



## **DNT000013 Fingerprint Code Lock BioAccess PRO User Manual**

[Home](#) » [dnt](#) » **DNT000013 Fingerprint Code Lock BioAccess PRO User Manual** 



**Fingerprint code lock BioAccess PRO  
Item Number: DNT000013  
User Manual**

Please read this user manual carefully before installation as well as first operation and save it for later reference. If you allow other persons to use this device, please hand over this user manual as well.

## Contents

- 1 Function
- 2 Proper Use, Scope of Supply
- 3 Operating, Service, and Safety Instructions
- 4 Installation/Assembly
- 5 Programming
  - 5.1 Resetting Device to Default Settings and Reading of Master Card
  - 5.2 Operation/Programming – Brief Overview
  - 5.3 Programming of Operating Mode
  - 5.4 Save User Fingerprints with Automatic ID Allocation
  - 5.5 Save User Fingerprints with Manual ID Allocation
  - 5.6 Save User Numerical Code (PIN) with Automatic ID Allocation
  - 5.7 Save User Numerical Code (PIN) with Manual ID Allocation
  - 5.8 xx123434xx or xx123434 x= 0...9
  - 5.9 Save User RFID Cards with Manual ID Allocation
  - 5.10 Save User RFID in the Block
  - 5.11 Use of Master Fingerprint/Master Card in order to Add/Delete Users
  - 5.12 Entry of Users for the Panic Function (Activation of Panic Alarm)
  - 5.13 Entry of Visitors
  - 5.14 Change User PIN
  - 5.15 Adjust Behaviour of Switching Relay
  - 5.16 Adjust Type of Access
  - 5.17 Alarm/Interlock in Case of Manipulation/Failed Attempts, End Alarm
  - 5.18 Registration/Alerting in Case of Door Open Detection
  - 5.19 Programming of Audible Signals and Visual Displays
- 6 Operation
- 7 Wiegand Interface
- 8 Extended Functions
- 9 Connection of Two Systems (Lock)
- 10 Technical Data
- 11 Declaration of Conformity
- 12 Disposal
- 13 Contact
- 14 Documents / Resources
  - 14.1 References
- 15 Related Posts

## Function

The fingerprint code lock BioAccess PRO allows for simple access via the biometric identifier “fingerprint” as well as via RFID transponder and numerical code. For the sake of increased access security, multiple types of access can be combined. The weatherproof and vandal-proof device is capable of administering up to 1000 accesses. By means of a 26/44-bit Wiegand interface, a particularly safe data transmission/navigation via external Wiegand controller is possible. The device is able to interact with Wiegand controllers, to function as a Wiegand controller itself, or to function as a stand-alone device.

- Robust, weatherproof (IP66), and vandal-proof fingerprint code lock
- Capacitive fingerprint sensor, touch keypad
- EM RFID (125 kHz) and MiFare (13,56 MHz) RFID access
- Numerical code access with 4 to 6 digits, backlit input field with automatic shutdown after 20 s
- For up to 1000 accesses (100 fingerprints + 888 RFID cards/PINs + 2 panic codes + 10 visitors)
- Programmable relay switch output, potential-free

- 26/44-bit Wiegand interface, MiFare: 56/58-bit in-/output, access data administration in Wiegand controller
- Stand-alone operation or interlock operation for 2 doors possible
- Latch mode (self-sustaining operation to keep the door open) available
- Door contact monitoring
- Door opener button input (exit button) for door opener control from the inside
- Fail secure lock or fail safe lock operation
- Access via fingerprint, RFID, numerical code, or combination of different types of access possible
- Sabotage sensor against disassembly/manipulation
- Multi-colour status display
- Internal signal transmitter and external signal output

## Proper Use, Scope of Supply

The BioAccess PRO is intended for use as general access control device. It is admitted for exterior use (IP66). We assume no liability for consequential damages resulting from non-observance of these rules for use as well as this user manual, warranty claims lapse as well. This also applies to modifications and changes.

### Scope of Supply:

- Fingerprint code lock BioAccess PRO
- Protective diode IN4004
- 2x wall plugs and mounting screws (4x 25 mm)
- Mounting key
- User manual
- RFID master card

## Operating, Service, and Safety Instructions



### Warning

Is used to mark safety instructions or to draw attention to special dangers and risks.



### Notice

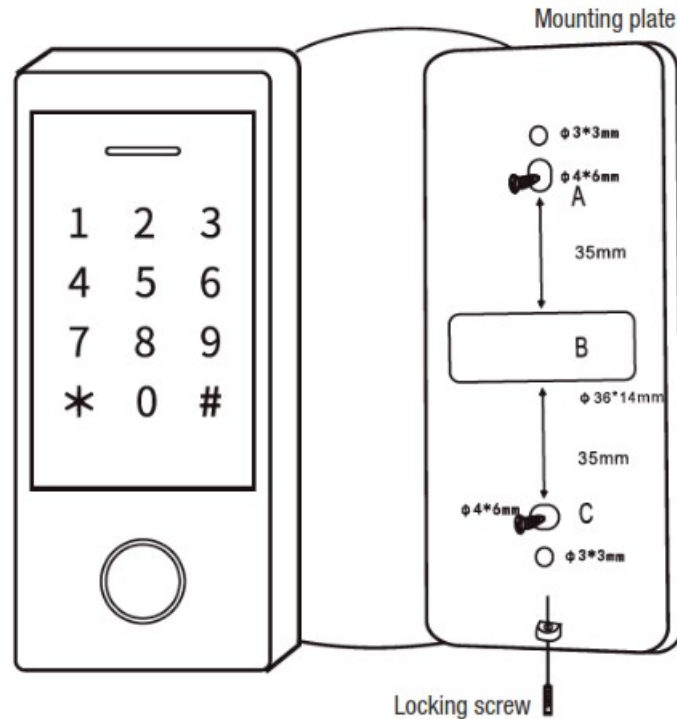
Is used to mark additional information or important notices.

