chapter 7, item E) on the bottom of the code lock (an L-key for the special screw is included) and then remove the mounting plate on the back of the code lock.

• Attach the mounting plate to a wall using suitable screws. Depending on the surface, dowels may also be required.

   If necessary, drill a hole for the connecting cables before attaching the mounting plate.
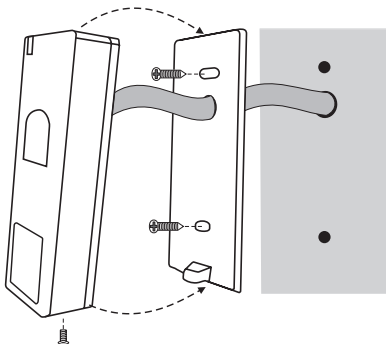
The mounting plate must be mounted so that the screw hole for the fixing screw points downwards.

Ensure that no cables or wires are damaged when drilling holes or tightening screws.

- Wire the connection cables according to the following circuit examples. Ensure that there is suitable insulation (e.g. heat shrink tubing).

- Suitable protective diodes for connecting a door opener are included. They protect the code lock from damage caused by voltage peaks. Pay attention to the correct polarity, see following connection examples (the white ring on the protective diode must point in the direction of the positive terminal/+ when connecting).

Warning!

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/-).

- Attach the code lock to the mounting plate. Ensure that the cables are not pinched. The code lock can be fixed to the mounting plate using the fixing screw on the bottom. Use the included L-key that is suitable for the special screw.

Connection to conventional voltage/power supply:

If a conventional power supply unit with an output voltage of 12 V/DC will be used to operate the code lock, please note the following connection diagram:

With "Fail Secure" door opener:

→ This releases the locking latch only when its operating voltage is applied (common design for front doors).

A "Fail Secure" door opener

B Power adapter

C Code lock

D Door opener button (NO contact, normally open contact)

E Door sensor (NC contact, normally closed contact)

F Protection diode: The protective diode must be connected near the door opener with the correct polarity. This protects the code lock from voltage peaks.

G Alarm siren

With "Fail Safe" door opener:

⟶ The locking latch is only released when the operating voltage is absent (rare type, used, for example, for escape route doors, as the door can be opened in the event of a power failure).

A "Fail Safe" door opener

B Power adapter

C Code lock

D Door opener button (NO contact, normally open contact)

E Door sensor (NC contact, normally closed contact)

F Protection diode: The protective diode must be connected near the door opener with the correct polarity. This protects the code lock from voltage peaks.

G Alarm siren

Connection to a special power supply for access control systems:

Such a power supply can be identified by its connection for the door opener, amongst other things.
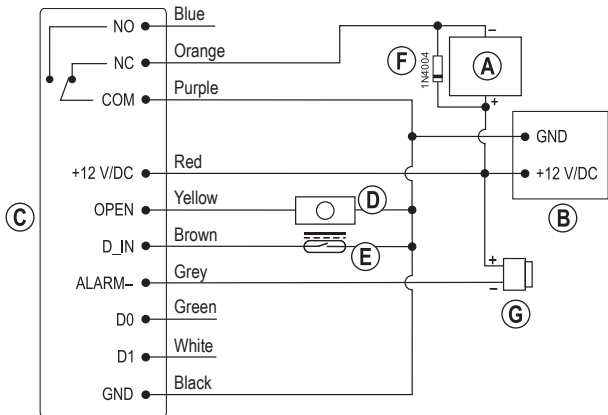
With "Fail Secure" door opener:

→ This releases the locking latch only when its operating voltage is applied (common design for front doors).

A "Fail Secure" door opener

B Special power adapter for access control systems

C Code lock

D Door opener button (NO contact, normally open contact)

E Door sensor (NC contact, normally closed contact)

F Alarm siren

With "Fail Safe" door opener:

→ The locking latch is only released when the operating voltage is absent (rare type, used, for example, for escape route doors, as the door can be opened in the event of a power failure).
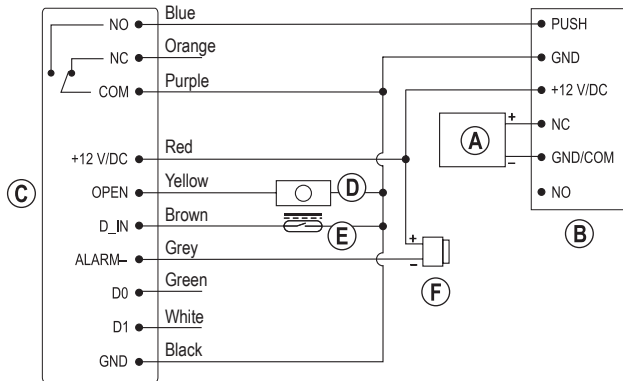
A "Fail Safe" door opener

B Special power adapter for access control systems

C Code lock

D Door opener button (NO contact, normally open contact)

E Door sensor (NC contact, normally closed contact)

F Alarm siren

Circuit diagram with two code locks for double door systems:

For programming, see chapter 12.

⟶ The use of two code locks makes it possible, for example, to control special access systems when accessing a room/area with double doors, of which only one may be opened.

With "Fail Secure" door opener:

⟶ This releases the locking latch only when its operating voltage is applied (common design for front doors).

A   "Fail Secure" door opener

B   Power adapter

C   Code lock

D   Door opener button (NO contact, normally open contact)

E   Door sensor (NC contact, normally closed contact)

F   Protection diode: The protective diode must be connected near the door opener with the correct polarity. This protects the code lock from voltage peaks.

With "Fail Safe" door opener:

⟶ The locking latch is only released when the operating voltage is absent (rare type, used, for example, for escape route doors, as the door can be opened in the event of a power failure).
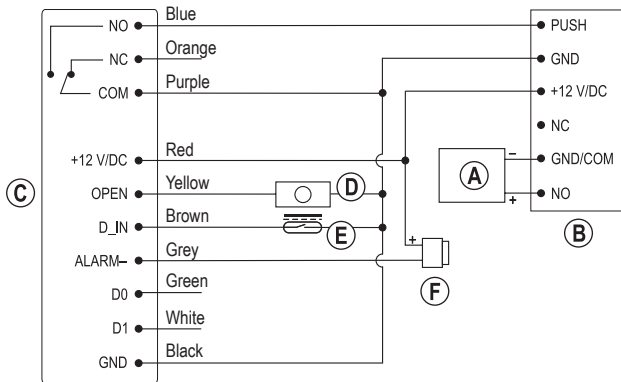
A   "Fail Safe" door opener

B   Power adapter

C   Code lock

D   Door opener button (NO contact, normally open contact)

E   Door sensor (NC contact, normally closed contact)

F   Protection diode: The protective diode must be connected near the door opener with the correct polarity. This protects the code lock from voltage peaks.

