Fingerprint-Codeschloss BioAccess PRO

Artikelnummer: DNT000013 Bedienungsanleitung

Bitte lesen Sie diese Bedienungsanleitung vor der Installation und Inbetriebnahme komplett durch und bewahren Sie die Bedienungsanleitung für späteres Nachlesen auf. Wenn Sie das Gerät anderen Personen zur Nutzung überlassen, übergeben Sie auch diese Bedienungsanleitung.

1. Funktion

Das Fingerprint-Codeschloss BioAccess PRO ermöglicht den einfachen Zugang über das biometrische Zugangsmerkmal „Fingerabdruck“ sowie per RFID-Transponder und Zifferncode. Zur erhöhten Zugangssicherheit können mehrere Zugangsarten kombiniert werden. Das wetterfeste und vandalismussichere Gerät kann bis zu 1000 Zugänge verwalten. Über ein 26/44-Bit-Wiegand-Interface ist eine besonders sichere Datenübertragung/Steuerung per externem Wiegand-Controller möglich. Das Gerät kann mit Wiegand-Controllern interagieren, selbst als Wiegand-Controller oder als Stand-alone-Gerät arbeiten.

- Robustes, wetterfestes (IP66) und vandalismussicheres Fingerprint-Codeschloss
- Kapazitiver Fingerprint-Sensor, Touch-Tastenfeld
- EM-RFID-Zugang (125 kHz) und Mifare-RFID-Zugang (13,56 MHz)
- Zifferncode-Zugang mit 4 bis 6 Ziffern, Eingabefeld hinterleuchtet, mit automatischer Abschaltung nach 20 s
- Für bis zu 1000 Zugänge (100 Fingerprint + 888 RFID/PIN + 2x Panikcode + 10 Besucher)
- Ein programmierbarer Relais-Schaltausgang, potentialfrei
- 26/44-Bit-Wiegand-Interface, Mifare: 56/58 Bit Ein-/Ausgang, Zugangsdatenverwaltung im Wiegand-Controller
- Stand-alone-Betrieb oder Interlock-Betrieb für 2 Türen möglich
- Latch-Mode (selbsthaltender Betrieb für Tür-Offenhalten) verfügbar
- Türkontakt-Überwachung
- Türoffner-Taster-Eingang (Exit-Button) zur Türöffner-Ansteuerung von innen
- Fail-Secure-Schloss- oder Fail-Safe-Schloss-Betrieb
- Zugang per Fingerprint, RFID, Zifferncode oder kombiniert möglich
- Sabotagesensor gegen Demontage/Manipulation
- Mehrfarbige Statusanzeige
- Interner Signalgeber und externer Signalausgang

2. Bestimmungsgemäßer Einsatz, Lieferumfang

Das BioAccess PRO ist für den Einsatz als allgemeines Zugangskontrollgerät vorgesehen. Es ist für den Außeneinsatz (IP66) zugelassen.

Für Folgeschäden, die aus Nichtbeachtung dieser Gebrauchsregeln und der Bedienungsanleitung resultieren, übernehmen wir keine Haftung, Gewährleistungsansprüche erlöschen ebenfalls. Dies gilt auch für Umbauten und Veränderungen.

Lieferumfang:

- Fingerprint-Codeschloss BioAccess PRO
- Schutzdiode IN4004
- 2x Wanddübel und Montageschrauben (4x 25 mm)
- Montageschlüssel
- Bedienungsanleitung
- RFID-Mastercard

3. Betriebs-, Wartungs- und Sicherheitshinweise

Warnung
Wird verwendet, um Sicherheitshinweise zu kennzeichnen oder um Aufmerksamkeit auf besondere Gefahren und Risiken zu lenken.

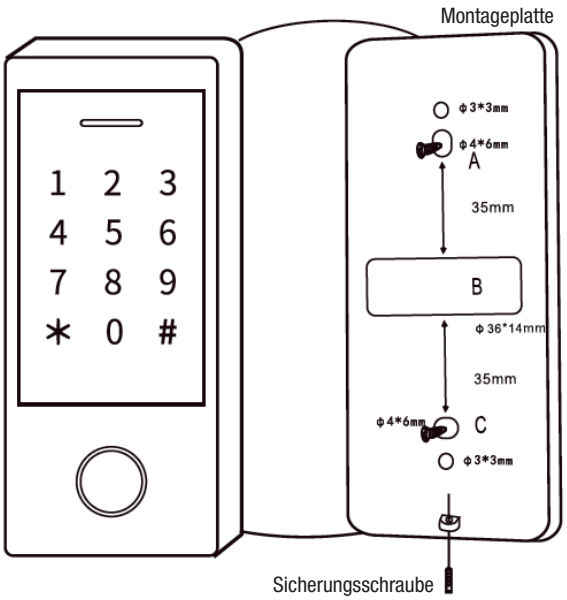
Hinweis
Wird verwendet, um zusätzliche Informationen oder wichtige Hinweise zu kennzeichnen.

- Aus Sicherheits- und Zulassungsgründen (CE) ist das eigenmächtige Umbauen und/oder Verändern des Produkts nicht gestattet.
- Setzen Sie das Gerät keinem Einfluss von Feuchtigkeit über die IP66-Bedingungen hinaus aus – keinen Vibrationen, keiner ständiger Wärmeeinstrahlung, extremer Kälte, keinen starken elektromagnetischen Feldern und keinen mechanischen Belastungen.
- Beachten Sie alle Hinweise in der Bedienungsanleitung zum Anschluss von Spannungen. Falsche oder verpolte Spannungen zerstören das Gerät.
- Lassen Sie das Verpackungsmaterial nicht achtlos liegen, Plastikfolien/-tüten, Styroporteile, etc. könnten für Kinder zu einem gefährlichen Spielzeug werden.
- Wurde das Gerät beschädigt, nehmen Sie es außer Betrieb und wenden Sie sich an unseren Service.

Bei Sach- oder Personenschäden, die durch unsachgemäße Handhabung oder Nichtbeachten der Sicherheitshinweise und der Bedienungsanleitung verursacht werden, übernehmen wir keine Haftung. In solchen Fällen erlischt jeder Gewährleistungsanspruch! Für Folgeschäden übernehmen wir keine Haftung.

Öffnen Sie das Gerät nicht, unternehmen Sie keine Reparaturversuche, nehmen Sie keine Umbauten oder Veränderungen vor – dies führt zum Verlust des Gewährleistungsanspruchs. Für Folgeschäden übernehmen wir keine Haftung.

4. Installation/Montage



Wählen Sie den Montageort so aus, dass gewährleistet ist, dass die Montageplatte dicht, komplett und plan aufliegen kann. Anderenfalls kann eine Sabotage erleichtert werden und es kann zu Fehlauslösungen des Sabotagealarms durch ungewollten Lichteinfall in das Gerät kommen.

- Lösen Sie mit dem Montageschlüssel die Sicherungsschraube unten am Gehäuse und nehmen Sie das Gerät von der Montageplatte ab.
- Zeichnen Sie anhand der Löcher in der Montageplatte bzw. der Skizze oben die Bohrlöcher auf der Montagefläche (Wand) an und bohren Sie die Montagelöcher/Kabeldurchführung (Vorher sollte natürlich kontrolliert werden, dass keine Leitungen oder Rohre in der Wand verlaufen). *Die 3-mm-Löcher sind als zusätzliche Sicherung für die mögliche Befestigung auf z. B. einer Metallplatte mit Gewindeschrauben gedacht. Bei Nichtbenutzung mit einem Dichtmittel verschließen.*
- Führen Sie das Verbindungskabel durch die Wand und verschrauben Sie die Montageplatte an der Wand.
- Setzen Sie das Gerät auf die Montageplatte (zuerst oben einsetzen, dann unten Richtung Montagplatte schwenken) und sichern Sie es mit der Sicherungsschraube.