- For safety and approval reasons (CE), any unauthorised modifications and/or changes of the product are not allowed.
- Do not expose the device to an influence of humidity exceeding the IP66 conditions, vibrations, constant heat, extreme cold, strong electromagnetic fields, and mechanical stress.
- Observe all notices in the user manual concerning the connection of voltages. Wrong or polarity-reversed voltages will destroy the device.
- Do not leave packaging material lying around, plastic foils/bags, polystyrene parts, etc. can become a dangerous toy for children.
- If the device has been damaged, put it out of operation and contact our service.

In case of property or personal damage caused by improper handling or non-observance of the safety instructions and the user manual, we assume no liability. In such cases, any warranty claims lapse! We assume no liability for consequential damages.

Do not open the device, do not attempt to repair the device, do not perform any modifications or changes – this will lead to the loss of any warranty claims. We assume no liability for consequential damages.

## Installation/Assembly



When choosing the installation site, make sure that the mounting plate lies tight and flat on its supporting surface while making contact with all four corners. Otherwise, acts of sabotage can be facilitated, and faulty activations of the sabotage alarm due to unwanted incidence of light into the device are possible.

- Loosen the locking screw at the bottom of the enclosure with the mounting key and remove the device from the mounting plate.
- Mark the drill holes on the site of installation (wall) by means of the holes in the mounting plate or the illustration above and, after checking for electrical lines or pipes within the wall, drill the mounting holes or the cable bushing. The 3 mm holes are intended to be an additional safeguard for the possible installation on, for example, a metal plate by means of threaded bolts. In case of non-use, they should be sealed by means of a sealant.
- Run the connecting cable through the wall and screw the mounting plate to the wall.
- Place the device onto the mounting plate (first insert it at the top, then tilt it down towards the mounting plate) and secure it with the locking screw.

## Pin Assignment

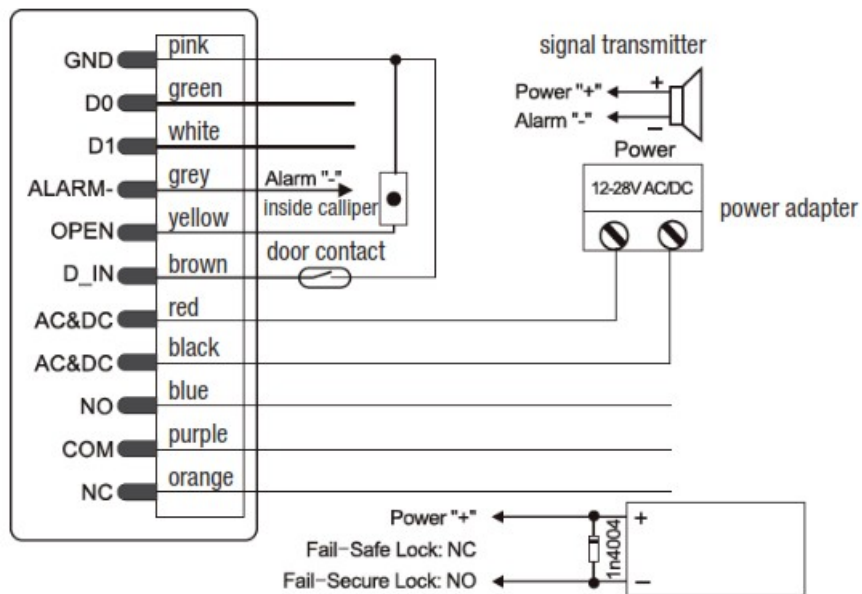
Wire Colour red	Function	Remarks
black	UB	operating voltage, 12–28 VAC/DC, DC = plus
pink	UB	operating voltage, 12–28 VAC/DC, DC = minus
blue	GND	ground line, see notes in the text
purple	relay, NO	relay contact, open against COM in idle state
orange	relay, COM	relay contact, centre contact
yellow	relay, NC	relay contact, closed against COM in idle state
green	OPEN	input for door opener button in the building
white	Data 0	Wiegand interface, line Data 0
grey	Data 1	Wiegand interface, line Data 1
brown	alarm output	alarm output for signal transmitter, switched against minus
	door contact	input for door contact monitoring, NC

## Audio and Light Signals

Signal/Condition	Indicator LED	Audio Signal
standby	red	off
start programming mode	flashes red	1x
device in programming mode	orange	1x
error/incorrect entry	off	3x
end programming mode	red	1x
door opener active	green	1x
alarm	quickly flashing red	continuous tone