G   Alarm siren
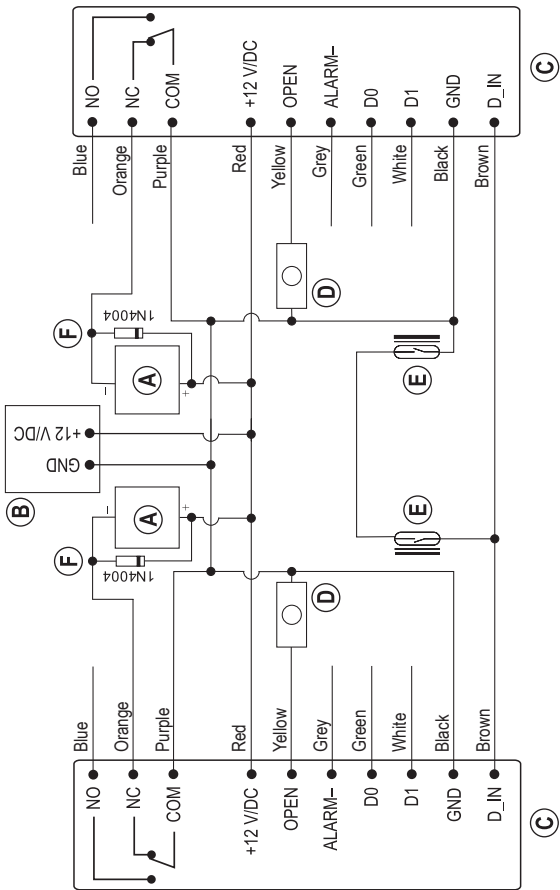
9. Setup

a) IR remote control

- If a small transparent plastic strip protrudes from the bottom of the IR remote control, the battery is already inserted. Pull the plastic strip out of the IR remote control and then it will be ready for use.

- To change the battery, simply pull out the battery holder on the bottom of the IR remote control. Replace the depleted battery (1x CR2025) with a new one. Push the correctly oriented battery holder back into the IR remote control (the plus pole/+ of the battery should point towards the bottom of the IR remote control).

$\longrightarrow$ A battery change is required if the IR range has decreased significantly over time or the code lock is no longer responding to the IR remote control.

b) Code lock

- Switch on the operating voltage after installation and connection.

- The fingerprint sensor illumination is activated briefly and the code lock emits a short beep. The control LED (see chapter 7, item A) on the top of the code lock lights up red.

- You can now start programming, see next chapter.

10. Programming

a) General notes

⚠ Do not disconnect the code lock from the power supply during programming. Otherwise, the existing data or programming could be damaged.

Note the following important information:

- The master code is required to enter programming mode. By default, the master code is "123456".

- Each user can be assigned a specific user ID (this is a number from 1 to 3000, without "0" at the beginning).

→ The tuning-in and saving of fingerprints or transponders is also possible without entering a user ID (the code lock assigns it automatically). In this case, however, a specific user can only be deleted later if their fingerprint or transponder is available.

We therefore recommend that you also assign a user ID for each fingerprint and transponder that you want to tune-in to the code lock.

You should enter it, together with other data, (employee name, fingerprint or transponder access) in a list.

Some of the 3000 available user IDs are reserved for special functions:

9 9 7 and 9 9 8: Superuser fingerprint (see chapter 13. d)

9 9 9: Master fingerprint for tuning-in user fingerprints

1 0 0 0: Master fingerprint for deleting user fingerprints

2 9 9 9 and 3 0 0 0: Superuser transponder (see chapter 13. d)

- User fingerprints can be stored in user IDs 1 .... 9 9 6, user transponders can be stored in user IDs 1 0 0 1 .... 2 9 9 8.

- As a transponder, any standard EM transponder which works with a transponder frequency of 125 kHz can be used.

- Two special transponder cards are included.

Inscription "Master Add Card": This card can be used to tune-in new transponders.

Inscription "Master Delete Card": This card can be used to delete tuned-in transponders.

b) Activating/exiting programming mode

To enter programming mode, you need to enter the master code using the IR remote control. In the default setting of the code lock (or after a reset), the master code is "123456".

⟶ The master code is used only to activate programming mode. The master code cannot be used to switch the relay in the code lock.

In the following programming examples, the default setting "123456" is used as a master code.

Change the master code when programming is completed at the latest.

Activating programming mode:

• The control LED on the top of the code lock must light up red; the code lock is in standby mode.

• Press the ✱ button. Once the code lock has detected the IR signal of the remote control, the control LED on the code lock flashes red (the code lock will automatically return to standby mode after four seconds without any further input (control LED lights up red)).

• Enter the master code ("123456" by default):

 1 2 3 4 5 6

• Press the # button to confirm your entry.

⟶ Before using the code lock in normal operation, you must change the "123456" master code default setting, as described in chapter 10. c).

• The code lock will emit a long beep, and the control LED will light up green briefly. The control LED will then flash red. Programming mode is active.

Exiting programming mode:

Press the ✱ button. The control LED will glow red steadily.

⟶ Programming mode is automatically exited after 30 seconds if no programming is performed. The code lock will then return to standby mode (control LED will light up red).

24

c) Changing the master code

- The code lock must be in standby mode; the control LED lights up red.

- Activate programming mode, as described in chapter 10. b); then the control LED will flash red. Example: ✱ 1 2 3 4 5 6 #

- Press the 0 button. The control LED will light up orange.

- Enter the new master code, for example: 4 5 6 7 8 9

  ⟶ The master code must always consist of six digits.

- Press the # button to confirm your entry. The control LED will light up green briefly for confirmation; then it will light up orange.

- Enter the new master code again to confirm: 4 5 6 7 8 9

- Press the # button to confirm your entry. The control LED will briefly light up green for confirmation; then it will flash red.

- Press the ✱ button to exit programming mode. The control LED now glows red steadily, and the code lock is in standby mode.

d) Setting the user fingerprint

General information:

The user fingerprints can be assigned a specific user ID (it is a number of $\boxed{1}$ .... $\boxed{9}\,\boxed{9}\,\boxed{6}$, without "0" at the beginning).

⟶ The user IDs $\boxed{9}\,\boxed{9}\,\boxed{7}$ ..... $\boxed{1}\,\boxed{0}\,\boxed{0}\,\boxed{0}$ have a special function. See chapter 10. a).

Fingerprints can also be tuned-in even without these user IDs. This speeds up the tuning-in of fingerprints.

If a user ID is not specified when tuning-in a user fingerprint, the code lock will automatically take the next free user ID; but then it is no longer possible to determine which one has been assigned.

⚠ If you do not assign a specific user ID to a user and enter it in a list, this can lead to problems later.

Because if an employee leaves the company or loses a user transponder, you cannot find out which user ID to delete. Because the fingerprint is not available for deletion in this case!

Instead of simply deleting one user ID with the fingerprint stored in it, all data stored in the code lock would have to be deleted for security reasons to prevent unauthorised access.

We therefore recommend that you assign a user ID for each authorised person and enter all data (employee name, user ID, transponder or fingerprint access, etc.) in a list.

Option 1: Tuning-in a user fingerprint with input of the user ID:

- The code lock must be in standby mode; the control LED lights up red.

- Activate programming mode, as described in chapter 10. b); then the control LED will flash red. Example: $\boxed{\star}$ $\boxed{1}$$\boxed{2}$$\boxed{3}$$\boxed{4}$$\boxed{5}$$\boxed{6}$ $\boxed{\#}$

- Press the $\boxed{1}$ button. The control LED will light up orange. The code lock is now in tuning-in mode.

