



Ⓒ Operating Instructions

Access System – Wi-Fi/RFID/Fingerprint

Item no. 3060831

|



1 Table of contents



2	Introduction	53
3	Product documentation	53
4	Intended use	53
5	Delivery content	54
6	Explanation of symbols	54
7	Safety instructions	55
8	Controls and connections	56
9	Installation and connection	57
	9.1 Installation	57
	9.2 Connecting to a conventional power supply	58
	9.3 Connecting to alarm system	59
	9.4 Wiegand interface	60
	9.4.1 Using the access system as an external reader	60
	9.4.2 Connecting an external reader to the access system	61
	9.5 Connect two access systems for interlock mode	62
10	Setup	63
11	Getting started	63
12	Programming	64
	12.1 Good practice	64
	12.2 General information	64
	12.3 Resetting all settings to factory defaults; teaching in master transponders	65
	12.3.1 Resetting the access system and teaching in the master transponder	65
	12.3.2 Resetting the access system without teaching in a master transponder	65
	12.3.3 Overview of the default settings	66
	12.4 Enabling/disabling programming mode	66
	12.5 Changing master code	67
	12.6 Teaching in/deleting the master fingerprint	67
	12.6.1 Teaching in master fingerprint	67
	12.7 Deleting master fingerprint	67
	12.8 Setting the Wiegand interface mode	68
	12.9 Configure open door detection	69
	12.10 Enable/disable interlock mode	70
	12.11 Selecting access mode	71
	12.12 Saving user PIN	72
	12.12.1 Automatically saving a user PIN in the next free memory cell	72

12.12.2	Assigning a user PIN to a specific memory cell	73
12.13	Deleting user PIN.....	74
12.13.1	Deleting a user PIN.....	74
12.13.2	Deleting a user PIN via memory cell number.....	74
12.14	Teaching in user transponders.....	75
12.14.1	Automatically saving a user transponder in the next free memory cell.....	75
12.14.2	Assigning a user transponder to a specific memory cell.....	76
12.14.3	Teaching in multiple user transponders with consecutive transponder number.....	76
12.14.4	Teaching in user transponders via collective mode	77
12.15	Deleting user transponder	78
12.15.1	Deleting a user transponder via transponder	78
12.15.2	Deleting a user transponder via transponder number.....	78
12.15.3	Deleting a user transponder via memory cell number	79
12.16	Teaching in a user fingerprint.....	79
12.16.1	Automatically saving a user fingerprint in the next free memory cell.....	79
12.16.2	Assigning a user fingerprint to a specific memory cell.....	80
12.17	Deleting user fingerprint.....	80
12.17.1	Deleting a user fingerprint via fingerprint	81
12.17.2	Deleting a user fingerprint via memory cell number.....	81
12.18	Clearing all memory cells.....	82
12.19	Setting the changeover contact activation time	82
12.20	Enabling or disabling protection against incorrect entries	83
12.21	Setting the alarm time for protection function	83
12.22	Enabling access for visitors	83
12.22.1	Teaching in a visitor transponder	84
12.22.2	Saving a visitor PIN.....	85
12.22.3	Deleting a visitor transponder or visitor PIN.....	85
12.23	Adding panic users	86
12.24	Enabling/disabling visual and acoustic indication	87
12.25	Enabling Wi-Fi	87
12.26	Transferring data between two access systems	88
12.27	Setting the Wiegand input data format	89
12.28	Setting the Wiegand output data format	90
13	Operation	91
13.1	Accessing via valid user PIN/transponder/fingerprint	91
13.2	Accessing via door opener button.....	91
13.3	Preventing the PIN from being revealed.....	91
13.4	Disabling the alarm/lock on incorrect entry.....	91

14	Troubleshooting	92
15	Declaration of Conformity (DOC)	94
16	Cleaning and maintenance	94
17	Disposal	94
18	Technical data	95
	18.1 Software	95
	18.2 Power supply	95
	18.3 Access	95
	18.4 Output	95
	18.5 Environment	95
	18.6 Others	95

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!