Anschlussbelegung

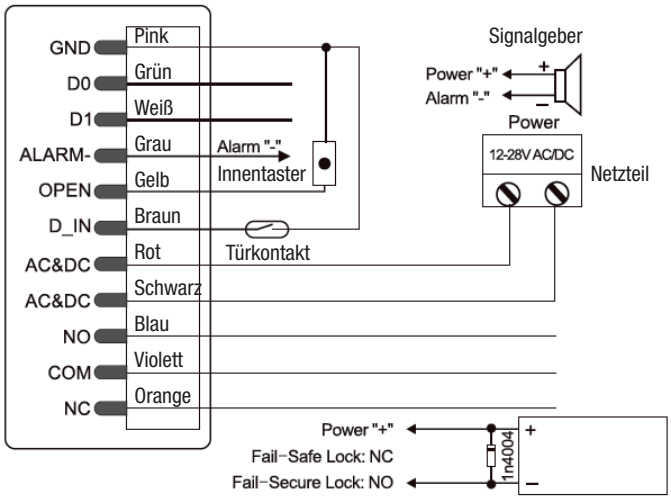
Adernfarbe	Funktion	Bemerkungen
Rot	Ub	Betriebsspannung, 12–28 VAC/DC, DC = Plus
Schwarz	Ub	Betriebsspannung, 12–28 VAC/DC, DC = Minus
Pink	GND	Masseleitung, siehe Hinweise im Text
Blau	Relais, NO	Relaiskontakt, im Ruhezustand offen gegen COM
Violett	Relais, COM	Relaiskontakt, Mittelkontakt
Orange	Relais, NC	Relaiskontakt, im Ruhezustand geschlossen gegen COM
Gelb	OPEN	Eingang für Türöffnertaste im Gebäude
Grün	Data 0	Wiegand-Interface, Leitung Data 0
Weiß	Data 1	Wiegand-Interface, Leitung Data 1
Grau	Alarmausgang	Alarmausgang für Signalgeber, gegen Minus geschaltet
Braun	Türkontakt	Eingang für Türkontaktüberwachung, NC

Ton- und Lichtsignale

Signal/Zustand	Indikator-LED	Tonsignal
Stand-by	Rot	Aus
Programmiermode starten	Blinkt Rot	1x
Gerät im Programmiermode	Orange	1x
Fehler/Falscheingabe	Aus	3x
Programmiermode beenden	Rot	1x
Türöffner aktiv	Grün	1x
Alarm	schnell Rot blinkend	Dauerton

Anschluss-Beschaltung

1. Einfacher Anschluss mit Netzteil



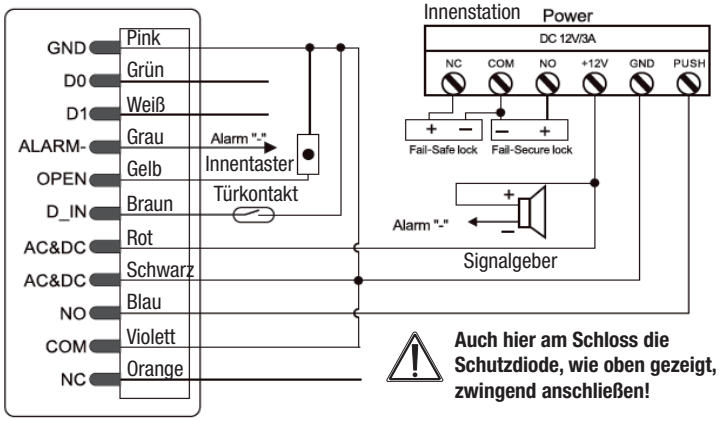
Fail-Safe Lock: elektrischer Türöffner oder Fail-Safe-Schloss

Fail-Safe-Schloss: z. B. Fail-Safe-Bolzenschloss: Bolzen eingefahren, wenn im Stand-by-Modus, Schloss öffnet bei Impuls von der Ansteuerung

Fail-Secure-Lock: z. B. Fail-Secure-Bolzenschloss: Bolzen ausgefahren, wenn im Stand-by-Modus, Schloss öffnet bei Impuls von der Ansteuerung

Bei dieser Art der Spannungsversorgung muss zwingend die mitgelieferte Diode 1N4004, wie im Schaltbild gezeigt, parallel zum Türöffner bzw. elektromagnetischen Schloss geschaltet werden. Diese Diode leitet induktive Spannungsspitzen, die beim Abschalten des Türöffners entstehen, ab. Wird sie nicht verbaut, können hohe Spannungsspitzen den Fingerabdruckscanner zerstören! Beachten Sie die polrichtige Anschaltung. Die Katode entspricht dem Farbring auf der Diode.

2. Anschluss über Innenstation/Interface



Auch hier am Schloss die Schutzdiode, wie oben gezeigt, zwingend anschließen!

Fail-Safe Lock: elektrischer Türöffner oder Fail-Safe-Schloss

Fail-Safe-Schloss: z. B. Fail-Safe-Bolzenschloss: Bolzen eingefahren, wenn im Stand-by-Modus, Schloss öffnet bei Impuls von der Ansteuerung

Fail-Secure-Lock: z. B. Fail-Secure-Bolzenschloss: Bolzen ausgefahren, wenn im Stand-by-Modus, Schloss öffnet bei Impuls von der Ansteuerung

5. Programmierung

5.1. Gerät auf Werkseinstellung zurücksetzen und Mastercard einlesen
Sollten die in der Folge beschriebenen Programmierschritte nicht entsprechend der Beschreibung erfolgreich zu absolvieren sein, so sollten Sie das Gerät auf die Werkseinstellung zurücksetzen. Dies gilt auch für eine Weitergabe des Geräts.

Bitte beachten!
Mit dem Geräte-Reset werden lediglich Master-Code und Einstellungen zurückgesetzt. Alle gespeicherten Zugangsdaten bleiben erhalten. Um diese ebenfalls zu löschen, gehen Sie bitte wie in Kapitel 5.2 beschrieben vor.

- Schalten Sie das Gerät an die Stromversorgung und schalten Sie diese noch nicht zu.
- Drücken Sie jetzt den Innentaster und halten Sie diesen gedrückt, während Sie nun die Stromversorgung zuschalten.
- Lassen Sie den Innentaster los, die Betriebsanzeige wechselt auf Gelb, dann können Sie eine EM-/MiFare-Karte bzw. die mitgelieferte RFID-Karte als Mastercard einlesen.
- Danach wechselt die Betriebsanzeige auf Rot – das Gerät ist auf die Werkseinstellung zurückgesetzt. Die eingelesene Karte ist die Mastercard.

Soll keine neue Mastercard eingelesen werden (z. B. bei Weitergabe des Geräts), so halten Sie nach Zuschalten der Stromversorgung den Innentaster für ca. 5 s gedrückt. Auch hier wechselt die Betriebsanzeige auf Rot, und die zuvor eingelesene Mastercard ist ungültig.

