Designed in Germany
C59501106 | 06 | 09.2022

TÜRTECHNIK | DOOR TECHNOLOGY

B-55600-23-4-8 | B-55600-20-4-8
B-55600-23-1-8 | B-55600-20-1-8

Vorsprung mit System
Securing technology for you

Inhaltsverzeichnis

Ihr Werkscode:

Alternativ befindet sich ein Aufkleber mit dem Werkscode auf der Rückseite des Programmiergeräts. Falls Sie einen eigenen Mastercode vergeben haben, muss dieser verwendet werden.

Bitte geben Sie das Dokument an den Benutzer weiter!

1. Informationen und Sicherheit

1.1 Allgemeine Hinweise zur Anleitung

Vielen Dank, dass Sie sich für den Fingerabdruckscanner (Fingerscanner) bzw. die Codetastatur als Zutrittskontrolle für motorische oder elektromechanische Verschlusssysteme entschieden haben.

Diese Betriebsanleitung enthält wichtige Hinweise und hilft, Gefahren zu vermeiden, Reparaturkosten und Ausfallzeiten zu vermindern sowie die Zuverlässigkeit und Lebensdauer zu erhöhen.

Die Betriebsanleitung ist von jeder Person **vor** dem Gebrauch des Produkts zu lesen und anzuwenden. Beachten Sie die Anleitung besonders bei:

- Montage und Elektroinstallation
- Inbetriebnahme, Betrieb und Wartung

Die Betriebsanleitung ist nach dem Montageabschluss dem Betreiber/Auftraggeber zu übergeben. Lesen Sie diese Anleitung vor der ersten Bedienung bitte sorgfältig durch und bewahren Sie diese auch für die spätere Nutzung auf. Weisen Sie bitte alle Betreiber/Auftraggeber an, die Betriebsanleitung zu lesen.

1.2 Sicherheitshinweise

Diese Betriebsanleitung richtet sich an geschultes Fachpersonal mit Kenntnissen in der Installation von Tür-, Beschlag- und Elektronikkomponenten. Sie bietet Hinweise zur Montage, Inbetriebnahme und Handhabung dieses Produktes.

Auftraggeber und Benutzer sind auf die Einhaltung dieser Angaben hinzuweisen um fehlerhafte Montage, sowie Fehlbedienungen zu vermeiden.

- Die jeweils lokal geltenden Montage- und Installationsbestimmungen, Richtlinien und Vorschriften sind einzuhalten. Das gilt insbesondere für VDE-Richtlinien und Vorschriften, z. B. DIN VDE 0100 und IEC 60364.

- Bei unsachgemäßem Einsatz, Montage und Installation sowie bei Verwendung von nicht originalen Zubehörteilen wird keine Haftung übernommen!
- Es ist zu gewährleisten, dass nur Fachkräfte (Definition siehe EN 50110-1, DIN VDE 0105 bzw. IEC 60364) mit jeglichen Arbeiten (Planung, Transport, Montage, Installation, Inbetriebnahme, Wartung, Reparatur, Demontage) an den Produkten beauftragt werden.
- Dabei ist sicherzustellen, dass Ihnen die Unterlagen zur Aufstellung, Inbetriebnahme, Bedienung, Wartung und Reparatur der Produkte zur Verfügung stehen und diese beachtet werden.
- Aus Sicherheits- und Zulassungsgründen (CE) sind eigenmächtige Umbauten und/oder Veränderungen am Produkt nicht erlaubt.
- Vor jeder Montage, Reparatur, Wartungs- oder Einstellarbeit sind alle zugehörigen Netzteile spannungslos zu schalten und gegen unbeabsichtigtes Wiedereinschalten abzusichern.
- Bei Schäden, welche durch Nichtbeachten dieser Anleitung verursacht werden, erlischt der Garantieanspruch! Für Folgeschäden wird keine Haftung übernommen!