## Wiring Instructions

### 1. Simple Connection with Power Adapter



**fail-safe lock:** electric door opener or fail safe lock

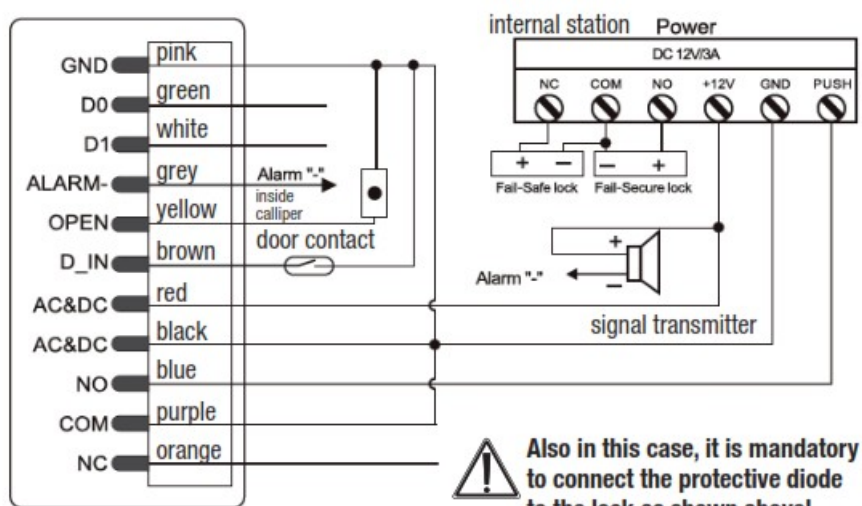
**fail-safe lock:** e.g. fail safe bolt lock: bolt retracted when in standby mode, lock opens due to pulse from control

**fail-secure lock:** e.g. fail secure bolt lock: bolt extracted when in standby mode, lock opens due to pulse from control



This type of power supply requires the supplied diode 1N4004 to be connected in parallel to the door opener or the electromagnetic lock, as shown in the diagram. This diode discharges inductive voltage peaks which occur when disabling the door opener. If it is not installed, high voltage peaks can destroy the fingerprint scanner! Please observe the correct polarity while connecting. The cathode corresponds to the colour ring on the diode.

## 2. Connection via Internal Station/Interface



**fail-safe lock:** electric door opener or fail-safe lock

**fail-safe lock:** e.g. fail safe bolt lock: bolt retracted when in standby mode, lock opens due to pulse from control

**fail-secure lock:** e.g. fail secure bolt lock: bolt extracted when in standby mode, lock opens due to pulse from control

## Programming

## Resetting Device to Default Settings and Reading of Master Card

In case you should not be able to successfully complete the programming steps described in the following according to the description, you should reset the device to its default settings. This also applies to passing on the device.



### **Please note!**

In the course of resetting the device, all saved access data are deleted as well!

The device reset only resets the master code and settings. All stored access data is retained. To delete them as well, please proceed as described in chapter 5.2.

- Connect the device to the power supply, but do not yet switch the power on.
- Press the inside calliper and hold it down while switching on the power supply.
- Let go of the inside calliper, the operating display changes to yellow, then you can read an EM/MiFare card or the supplied RFID card as a master card.
- Afterwards, the operating display changes to red – the device has been reset to its default settings. The read card is now the master card.

In case you do not wish to read a new master card (e.g. when passing on the device), you should hold the inside calliper down for about 5 s after switching on the power supply.

Also in this case, the operating display changes to red, and the previously read master card is invalid.

## **Operation/Programming – Brief Overview**

Hyphens are only supposed to provide clarity, do not type them in!

Function	Operation/Programming
Initiate programming	* – 123456 – # (default master code)
Enter personal/ new master code	0 – new code (6 digits) – # – repeat code – #
Delete user	2 – read fingerprint/user card/enter user PIN – # can be continued in this manner for further users
	2 – User ID – # can be continued in this manner for further users
	2 – RFID card number (8/10/17 digits)
Delete all users	2 – master code – #
Finish programming	*
Open door	read authorised fingerprint/PIN/RFID card – if
Delete alarm	enter master PIN/fingerprint/RFID card – # or enter authorised PIN/fingerprint/RFID card – #

**The programming differs depending on the type of access.  
Follow the respective programming instructions.**

**The allocation of user IDs facilitates the tracking of access attempts.**

#### **ID overview:**

- Fingerprint: 0...98; master fingerprint user ID: 99
- PIN/card: 100...987
- Panic use: 988, 989
- Visitors: 990...999

125 kHz cards (EM) or 13,56 MHz cards (MiFare) can serve as RFID cards.

In case of access via PIN, 4 to 6 digits are permitted.

**However, the digit sequence 8888 is excluded for the sake of special purposes.**

#### **Please note:**

- Do not enter user IDs with leading zero!
- If a user ID has been entered, it will be absolutely needed whenever changes of user data are to be carried out.

#### **Programming of Operating Mode**

The device can only be programmed for three operating modes: stand-alone/controller mode (with an additional reader with Wiegand interface), Wiegand reader for external controllers.

Function	Operation/Programming
Initiate programming	* – 123456 – # (default master code)
Stand-alone/controller mode	77 – # (default setting)
Wiegand reader	78 – #
Finish programming	*

#### **Save User Fingerprints with Automatic ID Allocation**

An automatic, continuous user ID allocation is carried out (1...98).