- Enter a user ID (a number from $\boxed{1}$ .... $\boxed{9}$$\boxed{9}$$\boxed{6}$).

  $\longrightarrow$ The user IDs $\boxed{9}$$\boxed{9}$$\boxed{7}$ ..... $\boxed{1}$$\boxed{0}$$\boxed{0}$$\boxed{0}$ have a special function. See chapter 10. a).

- Use the $\boxed{\#}$ button to confirm the user ID. The control LED will light up green briefly, and then orange again.

- Hold a finger on the fingerprint sensor. When the fingerprint has been detected, the code lock emits a beep.

- Take your finger off the fingerprint sensor.

- Place the same finger on the fingerprint sensor again. When the fingerprint has been detected and matches the first one, the code lock emits a beep and the control LED lights up green briefly. The control LED will then light up orange again.

- The new user fingerprint is stored in the previously entered user ID.

  $\longrightarrow$ If the two fingerprints do not match, the code lock emits three short audio signals, the control LED flashes red and then turns orange again. Then try the tuning-in process again.

  The same applies if a user ID has been entered for which a fingerprint is already stored.

  A fingerprint that has already been tuned-in/saved cannot be used again for another user ID.

- You can now tune-in another user fingerprint. First of all, enter the user ID.

- To abort the tuning-in process and exit programming mode, press the $\boxed{\star}$ button. The control LED now glows red steadily, and the code lock is in standby mode.

Option 2: Tuning-in a user fingerprint without a specific user ID (the code lock automatically uses the next free user ID, but it is not possible to determine which one it is):

- The code lock must be in standby mode; the control LED lights up red.
- Activate programming mode, as described in chapter 10. b); then the control LED will flash red. Example: ✱ ⬚1 ⬚2 ⬚3 ⬚4 ⬚5 ⬚6 ⬚#
- Press the ⬚1 button. The control LED will light up orange. The code lock is now in tuning-in mode.
- Hold a finger on the fingerprint sensor. When the fingerprint has been detected, the code lock emits a beep.
- Take your finger off the fingerprint sensor.
- Place the same finger on the fingerprint sensor again. When the fingerprint has been detected and matches the first one, the code lock emits a beep and the control LED lights up green briefly. The control LED will then light up orange again.
- The new user fingerprint is saved.

⟶ If the two fingerprints do not match, the code lock emits three short audio signals, the control LED flashes red and then turns orange again. Then try the tuning-in process again.

A fingerprint that has already been tuned-in/saved cannot be used again for another user ID.

- You can now tune-in another user fingerprint. To do this, place the next finger to be tuned-in on the fingerprint sensor.
- To abort the tuning-in process and exit programming mode, press the ✱ button. The control LED now glows red steadily, and the code lock is in standby mode.

Option 3: Tuning-in a user fingerprint using the supplied master transponder (inscription "Master Add Card"); the code lock automatically uses the next free user ID, but it is not possible to determine which one it is:

⟶   This function is also possible with a fingerprint stored in user ID $\boxed{9}\,\boxed{9}\,\boxed{9}$.

• The code lock must be in standby mode; the control LED lights up red.

• Hold the master transponder (inscription "Master Add Card") provided in front of the code lock (below the fingerprint sensor).

• The code lock will emit a beep and the control LED will light up green briefly and then orange. The code lock is now in tuning-in mode.

• Hold a finger on the fingerprint sensor. When the fingerprint has been detected, the code lock emits a beep.

• Take your finger off the fingerprint sensor.

• Place the same finger on the fingerprint sensor again. When the fingerprint has been detected and matches the first one, the code lock emits a beep and the control LED lights up green briefly. The control LED will then light up orange again.

• The new user fingerprint is saved.

⟶   If the two fingerprints do not match, the code lock emits three short audio signals, the control LED flashes red and then turns orange again. Then try the tuning-in process again.

   A fingerprint that has already been tuned-in/saved cannot be used again.

• You can now tune-in another user fingerprint. To do this, place the next finger to be tuned-in on the fingerprint sensor.

• To abort the tuning-in process and exit programming mode, hold the master transponder (inscription "Master Add Card") provided in front of the code lock (below the fingerprint sensor). The control LED now glows red steadily, and the code lock is in standby mode.

⟶   After a reset of the code lock (see chapter 10. o)), the login transponder is removed from the code lock memory and must be tuned-in anew. See chapter 10. o).

e) Tuning-in the user transponder

General information:

The user transponders can be assigned a specific user ID (it is a number from $\boxed{1}\,\boxed{0}\,\boxed{0}\,\boxed{1}$ .... $\boxed{2}\,\boxed{9}\,\boxed{9}\,\boxed{8}$).

⟶ The user IDs $\boxed{2}\,\boxed{9}\,\boxed{9}\,\boxed{9}$ and $\boxed{3}\,\boxed{0}\,\boxed{0}\,\boxed{0}$ have a special function. See chapter 10. a).

Transponders can also be tuned-in even without a user ID. This speeds up the tuning-in of transponders.

If a user ID is not specified when tuning-in a user transponder, the code lock will automatically take the next free user ID; but then it is no longer possible to determine afterwards which one has been assigned.

⚠ If you do not assign a specific user ID to a user and enter it in a list, this can lead to problems later.

Because if an employee leaves the company or loses a user transponder, you cannot find out which user ID to delete. Because in this case, the transponder is not available for deletion!

Instead of simply deleting a user ID with the transponder stored in it, all data stored in the code lock would have to be deleted for security reasons to prevent unauthorised access.

We therefore recommend that you assign a user ID for each authorised person and enter all data (employee name, user ID, transponder or fingerprint access, etc.) in a list.

Option 1: Tuning-in a user transponder with input of the user ID:

- The code lock must be in standby mode; the control LED lights up red.

- Activate programming mode, as described in chapter 10. b); then the control LED will flash red. Example: ⋆   1 2 3 4 5 6   #

- Press the 1 button. The control LED will light up orange. The code lock is now in tuning-in mode.

- Enter a user ID (a number of 1 0 0 1 .... 2 9 9 8).

  ⟶ The user IDs 2 9 9 9 and 3 0 0 0 have a special function. See chapter 10. a).

- Use the # button to confirm the user ID. The control LED will light up green briefly, and then orange again.

- To tune-in a user transponder, just hold it in front of the code lock (below the fingerprint sensor).

- When the transponder has been detected, the code lock emits a beep and the control LED lights up green briefly. The control LED will then light up orange again.

- The new user transponder is stored in the previously entered user ID.

  ⟶ A transponder that has already been tuned-in/saved cannot be used again. In this case, the code lock emits 3 short beeps, the control LED flashes red and then lights up orange again.

  The same applies if a user ID has been entered for which a transponder is already stored.

- You can now tune-in another user transponder. First of all, enter the user ID.

- To abort the tuning-in process and exit programming mode, press the ⋆ button. The control LED now glows red steadily, and the code lock is in standby mode.