5.2. Bedienung/Programmierung – Kurzübersicht
Trennstriche dienen nur der Übersichtlichkeit, nicht eingeben!

Funktion	Bedienung/Programmierung
Programmierung einleiten	* - 123456 - # (Werks-Master-Code)
Eigenen/neuen Master-Code eingeben	0 - neuer Code (6-stellig) - # - Code wiederholen - #
Benutzer löschen	2 - Fingerabdruck/User-Karte einlesen /User-Pin eingeben - # kann so für weitere Benutzer fortgeführt werden
	2 - Benutzer-ID - # kann so für weitere Benutzer fortgeführt werden
	2 - RFID-Karten-Nummer (8-/10-/17-stellig)
Alle Benutzer löschen	2 - Master-Code - #
Programmieren beenden	*
Tür öffnen	Berechtigten Fingerabdruck/PIN, RFID-Card einlesen - #
Alarm löschen	Master-PIN/Fingerabdruck/RFID-Card eingeben - # oder berechtigte PIN/Fingerabdruck/RFID-Card eingeben - #

Die Programmierung unterscheidet sich in Abhängigkeit der Zugangsart. Folgen Sie den jeweiligen Programmierhinweisen.

Die Vergabe von Benutzer-IDs erleichtert die Nachverfolgung von Zugangsversuchen.

ID-Übersicht:
- Fingerprint: 0...98: Master Fingerprint-Benutzer-ID: 99
- PIN/Card: 100...987
- Panik-Benutzung: 988, 989
- Besucher: 990...999

Als RFID-Karte können 125-kHz-Karten (EM) oder 13,56-MHz-Karten (Mifare) zum Einsatz kommen.

Beim Zugang per PIN sind 4 bis 6 Stellen zulässig.
Die 8888 ist allerdings für Sonderzwecke ausgeschlossen.

Bitte beachten:
- Benutzer-IDs nicht mit führender Null eingeben!
- Ist eine Benutzer-ID eingegeben, wird diese zwingend benötigt, wenn Änderungen der Nutzerdaten vorgenommen werden sollen

5.3. Programmierung der Betriebsart
Das Gerät kann für drei Betriebsarten programmiert werden: Stand-alone/Controller Mode (mit weiterem Reader mit Wiegand-Interface), Wiegand-Leser für externe Controller

Funktion	Bedienung/Programmierung
Programmierung einleiten	* - 123456 - # (Werks-Master-Code)
Stand-alone-/Controller-Mode	77 - # (Werkseinstellung)
Wiegand-Leser	78 - #
Programmieren beenden	*

5.4. Benutzer-Fingerprints speichern mit automatischer ID-Vergabe
Es erfolgt eine automatische, fortlaufende Benutzer-ID-Vergabe (1...98)

Funktion	Bedienung/Programmierung
Programmierung einleiten	* - MasterCode - # (Werks-Master-Code: 123456)
Benutzer-Fingerprint einlesen	1 - Fingerabdruck einlesen - Fingerabdruck einlesen 2x wiederholen (Einlesen kann so fortgeführt werden)
Programmieren beenden	*

5.5. Benutzer-Fingerprints speichern mit manueller ID-Vergabe

Funktion	Bedienung/Programmierung
Programmierung einleiten	* - MasterCode - # (Werks-Master-Code: 123456)
Benutzer-Fingerprint einlesen	1 - Benutzer-ID (1...98) - # - Fingerabdruck einlesen - Fingerabdruck einlesen 2x wiederholen (Einlesen kann so fortgeführt werden)
Programmieren beenden	*

5.6. Benutzer-Zifferncode (PIN) speichern mit automatischer ID-Vergabe

Funktion	Bedienung/Programmierung
Programmierung einleiten	* - MasterCode - # (Werks-Master-Code: 123456)
Benutzer-Zifferncode (PIN) einlesen	1 - PIN (4 bis 6 Stellen) - # (Einlesen kann so fortgeführt werden) (bei Benutzer-ID keine führende Null einsetzen!)
Programmieren beenden	*

5.7. Benutzer-Zifferncode (PIN) speichern mit manueller ID-Vergabe

Funktion	Bedienung/Programmierung
Programmierung einleiten	* - MasterCode - # (Werks-Master-Code: 123456)
Benutzer-Zifferncode (PIN) einlesen	1 - Benutzer-ID (1...987) - # - PIN (4 bis 6 Stellen) - # (bei Benutzer-ID keine führende Null einsetzen!)
Programmieren beenden	*

Hinweise für die PIN-Vergabe
Für eine höhere Sicherheit können Sie Ihre PIN auch in einer Ziffernfolge von bis zu 10 Stellen „verstecken". Dies muss folgende Form haben (Beispiel-PIN: 123434):

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

5.8. Benutzer-RFID-Karten speichern mit automatischer ID-Vergabe
Es erfolgt eine automatische, fortlaufende Benutzer-ID-Vergabe (100...987)

Funktion	Bedienung/Programmierung
Programmierung einleiten	* - MasterCode - # (Werks-Master-Code: 123456)
Benutzer-Karte einlesen	1 - Karte einlesen/RFID-Karten-Nummer (8-/10-/17-stellig) eingeben - # (Einlesen kann so fortgeführt werden)
Programmieren beenden	*

5.9. Benutzer-RFID speichern mit manueller ID-Vergabe

Funktion	Bedienung/Programmierung
Programmierung einleiten	* - MasterCode - # (Werks-Master-Code: 123456)
Benutzer-Karte einlesen	1 - Benutzer-ID (100...987) - # - RFID-Karten-Nummer (8-/10-/17-stellig) eingeben - # (Einlesen kann so fortgeführt werden)
Programmieren beenden	*

5.10. Benutzer-RFID im Block speichern
Dies erlaubt dem Master das fortlaufende Einspeichern von bis zu 987 Karten in einem Durchgang. Dies kann bis zu 2 Minuten dauern.

Funktion	Bedienung/Programmierung
Programmierung einleiten	* - MasterCode - # (Werks-Master-Code: 123456)
Karte im Block einlesen (Karten-Nummern müssen aufeinanderfolgend sein)	1 - Benutzer-ID (100...987) - # - Anzahl der einzulesenden Karten - /RFID-Karten-Nummer der ersten Karte (8-/10-/17-stellig) eingeben - # (Einlesen kann so fortgeführt werden)
Programmieren beenden	*

5.11. Einsatz des Master-Fingerabdrucks/Mastercard zum Hinzufügen/Löschen von Benutzern

Master-Fingerabdruck (ID=99) einlesen

Funktion	Bedienung/Programmierung
Programmierung einleiten	* - MasterCode - # (Werks-Master-Code: 123456)
Master-Fingerprint einlesen	1 (99) - #- Fingerabdruck 3x einlesen
Programmieren beenden	*

Benutzer hinzufügen/löschen mit Master-Fingerabdruck/Mastercard

Funktion	Bedienung/Programmierung
Benutzer hinzufügen	1. Master-Fingerabdruck/Mastercard einlesen 2. Benutzer-Fingerabdruck (3x)/Benutzer-Karte/ Benutzer-PIN einlesen - # (Schritt 2 für weitere Benutzer wiederholen) 3. Master-Fingerabdruck/Mastercard einlesen
Benutzer löschen	1. Master-Fingerabdruck/Mastercard) 2x innerhalb 5 s einlesen 2. Zu löschender Benutzer-Fingerabdruck//Benutzer-Karte/Benutzer-PIN einlesen. Bei Bedarf jetzt weitere Benutzer entsprechend Punkt 2 einlesen 3. Master-Fingerabdruck/Mastercard einlesen

5.12. Eingabe von Benutzern für die Panik-Funktion (Auslösung Panik-Alarm)
Hinweis: Benutzer-ID=988/989; PIN-Länge 4 bis 6 Ziffern, außer 8888

