sygonix®

GB Operating Instructions

RFID/touch/fingerprint access system

Item no. 2615507

CE

1 Table of contents

GB

2 Introduction

Thank you for purchasing this product.

This product complies with statutory, national and European regulations. To ensure that the product remains in this state and to guarantee safe operation, always follow the instructions in this manual.

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

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

3 Intended use

This product is designed to prevent unauthorised access to doors (e.g. in an office) and to activate/disable alarm systems. It can be controlled via the keypad, suitable transponders or fingerprints. You can store a maximum of 1000 users (100 users with fingerprints, 890 users with PIN/transponder and 10 visitors with PIN/transponder).

Entering a correct PIN, holding a taught-in transponder in front of the reading area or touching the sensor with a stored finger 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 (IP55).

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.

The product complies with statutory, national and European regulations.

4 Delivery content

- Access system
- Fasteners (2x special screws with matching L-key, 4x screw head stickers, mounting frame with 4x screws and 4x dowels)
- 1N4004 diode (for relay changeover contact)
- Quick start guide

5 Installation, connection, getting started, programming and operation

Detailed important instructions for this product and a programming overview sheet are downloadable from our website (enter the item number to call up the page with product details).

Alternatively, follow the link www.conrad.com/downloads or scan the QR code. Follow the instructions on the website.

There you will find the latest operating instructions for download.

6 Explanation of symbols

The text contains the following 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.

7 Safety instructions

Damage caused due to failure to observe these instructions will void the warranty/guarantee! 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 access system is suitable for indoor and outdoor installation and use (IP55).
- Handle the product carefully. Jolts, impacts or a fall even from a low height may damage the product. Do not expose the product to 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 the section “Technical data” and must not be exceeded.

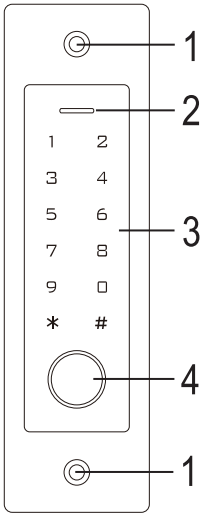
Caution!

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 product 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 plaything for children!
- Maintenance, modifications and repairs must be carried out only by a skilled 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.

8 Controls and connections

1. Opening for wall mounting
2. LED indicator
3. Keypad with an integrated RFID sensor
4. Fingerprint sensor with LED ring



Connection cable:

Colour	Inscription	Function
Red	12-18 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

→ When the access system is connected to a Wiegand controller as an external reader (see section 9.4.1), the yellow line of the access system can (if required) serve as a beep control (low level = sound activated) instead of a door opener signalling.

9 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 the power supply is switched off.

9.1 Installation

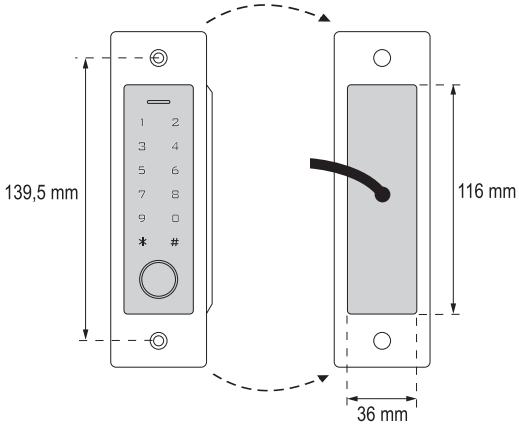
Use suitable screws and, if necessary, dowels to mount the mounting plate with the module on the wall (see figure on the right) depending on the type of wall.

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 substrate and installation position, and the access system should then be screwed tight.

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

A hole for the connection 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 chapter “Technical data”.

→ 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 the cable connection and successful start-up.

9.2 Connecting to conventional voltage/power supply

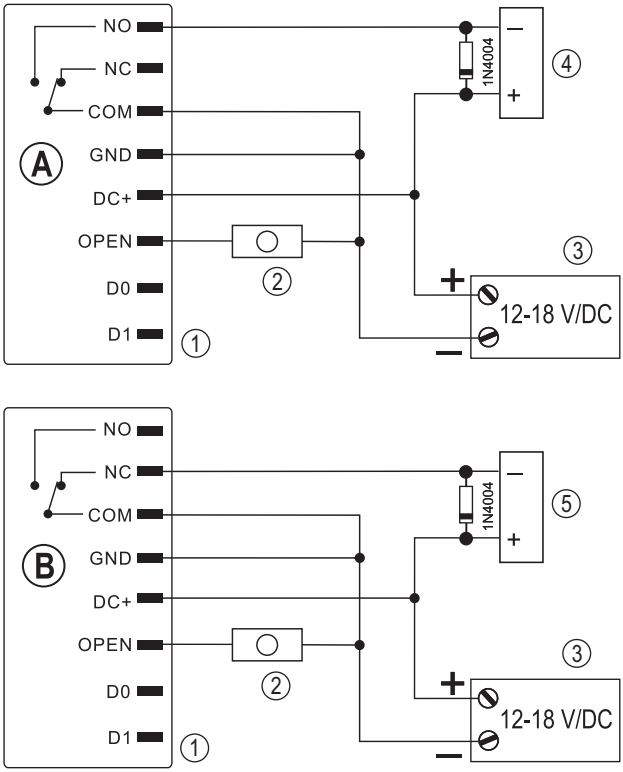
When a conventional power supply unit should be used, observe the following figures with the wiring diagram.

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

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

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

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



9.3 Connecting to alarm system

Observe the operating instructions for the alarm system used. The access system relay switches when a valid user code or transponder is recognised or when the sensor is touched with a stored finger. An alarm system can thus be enabled or disabled.

9.4 Wiegand interface

The Wiegand interface of the access system can be used in two different ways. For programming, see section 11.6.

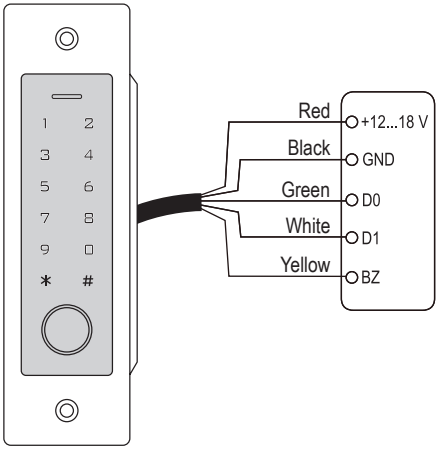
9.4.1 Using the access system as an external reader

The access system can be connected to a compatible Wiegand controller and used as an external reader. Virtually all access system settings have no function in this mode.

If required, the yellow line of the access system can serve as a beep control (low level = sound activated) instead of a door opener signalling.