Option 2: Tuning-in a user transponder without a specific user ID (the code lock automatically uses the next free user ID, but it is not possible to determine which one it is):

- The code lock must be in standby mode; the control LED lights up red.

- Activate programming mode, as described in chapter 10. b); then the control LED will flash red. Example: ✱ 1 2 3 4 5 6 #

- Press the 1 button. The control LED will light up orange. The code lock is now in tuning-in mode.

- To tune-in a user transponder, just hold it in front of the code lock (below the fingerprint sensor).

- When the transponder has been detected, the code lock emits a beep and the control LED lights up green briefly. The control LED will then light up orange again.

- The new user transponder is saved.

⟶ A transponder that has already been tuned-in/saved cannot be used again. In this case, the code lock emits 3 short beeps, the control LED flashes red and then lights up orange again.

- You can now tune-in another user transponder. Just hold it in front of the code lock as above.

- To abort the tuning-in process and exit programming mode, press the ✱ button. The control LED now glows red steadily, and the code lock is in standby mode.

Option 3: Tuning-in a user transponder using the supplied login transponder (inscription "Master Add Card"); the code lock automatically uses the next free user ID, but it is not possible to determine which one it is:

A special transponder with inscription "Master Add Card" is included. This transponder makes the login of user transponders very simple because code input via the IR remote control is not required.

$\longrightarrow$ This function is also possible with a fingerprint stored in user ID $\boxed{9}\ \boxed{9}\ \boxed{9}$.

Proceed as follows:

• The code lock must be in standby mode; the control LED lights up red.

• Hold the supplied login transponder (inscription "Master Add Card") in front of the code lock (below the fingerprint sensor).

• The code lock will emit a beep and the control LED will light up green briefly and then orange. The code lock is now in tuning-in mode.

• To tune-in a user transponder, just hold it in front of the code lock (below the fingerprint sensor).

• When the transponder has been detected, the code lock emits a beep and the control LED lights up green briefly. The control LED will then light up orange again.

• The new user transponder is saved.

$\longrightarrow$ A transponder that has already been tuned-in/saved cannot be used again. In this case, the code lock emits 3 short beeps, the control LED flashes red and then lights up orange again.

• You can now tune-in another user transponder. Simply hold it in front of the code lock as above.

• To cancel the tuning-in process and exit programming mode, hold the login transponder provided (inscription "Master Add Card") in front of the code lock (below the fingerprint sensor). The control LED now glows red steadily, and the code lock is in standby mode.

$\longrightarrow$ After a reset of the code lock (see chapter 10. o), the login transponder is removed from the code lock memory and must be tuned-in anew. See chapter 10. o).

Option 4: Tuning-in a user transponder with input of the user ID and the 8- or 10-digit transponder number:

- The code lock must be in standby mode; the control LED lights up red.

- Activate programming mode, as described in chapter 10. b); then the control LED will flash red. Example: ✳ 1 2 3 4 5 6 #

- Press the 1 button. The control LED will light up orange. The code lock is now in tuning-in mode.

- Enter a user ID (a number of 1 0 0 1 .... 2 9 9 8).

⟶ The user IDs 2 9 9 9 and 3 0 0 0 have a special function. See chapter 10. a).

- Use the # button to confirm the user ID. The control LED will light up green briefly, and then orange again.

- Enter the 8- or 10-digit transponder number. Press the # button to confirm. The control LED will light up green briefly, and then orange again.

- The new user transponder is stored in the previously entered user ID.

⟶ A transponder that has already been tuned-in/saved cannot be used again. In this case, the code lock emits 3 short beeps, the control LED flashes red and then lights up orange again.

   The same applies if a user ID has been entered for which a transponder is already stored.

- You can now tune-in another user transponder. First of all, enter the user ID.

- To abort the tuning-in process and exit programming mode, press the ✳ button. The control LED now glows red steadily, and the code lock is in standby mode.

Option 5: Tuning-in a user transponder without a specific user ID (the code lock automatically uses the next free user ID, but it is not possible to determine which one it is) and the 8- or 10-digit transponder number:

- The code lock must be in standby mode; the control LED lights up red.

- Activate programming mode, as described in chapter 10. b); then the control LED will flash red. Example: ✱ 1 2 3 4 5 6 #

- Press the 1 button. The control LED will light up orange. The code lock is now in tuning-in mode.

- Enter the 8- or 10-digit transponder number. Press the # button to confirm. The control LED will light up green briefly, and then orange again.

- The new user transponder is saved.

⟶ A transponder that has already been tuned-in/saved cannot be used again. In this case, the code lock emits 3 short beeps, the control LED flashes red and then lights up orange again.

- You can now tune-in another user transponder. To do this, enter the 8- or 10-digit transponder number.

- To abort the tuning-in process and exit programming mode, press the ✱ button. The control LED now glows red steadily, and the code lock is in standby mode.

Option 6: Mass installation of user transponders (with consecutive transponder numbers)

If you want to store a greater number of user transponders in the code lock and all have a consecutive 8- or 10-digit transponder number, the code lock has a separate function for this purpose.

⟶ The transponder number must be continuous, without spaces in the number sequence.

Proceed as follows:

• The code lock must be in standby mode; the control LED lights up red.

• Activate programming mode, as described in chapter 10. b); then the control LED will flash red. Example: ☒ ①②③④⑤⑥ #

• Press the ⑨ button. The control LED will light up orange. The code lock is now in tuning-in mode.

• Enter a start user ID (a number of ①⓪⓪① .... ②⑨⑨⑧). The transponders are stored from this user ID.

⟶ Make sure that there is enough free memory for the transponders after the start user ID, otherwise the code lock will report an error.

• Use the # button to confirm the start user ID. The control LED will light up green briefly, and then orange again.

• Enter the number of transponders to be saved. Press the # button to confirm. The control LED will light up green briefly, and then orange again.

• Enter the first 8- or 10-digit transponder number. Press the # button to confirm. The control LED will light up green briefly, and then orange again.

• All user transponders are now stored from the start user ID.

• To abort the tuning-in process and exit programming mode, press the ☒ button. The control LED now glows red steadily, and the code lock is in standby mode.

f) Deleting the user ID

A user ID can also be assigned when tuning-in a user fingerprint or user transponder.

If an employee leaves the company or a user transponder gets lost, the user fingerprint or user transponder can be deleted separately by deleting the associated user ID.

⚠️ If user fingerprints or user transponders have been tuned-in without entering the user ID, they can only be deleted separately if the fingerprint or transponder is available!

Instead of simply deleting a user ID with the fingerprint or transponder stored in it, all data stored in the code lock would have to be deleted for security reasons to prevent unauthorised access.

We therefore recommend that you assign a user ID for each authorised person (see chapters 10. d) and 10. e).

If you want to delete a user ID with a user fingerprint (or user transponder) stored in it, proceed as follows:

- The code lock must be in standby mode; the control LED lights up red.

- Activate programming mode, as described in chapter 10. b); then the control LED will flash red. Example: ✴ ⬚1 ⬚2 ⬚3 ⬚4 ⬚5 ⬚6 #

- Press the ⬚2 button. The control LED will light up orange. The code lock is now in delete mode.