Funktion	Bedienung/Programmierung
Programmierung einleiten	* - MasterCode - # (Werks-Master-Code: 123456)
RFID-Karte ***oder*** PIN	1 - (988 oder 989) - #- Karte / RFID-Karten-Nummer (8-/10-/17-stellig) einlesen - # 1 - (988 oder 989) - #- PIN - #
Programmieren beenden	*

5.13. Eingabe von Besuchern
Hinweis: Benutzer-ID=990...999; PIN-Länge 4 bis 6 Ziffern, außer 8888. Es sind bis zu 10 Besucher-PINs/Karten verfügbar, die für bis zu 10 Zugänge (0...9) benutzt werden können. Ist die festgelegte Anzahl von Zugängen erreicht, verfällt die PIN/Karte

Funktion	Bedienung/Programmierung
Programmierung einleiten	* - MasterCode - # (Werks-Master-Code: 123456)
RFID-Karte hinzufügen ***oder*** PIN	1 - (990 ...999) - #- (0...9) -# - Karte / RFID-Karten-Nummer (8-/10-/17-stellig) einlesen - # 1 - (990...999) - #- (0...9) -# - PIN - #
Programmieren beenden	*

5.14. PIN von Benutzern ändern
Hinweis: Hier wird außerhalb des Programmiermodus gearbeitet, Benutzer können die Änderung selbst vornehmen, PIN-Länge 4 bis 6 Ziffern, außer 8888

Funktion	Bedienung/Programmierung
PIN wechseln	1 - (Benutzer-ID) - #- alte PIN -# - neue PIN - # - neue PIN wiederholen #
PIN bei kombiniertem Zugang PIN + Karte wechseln	1 - (RFID-Karte einlesen) - #- alte PIN -# - neue PIN - # - neue PIN wiederholen #

5.15. Verhalten des Schaltrelais einstellen

Funktion	Bedienung/Programmierung
Programmierung einleiten	* - MasterCode - # (Werks-Master-Code: 123456)
Relais-Aktivzeit einstellen (Pulse-Mode) ***oder*** Relais-Mode (Latch) einstellen	3 - (1–99) - # (Relais bleibt für 1 bis 99 s angezogen = Tür offen, Werkseinstellung: 5 s) 30 - # (achaltet das Relais dauerhaft in eine Stellung, bis die Eingabe erneut erfolgt, dann geht das Relais dauerhaft in die andere Stellung). Diese Einstellung benutzt man z. B., wenn eine Tür über längere Zeit frei durchquerbar sein soll.
Programmieren beenden	*

5.16. Zugangsart einstellen
Bei Mehrfach-Zugangsversuchen mit gleichen Fingerabdrücken/PINs darf eine Zeit von 5 Sekunden nicht überschritten werden, sonst geht das Gerät ohne Reaktion wieder in den Bereitschaftsmodus zurück.

Funktion	Bedienung/Programmierung
Programmierung einleiten	* - MasterCode - # (Werks-Master-Code: 123456)
Nur Zugang per PIN	42 - #
oder	
Nur Zugang per Fingerabdruck	40 - #
oder	
Nur Zugang per RFID-Karte	41 - #
oder	
Zugang per PIN **und** RFID-Karte	43 - #
oder	
Zugang nur nach Eingabe durch mehrere Benutzer (2 bis 9); höhere Sicherheit)	43 - (2...9) - #
oder	
Zugang für Fingerabdruck **oder** PIN **oder** RFID-Karte	44 - # (Werkseinstellung)
Programmieren beenden	*

5.17. Alarm/Sperre bei Manipulations-/Fehlversuchen, Alarm beenden
Nach mehr als 10 Falscheingaben kann das Gerät den Zugang 10 Minuten lang für weitere Eingaben sperren oder einen Alarm auslösen. Auch bei einer Sperre kann die Tür noch mit der Türöffner-Taste im Gebäude geöffnet werden.

Funktion	Bedienung/Programmierung
Programmierung einleiten	* - MasterCode - # (Werks-Master-Code: 123456)
Alarm/Sperre deaktivieren	60 - # (Werkseinstellung)
oder	
Alarm/Sperre aktivieren	61 - # (Zugang nach Fehlversuchen 10 Minuten gesperrt)
oder	
Alarm/Sperre aktivieren (Akustisch)	62 - # (Zugang nach 10 Fehlversuchen gesperrt - akustischer Alarm)
Alarm aktivieren mit Alarmzeitbegrenzung	5 (0-3) - # (Werkseinstellung 1 Minute; 0=inaktiv)
	(Alarm beenden per Master-Code - # oder registriertem Fingerabdruck - # oder registrierter PIN - #)
Programmieren beenden	*

5.18. Registrierung/Alarmierung bei Tür-offen-Erkennung

1. Erkennung einer zu lange geöffneten Tür (DOTL)
Wenn man einen externen magnetischen Türkontakt an der Tür oder einen solchen Türkontakt innerhalb eines Türschlosses zur Überwachung einsetzt, kann ein Alarm ausgelöst werden, wenn die Tür nach einer ordnungsgemäßen Türschlossauslösung nach Ablauf einer Minute nicht wieder geschlossen wurde. Dann ertönt der integrierte Alarmgeber zur Erinnerung an das Verschließen der Tür. Der Alarm kann gelöscht werden durch Schließen der Tür, Master-Benutzer oder normale berechtigte Nutzer (Fingerabdruck/PIN/RFID-Karte). Ansonsten dauert der Alarm entsprechend der unter Kapitel 5.17 eingestellten Alarmdauer an.

2. Erkennung eines Aufbruchs
Wenn der externe Türkontakt ausgelöst wird, ohne dass zuvor ein autorisiertes Öffnen durch Fingerprint/PIN/RFID-Karte erfolgt ist, wird dies als Aufbruchsversuch registriert, und der Alarm wird im Gerät, und, wenn angeschlossen, durch den externen Alarmgeber ausgelöst. Der Alarm kann gelöscht werden durch Schließen der Tür, Master-Benutzer oder normale berechtigte Nutzer (Fingerabdruck/PIN/RFID-Karte). Ansonsten dauert der Alarm entsprechend der unter Kapitel 5.17 eingestellten Alarmdauer an. Dies gilt auch für Auslösen der Sabotagefunktion bei einem Demontageversuch des Gerätes.

Funktion	Bedienung/Programmierung
Programmierung einleiten	* - MasterCode - # (Werks-Master-Code: 123456)
Erkennung deaktivieren *oder* Erkennung aktivieren	63 - # (Werkseinstellung) 64 - #
Programmieren beenden	*

5.19. Akustische Signale und optische Anzeigen programmieren
Bei aktivierter automatischer Tastaturbeleuchtung schaltet sich diese automatisch bei Betätigen irgendeiner Taste ein. Erst danach wird eine reguläre Eingabe registriert.