1.3 Warnsymbole

⚠ VORSICHT	**VORSICHT kennzeichnet eine gefährliche Situation, die, wenn sie nicht vermieden wird, zu Verletzungen führen kann.**
ACHTUNG	**ACHTUNG kennzeichnet eine Situation, die zu Sachschäden führen kann.**
HINWEIS	**HINWEIS kennzeichnet eine rein informative Aussage.**

2. Produktbeschreibung

Der Fingerscanner und die Codetastatur sind Zutrittskontrollen zur Identifikation mittels biometrischem oder geistigem Merkmal. Der Fingerscanner erfasst die Merkmale (Minutien) der Fingerlinien, vergleicht sie mit den aus dem Referenz-Fingerbild gespeicherten biometrischen Informationen. Die Codetastatur erfasst eingetippte PIN-Codes und vergleicht sie mit den gespeicherten Referenz-PIN-Codes.

Bei Übereinstimmung der Merkmale wird durch eine verschlüsselte Übertragung an die Steuereinheit die Tür geöffnet. Das System dient primär der Öffnung von Haustüren, Wohnungstüren und Garagentoren im Heim- oder Gewerbebereich.

2.1 Technische Daten

Variante Edelstahl	B-55600-23-4-8 B-55600-20-4-8 	B-55600-23-1-8 B-55600-20-1-8 
Variante schwarz	B-55600-23-4-9 nur Fingerscanner	-
Ausführung für	Türeinbau	Wandmontage
Spannungsversorgung	8 ... 24 V DC	8 ... 30 V DC
Leistungsaufnahme	max. 1 W	max. 3 W
Relaisausgang	über SC200	24 V DC | 5,0 A
Abmessungen	44 x 75 x 29 mm	80,5 x 80,5 x 30 mm (55 x 55 x 30 mm ohne Rahmen)
Speicher	35 Fingerabdrücke 1000 Ereignisse im Zutrittsprotokoll 150 PIN-Codes für die Codetastatur	

Template	Aufnahmedauer: ca. 1 s Identifikationsdauer: ca. 10 ms pro Vergleich
Falschrückweisungs-rate (FRR)	ca. 0,5 %
Falschakzeptanzrate (FAR)	Besser als 1 zu 1 Million (bei FRR 0,5 %)
Fingererkennung	Abfrage der kapazitiven/leitenden elektromag-netischen Eigenschaften des Hautkontaktes beim Ziehen des Fingers über den CMOS-Sensor.
Batterie für Programmiergerät	CR2025
Umweltbedingungen	+85 °C -20 °C ≤ 95 % 40 °C IP65 (frontseitig)
Zertifizierungen	CE Die Zertifikate finden Sie auf www.g-u.com.

2.2 Bestimmungsgemäße Verwendung

Verwenden Sie das Produkt ausschließlich gemäß der Produktbeschreibung. Der Gebrauch beschränkt sich auf die im Weiteren beschriebenen Funktionen, technischen Daten, Anwendungen und Anweisungen. Die Verwendung ist nur innerhalb der in dieser Anleitung beschriebenen Nutzungsgrenzen erlaubt. Für diese wurde das Produkt konzipiert. Eine darüber hinaus gehende Nutzung ist nicht gestattet.

Der Fingerscanner und die Codetastatur dienen ausschließlich der Zutrittskontrolle mittels biometrischem Identifikationsmerkmal bzw. einem PIN-Code, an den verschiedensten Gebäudezugängen in einem Schließsystem. Die Hauptfunktion ist die Identifizierung. Zum Öffnen des Zutrittspunkts wird ein SECURY mit A-Öffner, SECURE*connect* 200, Relais als Steuereinheit oder ein EK-Schloss benötigt.

Ausgeführte Veränderungen am Produkt oder an den Anschlüssen ohne Zustimmung der Unternehmensgruppe Gretsch-Unitas, schließen eine Haftung des Herstellers für daraus resultierende Schäden aus.

2.3 Nicht bestimmungsgemäße Verwendung

Ein anderer oder darüber hinausgehender Gebrauch als zuvor beschrieben ist nicht gestattet und für hieraus entstehende Schäden haftet die Unternehmensgruppe Gretsch-Unitas nicht. Eine nicht bestimmungsgemäße Verwendung ist auch gegeben, wenn die Sicherheitshinweise nicht beachtet werden. Eigenmächtige Umbauten und/oder Veränderungen am Produkt sind nicht gestattet.