Function	Operation/Programming
Initiate programming	* – master code – # (default master code: 123456)
Read user fingerprint	1 – read fingerprint – repeat 2x reading of fingerprint (reading can be continued in this manner)
Finish programming	*

#### **Save User Fingerprints with Manual ID Allocation**

Function	Operation/Programming
Initiate programming	* – master code – # (default master code: 123456)
Read user fingerprint	1 – user ID (1...98) – # – read fingerprint – repeat 2x reading of fingerprint (reading can be continued in this manner)
Finish programming	*

#### Save User Numerical Code (PIN) with Automatic ID Allocation

Function	Operation/Programming
Initiate programming	* – master code – # (default master code: 123456)
Read user numerical code (PIN)	1 – PIN (4 to 6 digits) – # (reading can be continued in this manner) (Do not enter a leading zero for the user ID!)
Finish programming	*

#### Save User Numerical Code (PIN) with Manual ID Allocation

Function	Operation/Programming
Initiate programming	* – master code – # (default master code: 123456)
Read user numerical code (PIN)	1 – user ID (1...987) – # – PIN (4 to 6 digits) – # (Do not enter a leading zero for the user ID!)
Finish programming	*

#### Notes for PIN Allocation

For the sake of increased safety, you can “hide” your PIN in a digit sequence of up to 10 digits. This needs to have the following form (exemplary PIN: 123434):

**xx123434xx or xx123434 x= 0...9**

#### Save User RFID Cards with Automatic ID Allocation

An automatic, continuous user ID allocation is made (100...987).

Function	Operation/Programming
Initiate programming	* – master code – # (default master code: 123456)
Read user fingerprint	1 – read card/enter RFID card number (8/10/17 digits) – # (reading can be continued in this manner)
Finish programming	*

#### Save User RFID Cards with Manual ID Allocation

Function	Operation/Programming
Initiate programming	* – master code – # (default master code: 123456)
Read user fingerprint	1 – user ID (100...987) – # – enter RFID card number (8/10/17 digits) – # (reading can be continued in this manner)
Finish programming	*

#### Save User RFID in the Block

This allows the master to continuously save 987 cards in one run.  
This may take up to 2 minutes.

Function	Operation/Programming
Initiate programming	* – master code – # (default master code: 123456)
Read card into the block (card numbers must be consecutive)	1 – user ID (100...987) – # – amount of cards to be read – enter RFID card number of the first card (8/10/17 digits) – # (reading can be continued in this manner)
Finish programming	*

#### Use of Master Fingerprint/Master Card in order to Add/Delete Users

##### Read Master Fingerprint (ID=99)

Function	Operation/Programming
Initiate programming	* – master code – # (default master code: 123456)
Read master fingerprint	1 (99) – # – read fingerprint 3 times
Finish programming	*

#### Add/Delete Users with Master Fingerprint/Master Card

Function	Operation/Programming
Add user	<ol style="list-style-type: none"> <li>1. Read master fingerprint/master card</li> <li>2. Read user fingerprint (3x)/user card/user PIN – # (repeat step 2 for further users)</li> <li>3. Read master fingerprint/master card</li> </ol>
Delete user	<ol style="list-style-type: none"> <li>1. Read master fingerprint/master card twice within 5 s</li> <li>2. Read user fingerprint/user card/user PIN to be deleted (if required read more users according to step 2)</li> <li>3. Read master fingerprint/master card</li> </ol>

### Entry of Users for the Panic Function (Activation of Panic Alarm)

**Notice:** User ID=988/989; length of PIN = 4 to 6 digits, with the exception of 8888.

Function	Operation/Programming
Initiate programming	* – master code – # (default master code: 123456)
Add RFID card or PIN	1 – (988 or 989) – # – read card/RFID card number (8/10/17 digits) – # 1 – (988 or 989) – # – PIN – #
Finish programming	*

### Entry of Visitors

**Notice:** User ID = 990 ... 999; length of PIN = 4 to 6 digits, with the exception of 8888.

There are up to 10 visitor PINs/cards available which can be used for up to 10 accesses (0...9).

As soon as the specified number of accesses is reached, the PIN/card expires.

Function	Operation/Programming
Initiate programming	* – master code – # (default master code: 123456)
Add RFID card or PIN	1 – (990 ... 999) – # – (0 ... 9) – # – read card/RFID card number (8/10/17 digits) – # 1 – (990 ...999) – # – (0 ... 9) – # – PIN – #
Finish programming	*

### Change User PIN

**Notice:** In this case, you are working outside of the programming mode, users can carry out the changes themselves. Length of PIN = 4 to 6 digits, with the exception of 8888.

Function	Operation/Programming
Change PIN	1 – (user ID) – # – old PIN – # – new PIN – # – repeat new PIN #
Change PIN in case of combined access with PIN and card	1 – (read RFID card) – # – old PIN – # – new PIN – # -repeat new PIN #

### Adjust Behaviour of Switching Relay

Function	Operation/Programming
Initiate programming	* – master code – # (default master code: 123456)
Adjust active time of relay (pulse mode) or Adjust relay mode (latch)	3 – (1-99) – # (relay remains tightened for 1 to 99 s = door open, default setting: 5 s) 30 – # (permanently sets the relay into one position until the entry is carried out anew, then the relay permanently changes into the other position)  This setting is used, for example, if a door is supposed to be freely accessible for a longer period of time.
Finish programming	*

### Adjust Type of Access

In case of multiple access attempts with the same fingerprints/PINs, a period of 5 s must not be exceeded, otherwise the device will return to standby mode without reaction.

Function	Operation/Programming
Initiate programming	* – master code – # (default master code: 123456)
Exclusive access via PIN or Exclusive access via fingerprint or Exclusive access via RFID card or Access via PIN and RFID card or Exclusive access after entry by multiple users (2 to 9) (increased safety) or Access via fingerprint or PIN or RFID card	42 – # 40 – # 41 – # 43 – # 43 – (2...9) – # 44 – # (default setting)
Finish programming	*

### Alarm/Interlock in Case of Manipulation/Failed Attempts, End Alarm

After more than 10 incorrect entries, the device can deny any further entries for 10 minutes or trigger an alarm. Also in case of interlock, the door can still be opened by means of the door opener button inside of the building.