- Enter the user ID you want to delete (without "0" at the beginning in each case). Example for user ID 12: Enter: ⬚1 ⬚2

- Press the # button to confirm your entry. The control LED will light up green briefly, and then orange again.

- The user ID (and the fingerprint or transponder stored in it) will be deleted.

- You can now delete another user ID. First of all, enter the user ID.

- To cancel the deletion process and exit programming mode, press the ✴ button. The control LED now glows red steadily, and the code lock is in standby mode.

g) Deleting the user fingerprint

Option 1: Deleting a user fingerprint with the IR remote control:

- The code lock must be in standby mode; the control LED lights up red.

- Activate programming mode, as described in chapter 10. b); then the control LED will flash red. Example: ✱ 1 2 3 4 5 6 #

- Press the 2 button. The control LED will light up orange. The code lock is now in delete mode.

- Hold the fingerprint to be deleted from the code lock system on the fingerprint sensor.

- When the fingerprint has been detected, the code lock will emit a beep and the control LED will briefly light up green. The control LED will then light up orange again.

- The user fingerprint has been deleted.

⟶ If the fingerprint has not been detected or it cannot be found in the code lock memory, the code lock emits 3 short beeps, the control LED flashes red and then lights up orange again.

- You can now delete another user fingerprint. Just hold the finger on the fingerprint sensor as above.

- To cancel the deletion process and exit programming mode, press the ✱ button. The control LED now glows red steadily, and the code lock is in standby mode.

Option 2: Deleting a user fingerprint with the supplied deletion transponder "Master Delete Card":

A special transponder with inscription "Master Delete Card" is included. This transponder allows user fingerprints to be deleted quickly because no code input via the IR remote control is required.

$\longrightarrow$ This function is also possible with a fingerprint that is stored in a user ID
1 0 0 0 .

Proceed as follows:

- The code lock must be in standby mode; the control LED lights up red.

- Hold the supplied deletion transponder (inscription "Master Delete Card") in front of the code lock (below the fingerprint sensor).

- The code lock will emit a beep and the control LED will light up green briefly and then orange. The code lock is now in delete mode.

- Hold the fingerprint to be deleted from the code lock system on the fingerprint sensor.

- When the fingerprint has been detected, the code lock will emit a beep and the control LED will briefly light up green. The control LED will then light up orange again.

- The user fingerprint has been deleted.

$\longrightarrow$ If the fingerprint has not been detected or it cannot be found in the code lock memory, the code lock emits 3 short beeps, the control LED flashes red and then lights up orange again.

- You can now delete another user fingerprint. Just hold the finger on the fingerprint sensor as above.

- To cancel the deletion process and exit programming mode, hold the supplied deletion transponder (inscription "Master Delete Card") in front of the code lock (below the fingerprint sensor). The control LED now glows red steadily, and the code lock is in standby mode.

$\longrightarrow$ After a reset of the code lock (see chapter 10. o), the deletion transponder is removed from the code lock memory and must be tuned-in again. See chapter 10. o).

h) Deleting the user transponder

Option 1: Deleting a user transponder with the IR remote control:

• The code lock must be in standby mode; the control LED lights up red.

• Activate programming mode, as described in chapter 10. b); then the control LED will flash red. Example: $\boxed{*}$ $\boxed{1}\boxed{2}\boxed{3}\boxed{4}\boxed{5}\boxed{6}$ $\boxed{\#}$

• Press the $\boxed{2}$ button. The control LED will light up orange. The code lock is now in delete mode.

• To delete a user transponder, just hold it in front of the code lock (below the fingerprint sensor).

• When the transponder has been detected, the code lock emits a beep and the control LED lights up green briefly. The control LED will then light up orange again.

• The user transponder is deleted.

⟶ If the transponder cannot be found in the code lock memory, the code lock emits three short beeps, the control LED flashes red and then lights up orange again.

• You can now delete another user transponder. Simply hold it in front of the code lock as above.

• To cancel the deletion process and exit programming mode, press the $\boxed{*}$ button. The control LED now glows red steadily, and the code lock is in standby mode.

Option 2: Deleting a user transponder with the supplied deletion transponder "Master Delete Card":

A special transponder with inscription "Master Delete Card" is included. This transponder allows user transponders to be deleted quickly because code input via the IR remote control is not required.

⟶ This function is also possible with a fingerprint that is stored in a user ID $\boxed{1}\boxed{0}\boxed{0}\boxed{0}$.

Proceed as follows:

• The code lock must be in standby mode; the control LED lights up red.

• Hold the supplied deletion transponder (inscription "Master Delete Card") in front of the code lock (below the fingerprint sensor).

• The code lock will emit a beep and the control LED will light up green briefly and then orange. The code lock is now in delete mode.

• To delete a user transponder, just hold it in front of the code lock (below the fingerprint sensor).

• When the transponder has been detected, the code lock emits a beep and the control LED lights up green briefly. The control LED will then light up orange again.

• The new user transponder has been deleted.

⟶ If the transponder cannot be found in the code lock memory, the code lock emits three short beeps, the control LED flashes red and then lights up orange again.

• You can now delete another user transponder. Just hold it in front of the code lock as above.

• To cancel the deletion process and exit programming mode, hold the supplied deletion transponder (inscription "Master Delete Card") in front of the code lock (below the fingerprint sensor). The control LED now glows red steadily, and the code lock is in standby mode.

⟶ After a reset of the code lock (see chapter 10. o)), the deletion transponder is removed from the code lock memory and must be tuned-in again. See chapter 10. o).

Option 3: Deleting a user transponder with the card number

If you want to delete a user transponder using the printed card number, proceed as follows:

- The code lock must be in standby mode; the control LED lights up red.
- Activate programming mode, as described in chapter 10. b); then the control LED will flash red. Example: ⊠ 1 2 3 4 5 6 #
- Press the 2 button. The control LED will light up orange. The code lock is now in delete mode.
- Enter the 8- or 10-digit transponder number. Press the # button to confirm. The control LED will light up green briefly, and then orange again.
- The user transponder is deleted.

→ If the card number cannot be found in the code lock memory, the code lock emits three short beeps, the control LED flashes red and then lights up orange again.

   If both an 8-digit and a 10-digit number are printed on the transponder, try using both numbers to delete. Be sure to enter the complete 8- or 10-digit number (for example, 0004192454 for a 10-digit card number).

- You can now delete another user transponder. First of all, enter the 8- or 10-digit transponder number as above.
- To cancel the deletion process and exit programming mode, press the ⊠ button. The control LED now glows red steadily, and the code lock is in standby mode.

i) Deleting all user data

This function allows all user data (all fingerprints and transponders) to be deleted from the code lock memory.

Proceed as follows:

- The code lock must be in standby mode; the control LED lights up red.

- Activate programming mode, as described in chapter 10. b); then the control LED will flash red. Example: ⚹ 1 2 3 4 5 6 #

- Press the 2 button. The control LED will light up orange. The code lock is now in delete mode.

- Enter the master code, for example: 1 2 3 4 5 6

- Press the # button to confirm your entry. The control LED will light up green briefly, and then orange again.