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

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

3 Product documentation

The product is documented by different sets of instructions:

- Safety information
- Programming sheet
- Installation and hardware operating instructions (for download)
- Mobile app setup and operating instructions (for download)



Use the link www.conrad.com/downloads (alternatively scan the QR code) to download the instructions (or new/current versions if available). Follow the instructions on the web page.

4 Intended use

This product is designed to prevent unauthorised access via doors (e.g. in an office) and to activate/disable alarm systems. The product can be controlled via the following authentication methods:

- Keypad (PIN authentication)
- Transponder (Smart card authentication)
- Fingerprint
- Mobile app (Tuya Smart Life - Smart Living) (PIN and remote authentication)

You can store a maximum of 900 PIN/transponders and 100 fingerprints for different user types.

Successful user authentication activates a potential-free relay changeover contact.

The product is intended for vertical installation on a wall and is suitable for indoor and outdoor use (IP66).

For safety and approval purposes, do not rebuild and/or modify this product. Using the product for purposes other than those described above may damage the product. In addition, improper use can cause hazards such as a short circuit, fire or electric shock.

Read the operating instructions carefully and store them in a safe place. Only make this product available to third parties together with its operating instructions.

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

5 Delivery content

- Access system (with 90cm cable)
- Master card
- L-key
- 2x screws
- 2x dowels
- 1N4004 diode (for relay changeover contact)
- Product documentation

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 (IP66).
- 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

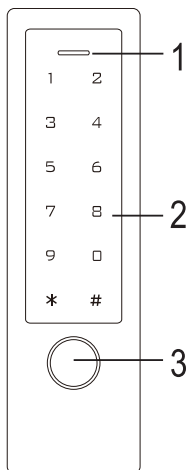
1 LED indicator

3 Fingerprint sensor with LED ring

2 Keypad with an integrated RFID sensor

Connection cable:

Colour	Inscription	Function
Red	DC+	Power supply 12 - 18 V/DC
Black	GND	GND/ground
Blue	Relay NO	NO (normally open) contact of relay
Purple	Relay common	Common connection for relay output
Orange	Relay NC	Normally closed relay output (Install diode provided)
Brown	Contact input	Door/Gate contact input (normally closed)
Grey	Alarm output	NC (normally closed) contact of relay
Yellow	OPEN	Request to exit (REX) Input
White	D1	Wiegand data1
Green	D0	Wiegand data0



→ When the access system is connected to a Wiegand controller as an external reader, 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



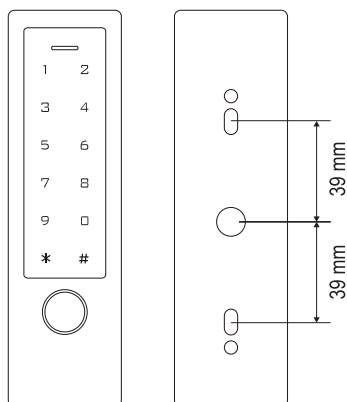
Ensure that the connection cables are not kinked or squashed. This can cause malfunctions, short circuits and device defects. Ensure that no cables or wires are damaged when drilling holes or tightening screws. Installation and connection may only be carried out when the power supply is switched off.

9.1 Installation



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".



- Remove the screw from the lower end of the access system.
- Lift the access system from the mounting plate and remove the front panel.
- Mount the mounting plate at the installation location using suitable screws and wall plugs.
- Attach the access system to the mounting plate and secure it with the screw again.

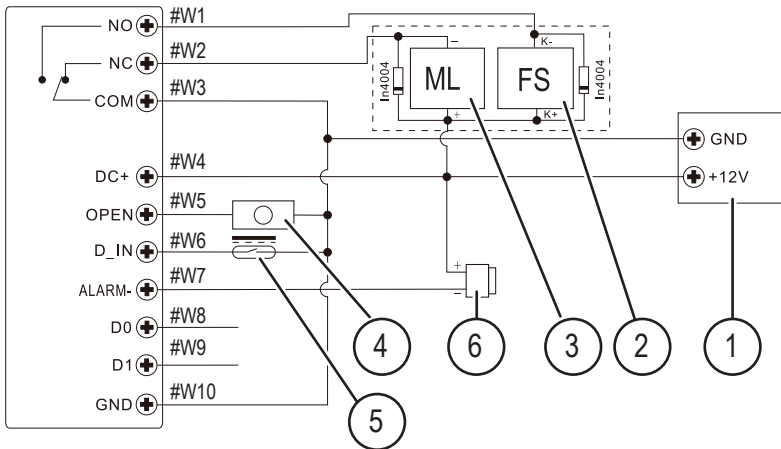
9.2 Connecting to a conventional power supply