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

With the access system, you can programme the bit rate for data transfer (the default setting of the access system is 26 bit, see section 11.23), which must be the same as that of the Wiegand controller. Follow the operating instructions for the Wiegand controller.



9.4.2 Connecting an external reader to the access system

The access system functions as a Wiegand controller and allows the operation of an external reader (e.g. for transponders).

⟶ 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 taught in via this card reader.

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

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 9.2. Always follow the operating instructions for the external card reader.

With the access system, you can programme the bit rate for data transfer (the default setting of the access system is 26 bit, see section 11.22), which must be the same as that of the reader. Follow the operating instructions for the reader.

10 Setup

After completing the installation and connection process, switch on the operating voltage. The access system emits a short beep, and the button illumination turns on. The LED lights up red, which indicates that the access system is in standby mode.

The access system automatically shuts off the button illumination if the sensor field is not touched within 20 seconds.

You can now start programming, as described in the next section.

11 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, user PIN, transponder number, etc., to know who can access the system. These data also enable easy deletion of individual user PINs, user transponders or user fingerprints.

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

The keypad is mainly used for programming.

You can also use a master transponder or master fingerprint to teach in or delete user PINs/transponders/fingerprints.

The access system can store up to 10 “visitor” PINs or transponders. Visitor PINs/transponders can have a 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. Subsequently, it is automatically removed from the access system memory and becomes invalid.

1000 memories are provided for the transponders and fingerprints:

- Memory cell number 0 - 98: user fingerprints
- Memory cell number 99: master fingerprint
- Memory cell number 100 - 989: user PINs and/or user transponders (depending on access mode)
- Memory cell number 990 - 999: visitor PINs or visitor transponders

11.1 General information

Please note:

- The access system automatically turns off the button illumination if the sensor field is not touched within 20 seconds. The **first** touch of the sensor field only activates the button illumination and is recognised as an entry; the access system emits no beep in this case.
- Each time the access system recognises a valid button press, it emits a short confirmation beep. A correct entry is followed by a long confirmation beep, and the LED lights up green briefly.
- In case of an incorrect entry, the access system emits 3 brief beeps, and the red LED flashes 3 times.

11.2 Resetting all settings to factory defaults; teaching in master transponders

With a master transponder, you can easily teach in or delete user PINs, user transponders or user fingerprints without having to call up the programming mode now and then.

⟶ For security reasons, you can only create a master transponder while resetting the access system to factory defaults.

It is possible to have **no** master transponder, for example, if, for security reasons, you wish to teach in or delete user PINs/transponders/fingerprints only via the programming mode and not via the master transponder.

11.2.1 Resetting the access system and teaching in the master transponder

⟶ If you have already taught in a master transponder, it will automatically be deleted through the teach-in of another transponder. It means that you can only have **one** master transponder at a time. Ensure the transponder to be used as the master transponder is **not yet** registered with the access system (e.g. as a user transponder).

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

⟶ The used transponder that is already taught in as the user transponder cannot be used as a master transponder. The access system will emit 3 brief beeps, and the LED will flash red.

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

11.2.2 Resetting the access system without teaching in a master transponder (or deleting the existing master transponder)

→ The procedure described below allows the operation of the access system without a master transponder. In addition, it also allows you to delete an existing master transponder, e.g. if it has been lost.

- De-energise the access system and wait for the LED to go off.
- Press and hold the door opener button connected to the access system.
- Energise the access system. The access system will emit two beeps.
- Wait for around 5 seconds, keep the door opener button pressed and do not release it.
- The access system emits a beep and the LED lights up red.
- You can now release the door opener button for the access system to go back to standby mode. All settings have been reset to factory defaults; there is **no** master transponder.

11.2.3 Overview of the default settings

Function	**Adjustment after resetting to factory defaults**
Master code	123456
master fingerprint	is retained/not deleted
user or visitor PINs/transponders/fingerprints	are retained/not deleted
Mode	77 (use as access system or Wiegand controller)
Wiegand bit rate	26 bit
Wiegand parity bit	on
Output format when used as a Wiegand card reader	4 bit
Alarm after 10 incorrect entries	off
Alarm duration after 10 incorrect entries	1 minute
Beep when a button is pressed	on
Status LED	on
Button illumination	switches off automatically after 20 seconds of inactivity
Switch output activation time	5 seconds
Output activation	Access upon a correct entry of a PIN, transponder **or** fingerprint
Automatic teach-in of new transponders	Off

11.3 Enabling/disabling programming mode

- To go into programming mode, enter the 6-digit master code as follows (default setting = 123456):

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

- The LED then flashes red (programming mode is active). This mode allows teaching in/deleting user PINs/transponders or making various settings.
- To exit the programming mode (red LED flashes), press the [*] button. A permanently lit LED indicates that the access system is in standby mode.

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

11.4 Changing master code

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

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

→ The master code must always consist of six digits.

- Enable the programming mode as described in section 11.3; the LED starts to flash red.
- Enter 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.

11.5 Teaching in/deleting the master fingerprint

A single master fingerprint can be taught in to the access system. It allows you to quickly teach in or delete user PINs, transponders or fingerprints.

⟶ Memory cell number 99 is reserved for the master fingerprint.

11.5.1 Teaching in master fingerprint

- Enable the programming mode as described in section 11.3; the LED starts to flash red.
- Enter programming code [1] to start the teach-in process. The yellow LED will then light up.
- Enter memory cell number [9] [9] for the master fingerprint.
- Press the [#] button to confirm your entry.

⟶ When memory cell number 99 is already occupied by a master fingerprint, the access system emits 3 brief beeps, and the LED flashes red 3 times. It is no longer possible to overwrite an existing master fingerprint. Start by deleting memory cell 99 (see below) before storing another master fingerprint.

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

  After the third correct reading, the access system emits a long beep and the fingerprint is stored. The LED indicator lights up yellow.

⟶ If the fingerprint cannot be read correctly, you will hear 3 beeps, and the LED ring will flash red 3 times. The same happens if you try to scan a fingerprint that has already been stored.

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

11.5.2 Deleting master fingerprint

- Enable the programming mode as described in section 11.3; the LED starts to flash red.
- Enter programming code [2] to activate delete mode. The yellow LED will then light up.
- Enter memory cell number [9] [9] for the master fingerprint.
- Press the [#] button to confirm your entry.

⟶ If the memory cell is already blank, the access system emits 3 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.

11.6 Setting the Wiegand interface mode

As already mentioned in section 9.4, the access system can function as an external reader (section 9.4.1) for a Wiegand controller or as a Wiegand controller for an external reader (section 9.4.2). The access system allows you to configure the desired mode.