- All user data (fingerprints, transponders) are deleted.

- To cancel the deletion process and exit programming mode, press the ⚹ button. The control LED now glows red steadily, and the code lock is in standby mode.

j) Setting the activation duration for output or toggle operation

The potential-free changeover contact of the code lock can be activated via a user transponder or a user fingerprint.

The following functions are possible:

- Changeover contact is activated for 2....99 seconds (5 seconds by default); optimal e.g. for a door opener
- Changeover contact is activated for 100 ms (pulsed operation); optimal e.g. for controlling an alarm system
- Toggle operation; the changeover contact toggles between the two switching positions for each valid access attempt; optimal e.g. for activation/deactivation of an alarm system

Proceed as follows:

- The code lock must be in standby mode; the control LED lights up red.
- Activate programming mode, as described in chapter 10. b); then the control LED will flash red. Example: ⨯ 1 2 3 4 5 6 #
- Press the 3 button. The control LED will light up orange.
- Enter the desired time/function: 0 .... 9 9

  0 = Toggle operation, output is switched

  1 = Pulsed operation, output is activated for 100 ms

  2 .... 9 9 = Output is activated for 2...99 seconds

- Press the # button to confirm your entry. The control LED briefly lights up green and then flashes red (programming mode).
- To exit programming mode, press the ⨯ button. The control LED now glows red steadily, and the code lock is in standby mode.

k) Selecting access mode

There are several options for activating the changeover contact (relay) of the code lock:

- **Activating the changeover contact with the user transponder**

  Hold a transponder in front of the sensor surface. If a valid transponder has been detected by the code lock, the changeover contact will be activated.

  The changeover contact cannot be activated with fingerprints stored in the code lock.

- **Activating the changeover contact only via the user fingerprint**

  Hold your finger on the fingerprint sensor. If a valid fingerprint has been detected by the code lock, the changeover contact will be activated.

  The changeover contact cannot be activated with transponders stored in the code lock.

- **Activating the changeover contact via user fingerprint or user transponder (default setting)**

  Hold a transponder in front of the sensor surface or place your finger on the fingerprint sensor. If the transponder or the fingerprint is valid, the changeover contact will be activated.

- **Activating the changeover contact with a certain number of user fingerprints or user transponders**

  The changeover contact is only activated when multiple valid access attempts have been carried out using different fingerprints/transponders one after the other. The number of valid access attempts is adjustable (2....9).

  Example: Two access attempts are programmed.

  If the code lock detects the first valid access attempt (user fingerprint or transponder), the control LED will flash green for approx. four seconds. During this time, another valid access attempt by another fingerprint/transponder is required. The changeover contact will only be activated after these two valid access attempts.

  This ensures a higher level of security because, for example, a transponder card and then a fingerprint are required to activate the changeover contact.

Proceed as follows:

- The code lock must be in standby mode; the control LED lights up red.
- Activate programming mode, as described in chapter 10. b); then the control LED will flash red. Example: $\boxed{*}$ $\boxed{1}\boxed{2}\boxed{3}\boxed{4}\boxed{5}\boxed{6}$ $\boxed{\#}$
- Press the $\boxed{4}$ button. The control LED will light up orange.
- Enter the desired function for access mode:

  $\boxed{0}$ = Access only via the transponder

  $\boxed{2}$ = Access via the transponder or fingerprint (by default)

  $\boxed{3}$ = Access only via the fingerprint

  $\boxed{4}$ = Access via multiple different transponders/fingerprints

  Directly after selecting function $\boxed{4}$, enter the required number of fingerprints/transponders: $\boxed{2}$ .... $\boxed{9}$

- Press the $\boxed{\#}$ button to confirm your entry. The control LED briefly lights up green and then flashes red (programming mode).
- To exit programming mode, press the $\boxed{*}$ button. The control LED now glows red steadily, and the code lock is in standby mode.

46

l) Setting the alarm duration

If a door secured with the code lock is also provided with a door sensor, the code lock can detect a violent attempt to open the door and then emit an alarm. For this purpose, an alarm siren can be connected to the code lock; otherwise, the alarm output must be connected to an alarm system.

The alarm output of the code lock can also be activated if ten invalid access attempts have been made consecutively, as described in chapter 10. m).

→ An alarm will also be emitted if the code lock case is tampered with during operation (tampering attempt).

The alarm duration is adjustable (1....3 minutes).

Proceed as follows:

· The code lock must be in standby mode; the control LED lights up red.

· Activate programming mode, as described in chapter 10. b); then the control LED will flash red. Example: ✳ 1 2 3 4 5 6 #

· Press the 5 button. The control LED will light up orange.

· Enter the desired function:

   0 = Alarm disabled

   1 = Alarm enabled

   Directly after selecting function 1, enter the alarm duration in minutes (1...3 minutes is possible, one minute by default): 1 3

For example, press the following two buttons in succession for two minutes:

   1 = Alarm enabled

   2 = Set alarm duration to two minutes

· Press the # button to confirm your entry. The control LED briefly lights up green and then flashes red (programming mode).

· To exit programming mode, press the ✳ button. The control LED now glows red steadily, and the code lock is in standby mode.

m) Security function for invalid access attempts

The code lock may be locked if ten invalid access attempts have been made consecutively (for example, in an attempt to test transponders).

The following functions are available:

- **No lock (default setting)**

  Invalid access attempts are ignored.

- **Lock for ten minutes**

  If ten invalid access attempts have been made via the transponders or fingerprints, the code lock will be locked for ten minutes. The control LED will flash red. During this time, access cannot be gained, even with valid transponders or fingerprints.

- **Triggering an alarm**

  If ten invalid access attempts have been made with transponders or fingerprints, the code lock will emit an alarm sound, and the alarm output will be activated (thus an alarm siren can be operated; otherwise, the alarm output can be connected to an alarm system).

  The alarm duration is adjustable (1...3 minutes is possible, one minute by default), as described in chapter 10. l). The alarm can be cancelled using a valid transponder or fingerprint.

Proceed as follows:

- The code lock must be in standby mode; the control LED lights up red.
- Activate programming mode, as described in chapter 10. b); then the control LED will flash red. Example: ⁎ 1 2 3 4 5 6 #
- Press the 5 button. The control LED will light up orange.
- Enter the desired function:

  4 = Security function disabled

  5 = Lock for ten minutes

  6 = Trigger an alarm

- Press the # button to confirm your entry. The control LED briefly lights up green and then flashes red (programming mode).
- To exit programming mode, press the ⁎ button. The control LED now glows red steadily, and the code lock is in standby mode.

n) Security function with door sensor

In the default setting of the code lock, the door sensor function is deactivated.

If you connect a door sensor (NC contact / normally closed contact) to the code lock and enable the door sensor function, the following functions will be available:

- In case of a violent attempt to open the door (the door is opened without a valid access attempt having been made in advance using a transponder or fingerprint), the code lock emits an alarm sound and the alarm output is activated. An alarm siren can be connected to the alarm output; otherwise, the alarm output must be connected to an alarm system.

  The alarm can be terminated using a valid transponder or fingerprint.