Connect the access system to a conventional power supply using the option that serves your use case:

- **Fail-secure door opener:** The door opener releases the locking latch only if its operating voltage is applied (common design for front doors).
- **Fail-safe door opener:** The door opener releases the locking latch only if 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).

Fail-secure door opener

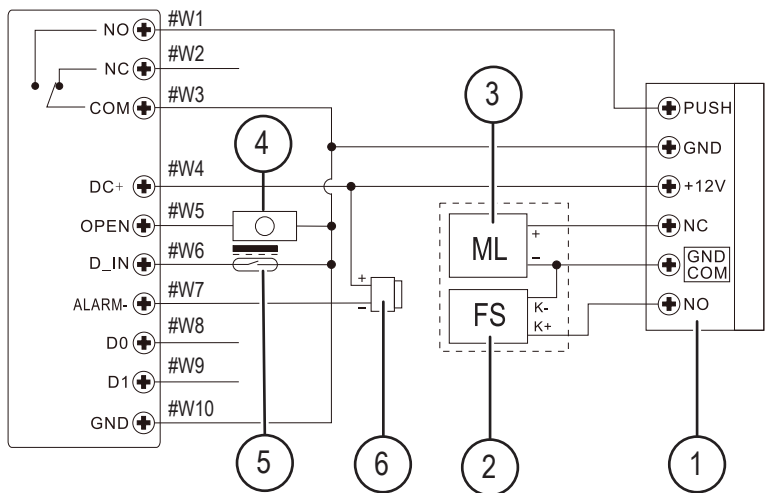
→ The included diode must be connected correctly near the door opener to protect the access system from voltage surges. Observe the connection direction.



	Component		Component
1	Power supply	4	Exit button
2	Fail-secure lock	5	Door contact
3	Magnetic lock or Fail-safe lock	6	Alarm

	Wire colour		Wire colour
#W1	Blue	#W6	Brown
#W2	Orange	#W7	Grey
#W3	Purple	#W8	Green
#W4	Red	#W9	White
#W5	Yellow	#W10	Black

Fail-safe door opener



	Component		Component
1	Power supply	4	Exit button
2	Fail-secure lock	5	Door contact
3	Magnetic lock or Fail-safe lock		

	Wire colour		Wire colour
#W1	Blue	#W6	Brown
#W2	Orange	#W7	Grey
#W3	Purple	#W8	Green
#W4	Red	#W9	White
#W5	Yellow	#W10	Black

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.

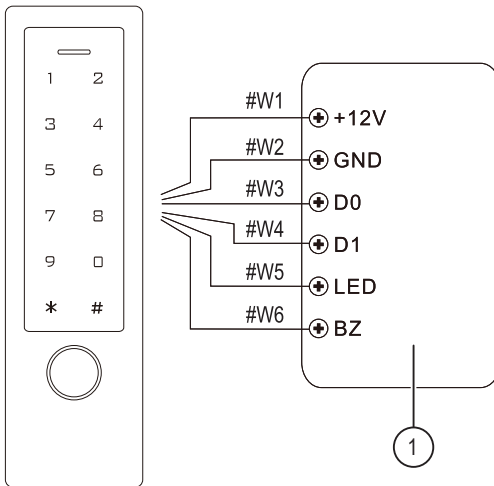
9.4 Wiegand interface

The Wiegand interface of the access system can be used in two different ways.

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 program the bit rate for data transfer, which must be the same as that of the Wiegand controller. Follow the operating instructions for the Wiegand controller.