- Enable the programming mode as described in section 11.3; the LED starts to flash red. Enter programming code [7] to activate setup mode. The yellow LED will then light up.
- Select the desired function:

  [7] = Access system functions as a Wiegand controller or as a stand-alone unit (default setting)

  [8] = Access system functions as a reader for an external Wiegand controller
- Press the [#] button to exit setup mode. The LED flashes red again, which means that you can continue programming or exit the programming mode with the [*] button.

→ When the access system is operated as a stand-alone unit (without an additional external reader), the default setting ([7]) must be used.

When the access system is operated as a reader ([8]), virtually all access system settings have no function as the external Wiegand controller takes it over. The yellow connection cable of the access system no longer activates a door opener button and can be used to control a beeping transmitter in the access system (low signal = beep active).

11.7 Selecting access mode

There are various options for activating the changeover contact in the access system:

- Only with a fingerprint
- Only with a transponder
- Only with a PIN
- With a transponder **and** PIN
- With a PIN**,** transponder **or** fingerprint (default setting)
- Only with 2 - 9 transponders (access is granted only when multiple persons are there and attempt access in strict succession (max. 5 seconds per person), e.g. for high-security rooms; in this case, a single person has no access despite having a valid transponder)

→ The master transponder or master fingerprint cannot be used to activate the changeover contact of the access system.

Proceed as follows:

- Enable the programming mode as described in section 11.3; the LED starts to flash red.
- Enter programming code [4] for the access mode. The yellow LED will then light up.
- Select the desired access mode:

  [0] = Only with a fingerprint

  [1] = Only with a transponder

  [2] = Only with a PIN

  [3] = With a transponder **and** PIN

  [3] + ([2] ..... [9]) = Multi-user access

  Example: [3] [4] = The changeover contact is activated and access granted only if 4 persons perform a valid access attempt using a transponder strictly one after the other within no more than 5 seconds per person

  [4] = With a PIN**,** transponder **or** fingerprint (default setting)
- 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.

11.8 Saving user PIN

The access system has 890 memory cells to store user PINs and/or user transponders. Memory cell numbers 100 - 989 are provided for these transponders.

You can use the keypad, master transponder or master fingerprint for storage.

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

Besides, it enables you to easily delete a specific user who is no longer allowed access, has forgotten their user PIN or has lost a user transponder.

Otherwise, it might be necessary to clear all memory cells and start over.

You can save a user PIN in two different ways:

- Save the user PIN in the next free memory cell
- Save the user PIN in a specific memory cell

11.8.1 Automatically saving a user PIN in the next free memory cell

⟶ This storage mode enables quick and easy teaching in of new user PINs in the next free memory cell.

In this case, a specific user PIN can only be deleted via the PIN itself, as the assignment between the user PIN and the memory cell number is unknown. In that case, all memory cells would need to be cleared.

- Enable the programming mode as described in section 11.3; the LED starts to flash red. Enter programming code [1] to activate storage mode. The yellow LED will then light up.

⟶ Otherwise, you can hold the master transponder **once** in front of the reading area or touch the fingerprint sensor **once** with the master fingerprint. This activates the storage mode, and the LED indicator lights up yellow.

- Next, enter the desired user PIN and then press the [#] button to confirm your entry.

  Example: [2] [2] [2] [2] [#] = Save user PIN 2222

⟶ The user PIN can consist of 4 to 6 digits. You cannot use the 8888 digit combination because it is a service combination (default user code).

When the PIN is already stored in the memory, the access system emits 3 brief beeps, and the LED flashes red. The same PIN can be assigned only once.

- You can save multiple user PINs if desired. To do so, enter the desired user PIN consisting of 4 to 6 digits and then press the [#] button to confirm.
- 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.

11.8.2 Assigning a user PIN to a specific memory cell

→ This process takes more time but enables you to delete a specific user PIN (via the memory cell number) if you have forgotten it (provided you have a table with the access data in place that was recommended at the beginning of the chapter).

- Enable the programming mode as described in section 11.3; the LED starts to flash red. Enter programming code [1] to start the teach-in process. The yellow LED will then light up.

→ Otherwise, you can hold the master transponder **once** in front of the reading area or touch the fingerprint sensor **once** with the master fingerprint. This activates the storage mode, and the LED indicator lights up yellow.

- Enter the memory cell number ([1] [0] [0] ..... [9] [8] [9]) in which you wish to save the user PIN, and then press the [#] button to confirm your entry.

  Example: [6] [5] [4] [#] = Save the user PIN in memory cell 654

→ If the memory cell number has already been assigned, the access system emits 3 brief beeps, and the LED flashes red. A memory cell cannot be overwritten. First, clear the respective memory cell before another user PIN can be stored there, as described in section 11.9.

- Next, enter the desired user PIN and then press the [#] button to confirm your entry.

  Example: [2] [2] [2] [2] [#] = Save user PIN 2222

→ The user PIN can consist of 4 to 6 digits. You cannot use the 8888 digit combination because it is a service combination (default user code).

When the PIN is already stored in the memory, the access system emits 3 brief beeps, and the LED flashes red. The same PIN can be assigned only once.

- You can save multiple user PINs if desired. Simply enter the 3-digit memory cell number ([1] [0] [0] ..... [9] [8] [9]) and press the [#] button to confirm. Then enter the desired user PIN consisting of 4 to 6 digits and press the [#] button to confirm.
- 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.

11.9 Deleting user PIN

The respective user will no longer have access via their user PIN once the corresponding user PIN has been deleted.

You can delete a user PIN in two different ways:

- Delete the user PIN
- Clear the memory cell in which the user PIN is stored (if known, see note at the beginning of section 11.8)

11.9.1 Deleting a user PIN

- Enable the programming mode as described in section 11.3; the LED starts to flash red. Enter the programming code [2] to start deletion mode. The yellow LED will then light up.

→ Otherwise, you can hold the master transponder **twice** in front of the reading area or touch the fingerprint sensor **twice** with the master fingerprint (each time for 5 seconds). This activates the delete mode, and the LED indicator lights up yellow.

- Enter the user PIN you wish to delete and press the [#] button to confirm. The user PIN will be deleted.

  Example: [6] [5] [4] [3] [#] = Delete user PIN 6543

- You can also delete other user PINs if you wish (enter the desired user PIN and press the [#] button to confirm).

→ When the user PIN is unknown and/or already deleted, the access system emits 3 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.

11.9.2 Deleting a user PIN via memory cell number

- Enable the programming mode as described in section 11.3; the LED starts to flash red. Enter the programming code [2] to start deletion mode. The yellow LED will then light up.

→ Otherwise, you can hold the master transponder **twice** in front of the reading area or touch the fingerprint sensor **twice** with the master fingerprint (each time for 5 seconds). This activates the delete mode, and the LED indicator lights up yellow.

- Enter the 3-digit memory cell number ([1] [0] [0] ..... [9] [8] [9]) you wish to clear and press the [#] button to confirm your entry. The memory cell (with the data stored in it) will be cleared.