- If the door is not closed within one minute of a valid access attempt using a transponder or fingerprint, the code lock will emit an alarm sound and the alarm output will be activated. An alarm siren can be connected to the alarm output; otherwise, the alarm output must be connected to an alarm system.

  The alarm can be terminated by closing the door or using a valid transponder or fingerprint.

Proceed as follows:

- The code lock must be in standby mode; the control LED lights up red.
- Activate programming mode, as described in chapter 10. b); then the control LED will flash red. Example: ✻ 1 2 3 4 5 6 #
- Press the 6 button. The control LED will light up orange.
- Enter the desired function:

  0 = Door sensor function disabled (default setting)

  1 = Door sensor function enabled

- Press the # button to confirm your entry. The control LED briefly lights up green and then flashes red (programming mode).
- To exit programming mode, press the ✻ button. The control LED now glows red steadily, and the code lock is in standby mode.

o) Reset

When the code lock is reset, it returns to the default settings.

⟶ However, the user fingerprints and user transponders stored are retained after reset. To delete these as well, please refer to chapter 10. i).

Two special preprogrammed transponder cards are included.

• Inscription "Master Add Card": This card can be used to tune-in new transponders.

• Inscription "Master Delete Card": This card can be used to delete tuned-in transponders.

When the code lock is reset, the data of these two transponders is also deleted from the code lock. So when the code lock is reset, you can either:

• tune-in the same transponder cards again

• tune-in two other new transponders as "Master Add Card" and "Master Delete Card"

• not tune-in any transponders for the above functions.

Resetting <u>and</u> tuning-in two transponder cards:

- Disconnect the code lock from the voltage/power supply. Wait until the control LED goes off.
- Keep the door opener button pressed and connect the code lock to the voltage/power supply.
- The code lock will emit two beeps, and the control LED will light up orange. Then release the door opener button.
- You now have approx. ten seconds (orange LED lights up) to tune-in two transponders.

  Hold two transponders in front of the code lock, one after the other.

  The first transponder is the one new transponders can be tuned-in with (= "Master Add Card").

  The second transponder is the one with which tuned-in transponders can be deleted (= "Master Delete Card").

- After the second transponder has been tuned-in, the control LED lights up green briefly and then glows red steadily, the reset has been completed, the code lock is in standby mode and ready for use.

Resetting <u>without</u> tuning-in two transponder cards:

- Disconnect the code lock from the voltage/power supply. Wait until the control LED goes off.
- Keep the door opener button pressed and connect the code lock to the voltage/power supply.
- The code lock will emit two beeps, and the control LED will light up orange. Keep the door opener button pressed and do not release it.
- After approx. ten seconds, the code lock will emit a long beep and the control LED will light up green. Now release the door opener button.

11. Wiegand function

The code lock can serve as an external reader connected to a Wiegand controller. Follow the operating instructions for the controller or monitoring system operating the code lock.

a) Connection

Red	+12 V/DC
Black	GND
Green	D0
White	D1
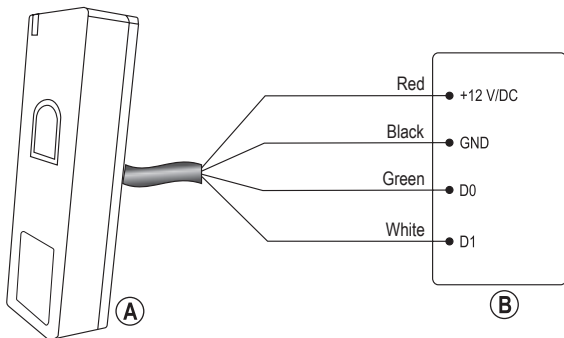
A   Code lock

B   Wiegand controller / monitoring system

b) Setting Wiegand device ID

→ This setting function should only be used if fingerprints are to be read and transmitted by the code lock.

The code lock can be assigned a different device ID ("0" by default) in order to establish a connection with a Wiegand controller, if required.

If the code lock is used as a Wiegand reader and detects a valid fingerprint, it will transmit a virtual transponder number.

If, for example, the device ID 255 has been programmed and the user ID of the valid fingerprint is "3", the virtual transponder number 255,00003 will be transmitted (example for Wiegand controllers with a bit rate of 26 bits).

Proceed as follows:

- The code lock must be in standby mode; the control LED lights up red.
- Activate programming mode, as described in chapter 10. b); then the control LED will flash red. Example: ✱ 1 2 3 4 5 6 #
- Press the 7 button. The control LED will light up orange.
- Enter the device ID: 0 .... 2 5 5
- Press the # button to confirm your entry. The control LED briefly lights up green and then flashes red (programming mode).
- To exit programming mode, press the ✱ button. The control LED now glows red steadily, and the code lock is in standby mode.

c) Configuring the Wiegand output

The code lock can output data to the Wiegand output with different bit formats. Check the operating instructions of the controller or surveillance system being used with the code lock to find out which bit format is supported.

The Wiegand output can also be disabled.

⟶ By default, the Wiegand output is enabled; the bit rate is set to 26 bits.

Proceed as follows:

• The code lock must be in standby mode; the control LED lights up red.

• Activate programming mode, as described in chapter 10. b); then the control LED will flash red. Example: ⋆ 1 2 3 4 5 6 #

• Press the 8 button. The control LED will light up orange.

• Now either disable the Wiegand output or set the bit rate:

   0 = Wiegand output disabled

   2 6 .... 4 4 = Wiegand output enabled with bit rate of 26 bits .... 44 bits

⟶ The code lock should have the same bit rate as all other devices connected to the Wiegand bus.

• Press the # button to confirm your entry. The control LED briefly lights up green and then flashes red (programming mode).

• To exit programming mode, press the ⋆ button. The control LED now glows red steadily, and the code lock is in standby mode.

d) Using fingerprints with the Wiegand controller

If the code lock is used as a Wiegand reader and detects a valid fingerprint, it will transmit a virtual transponder number.

If, for example, the device ID 255 has been programmed (see chapter 11. a)) and the user ID of the valid fingerprint is "3", the virtual transponder number 255,00003 will be transmitted (example for Wiegand controllers with a bit rate of 26 bits).

If the code lock is only used as a Wiegand reader and you want to use a fingerprint as an access point for the Wiegand controller or the Wiegand access system, proceed as follows:

• Tune-in the fingerprints to the code lock, as described in chapter 10. d).

• If necessary, set an unused device ID for the code lock, as described in chapter 11. a).

• To tune-in new transponders via the Wiegand interface, switch the Wiegand controller or the Wiegand access system to tuning-in mode.

• Place your finger on the fingerprint sensor of the code lock so that it is detected as a valid access attempt.

• The code lock will transmit a virtual transponder number.

• Proceed like this for all other fingerprints.

• After all fingerprints have been transmitted as a virtual transponder number to the Wiegand controller or Wiegand access system, exit tuning-in mode.

If a valid attempt is now made to access the code lock using a fingerprint, a virtual transponder number will be transmitted as described above and, for example, a door lock will be activated by the Wiegand controller or Wiegand access system.

12. Interlock function

The connection diagrams for interlocking two code locks can be found in chapter 8.