	Component
1	Access controller

	Wire colour		Wire colour
#W1	Red	#W4	White
#W2	Black	#W5	Brown
#W3	Green	#W6	Yellow

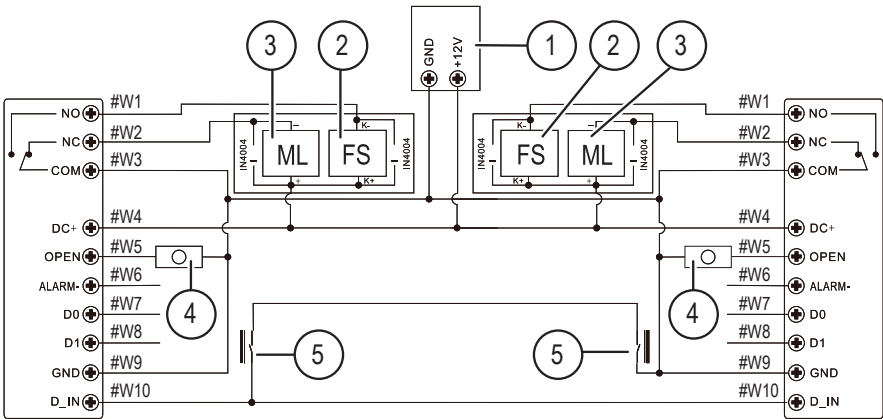
9.4.2 Connecting an external reader to the access system

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 are supported.
- 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. Always follow the operating instructions for the external card reader.
- With the access system, you can programme the bit rate for data transfer, which must be the same as that of the reader. Follow the operating instructions for the reader.

9.5 Connect two access systems for interlock mode

For the interlock mode, you configure two access systems and two doors. The two access systems ensure that only one door can be open at a time: if one door is open, the other door must be closed.



	Component		Component
1	Power supply	4	Exit button
2	Fail-secure lock	5	Door contact
3	Magnetic lock or Fail-safe lock		

	Wire colour		Wire colour
#W1	Blue	#W6	Grey
#W2	Orange	#W7	Green
#W3	Purple	#W8	White
#W4	Red	#W9	Black
#W5	Yellow	#W10	Brown

- Wire the interlock function according to the wiring diagram.
- Before you can use the interlock mode, you must configure it on both devices. Refer to [“12.10 Enable/disable interlock mode” on page 23](#) for details.

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. The access system is ready for programming.

11 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.

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). See [“12.3 Resetting all settings to factory defaults: teaching in master transponders” on page 18.](#)
- Think of a master code (should consist of 6 digits) and programme it. The default master code is “123456” (or after resetting the access system). See [“12.5 Changing master code” on page 20.](#)
- If desired, teach in a master fingerprint (which allows quick and easy access to the teach-in and delete mode). See [“12.6 Teaching in/deleting the master fingerprint” on page 20.](#)
- Select the desired access mode. See [“12.11 Selecting access mode” on page 24.](#)
- Set the changeover contact activation time to be used e.g. for switching a door lock (default setting is 5 seconds). See [“12.19 Setting the changeover contact activation time” on page 35.](#)
- If desired, enable protection against incorrect entries. See [“12.20 Enabling or disabling protection against incorrect entries” on page 36](#) and [“12.21 Setting the alarm time for protection function” on page 36.](#)
- You can now proceed to save user PIN, transponders and fingerprints depending on the set 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).
- **Interlock users:** If you connected two devices to operate in interlock mode, configure the interlock mode. See [“12.10 Enable/disable interlock mode” on page 23.](#)

12 Programming

12.1 Good practice

- Note down settings. You will thus be able to refer to them over time and adapt them to new requirements.
- 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.

12.2 General information

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 program 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 - 987: user PINs and/or user transponders (depending on access mode)
- Memory cell number 988 or 989: panic user groups
- Memory cell number 990 - 999: visitor PINs or visitor transponders
- 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.

12.3 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.

12.3.1 Resetting the access system and teaching in the master transponder

→ You can only have **one** master transponder registered at a time. If you have already taught in a master transponder, it will automatically be deleted through the teach-in of another 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.