  Example: [6] [5] [4] [#] = Clear memory cell 654

→ When the memory cell number is already blank, the access system emits 3 brief beeps, and the LED flashes red.

- You can also clear other memory cells if you wish (enter the memory cell number and press the [#] button to confirm).
- 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.

11.10 Changing a user PIN

You can only change a user PIN when the programming mode is disabled. The point is that a user can change their own user PIN themselves without having to know the master code. This provides extra security because the new PIN is only known to the user.

You can change a user PIN in 2 different ways:

- Change the user PIN with the user transponder; access mode [3] must be selected in section 11.7 (= access with transponder **and** PIN)
- Change the user PIN with the memory cell number

11.10.1 Changing a user PIN via user transponder

- Press the [*] button. The red LED flashes.
- Hold the user transponder for which you want to change the user PIN close in front of the RFID sensor. When the transponder is recognised, the access system emits a beep.
- Enter the old user PIN.
- Press the [#] button to confirm your entry.
- Enter the new user PIN.

→ The user PIN can consist of 4 to 6 digits. You cannot use the 8888 digit combination because it is a service combination (default user code).

- Press the [#] button to confirm your entry.
- Enter the new user PIN once again for security reasons.
- Press the [#] button to confirm your entry.
- The access system is now in standby mode and ready for use.

11.10.2 Changing a user PIN via memory cell number

- Press the [*] key. The red LED flashes.
- Enter the memory cell number ([1] [0] [0] ..... [9] [8] [9]) whose user PIN you wish to change.
- Press the [#] button to confirm your entry.
- Enter the old user PIN.
- Press the [#] button to confirm your entry.
- Enter the new user PIN.

→ The user PIN can consist of 4 to 6 digits. You cannot use the 8888 digit combination because it is a service combination (default user code).

- Press the [#] button to confirm your entry.
- Enter the new user PIN once again for security reasons.
- Press the [#] button to confirm your entry.
- The access system is now in standby mode and ready for use.

11.11 Teaching in user transponders

The access system has 890 memory cells to store user transponders and/or user PINs. Memory cell numbers 100 - 989 are provided for these transponders.

You can use the keypad, master transponder or master fingerprint for storage.

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

Besides, it enables you to easily delete a specific user who is no longer allowed access, has lost a user transponder or when the user transponder is defective.

Otherwise, it might be necessary to clear all memory cells and start over.

There are three different teach-in options:

- Quick teach-in of a user transponder to the next free memory cell
- Teach-in of a user transponder to a specific memory cell
- Teach-in of multiple user transponders with consecutive transponder numbers

11.11.1 Automatically saving a user transponder in the next free memory cell

⟶ This teach-in process enables quick and easy teach-in of new user transponders to the next free memory cell.

In this case, a specific user transponder can only be deleted via the transponder itself, as the assignment between the user transponder and the memory cell number is unknown. In that case, all memory cells would need to be cleared.

- Enable the programming mode as described in section 11.3; the LED starts to flash red. Enter programming code [1] to activate storage mode. The yellow LED will then light up.

⟶ Otherwise, you can hold the master transponder **once** in front of the reading area or touch the fingerprint sensor **once** with the master fingerprint. This activates the storage mode, and the LED indicator lights up yellow.

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

  Other than holding the transponder in front of the RFID sensor, you can enter the 8- or 10-digit number of the transponder and press the [#] button to confirm.

  Example: [0] [0] [0] [3] [1] [7] [1] [4] [5] [6] [#]

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

- You can also teach in other transponders by proceeding as described above; to do so, hold the transponder in front of the RFID sensor **or** enter the transponder number and press the [#] button to confirm.
- 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.

11.11.2 Assigning a user transponder to a specific memory cell

→ Although this teach-in process takes more time, it enables you to delete a specific user transponder (via the memory cell number) even when it is defective or lost.

- Enable the programming mode as described in section 11.3; the LED starts to flash red. Enter programming code [1] to start the teach-in process. The yellow LED will then light up.

→ Otherwise, you can hold the master transponder **once** in front of the reading area or touch the fingerprint sensor **once** with the master fingerprint. This activates the storage mode, and the LED indicator lights up yellow.

- Enter the memory cell number ([1] [0] [0] ..... [9] [8] [9]) in which you wish to save the user transponder, and then press the [#] button to confirm the memory cell number.

  Example: [6] [5] [4] [#] = Save the transponder in memory cell 654

→ When the memory cell number is already occupied, the access system emits three brief beeps and the LED flashes red. A memory cell cannot be overwritten. First, clear the respective memory cell before a user transponder can be stored there.

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

  Other than holding the transponder in front of the RFID sensor, you can enter the 8- or 10-digit number of the transponder and press the [#] button to confirm.

  Example: [0] [0] [0] [3] [1] [7] [1] [4] [5] [6] [#]

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

- If you wish to teach in another user transponder, first enter the memory cell number again 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.

11.11.3 Teaching in multiple user transponders with consecutive transponder number

This option enables you to save multiple transponders with consecutive transponder numbers (consisting of 8 or 10 digits) at the same time using the mass storage option.

→ Since the memory cell numbers are also consecutive, transponders can be assigned to them; it is also possible to delete an individual transponder that is defective or lost via the memory cell number.

However, you should first create a list of transponder numbers and memory cell numbers. Besides, no memory cell involved in the mass storage must be occupied; otherwise, the occupied memory cell will be skipped during the mass storage, with all subsequent assignments between transponders and memory cell numbers shifted accordingly.

- Enable the programming mode as described in section 11.3; the LED starts to flash red. Enter programming code [1] to start the teach-in process. The yellow LED will then light up.
- Enter the memory cell number ([1] [0] [0] ..... [9] [8] [9]) from which the mass storage should take place and press the [#] button to confirm.

  Example: [3] [0] [0] [#] = first memory cell in the mass storage

→ When this memory cell number is already occupied, the access system emits 3 brief beeps, and the LED flashes red.

- Enter the number of transponders you want to save at the same time using the mass storage option and press the [#] button to confirm.

  Example: [1] [0] [0] [#] = 100 transponders with consecutive numbers are to be saved

→ Make sure that there are enough memory cells available from the entered memory cell number to accommodate all the transponders to be saved. For example, it is not possible to save 200 transponders starting from memory cell 800 since the access system has a total of only 890 memory cells. Should that be the case, the access system will emit 3 brief beeps, and the LED will flash red.

- Enter the number of the first transponder (8 or 10 digits) and press the [#] button to confirm.

  Example: [0] [0] [0] [3] [1] [7] [1] [4] [5] [6] [#]

- The access system will then save the entered number of user transponders in the memory cell. The whole procedure lasts up to 2 minutes depending on the number of transponders.
- Press the [#] button to exit the pairing mode. The LED flashes red again, which means that you can continue programming or exit the programming mode with the [*] button.