Function	Operation/Programming
Initiate programming	* – master code – # (default master code: 123456)
Disable alarm/interlock or Activate alarm/interlock or Activate alarm/interlock (acoustic) Activate alarm with alarm time limit	60 – # (default setting) 61 – # (access blocked for 10 minutes after failed attempts) 62 – # (access blocked after 10 failed attempts – acoustic alarm) 5 (0–3) – # (default setting 1 minute; 0=inactive) (end alarm via master code – # or enrolled fingerprint – # or enrolled PIN – #)
Finish programming	*

### Registration/Alerting in Case of Door Open Detection

#### 1. Detection of a door that has been open for too long (DOTL)

If you use an external magnetic door contact at the door or inside of the door lock for the sake of surveillance, an alarm can be triggered if the door has not been closed after the expiration of one minute after a proper door lock activation. Then, the integrated alarm transmitter will sound to remind you of closing the door. The alarm can be ended by closing the door, by the master user or by normal authorised users (fingerprint/PIN/RFID card). Otherwise, the alarm will carry on according to the adjusted alarm duration as described in chapter 5.17.

#### 2. Detection of a break-in

If the external door contact is triggered without a previous authorised opening via fingerprint/PIN/RFID card, this is registered as an attempted break-in, and the alarm is triggered within the device and, if connected, through the external alarm transmitter. The alarm can be ended by closing the door, by the master user or by normal authorised users (fingerprint/PIN/RFID card). Otherwise, the alarm will carry on according to the adjusted alarm duration as described in chapter 5.17. This also applies to the activation of the sabotage function in case of attempted disassembly of the device.

Function	Operation/Programming
Initiate programming	* – master code – # (default master code: 123456)
Disable detection or Activate detection	63 – # (default setting) 64 – #
Finish programming	*

### Programming of Audible Signals and Visual Displays

If the automatic keypad lighting is activated, it will automatically turn on when pressing any button. Only afterwards, a regular entry will be registered.

Function	Operation/Programming
Initiate programming	* – master code – # (default master code: 123456)
Disable audible handshaking signal Activate or Operating display always off Operating display always on or Keypad lighting always off Keypad lighting always on automatically switch off keypad lighting after 20 s	70 – # 71 – # (default setting) 72 – # 73 – # (default setting) 74 – # 75 – # 76 – # (default setting)
Finish programming	*

## Operation

### Open the door exclusively via fingerprint/RFID card

- Lay on enrolled RFID card or enrolled finger

### Open the door exclusively via PIN

- Enter enrolled PIN, confirm with #

### Open the door via multi-user PIN/fingerprint/RFID card

- Lay on/enter enrolled multi-user access (2–9 users, see chapter 5.16)

### Open the door via PIN or fingerprint or RFID card

- Lay on/enter enrolled access (see chapter 5.16)

### End alarm

- Enter enrolled PIN or lay on enrolled finger or master fingerprint or enter master code #

## Wiegand Interface

Wiegand is a standardised interface for the exchange of data between access control devices and control panels. It is used for the data transfer from the reader to a control device. This provides an especially safe system, as no access data have to be saved in the reader.



In the interaction with a control panel/RFID controller, the device has to be supplied with 12 VDC voltage! In this case, the black wire is not connected!

### Note:

When using the 4-bit pin output format in connection with a Wiegand interface, all three input versions can be used (number code, RFID and fingerprint together or in any combination). When changing to the 10-bit pin output format, the fingerprint version cannot be used, as this could lead to a security gap.

The interface requires four wires:

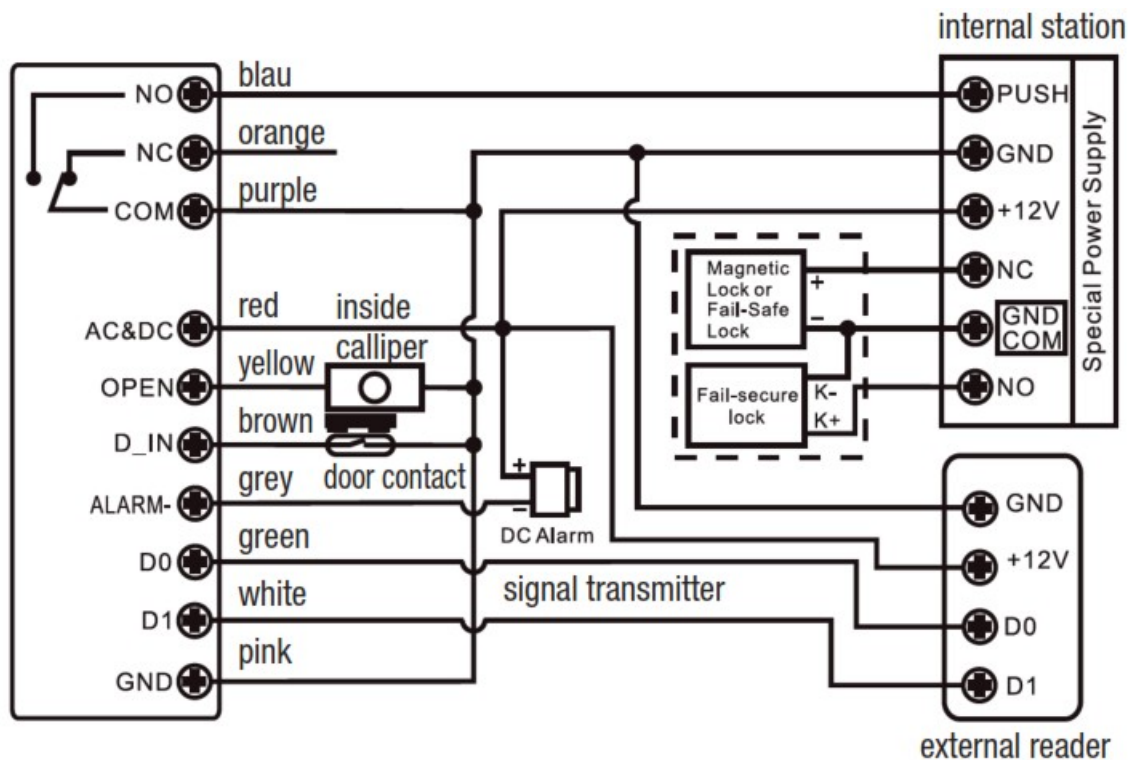
- +12V (red wire, in case of power supply over the interface)
- Ground (GND, pink wire)