12.3.2 Resetting the access system without teaching in a 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.

12.3.3 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

12.4 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.

12.5 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 ["12.4 Enabling/disabling programming mode" on page 19](#); 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.

12.6 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.

12.6.1 Teaching in master fingerprint

- Enable the programming mode as described in ["12.4 Enabling/disabling programming mode" on page 19](#) 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.

12.7 Deleting master fingerprint

- Enable the programming mode as described in ["12.4 Enabling/disabling programming mode" on page 19](#) 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.

12.8 Setting the Wiegand interface mode

The access system can function as an external reader for a Wiegand controller or as a Wiegand controller for an external reader. The access system allows you to configure the desired mode.

- Enable the programming mode as described in [“12.4 Enabling/disabling programming mode” on page 19](#) 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).

12.9 Configure open door detection

Configure the door open detection to alert you if a door stays open beyond a set timer or if the door is pushed open with force. Door open detection only works if you connect an additional magnetic contact or if you use a built-in magnetic contact.

Mechanism	Description
Door stays open beyond the timer	If the door stays open for longer than the set timer, the built-in buzzer sounds. Closing the door stops the buzzer.
Door is pushed open	If the door is pushed open, the built-in buzzer sounds for a set amount of time (timer) and a connected alarm system (if any) is triggered. The alarm deactivates after the set timer elapses. The alarm can be deactivated by an authorized person.

Enabling/disabling open door detection

All mechanisms are activated or deactivated at the same time. The set timer applies to both mechanisms.

Enabling detection	Disabling detection	Key combinations/Operation
1. Activate the programming mode	1. Activate the programming mode	[*] (Mastercode) [#]
	2. Disable open door detection	[6] [3] [#]
2. Enable open door detection		[6] [4] [#]
3. Set the timer		[5] (0 ... [3]) [#] (0, [1] = 1 minute, [3] = 3 minutes) Suppress any alarm by setting the timer to 0.
4. Exit programming mode	3. Exit programming mode	[*]

Deactivating alarms

Mechanism	Deactivating alarms
Door stays open beyond time threshold	■ Close the door. ■ Use a registered master/normal transponder, master/normal fingerprint, master/normal PIN to activate the access system (open the door).
Door is pushed open	■ Use a registered master/normal transponder, master/normal fingerprint, master/normal PIN to activate the access system (open the door).

12.10 Enable/disable interlock mode

After you connect two access systems to operate in interlock mode, you must enable the interlock mode on both access systems.

Enabling

Steps	Key combinations/Operation
1. Configure settings on the first access system.	Configure PINs, fingerprints and transponders on one device.
2. Transfer the settings of the first access system to the second access system.	Refer to „12.26 Transferring data between two access systems“ on page 41
3. Activate the programming mode on both devices.	 (Master code) 
4. Enable the interlock function on both devices.	9 0  (factory default)
5. Exit programming mode.	
6. Test the interlock mode.	1. Open the first door that is controlled by one access system. 2. Wait until the first door is closed. 3. Open the second door that is controlled by the second access system.

Disabling

Steps	Key combinations/Operation
1. Activate the programming mode on both devices.	 (Master code) 
2. Disable the interlock function on both devices.	9 1  (factory default)
3. Exit programming mode	

12.11 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 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 ["12.4 Enabling/disabling programming mode" on page 19](#) 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] + ([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.

12.12 Saving user PIN

The access system has 888 memory cells to store user PINs and/or user transponders. Memory cell numbers 100 - 987 are provided for PINs/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

12.12.1 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 ["12.4 Enabling/disabling programming mode" on page 19](#) 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.

12.12.2 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 [“12.4 Enabling/disabling programming mode” on page 19](#) 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 (**[1]** **[0]** **[0]** **[9]** **[8]** **[7]**) 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.
- 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]** **[7]**) 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.

12.13 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.

12.13.1 Deleting a user PIN

- Enable the programming mode as described in ["12.4 Enabling/disabling programming mode" on page 19](#) 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.