Funktion	Bedienung/Programmierung
Programmierung einleiten	* - MasterCode - # (Werks-Master-Code: 123456)
Akustisches Quittungssignal deaktivieren	70 - #
aktivieren	71 - # (Werkseinstellung)
oder	
Betriebsanzeige immer aus	72 - #
Betriebsanzeige immer an	73 - # (Werkseinstellung)
oder	
Tastaturbeleuchtung immer aus	74 - #
Tastaturbeleuchtung immer an	75 - #
Tastaturbeleuchtung nach 20 s automatisch abschalten	76 - # (Werkseinstellung)
Programmieren beenden	*

6. Bedienung

Tür öffnen nur mit Fingerabdruck/RFID-Karte
- Registrierte RFID-Karte oder registrierten Finger auflegen

Tür öffnen nur mit PIN
- Registrierte PIN eingeben, mit # bestätigen

Tür öffnen mit Multi-PIN/Fingerabdruck/RFID-Karte
- Registrierten Multi-Zugang (2–9 Nutzer, siehe Kapitel 5.16) auflegen/eingeben

Tür öffnen mit PIN oder Fingerabdruck oder RFID-Karte
- Registrierten Zugang (siehe Kapitel 5.16) auflegen/eingeben

Alarm löschen
- Registrierte PIN eingeben oder registrierten Finger auflegen oder Master-Fingerabdruck eingeben oder Master-Code #

7. Wiegand-Interface

Wiegand ist ein genormtes Interface für den Datenaustausch zwischen Zugangskontrollgeräten und Kontroll-Panels. Es wird für den Datentransfer vom Lesegerät zu einem Kontrollgerät benutzt. So entsteht ein besonders sicheres System, da keine Zugangsdaten im Lesegerät gespeichert werden müssen.

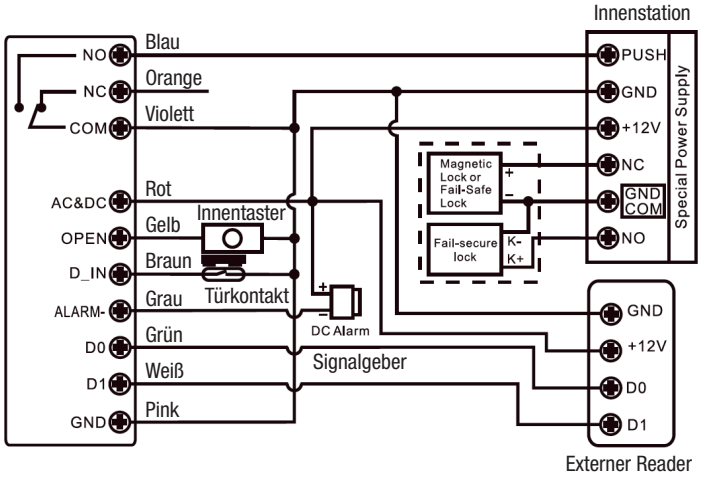
Beim Zusammenwirken mit einem Kontroll-Panel/RFID-Controller muss das Gerät mit 12 V Gleichspannung versorgt werden! Die schwarze Leitung wird hier nicht angeschlossen!

Hinweis:
Bei Verwendung des 4-Bit-Pin-Ausgabeformates in Verbindung mit einer Wiegand Schnittstelle können alle drei Eingabeversionen genutzt werden (Zahlencode, RFID und Fingerprint gemeinsam oder in beliebiger Kombination). Beim Umstellen auf das 10-Bit-Pin-Ausgabeformat darf die Fingerprintversion nicht genutzt werden, da dies zu einer Sicherheitslücke führen könnte.

Das Interface benötigt vier Leitungen:
- +12 V (rote Leitung, bei Versorgung über das Interface)
- Ground (GND, pinke Leitung)
- Datenleitung DATA 0 (grüne Leitung)
- Datenleitung DATA 1 (weiße Leitung)

Bei Controllern, die über Ausgänge für eine Quittungs-LED und einen Signalgeber im Türgerät verfügen, kommen zusätzlich die Leitungen D-IN (Braun) und OPEN (Gelb) zum Einsatz.

Anschluss an ein externes Zugangsgerät (Reader) mit Wiegand-Interface
Das Gerät kann mit einem weiteren Reader mit Wiegand-Interface zusammenarbeiten. Dazu ist das Gerät in die Betriebsart 77 (siehe Kapitel 5.3.) zu versetzen.



Auch hier am Türöffner die Schutzdiode, wie im Kapitel 4 (Anschlussbeschaltung) gezeigt, zwingend anschließen!

Für die Verbindung zwischen Fingerprint-Codeschloss und externem Reader müssen an beiden Geräten die gleichen Wiegand-Formate eingestellt sein.

Wiegand-Format:

Funktion	Bedienung/Programmierung
Programmierung einleiten	* - MasterCode - # (Werks-Master-Code: 123456)
Wiegand-Format festlegen	8 - (EM: 26...44; Mifare: 26 ...44, 56, 58) - # (Werkseinstellung: 26 Bit)
Parity-Bit deaktivieren Parity-Bit aktivieren	80 - # (für Wiegand-Reader mit 32, 40 oder 56-Bit-Ausgang) 81 - # (Werkseinstellung)
Programmieren beenden	*

Programmierung
Die Basis-Programmierung entspricht der Stand-alone-Programmierung. Die Abweichungen sind im Folgenden zusammengefasst:

Bei Anschluss eines EM/Mifare-Readers: Benutzer sind an beiden Readern anmeld- oder löschbar. Bei Anschluss eines HID Card-Readers: Benutzer sind nur am externen Gerät anmeld- und löschbar.

Beispiel für den Einbindung eines Fingerabdruck-Readers:
Schritt 1: Lesen Sie den Fingerabdruck am externen Gerät ein.
Schritt 2: Lesen Sie den gleichen Fingerabdruck am DNT-Zugangsgerät ein

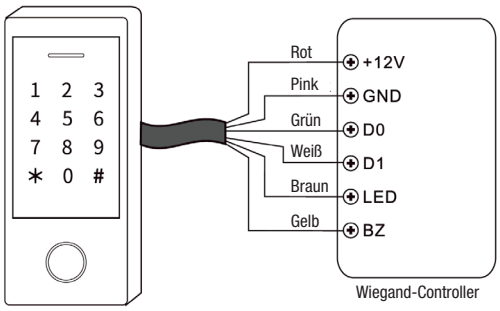
Funktion	Bedienung/Programmierung
Programmierung einleiten	* - MasterCode - # (Werks-Master-Code: 123456)
Version 1 ***oder*** Version 2	1 - Fingerabdruck am externen Gerät einlesen - # (automatische ID-Vergabe) 1 - (Benutzer-ID) - # Fingerabdruck am externen Gerät einlesen - # (vergebene ID benutzen)
Programmieren beenden	*

Beispiel für den Einbindung eines Zifferncode-Readers:
Der Reader muss das 4-, 8- oder 10-Bit-Ausgangsformat unterstützen

Funktion	Bedienung/Programmierung
Programmierung einleiten	* - MasterCode - # (Werks-Master-Code: 123456)
PIN Eingangsformat	8 (4/8/10) - # (Werkseinstellung: 4 Bit)
Programmieren beenden	*

Zum Hinzufügen können PINs an allen beteiligten Geräten angelernt werden.
Das Löschen von PINs erfolgt ebenfalls an allen beteiligten Geräten.

Betrieb als Wiegand-Lesegerät (Reader) an einem Wiegand-Controller
Das Gerät kann als externer Wiegand-Reader mit einem Wiegand-Controller zusammenarbeiten. Dazu ist das Gerät in die Betriebsart 78 (siehe Kapitel 5.3.) zu versetzen.