- Data line DATA 0 (green wire)
- Data line DATA 1 (white wire)

In the case of controllers which are equipped with outputs for a handshaking LED and a signal transmitter within the door device, the wires D-IN (brown) and OPEN (yellow) are used as well.

### Connection to an External Access Device (Reader) with Wiegand Interface

The device can interact with another reader with Wiegand interface. For this purpose, the device has to be set into operating mode 77 (see chapter 5.3.).



Also in this case, it is mandatory to connect the protective diode to the door opener as shown in chapter 4 (wiring instructions)!

For the connection between fingerprint code lock and external reader, the same Wiegand format has to be used for both devices.

Function	Operation/Programming
Initiate programming	* – master code – # (default master code: 123456)
Adjust Wiegand format	8 – (EM: 26...44; MiFare: 26 ...44, 56, 58) – # (default setting: 26 bit)
Disable parity bit Activate parity bit	80 – # (for Wiegand reader with 32-, 40-, or 56-bit output) 81 – # (default setting)
Finish programming	*

### Programming

The basic programming corresponds to the stand-alone programming. The discrepancies are summarised in the following:

When connecting an EM/MiFare reader, users can be registered or deleted in both readers. When connecting an HID card reader, users can only be registered or deleted in the external device.

#### Example for the embedding of a fingerprint reader:

Step 1: Read the fingerprint into the external device.

Step 2: Read the same fingerprint into the DT access device.

Function	Operation/Programming
Initiate programming	* – master code – # (default master code: 123456)
Version 1 or Version 2	1 – read fingerprint into external device – # (automatic ID allocation) 1 – (user ID) – # read fingerprint into external device – # (use allocated ID)
Finish programming	*

#### Example for the embedding of a numerical code reader:

The reader has to support the 4-, 8-, or 10-bit output format.

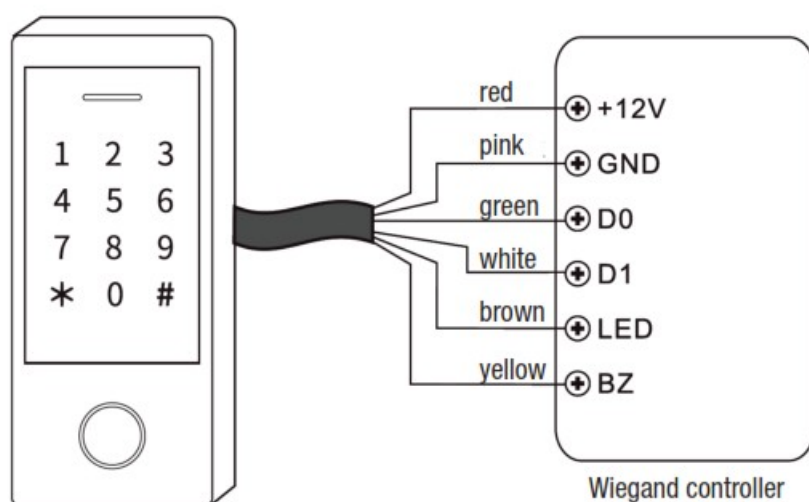
Function	Operation/Programming
Initiate programming	* – master code – # (default master code: 123456)
PIN input format	8 (4/8/10) – # (default setting: 4 bit)
Finish programming	*

In order to add PINs, they can be trained in all included devices. The deletion of PINs also has to be carried out in all included devices.

#### Operation as a Wiegand Reader with a Wiegand Controller

The device can function as an external Wiegand reader in combination with a Wiegand controller.

For this purpose, the device has to be set into operating mode 78 (see chapter 5.3.).



#### Please note:

- In the case of this connection, numerous settings of the device become invalid since they are carried out from

the external Wiegand controller.

- The brown wire (D\_IN) leads to access signalling through green flashing of the operating display (low-active).
- The yellow wire (OPEN) leads to access signalling through the internal signal transmitter (low-active).