12.13.2 Deleting a user PIN via memory cell number

- Enable the programming mode as described in ["12.4 Enabling/disabling programming mode" on page 19](#) 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][7]**) 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.

12.14 Teaching in user transponders

The access system has 888 memory cells to store user PINs and/or user transponders. Memory cell numbers 100 - 987 are provided for PINs/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

12.14.1 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 ["12.4 Enabling/disabling programming mode" on page 19](#) 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.

12.14.2 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 ["12.4 Enabling/disabling programming mode" on page 19](#) 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 (**1 0 0** **9 8 7**) 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.

12.14.3 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 ["12.4 Enabling/disabling programming mode" on page 19](#) the LED starts to flash red.

- Enter programming code **1** to activate storage mode. The yellow LED will then light up.

- Enter the memory cell number (**1 0 0** **9 8 7**) 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. 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.

12.14.4 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 ["12.4 Enabling/disabling programming mode" on page 19](#) 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.

12.15 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.
- Clear the memory cell in which the user transponder is stored.

12.15.1 Deleting a user transponder via transponder

- Enable the programming mode as described in ["12.4 Enabling/disabling programming mode" on page 19](#) 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 **X** button.

12.15.2 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 ["12.4 Enabling/disabling programming mode" on page 19](#) 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 **X** button.

12.15.3 Deleting a user transponder via memory cell number

- Enable the programming mode as described in ["12.4 Enabling/disabling programming mode" on page 19](#) 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]** **[7]**) 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.

12.16 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

12.16.1 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 ["12.4 Enabling/disabling programming mode" on page 19](#) 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.

12.16.2 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 ["12.4 Enabling/disabling programming mode" on page 19](#) 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.

12.17 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

12.17.1 Deleting a user fingerprint via fingerprint

- Enable the programming mode as described in "[12.4 Enabling/disabling programming mode](#)" on page 19 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.

12.17.2 Deleting a user fingerprint via memory cell number

- Enable the programming mode as described in "[12.4 Enabling/disabling programming mode](#)" on page 19 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 memory cell number ([0] [9] [8]) 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] [#] = Clear memory cell 6
- 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.

12.18 Clearing all memory cells

→ This option deletes all 1000 memory cells.

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

- Enable the programming mode as described in [“12.4 Enabling/disabling programming mode” on page 19](#) 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.

12.19 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 [“12.4 Enabling/disabling programming mode” on page 19](#) 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.

12.20 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 ["12.4 Enabling/disabling programming mode" on page 19](#) 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 ["12.21 Setting the alarm time for protection function" on page 36](#)); 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.

12.21 Setting the alarm time for protection function

With the [2] function (lock with alarm) activated as described in ["12.20 Enabling or disabling protection against incorrect entries" on page 36](#), 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 ["12.4 Enabling/disabling programming mode" on page 19](#) 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.

12.22 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.

12.22.1 Teaching in a visitor transponder

- Enable the programming mode as described in [“12.4 Enabling/disabling programming mode” on page 19](#) 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 **X** button.

12.22.2 Saving a visitor PIN

- Enable the programming mode as described in [“12.4 Enabling/disabling programming mode” on page 19](#) 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.

- 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.

12.22.3 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 [“12.15 Deleting user transponder” on page 31](#).
- For deletion of a PIN, see [“12.13 Deleting user PIN” on page 27](#).

12.23 Adding panic users

Panic users can trigger an extra security alarm to inform security personnel of a security incidence. For a panic user setup, an additional alarm is required. Two (2x) panic users can be registered in total.

Requirement

- User ID: 988, 989

Register a transponder

Steps	Key combinations/Operation
1. Activate the programming mode	[*] (Master code) [#]
2. Register the transponder.	Using the card: [1] (User ID) [#] (Read card) [#] Using the card number: [1] (User ID) [#] (8/10/17 digit card number) [#]
3. Exit the programming mode	[*]

Register a PIN

Steps	Key combinations/Operation
1. Activate the programming mode	[*] (Master code) [#]
2. Register the PIN.	PIN length: 4 - 6 digits (except 8888) [1] (User ID) [#] (PIN) [#]
3. Exit the programming mode	[*]

Deleting panic transponders and PINs

- For deletion of a transponder, see [“12.15 Deleting user transponder” on page 31.](#)
- For deletion of a PIN, see [“12.13 Deleting user PIN” on page 27.](#)

12.24 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 ["12.4 Enabling/disabling programming mode" on page 19](#) 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.