11.11.4 Teaching in user transponders via collective mode

With this mode activated, each transponder can activate the changeover contact. The transponder is simultaneously automatically stored in the next free memory cell as a user transponder.

→ This pairing procedure enables quick and easy pairing of new user transponders in the next free memory cell.

In this case, a specific user transponder can only be deleted via the transponder itself, as the assignment between the user transponder and the memory cell number is unknown. You would then have to delete all memory cells if only a single transponder should be denied access.

- Enable the programming mode as described in section 11.3; the LED starts to flash red. Enter programming code [9]. The yellow LED will then light up.
- Select the desired function:

  [2] = Collective mode disabled (default setting)

  [3] = Collective mode enabled

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

→ With the collective mode activated, each transponder activates the changeover contact. The transponder is simultaneously automatically stored in the next free memory cell as a user transponder.

If you again hold an already taught-in transponder in front of the RFID sensor, it will not be stored again (but the changeover contact will be activated).

Always switch off the collective mode when you do not use it. Otherwise, any person holding a transponder in front of the RFID sensor of the access system can gain access.

11.12 Deleting user transponder

The respective user will no longer have access once the corresponding user transponder has been deleted.

You can delete a user transponder in three different ways:

- Delete the user transponder via reading
- Delete the user transponder via the transponder number (if known, see note at the beginning of section 11.8)
- Clear the memory cell in which the user transponder is stored (if known, see note at the beginning of section 11.8)

11.12.1 Deleting a user transponder via transponder

- Enable the programming mode as described in section 11.3; the LED starts to flash red. Enter the programming code [2] to start deletion mode. The yellow LED will then light up.

→ Otherwise, you can hold the master transponder **twice** in front of the reading area or touch the fingerprint sensor **twice** with the master fingerprint (each time for 5 seconds). This activates the delete mode, and the LED indicator lights up yellow.

- Hold the user transponder close in front of the RFID sensor. If the transponder is recognised, the access system emits a short beep and the transponder is deleted.

→ When the user transponder is unknown and/or already deleted, the access system emits 3 brief beeps, and the LED flashes red 3 times.

- You can then delete another user transponder as described above (by holding it in front of the RFID sensor).
- 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.

11.12.2 Deleting a user transponder via transponder number

Most of the transponders have an 8- or 10-digit number printed on them. You can delete a defective transponder (e.g. broken transponder card) by entering this number.

- Enable the programming mode as described in section 11.3; the LED starts to flash red. Enter the programming code [2] to start deletion mode. The yellow LED will then light up.

→ Otherwise, you can hold the master transponder **twice** in front of the reading area or touch the fingerprint sensor **twice** with the master fingerprint (each time for 5 seconds). This activates the delete mode, and the LED indicator lights up yellow.

- Enter the 8- or 10-digit transponder number and press the [#] button to confirm.

  Example: [0] [0] [0] [3] [1] [7] [1] [4] [5] [6] [#]

→ When the transponder number is unknown and/or already deleted, the access system emits 3 brief beeps, and the LED flashes red 3 times.

- You can then delete another user transponder as described above (by entering the transponder number and pressing the [#] button to confirm).
- 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.

11.12.3 Deleting a user transponder via memory cell number

- Enable the programming mode as described in section 11.3; the LED starts to flash red. Enter the programming code [2] to start deletion mode. The yellow LED will then light up.

→ Otherwise, you can hold the master transponder **twice** in front of the reading area or touch the fingerprint sensor **twice** with the master fingerprint (each time for 5 seconds). This activates the delete mode, and the LED indicator lights up yellow.

- Enter the 3-digit memory cell number ([1] [0] [0] ..... [9] [8] [9]) you wish to clear and press the [#] button to confirm your entry. The memory cell (with the data stored in it) will be cleared.

  Example: [6] [5] [4] [#] = Clear memory cell 654

→ When the memory cell number is already blank, the access system emits 3 brief beeps, and the LED flashes red 3 times.

- You can also clear other memory cells if you wish (enter the memory cell number and press the [#] button to confirm).
- 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.

11.13 Teaching in a user fingerprint

The access system can accommodate up to 99 different user fingerprints. Memory cell numbers 0 - 98 are provided for user fingerprints.

You can use the keypad, master transponder or master fingerprint for teaching-in.

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

Besides, it enables you to easily delete a specific user who is no longer allowed access.

Otherwise, it might be necessary to clear all memory cells and start over.

You can save a user fingerprint in two different ways:

- Save the user fingerprint in the next free memory cell
- Save the user fingerprint in a specific memory cell

11.13.1 Automatically saving a user fingerprint in the next free memory cell

⟶ This teach-in process enables quick and easy teach-in of new user fingerprints to the next free memory cell.

In this case, a specific user fingerprint can only be deleted via the fingerprint, as the assignment between the user fingerprint and the memory cell number is unknown. In that case, all memory cells would need to be cleared.

- Enable the programming mode as described in section 11.3; the LED starts to flash red. Enter programming code [1] to activate storage mode. The yellow LED will then light up.

⟶ Otherwise, you can hold the master transponder **once** in front of the reading area or touch the fingerprint sensor **once** with the master fingerprint. This activates the storage mode, and the LED indicator lights up yellow.

- To teach in a user fingerprint, touch the fingerprint sensor 3 times in succession with the same finger. As your finger touches the sensor, an LED ring around the sensor lights up blue. The LED ring lights up green and a short beep is emitted if the fingerprint is recognised correctly. After the third correct fingerprint scan, the access system emits a long beep, and the LED lights up green; the fingerprint has been saved.

⟶ If the fingerprint cannot be read correctly, 3 beeps are emitted and the LED ring flashes red. The same applies if you attempt to read a stored fingerprint.

- Proceed as above if you want to teach in another user fingerprint (touch the fingerprint sensor 3 times in succession).
- 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.

11.13.2 Assigning a user fingerprint to a specific memory cell

→ Although this teach-in process takes more time, a specific user fingerprint can be deleted (via the memory cell number) even if the person is no longer available to do so.

- Enable the programming mode as described in section 11.3; the LED starts to flash red. Enter programming code [1] to activate storage mode. The yellow LED will then light up.

→ Otherwise, you can hold the master transponder **once** in front of the reading area or touch the fingerprint sensor **once** with the master fingerprint. This activates the storage mode, and the LED indicator lights up yellow.

- Enter the memory cell number ([0] ..... [9] [8]) in which you wish to save the user fingerprint (without leading zero for single-digit memory cell numbers), and then press the [#] button to confirm the memory cell number.

  Example 1: [6] [#] = Save the user fingerprint in memory cell 6

  Example 2: [5] [4] [#] = Save the user fingerprint in memory cell 54

→ When the memory cell number is already occupied, the access system emits three brief beeps and the LED flashes red. A memory cell cannot be overwritten. First, clear the respective memory cell before another user fingerprint can be stored there.