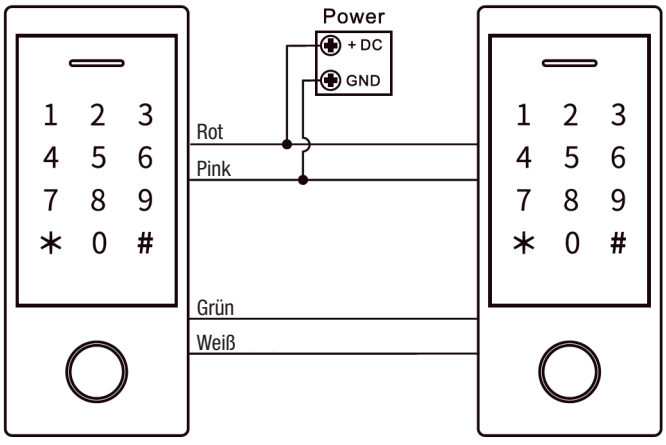
Bitte beachten:
- Bei diesem Anschluss werden zahlreiche Einstellungen des Gerätes ungültig, weil diese vom externen Wiegand-Controller aus erfolgen.
- Die braune Leitung (D_IN) führt zur Signalisierung des Zugangs durch grünes Aufleuchten der Betriebsanzeige (low-aktiv).
- Die gelbe Leitung (OPEN) führt zur Zugangssignalisierung durch den internen Signalgeber (low-aktiv).

Wiegand-Formate einstellen
- Stellen Sie am Zugangsgerät das gleiche Wiegand-Ausgangsformat ein, wie es am Wiegand-Controller als Eingangsformat eingestellt ist.
- Bei Wiegand-Controllern mit 32-/40-/56-Bit-Eingangsformat Parity-Bit deaktivieren

Funktion	Bedienung/Programmierung
Programmierung einleiten	* - MasterCode - # (Werks-Master-Code: 123456)
Wiegand-Ausgangsformat	8 - (EM: 26...44; Mifare: 26...44, 56, 58) - # (Werkseinstellung EM: 26 Bit; Mifare: 34)
PIN-Ausgangsformat	8 (4/8/10) - # (Werkseinstellung 4 Bit) (**Hinweis:** Bei Verwendung des 4-Bit-Pin-Ausgabeformates in Verbindung mit einer Wiegand Schnittstelle können alle drei Eingabeversionen genutzt werden (Zahlencode, RFID und Fingerprint gemeinsam oder in beliebiger Kombination). Beim Umstellen auf das 10-Bit-Pin-Ausgabeformat darf die Fingerprintversion nicht genutzt werden, da dies zu einer Sicherheitslücke führen könnte.)
Parity-Bit deaktivieren	80 - #
Parity-Bit aktivieren	81 - # (Werkseinstellung)
Programmieren beenden	*

8. Erweiterte Funktionen

Benutzerdaten weitergeben
Zwischen zwei Geräten des gleichen Typs können die Benutzerdaten ausgetauscht werden. Dies vereinfacht die Programmierung bei mehreren Zugängen durch die gleichen Benutzer. Der Austausch ist nur für RFID-Karten- und PIN-Zugänge möglich.



Bitte beachten:
- Der Austausch ist nur zwischen typgleichen Geräten der gleichen Serie möglich.
- Der Master-Code muss auf beiden Geräten der gleiche Code sein.
- Der Transfer ist nur vom als Master eingesetzten Gerät aus möglich.
- Nach der Datenübertragung ist das empfangende Gerät gesperrt für eigene Programmierungen.
- Die Übertragungszeit für 900 Benutzer kann bis zu 30 s betragen.

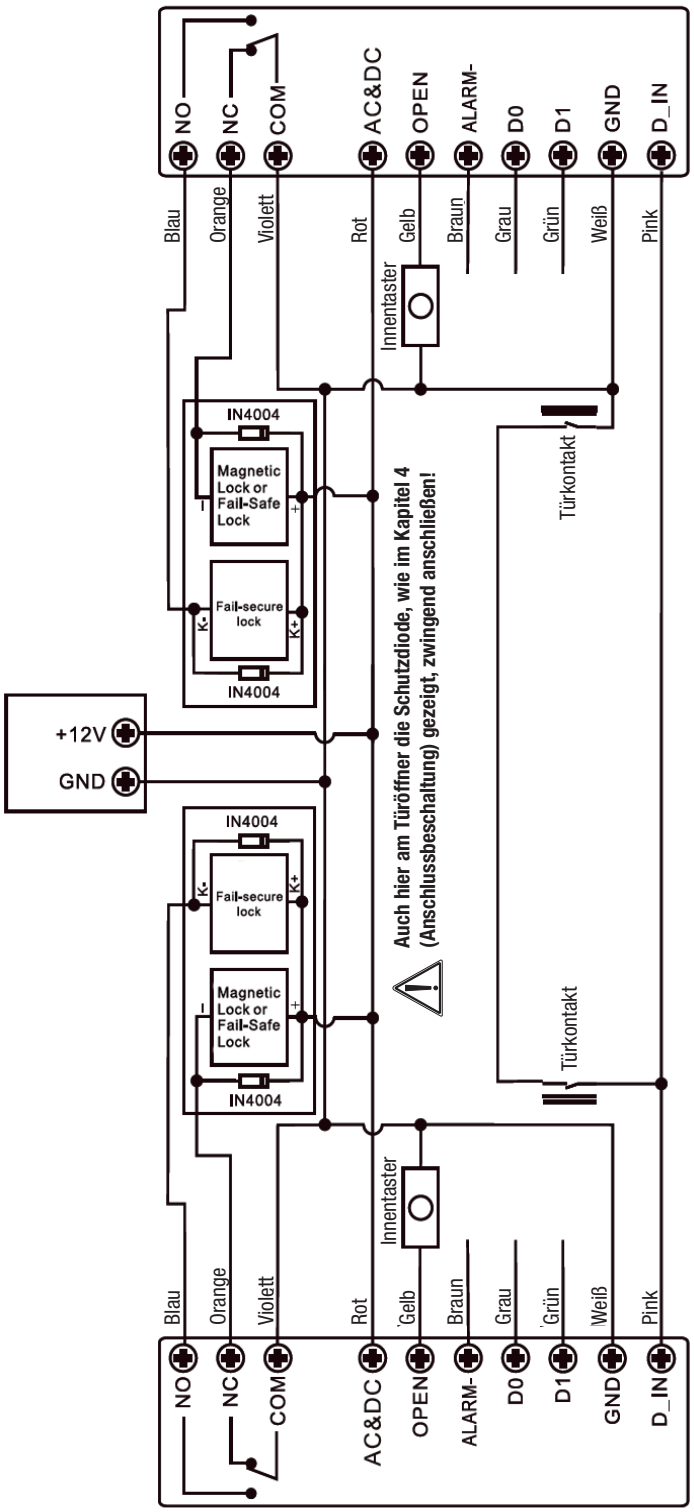
- Nach dem Start des Transfers leuchtet die Betriebsanzeige nach einem Bestätigungston für 30 s grün, nach Abschluss des Transfers rot.

Programmierung am Master-Gerät:

Funktion	Bedienung/Programmierung
Programmierung einleiten	* - Master-Code - # (Werks-Master-Code: 123456)
Transfer starten	98 - #
Programmieren beenden	*

9. Verbindung zweier Systeme (Schleuse)

Für eine erhöhte Sicherheit des Zugangs/Ausgangs, z. B. in Banken, JVA, Labor etc. können zwei Systeme so verbunden werden, dass sie sich gegenseitig verriegeln. Dies bezeichnet man als Interlock.