## Adjust Wiegand Formats

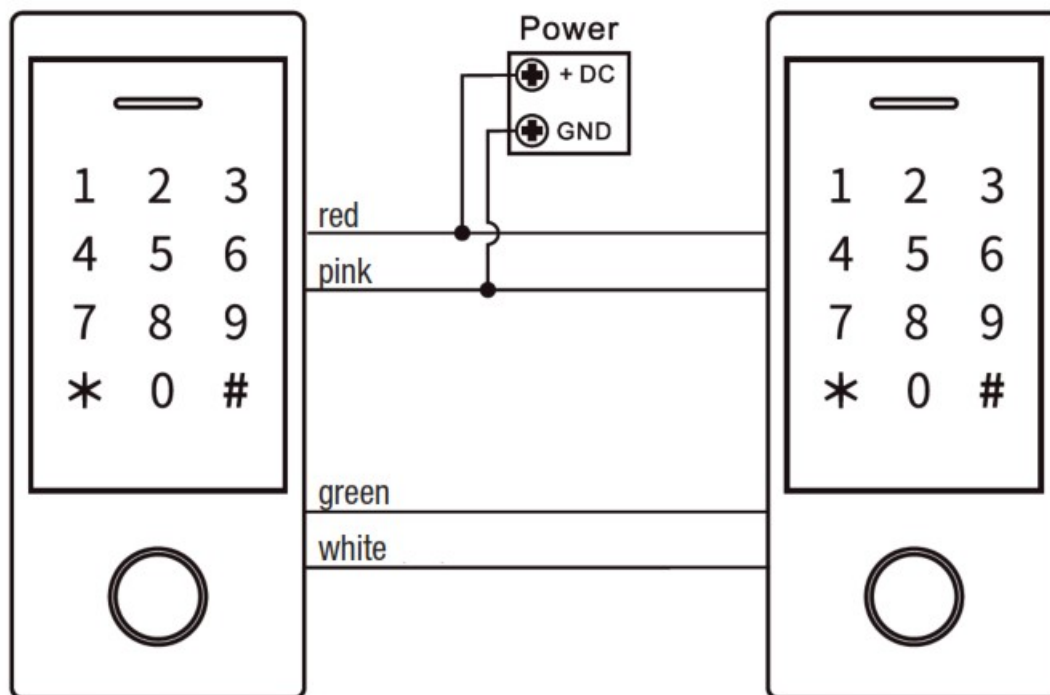
- For the access device, you should use the same Wiegand output format as the input format you are using in the case of the Wiegand controller.
- Disable parity bit in the case of Wiegand controllers with 32-/40-/56-bit input format

Function	Operation/Programming
Initiate programming	* – master code – # (default master code: 123456)
Wiegand output format PIN output format	8 – (EM: 26 ... 44; MiFare: 26 ... 44, 56, 58) – # (default setting EM: 26 bit; MiFare: 34) 8 (4/8/10) – # (default setting 4 bit) <b>(Note:</b> When using the 4-bit pin output format in connection with a Wiegand interface, all three input versions can be used (number code, RFID and fingerprint together or in any combination). When changing to the 10-bit pin output format, the fingerprint version cannot be used, as this could lead to a security gap.)
Disable parity bit Activate parity bit	80 – # 81 – # (default setting)
Finish programming	*

## Extended Functions

### Passing on of User Data

User data can be exchanged between two devices of the same type. This facilitates the programming of multiple accesses by the same users. The exchange is only possible for RFID card or PIN accesses.



**Please note:**

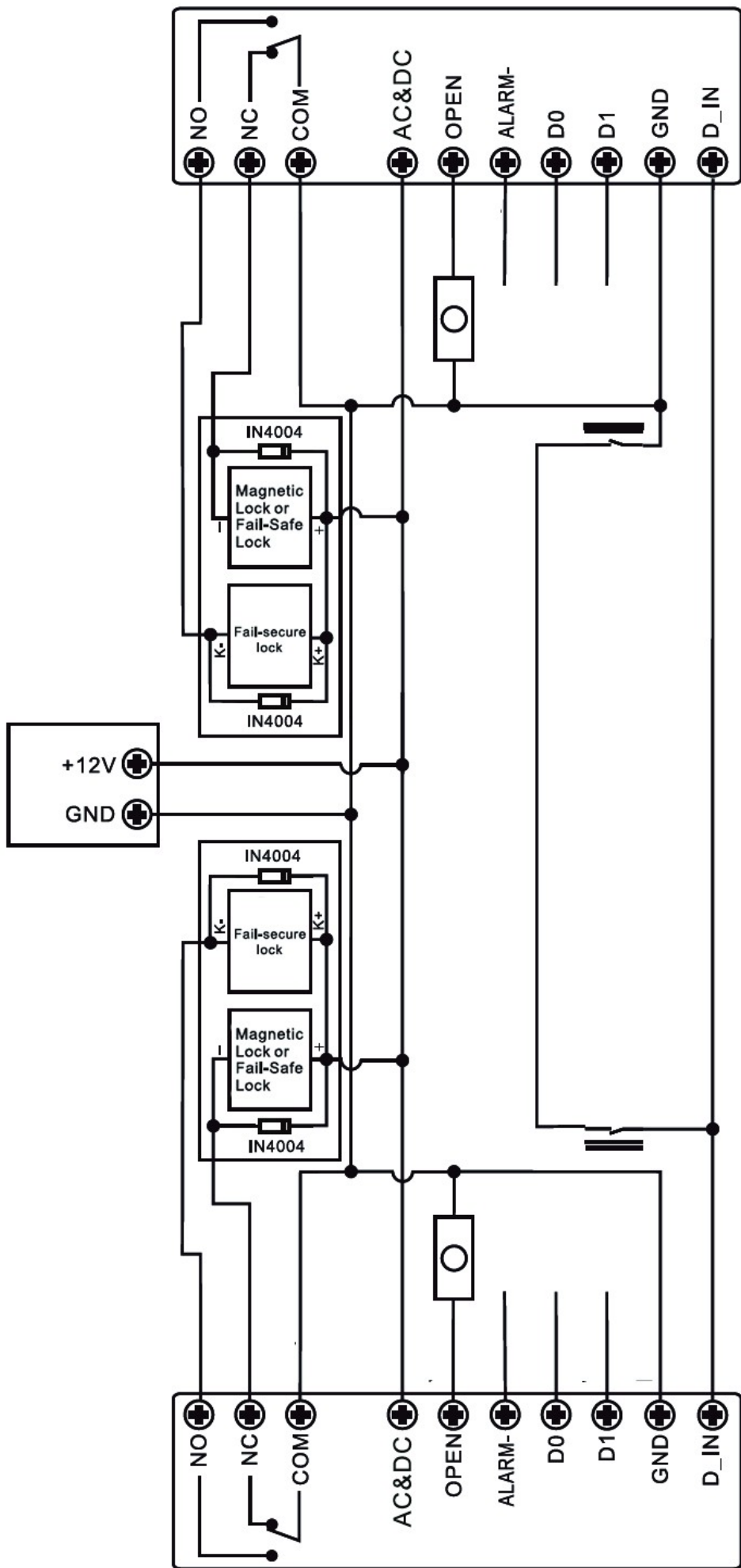
- The exchange is only possible between devices of the same type and the same series.
- The master code has to be the same for both devices.
- The data transfer is only possible from the device which is set as master.
- After the data transfer, the receiving device is blocked for programming.
- The transfer time for 900 users can take up to 30 s.
- After starting the data transfer, the operating display shows a green light, preceded by a confirmation tone for 30 s. After conclusion of the data transfer, the operating display shows a red light.