- To teach in a user fingerprint, touch the fingerprint sensor 3 times in succession with the same finger. As your finger touches the sensor, an LED ring around the sensor lights up blue. The LED ring lights up green and a short beep is emitted if the fingerprint is recognised correctly. After the third correct fingerprint scan, the access system emits a long beep, and the LED lights up green; the fingerprint has been saved.

→ If the fingerprint cannot be read correctly, you will hear three beeps and the LED ring will flash red. The same applies if you attempt to read a stored fingerprint.

- If you wish to teach in another user fingerprint, first enter the memory cell number again 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.

11.14 Deleting user fingerprint

The respective user will no longer have access once the corresponding user fingerprint has been deleted.

You can delete a user fingerprint in two different ways:

- Delete the user fingerprint via scanning
- Delete the memory cell in which the user fingerprint is stored (if known, see note at the beginning of section 11.8)

11.14.1 Deleting a user fingerprint via fingerprint

- Enable the programming mode as described in section 11.3; the LED starts to flash red. Enter the programming code [2] to start deletion mode. The yellow LED will then light up.

→ Otherwise, you can hold the master transponder **twice** in front of the reading area or touch the fingerprint sensor **twice** with the master fingerprint (each time for 5 seconds). This activates the delete mode, and the LED indicator lights up yellow.

- Touch the fingerprint sensor with the user finger you wish to delete. If the fingerprint is recognised, the access system emits a short beep and the fingerprint is deleted.

→ When the user fingerprint is unknown and/or already deleted, the access system emits 3 brief beeps, and the LED flashes red.

- Other user fingerprints can be deleted by following the instructions above.
- 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.

11.14.2 Deleting a user fingerprint via memory cell number

- Enable the programming mode as described in section 11.3; the LED starts to flash red. Enter the programming code [2] to start deletion mode. The yellow LED will then light up.

→ Otherwise, you can hold the master transponder **twice** in front of the reading area or touch the fingerprint sensor **twice** with the master fingerprint (each time for 5 seconds). This activates the delete mode, and the LED indicator lights up yellow.

- Enter the 3-digit memory cell number ([1] [0] [0] ..... [9] [8] [9]) you wish to clear and press the [#] button to confirm your entry. The memory cell (with the data stored in it) will be cleared.

  Example: [6] [5] [4] [#] = Clear memory cell 654

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

- You can also clear other memory cells if you wish (enter the memory cell number and press the [#] button to confirm).
- 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.

11.15 Clearing all memory cells

→ This option deletes all 1000 memory cells (890 user PINs/transponders, 10 visitor transponders, 99 user fingerprints and the master fingerprint).

The master transponder and presets (e.g. changeover contact activation time) are retained.

- Enable the programming mode as described in section 11.3; the LED starts to flash red. Enter the programming code [2] to start deletion mode. The yellow LED will then light up.

→ Otherwise, you can hold the master transponder **twice** in front of the reading area or touch the fingerprint sensor **twice** with the master fingerprint (each time for 5 seconds). This activates the delete mode, and the LED indicator lights up yellow.

- Enter the master code and press the [#] button to confirm. All 1000 memory cells will be cleared.
- 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.

11.16 Setting the changeover contact activation time

This function enables you to set the changeover contact activation time from 1 to 99 seconds after valid access to the access system (the 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.

- Enable the programming mode as described in section 11.3; the LED starts to flash red.
- Enter programming code [3] to set the activation time. The yellow LED will then light up.
- Enter the desired changeover contact activation time. Possible is [1] ..... [9] [9] (= 1 - 99 seconds; without leading zero for single-digit memory cell numbers).

  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.

11.17 Enabling or disabling protection against incorrect entries

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

- Enable the programming mode as described in section 11.3; the LED starts to flash red.
- Enter 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] = 10-minute lock (during this time, you cannot access the system with a valid PIN/transponder/fingerprint or via the keypad; the master transponder and master fingerprint have no function; changeover contact can be activated with the door opener button); the 10-minute lock can be early terminated by briefly de-energising the access system

  [2] = Lock with alarm for 1 to 3 minutes (alarm time can be set as described in section 11.17); lock and alarm can be early terminated using a valid PIN/transponder/fingerprint

Caution!

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

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

11.18 Setting the alarm time for protection function

With the [2] function (lock with alarm) activated as described in section 11.16, you can set the alarm time as described below (from 1 to 3 minutes, default setting: 1 minute).

- Enable the programming mode as described in section 11.3; the LED starts to flash red.
- Enter 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 - 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.

11.19 Enabling access for visitors

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

Visitor transponders and visitor PINs can have a 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 preset number of access attempts has been used for the visitor transponder/PIN, the access system automatically deletes the transponder/PIN from the memory. A new visitor transponder/PIN can now be assigned to the cleared memory cell number.

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

11.19.1 Teaching in a visitor transponder

- Enable the programming mode as described in section 11.3; the LED starts to flash red. Enter programming code [1] to start the teach-in process. The yellow LED will then light up.

⟶ Otherwise, you can hold the master transponder **once** in front of the reading area or touch the fingerprint sensor **once** with the master fingerprint. This activates the storage mode, and the LED indicator lights up yellow.

- Enter the memory cell number ([9] [9] [0] ..... [9] [9] [9]) in which you wish to save the visitor transponder, and then press the [#] button to confirm the memory cell number.

  Example: [9] [9] [5] [#] = Save the visitor transponder in memory cell 995

⟶ When the memory cell number is already occupied, the access system emits three brief beeps and the LED flashes red. A memory cell cannot be overwritten. First, clear the respective memory cell before a visitor transponder can be stored there.

- Enter the number of times the visitor transponder may be used ([0] to [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.
- Hold a transponder in front of the RFID sensor. Once a new transponder is recognised, the access system emits a short beep and the transponder is saved.

  Other than holding the transponder in front of the RFID sensor, you can enter the 8- or 10-digit number of the transponder and press the [#] button to confirm.

  Example: [0] [0] [0] [3] [1] [7] [1] [4] [5] [6] [#]

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

- If you wish to teach in another visitor transponder, first enter the memory cell number again 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.

11.19.2 Saving a visitor PIN

- Enable the programming mode as described in section 11.3; the LED starts to flash red. Enter programming code [1] to start the teach-in process. The yellow LED will then light up.

→ Otherwise, you can hold the master transponder **once** in front of the reading area or touch the fingerprint sensor **once** with the master fingerprint. This activates the storage mode, and the LED indicator lights up yellow.

- Enter the memory cell number ([9] [9] [0] ..... [9] [9] [9]) in which you wish to save the visitor PIN, and then press the [#] button to confirm the memory cell number.