Programmierung:
Schritt 1: Lesen Sie alle berechtigten Benutzer zuerst an einem Gerät ein und übertragen Sie dann, wie unter „Benutzerdaten weitergeben" beschrieben, die Daten an das zweite Gerät..
Schritt 2 Setzen Sie beide Geräte auf „Interlock aktiv":

Funktion	Bedienung/Programmierung
Programmierung einleiten	* - MasterCode - # (Werks-Master-Code: 123456)
Interlock inaktiv *oder* Interlock aktiv	90 - # (Werkseinstellung) 91 - #
Programmieren beenden	*

10. Technische Daten

Anzahl der Nutzer: .....1000 (100 Fingerprints/888 Cards/PINs, 2 Panik, 10 Besucher)
Fingerabdruckleser: .....kapazitiv
PIN: .....4–6 Stellen
RFID-Leser: .....EM (125 kHz), Mifare (13,56 MHz), Erfassungsbereich 2–6 cm
Relaisausgang: .....Wechsler (NO/COM/NO), max. 2 A
Relais-Aktivzeit: .....0–99 s (Werkseinstellung: 5 s)
Innentaster (Exit Button): .....gegen Masse schaltend
Sabotagealarm: .....optischer Sensor
Spannungsversorgung: .....12–28 VAC/DC
Stromaufnahme: .....Bereitschaft: 60 mA, aktiv: max. 150 mA
Umgebungsbedingungen: .....-30 °C bis +60 °C, 0–98 % rH
Schutzart: IP66
Abmessungen (B x H x T): .....68 x 145 x 25 mm
Gewicht: .....500 g

11. Konformitätserklärung

Hiermit erklärt die dnt Innovation GmbH, Maiburger Straße 29, 26789 Leer, Deutschland, dass sich das Gerät

„Fingerprint-Codeschloss BioAccess PRO"

in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2014/30/EU befindet.
Die Konformitätserklärung kann unter folgender Adresse gefunden werden: www.dnt.de

12. Entsorgung

Gerät nicht im Hausmüll entsorgen!
Elektronische Geräte sind entsprechend der Richtlinie über Elektro- und Elektronik-Altgeräte über die örtlichen Sammelstellen für Elektronik-Altgeräte zu entsorgen!

13. Kontakt

Sie haben Fragen zum Produkt oder zur Bedienung?

Unser **Technischer Kundendienst** erteilt Ihnen gerne umfassende und qualifizierte Auskünfte: E-Mail: info@dnt.de

1. Ausgabe Deutsch 07/2022

Es ist möglich, dass die vorliegende Bedienungsanleitung noch drucktechnische Mängel oder Druckfehler aufweist. Die Angaben in dieser Bedienungsanleitung werden jedoch regelmäßig überprüft und Korrekturen in der nächsten Ausgabe vorgenommen. Für Fehler technischer oder drucktechnischer Art und ihre Folgen übernehmen wir keine Haftung. Alle Warenzeichen und Schutzrechte werden anerkannt. Änderungen im Sinne des technischen Fortschritts können ohne Vorankündigung vorgenommen werden. DNT000013-07/2022, Version 1.02

Importeur: dnt Innovation GmbH
Maiburger Straße 29 · 26789 Leer · Germany · www.dnt.de

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.

1. 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

2. 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

3. Operating, Service, and Safety Instructions

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

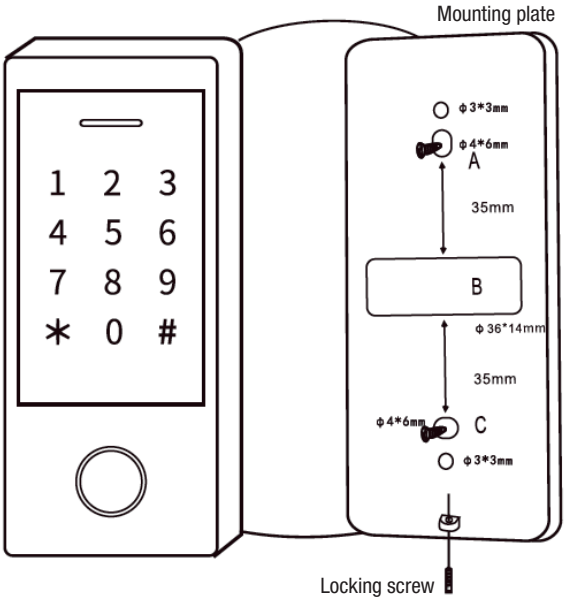
Notice
Is used to mark additional information or important notices.

- 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.

4. 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

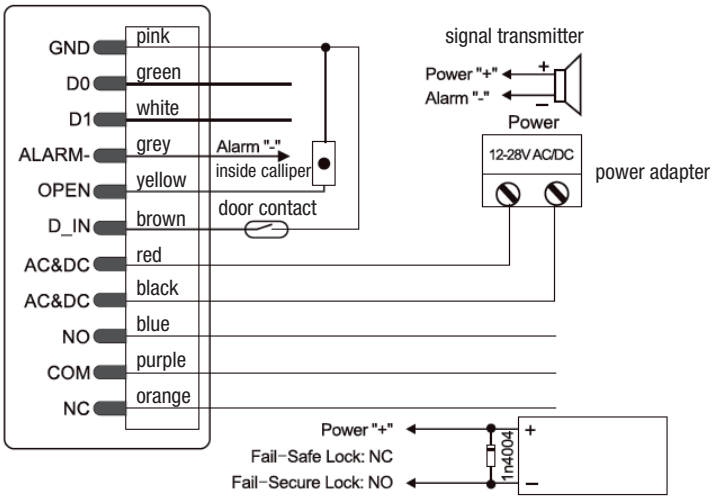
Wire Colour	Function	Remarks
red	UB	operating voltage, 12–28 VAC/DC, DC = plus
black	UB	operating voltage, 12–28 VAC/DC, DC = minus
pink	GND	ground line, see notes in the text
blue	relay, NO	relay contact, open against COM in idle state
purple	relay, COM	relay contact, centre contact
orange	relay, NC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



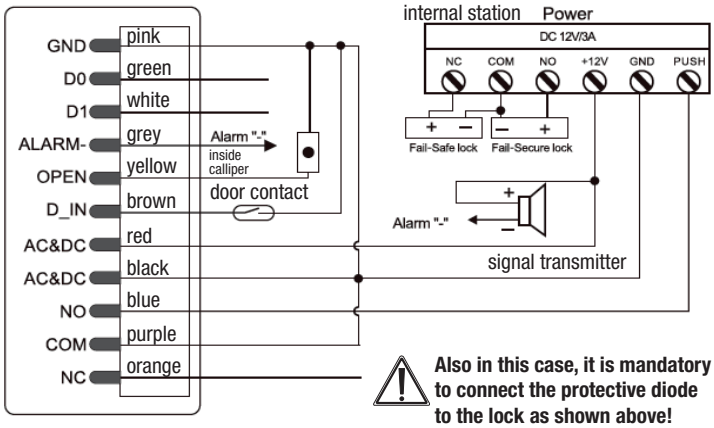
fail safe lock: electric door opener or fail safe lock

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



Also in this case, it is mandatory to connect the protective diode to the lock as shown above!

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

5. Programming

5.1. 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.

5.2. 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 - #
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.

5.3. 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	*

5.4. 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	*

5.5. 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	*

5.6. 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	*

5.7. 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

5.8. 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	*

5.9. 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	*

5.10. 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	*

5.11. 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	1. Read master fingerprint/master card 2. Read user fingerprint (3x)/user card/user PIN - # (repeat step 2 for further users) 3. Read master fingerprint/master card
Delete user	1. Read master fingerprint/master card twice within 5 s 2. Read user fingerprint/user card/user PIN to be deleted (if required read more users according to step 2) 3. Read master fingerprint/master card

5.12. 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	*

5.13. 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	*

5.14. 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 #

5.15. 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	*

5.16. 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	*

5.17. 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	*

5.18. 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	*

5.19. 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	*

6. 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 #

7. 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.