The interlock function can be used, for example, to control special access systems when accessing a room/area with double doors, of which only one may be opened.

⟶ To enable the interlock function, switch on the interlock function on both code locks. Every door must be equipped with a door sensor.

Proceed as follows:

- The code lock must be in standby mode; the control LED lights up red.
- Activate programming mode, as described in chapter 10. b); then the control LED will flash red. Example: ✱ 1 2 3 4 5 6 #
- Press the 6 button. The control LED will light up orange.
- Enter the desired function:

  2 = Interlock function disabled (default setting)

  3 = Interlock function enabled

- Press the # button to confirm your entry. The control LED briefly lights up green and then flashes red (programming mode).
- To exit programming mode, press the ✱ button. The control LED now glows red steadily, and the code lock is in standby mode.

Operating principle:

- Door #1 can only be opened via the corresponding code lock #1 if door #2 is closed.
- Door #2 can only be opened via the corresponding code lock #2 if door #1 is closed.

⟶ When the interlock function is enabled, only one of the two doors can be opened. Simultaneously opening both doors is prevented.

13. Operation

a) Enabling the changeover contact

Activation via user transponder

The transponder must be held in front of the sensor surface (area below the fingerprint sensor) (max. distance approx. three cm). If a valid transponder has been detected, the code lock emits a long audio signal, the control LED briefly lights up green and the changeover contact is activated.

Activation via user fingerprint

Place your finger on the sensor surface. If a valid fingerprint has been detected, the code lock emits a long audio signal, the control LED briefly lights up green and the changeover contact is activated.

b) Enabling the changeover contact via button

If a door opener button has been connected to the code lock (see connection examples in chapter 8), the changeover contact can be activated by briefly pressing the button. The activation time is the same as that used for a valid user transponder or user fingerprint (the button can be used in toggle operation to change the switching position of the changeover contact).

$\longrightarrow$ If a door opener is triggered via the changeover contact, the door opener can be activated with the button without the need to use a valid user transponder or user fingerprint.

c) Terminating the alarm sound

The code lock uses a door sensor to monitor the door status and, for example, can emit an alarm in the event of a violent attempt to open the door; see chapter 10. n).

$\longrightarrow$ An alarm will also be emitted if the code lock case is tampered with during operation (tampering attempt).

The alarm can be terminated using a transponder or fingerprint that is tuned-in to the code lock. Alternatively, enter the master code using the IR remote control and press the #️⃣ button.

d) Superuser lock function

Some of the 3000 available user IDs are reserved for special functions, as described in chapter 10. a).

$\boxed{9}\boxed{9}\boxed{7}$ and $\boxed{9}\boxed{9}\boxed{8}$: Superuser fingerprint

$\boxed{2}\boxed{9}\boxed{9}\boxed{9}$ and $\boxed{3}\boxed{0}\boxed{0}\boxed{0}$: Superuser transponder

If fingerprints or transponders are stored in these user IDs, the code lock can be temporarily locked. In this state, it is no longer possible to access the code lock via user fingerprints or user transponders.

How to lock the code lock:

- The code lock must be in standby mode; the control LED lights up red.
- Allow the code lock to read a superuser fingerprint or superuser transponder stored in the aforementioned user IDs.
- The control LED will flash red several times. The code lock will emit a long beep, and the control LED will glow red steadily.
- The code lock is now locked. In this state, it is no longer possible to access the code lock via user fingerprints or user transponders.

How to unlock the code lock:

- The code lock must be in standby mode; the control LED lights up red.
- Allow the code lock to read a superuser fingerprint or superuser transponder stored in the aforementioned user IDs.
- The control LED will flash green several times. The code lock will emit a long beep, and the control LED will glow red steadily.
- The code lock is now unlocked. It is possible to access the code lock via user fingerprints or user transponders.

14. Sound signals and LED displays

Function	LED	Beep
Standby	LED lights up red	-
Program mode	Flashing red LED	1x short beep
Programming code has been entered; awaiting further code entries	Orange LED	1x short beep
Error	LED flashes red three times	3x short beep
Valid access attempt via transponder or fingerprint	LED flashes green once	1x long beep
Door opener button is pressed	LED flashes green once	1x long beep
Alarm	Flashing red LED	Continuous short beeps

→ A detailed description of the control LED and sound signals can be found in the respective sections of these operating instructions.

15. 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.

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 supplies voltage/power to the door opener.

• If the door opener has polarity markings (plus/+ and minus/-), ensure that it is connected to the code lock in the correct polarity.

• Check the polarity of the protective diode connected to the door opener.

• The used fingerprint or transponder is not tuned-in.

• The changeover contact cannot be activated with the superuser fingerprint or superuser transponder.

The transponder does not work

• Always hold only one transponder in front of the code lock, the correct position is below the fingerprint sensor.

• 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 in the vicinity of the code lock or transponder can impair the function of a transponder (for example, if the transponder is in a wallet together with coins).

• The code lock has been locked with a superuser fingerprint or superuser transponder.

Functional problems associated with the fingerprint sensor

• Keep the glass of the fingerprint sensor clean.

• The detection is based on the different lines (skin ridges) on the fingertip. Therefore, even thin disposable gloves prevent detection.

Other functionality issues

- Reset the code lock (see chapter 10. o) or delete all existing data (see chapter 10. i) and restart the programming.

- Check that the cables are connected correctly.

- Check the voltage/power supply. The code lock requires a stabilised DC voltage (12 V/DC).

16. Care and Cleaning

- Use a dry, lint-free cloth to clean the product. In case of heavy soiling, lightly moisten the cloth with water.

- Never use aggressive detergents, rubbing alcohol or other chemical solutions, as these may damage the case or cause the product to malfunction.

17. Declaration of Conformity (DOC)

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

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

www.conrad.com/downloads

Select a language by clicking on the corresponding flag symbol, and then enter the product order number in the search box. The EU Declaration of Conformity is available for download in PDF format.

18. 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 according to the relevant statutory regulations.

Remove any inserted battery from the remote control and dispose of it separately from the product.

b) Battery information

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 designations for the heavy metals involved 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.

19. Technical Data

a) Code lock

Operating voltage	12 V/DC
Current consumption	standby < 45 mA; max. 175 mA
Transmission frequency range	124.6 - 125.4 kHz
Transmission power	< 11.62 dBm
Wiegand connection	yes (programmable bit format 26 bits .... 44 bits)
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)
	Contact rating max. 12/24 V/DC, 1/2 A
	Switching time adjustable (100 ms or 2 – 99 seconds or toggle operation)
Alarm output	yes (12 V/DC, max. 2 A)
Memory	Transponder: 2000
	Fingerprints: 1000
Fingerprint sensor resolution	500 dpi
	FAR: <0.001%
	FRR: <0.01%
	Detection time: <1 s
Mounting location	Indoors/outdoors
Protection class	IP66
Operating conditions	Temperature -30 °C to +60 °C
Storage conditions	Temperature -40 °C to +70 °C
Dimensions	48 x 128 x 26 mm (W x H x D)
Weight	approx. 400 g

b) IR remote control

Power supply	1x CR2025 battery