  Example: [9] [9] [5] [#] = Save the visitor PIN in memory cell 995

→ When the memory cell number is already occupied, the access system emits three brief beeps and the LED flashes red. A memory cell cannot be overwritten. First, clear the respective memory cell before another visitor PIN can be stored there, as described in section 11.9.

- Enter the number of times the visitor PIN may be used ([0] ..... [9], where "0" stands for 10 uses).

  Example 1: [2] = Visitor can use the PIN two times, after which it becomes invalid

  Example 2: [0] = Visitor can use the PIN ten times, after which it becomes invalid

- Confirm the number with the [#] button.
- Next, enter the desired visitor PIN and then press the [#] button to confirm your entry.

  Example: [2] [2] [2] [2] [#] = Save visitor PIN 2222

→ The visitor PIN can consist of 4 to 6 digits. You cannot use the 8888 digit combination because it is a service combination (default user code).

When the PIN is already stored in the memory, the access system emits 3 brief beeps, and the LED flashes red. The same PIN can be assigned only once.

- You can also save other visitor PINs as described above, starting with the entry of the memory cell number.
- 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.

11.19.3 Deleting a visitor transponder or visitor PIN

After the preset number of access attempts, a visitor transponder or a visitor PIN is automatically deleted from the memory.

If you wish to delete the visitor transponder or PIN before all access attempts have been used, proceed exactly as for deleting a user transponder or user PIN; only enter the corresponding memory cell number ([9] [9] [0] ..... [9] [9] [9]) for visitors.

- For deletion of a transponder, see section 11.11.3 or 11.11.2.
- For deletion of a PIN, see section 11.9.2.

11.20 Enabling/disabling visual and acoustic indication

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

- Enable the programming mode as described in section 11.3; the LED starts to flash red. Enter programming code 7 to set LED indications and beeps. The yellow LED will then light up.
- Select the desired function:

  0 = Beeps disabled

  1 = Beeps enabled (default setting)

  2 = LED disabled

  3 = LED enabled (default setting)

  4 = Button illumination disabled

  5 = Button illumination enabled

  6 = Button illumination is activated when you press the button (the first button press only activates the button illumination); the button illumination is automatically disabled if no button is pressed within 20 seconds (factory default)
- 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.

11.21 Transferring data between two access systems

When using two identical access systems, transponder and PIN data can be exchanged between the units.

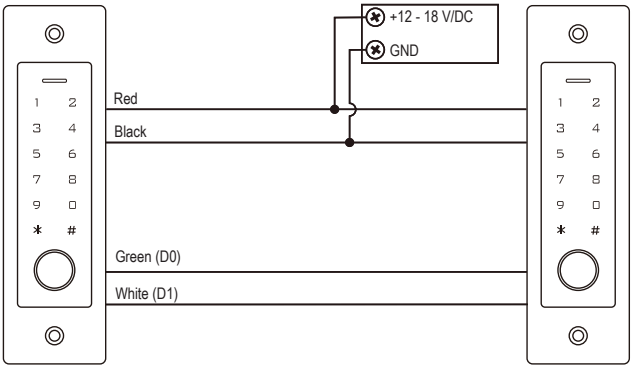
⟶ **Please note:**

Fingerprint data cannot be transmitted.

Both access systems must have the same master code.

Proceed as follows:

- Follow the steps below to connect the two identical access systems:



- Turn on the power supply.

⟶ **Please note:**

The following entries should only be made on the unit whose transponder or PIN data are to be transmitted.

No entries are required on the target unit (which is to receive the data).

- Enter the programming mode on the access system whose transponder or PIN data you wish to transmit as described in section 11.3; the LED flashes red.
- Enter programming code [9] [8] and press the [#] button to initiate the data transmission. The LED lights up green; the transmission can take up to 30 seconds. The access system will then emit a beep, and the LED will light up red.
- Press the [*] button to exit programming mode.
- Disconnect both access systems from the power supply. After that, you can mount and wire the units as usual; then programme both access systems separately (e.g. Changeover contact activation time).

11.22 Setting the Wiegand input data format

This option is required if you wish to operate an external reader via the Wiegand interface of the access system (the access system functions as a master or Wiegand controller, see section 9.4.2).

Refer to the operating instructions for the external reader for the output data format. Then customise the access system settings accordingly.

- Enable the programming mode as described in section 11.3; the LED starts to flash red. Enter programming code [8] to activate setup mode. The yellow LED will then light up.
- Now enter:

  [2] [6] ..... [4] [4] = Bit rate 26 to 44 bit (default setting 26 bit)

  or

  [4] = PIN input format 4 bit (default setting)

  or

  [8] = PIN input format 8 bit

  or

  [1] [0] = PIN input format 10 bit

  or

  [0] = Parity bit disabled

  or

  [1] = Parity bit enabled (default setting)
- 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.

→ For readers with a bit rate of 32 or 40 bit, the parity bit must be disabled.

11.23 Setting the Wiegand output data format

This option is required if you wish to operate the access system as a reader on a Wiegand controller (see section 9.4.1).

You can set the bit rate and enable/disable the parity bit. Refer to the operating instructions for the Wiegand controller for the data format. Next, set the same bit rate on the access system and enable or disable the parity bit accordingly.

- Enable the programming mode as described in section 11.3; the LED starts to flash red. Enter programming code [8] to activate setup mode. The yellow LED will then light up.
- Now enter:

  [2] [6] ..... [4] [4] = Bit rate 26 to 44 bit (default setting 26 bit)

  or

  [4] = PIN output format 4 bit (default setting)

  or

  [8] = PIN output format 8 bit

  or

  [1] [0] = PIN output format 10 bit

  or

  [0] = Parity bit disabled

  or

  [1] = Parity bit enabled (default setting)
- 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.

⟶ For the Wiegand controller interface with a bit rate of 32 or 40 bit, the parity bit must be disabled.

12 Operation

12.1 Getting started

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

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

You should take the following steps:

- Create a table and fill in all settings, including user names, PIN numbers and transponder numbers to be given access via the access system.
- You must first reset the access system to factory defaults before creating a master transponder (which allows quick and easy access to the teach-in and delete mode). The procedure is described in section 11.2.
- Think of a master code (should consist of 6 digits) and programme it (see section 11.4). The default master code is “123456” (or after resetting the access system).
- If desired, teach in a master fingerprint (which allows quick and easy access to the teach-in and delete mode), as described in section 11.5.
- Select the desired access mode, as described in section 11.7.
- Set the changeover contact activation time (see section 11.16) to be used e.g. for switching a door lock (default setting is 5 seconds).
- If desired, enable protection against incorrect entries, as described in sections 11.17 and 11.18.
- You can now proceed to save user PINs (section 11.8), teach in user transponders (section 11.11) and/or teach in user fingerprints (section 11.13), depending on the access mode.
- Check whether the stored user PINs, user transponders or user fingerprints can be used to activate the changeover contact (and e.g. a door lock that is controlled via the changeover contact).