**Programming in the Master Device:**

Function	Operation/Programming
Initiate programming	* – master code – # (default master code: 123456)
Transfer starten	98 – #
Finish programming	*

**Connection of Two Systems (Lock)**

For an increased safety of access/egress, e.g. in banks, prisons, laboratories, etc., two systems can be connected so that they lock each other. This is also known as interlock.



## Programming:

Step 1: First, read all authorised users into one device and then transfer the data, as described in „Passing on of User Data,” to the second device.

Step 2: Set both devices to „interlock active.”

Function	Operation/Programming
Initiate programming	* – master code – # (default master code: 123456)
interlock inactive or interlock active	90 – # (default setting) 91 – #
Finish programming	*

## Technical Data

Number of users:.....1000 (100 fingerprints, 888 cards/PINs, 2 panic codes, 10 visitors)

Fingerprint reader:.....capacitive

PIN:.....4 to 6 digits

RFID reader:.....EM (125 kHz), MiFare (13,56 MHz), coverage 2 to 6 cm

Relay output:.....changer (NO/COM/NO), max. 2 A

Relay active time:.....0 to 99 s (default setting: 5 s)

Inside calliper (exit button):.....switching to ground

Sabotage alarm:.....optical sensor

Power supply:.....12 to 28 VAC/DC

Power consumption:.....standby: 60 mA, active: max. 150 mA

Surrounding conditions:.....-30 °C to +60 °C, 0 to 98 % rh

Protection class:.....IP66

Dimensions (W x H x D):.....68 x 145 x 25 mm

Weight:.....500 g

## Declaration of Conformity

The dnt Innovation GmbH, Maiburger Straße 29, 26789 Leer, Germany, herewith declares that the device “fingerprint code lock BioAccess PRO”

is in compliance with the essential requirements and the other relevant provisions of Directive 2014/30/EU. The declaration of conformity can be found at the following address: [www.dnt.de](http://www.dnt.de)

## Disposal



### **This device may not be disposed of with domestic waste!**

According to the directive concerning electronic devices and electronic old devices, they are to be disposed of at the local collection centres for electronic old devices!

## Contact

Do you have any questions regarding the product or its operation?

Our Technical Customer Service would be pleased to provide you with comprehensive and qualified information.

E-Mail: [info@dnt.de](mailto:info@dnt.de)

1. German edition 07/2022

Documentation © 2021 dnt Innovation GmbH


All rights reserved. Without the publisher's written consent, this user manual may not be reproduced or copied in

any way, whether in full or in part. It is possible that the user manual at hand still contains printing faults or errors. Nevertheless, the information given in this user manual is regularly reviewed for correctness, and any corrections will be made in the next edition. We do not assume liability for technical or typographical mistakes as well as their consequences. All trademarks and property rights are recognised. Changes in accordance with technical advances can be carried out without prior notice.

DNT000013-07/2022, version 1.02

Importer: dnt Innovation GmbH  
Maiburger Straße 29 · 26789 Leer · Germany · [www.dnt.de](http://www.dnt.de)

## Documents / Resources

	<p><a href="#">dnt DNT000013 Fingerprint Code Lock BioAccess PRO</a> [pdf] User Manual DNT000013, Fingerprint Code Lock BioAccess PRO, Code Lock BioAccess PRO, Fingerprint Code Lock, Code Lock, DNT000013, Lock</p>
---	---

## References

- [dnt<sup>®</sup> dnt Innovation GmbH: hochwertige Elektronik-Lösungen](#)