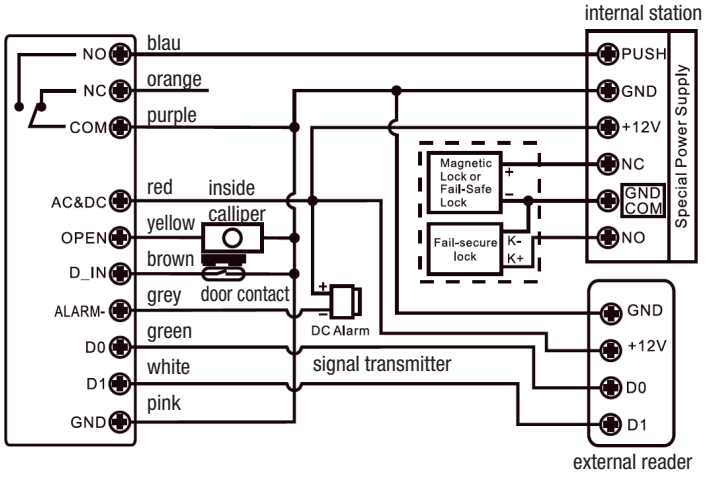
In the interaction with a control panel/RFID controller, the device has to be supplied with 12 VDC voltage! In this case, the black wire is not connected!

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.

Wiegand format:

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.

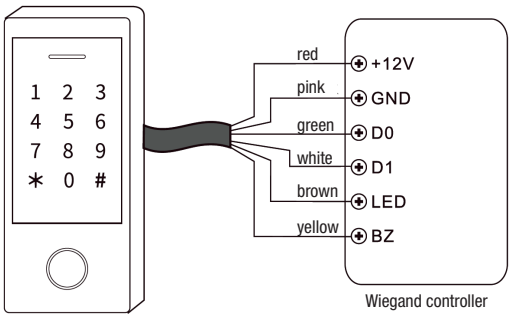
Function	Operation/Programming
Initiate programming	* - master code - # (default master code: 123456)
Version 1 ***or*** Version 2	1 - read fingerprint into external device - # (automatic ID allocation) 1 - (user ID) - # read fingerprint into external device - # (use allocated ID)
Finish programming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

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.).



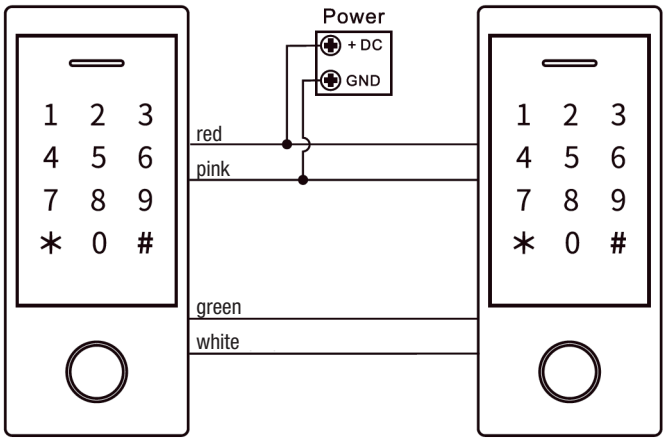
Please note:
- In the case of this connection, numerous settings of the device become invalid since they are carried out from the external Wiegand controller.
- The brown wire (D_IN) leads to access signalling through green flashing of the operating display (low-active).
- The yellow wire (OPEN) leads 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	Bedienung/Programmierung
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) (**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.)
Disable parity bit Activate parity bit	80 - # 81 - # (default setting)
Finish programming	*

8. 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.

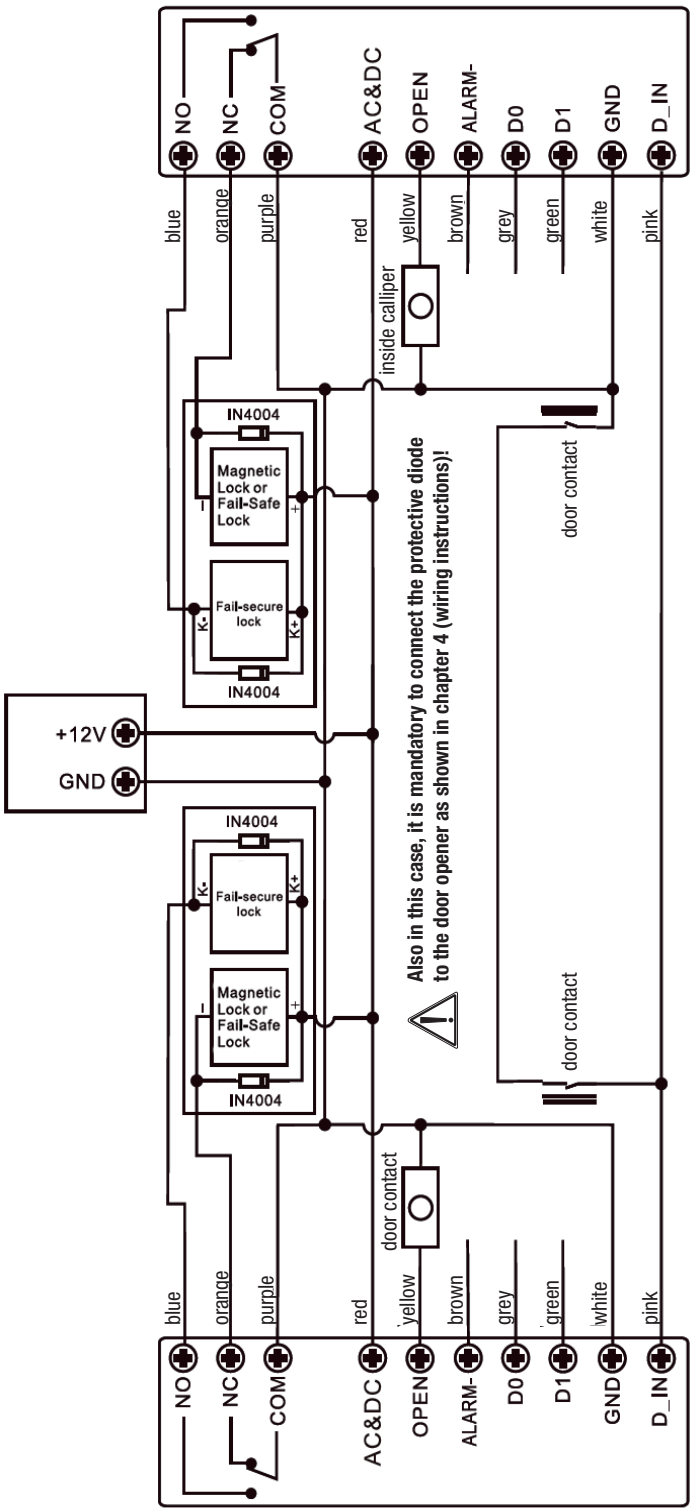
- The transfer time for 900 users can take up to 30 s.
- After starting the data transfer, the operating display shows a green light, preceded by a confirmation tone for 30 s. After conclusion of the data transfer, the operating display shows a red light.

Programming in the Master Device:

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

9. 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	*

10. 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

11. 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

12. 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!

13. 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

1. German edition 07/2022

DNT000013-07/2022, version 1.02

Importer: dnt Innovation GmbH
Maiburger Straße 29 · 26789 Leer · Germany · www.dnt.de