12.2 Accessing via valid user PIN/transponder/fingerprint

Once the access system has recognised a valid user PIN, user transponder or user fingerprint, the changeover contact (and e.g. A door lock that is controlled via the changeover contact) is activated for the preset time and the LED lights up green. When the time is up, the LED lights up red (standby).

⟶ After enabling the toggle mode (as described in section 11.16), each valid access attempt permanently switches the changeover contact to the other position.

12.3 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 11.16), each press of the door opener button permanently switches the changeover contact to the other position.

12.4 Preventing the PIN from being revealed

It is a special feature that allows you to enter extra digits before or after the actual PIN when entering the PIN. You can enter up to 10 digits in which you can “hide” the actual PIN.

⟶ **Please note:**

This option is only available for 6-digit PINs.

Example: User PIN = 1 2 1 2 1 2

Enter: 9 9 9 1 2 1 2 1 2 9 #

⟶ It does not matter whether and how many digits you enter before and/or after the actual PIN. There should be a total of 10 digits which must contain the correct PIN.

12.5 Disabling the alarm/lock on incorrect entry

When the 2 function selected in section 11.17 (lock with alarm for 1 to 3 minutes; for setting the alarm time, see section 11.18) is enabled, the access system emits an alarm tone for the preset time, and the LED flashes red.

You can terminate the alarm by a valid access attempt (valid user PIN, user transponder or user fingerprint) or the master transponder or master fingerprint.

⟶ **Please note:**

When a 10-minute lock function 1 (see section 11.17) is enabled, it can be early terminated by briefly disconnecting the access system from the power supply.

13 Troubleshooting

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

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

The door opener does not work

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

A new user PIN will not save

- You cannot use the 8888 digit combination because it serves as the default setting for the internal memory in the “PIN + transponder” access mode.
- The user PIN is already in use. You cannot save the same PIN twice.

The transponder is not recognised

- Always hold only one transponder in front of the RFID sensor at a time.
- Ensure the transponder is close enough (approx. 2 cm) to the access system.
- Only EM transponders with a frequency of 125 kHz can be used.
- Metal objects can adversely affect a transponder's functionality (for example, if you keep the transponder in a wallet with metal coins).

A new user transponder will not teach in

- Always hold only one transponder in front of the RFID sensor at a time.
- Ensure the transponder is close enough (approx. 2 cm) to the access system.
- Only EM transponders with a frequency of 125 kHz can be used.
- The memory is already occupied. Use another memory cell or clear the existing one before teaching in another transponder to the same memory cell.
- When the Wiegand controller uses a MIFARE® smart card reader, new transponders can only be taught in via this card reader.
- When the Wiegand controller uses a card reader for 125 kHz transponders, teach-in can be performed both via the access system and the external card reader. Use an external card reader to check the functionality.

User fingerprint teach-in does not work or works incorrectly

- If required, use another finger to test it. The fingerprint sensor must recognise enough papillary ridges (protrusions) for the fingerprint to be valid.
- Place your finger in the centre and over the entire surface. The recognised area of the skin surface must have a minimum size to be valid. It does not matter which way around the finger is oriented. Hence, you can always teach in your finger “vertically” and place it at 90° to gain access.
- Do not wear gloves.
- Use a clean, soft, dry cloth to clean the fingerprint sensor.

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

- The changeover contact activation time has been set to “0” and is in toggle mode (see section 11.16). Each valid access to the code lock changes the changeover contact switch position.

The changeover contact cannot be activated with the correctly taught-in user PIN, user transponder or user fingerprint

- Check the access mode setting, as described in section 11.7.

After resetting to factory defaults, the user PINs, user transponders, user fingerprints and the master fingerprint are not deleted

- This is normal. To clear all memory cells, proceed as described in section 11.15.

The visitor PIN or visitor transponder will not work

- A visitor PIN or visitor transponder is only valid for a preset number of access attempts (1 to 10 access attempts, see section 11.19.). After that, the visitor PIN or visitor transponder automatically becomes invalid and is removed from the access system memory.
- You can make the used transponder valid again and give it to another visitor by reprogramming it with a certain number of access attempts using the access system (see section 11.19.1).

The Wiegand interface 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.
- Set the correct mode, as described in section 11.22.
- Programme the Wiegand interface, as described in sections 11.23 and 11.24.
- Always follow the operating instructions for the unit to be connected to the Wiegand interface.

14 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 a flag symbol and enter the product order number in the search box. You can then download the EU declaration of conformity in PDF format.

15 Cleaning and maintenance

This product does not require maintenance. Use a dry, lint-free cloth for occasional cleaning. Use a cloth moistened with lukewarm water for heavy soiling.

Never use aggressive cleaning agents, rubbing alcohol or other chemical solutions, as these may cause discolouration or damage.

16 Disposal

This symbol must appear on any electrical and electronic equipment placed on the EU market. This symbol indicates that this device should not be disposed of as unsorted municipal waste at the end of its service life.

Owners of WEEE (Waste from Electrical and Electronic Equipment) shall dispose of it separately from unsorted municipal waste. Spent batteries and accumulators, which are not enclosed by the WEEE, as well as lamps that can be removed from the WEEE in a non-destructive manner, must be removed by end users from the WEEE in a non-destructive manner before it is handed over to a collection point.

Distributors of electrical and electronic equipment are legally obliged to provide free take-back of waste. Conrad provides the following return options **free of charge** (more details on our website):

- in our Conrad offices
- at the Conrad collection points
- at the collection points of public waste management authorities or the collection points set up by manufacturers or distributors within the meaning of the ElektroG

End users are responsible for deleting personal data from the WEEE to be disposed of.

It should be noted that different obligations about the return or recycling of WEEE may apply in countries outside of Germany.

17 Technical data

Power supply	12 - 18 V/DC
Power consumption	standby <= 60 mA; max. <= 150 mA
Frequency range	124.57 - 125.42 kHz
Transmission power	19.06 dBm
Max. reading distance	approx. 2 cm
Data retention in case of a power cut	yes
Suitable transponders	Commercially available EM transponders for frequency 125 kHz
Output	Floating 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
Memory cells for transponders/PINs	900 (of which 890 user transponders/PINs and 10 visitor transponders/PINs)
Memory cells for fingerprints	100 (of which 99 user fingerprints and 1 master fingerprint)
Mounting location	indoors/outdoors
Protection class	IP55
Ambient conditions	temperature -30 °C to +60 °C
Cable length	approx. 30 cm
Dimensions	168 x 52 x 32 mm (H x W x D)
Weight	approx. 201 g

2615507_V1_1122_02_VTP_m_en