12.25 Enabling Wi-Fi

- Connect the access system to the power supply to activate Wi-Fi.

12.26 Transferring data between two access systems

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

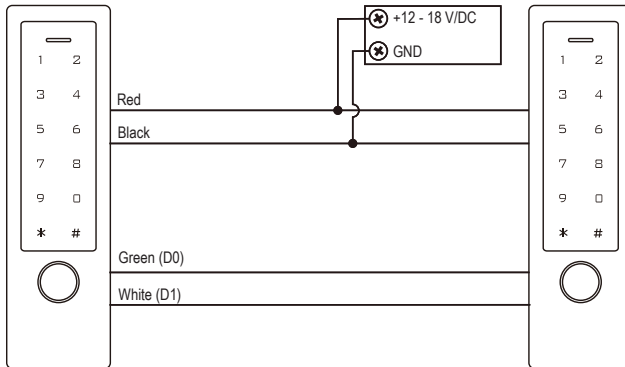
→ Please note:

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 ["12.4 Enabling/disabling programming mode" on page 19](#); 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).

12.27 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).

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 ["12.4 Enabling/disabling programming mode" on page 19](#) 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.

12.28 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.

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 [“12.4 Enabling/disabling programming mode” on page 19](#) 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.

13 Operation

13.1 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).

- If the user must enter more than one credential to authenticate (example: transponder + PIN), the user must enter all credentials within 5 seconds. After 5 seconds, the access system goes into standby mode. Refer to [“12.11 Selecting access mode” on page 24](#) for details.

13.2 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.

13.3 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.

13.4 Disabling the alarm/lock on incorrect entry

If the protection against incorrect entries 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** is enabled, it can be early terminated by briefly disconnecting the access system from the power supply.

Refer to [“12.20 Enabling or disabling protection against incorrect entries” on page 36](#) for configuration details.

14 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 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. 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. Refer to [“12.11 Selecting access mode” on page 24](#).

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

- This is normal.

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. 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.

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.
- Programme the Wiegand interface. For instructions, see [“12.27 Setting the Wiegand input data format” on page 42](#) and [“12.28 Setting the Wiegand output data format” on page 43](#).
- Always follow the operating instructions for the unit to be connected to the Wiegand interface.

15 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.

16 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.

17 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.

18 Technical data

18.1 Software

Mobile app Tuya Smart Life – Smart Living

18.2 Power supply

Power supply 12-18V/DC

Current consumption standby ≤ 60 mA; max. ≤ 150 mA

18.3 Access

Wiegand interface Yes; 26 - 44 bits input and output

Suitable transponders Commercially available EM transponders for frequency 125 kHz

Data retention in case of a power cut Yes

Card reading distance max. 3 cm

Card frequency range 124.6 - 125.4 kHz

Card transmission power 11.62 dBm

Memory cells for transponders/PINs 1000 (988 common user, 2 panic users, 10 visitor users)

Memory cells for fingerprints 100 (of which 99 user fingerprints and 1 master fingerprint)

WiFi frequency 2.4GHz

WiFi standard IEEE 802.11b/g/n

WiFi frequency range 2412 - 2472 MHz

WiFi transmission power 16.39 dBm

WiFi distance max. 25 m (in open area)

18.4 Output

Type 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)

18.5 Environment

Mounting location Indoors/outdoors

Protection class IP66

Ambient conditions Temperature -30 to +60°C

18.6 Others

Material Zinc-alloy

Cable length approx. 90 cm

Dimensions (WxHxD) 166 x 45 x 22 mm

Weight approx. 387g

GB This is a publication by Conrad Electronic SE, Klaus-Conrad-Str. 1, D-92242 Hirschau (www.conrad.com).

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

Copyright 2024 by Conrad Electronic SE.