Insbesondere, aber nicht abschließend, stellt es eine nicht bestimmungsgemäße Verwendung dar, wenn das Produkt in einer der im Folgenden beschriebenen Bedingungen verwendet wird.

- Fehler in der Polung der Anschlüsse.
- Am Produkt sind unautorisierte Modifikationen vorgenommen worden.
- Beim Betrieb im Türeinbau mit SECURE*connect* sind Spannungen größer 24 V + 10 % DC nicht zulässig und führen zu einer Beschädigung.

2.4 Funktion

2.4.1 Funktion Fingerscanner

Der Fingerscanner erfasst den Fingerabdruck durch einen Zeilensensor und wertet diesen aus. Das Ergebnis wird mit den biometrischen Informationen des vorher als Referenz gespeicherten Fingerabdrucks verglichen. Bei Übereinstimmung wird die Autorisierung gesendet, wodurch ein Zutritt durch die Tür gewährt wird. Aus Sicherheitsgründen wird im Fingerscanner ein Zeilensensor verwendet, der automatisch bei jeder Nutzung durch das Ziehen des Fingers die Abdruckspur beseitigt und die Sensoroberfläche reinigt.

2.4.2 Funktion Codetastatur

Die Codetastatur vergleicht die Eingabe auf der Tastatur mit dem von Ihnen als Referenz vergebenen Benutzercode. Bei Übereinstimmung wird die Autorisierung gesendet, wodurch ein Zutritt durch die Tür gewährt wird.

2.5 Lieferumfang, Transport und Lagerung

Der Lieferumfang ist auf Vollständigkeit und Beschädigungen zu prüfen. Im Schadensfall ist der Händler zu informieren. Nur Produkte im technisch einwandfreien Zustand montieren und in Betrieb nehmen.

Die Lieferung besteht aus den folgenden Artikeln:

- Zutrittskontrolle (Fingerscanner oder Codetastatur)
- Programmiergerät (nur bei Fingerscanner)
- Systemkabel zur Steuereinheit (nur bei Gerät zur Türmontage)
- Relaismodul „Whitebox“ (nur bei Gerät zur Wandmontage)
- Befestigungsmaterialien
- Betriebsanleitung

Lagern Sie das Produkt nur in der Originalverpackung und unter folgenden Bedingungen:

- Aufbewahrungsort nur in trockenen, sauberen und mäßig gelüfteten Innenräumen, nicht im Freien. Produkt keinen Bewegungen und Vibrationen aussetzten
- Temperaturbereich von +15 °C bis +40 °C, ohne starke Temperaturschwankungen
- Luftfeuchtigkeit mit einer relative Feuchte 30 % bis 70 %, keine Betauung
- Inspektion des allgemeinen Zustands bei längerer Lagerzeit regelmäßig durchführen

Transportieren Sie das Produkt nur in der Originalverpackung. Achten Sie bei der Beförderung auf eine Sicherung gegen Herunterfallen wie auch einen Schutz vor Nässe. Ebenso sind harte Stöße zu vermeiden.

2.6 Zubehör

■ Ersatz-Montagerahmen AP/UP	B-55606-00-0-1 2
■ Edelstahlfrontblende mit BKS-Logo	B-55606-00-1-1 3
■ Edelstahlfrontblende mit BKS-Logo schwarz	B-55606-00-7-1 3
■ Edelstahlfrontblende ohne BKS-Logo	B-55606-00-2-1 4

3. Montage

Der Fingerscanner oder die Codetastatur wird in der Regel im Außenbereich auf der Türaußenseite montiert. Je nach Ausführung wird er in der Tür oder in der Wand eingebaut. Mit einer Datenleitung wird die Verbindung zur Steuerung des Zutrittspunkts hergestellt (SECURE*connect*/EK-Schloss oder Relaisbox „Whitebox“). Verwenden Sie die BKS-Systemkabel zum Anschließen.

ACHTUNG

Bei Installation und Leitungsverlegung müssen die Vorschriften und Normen für Sicherheitskleinspannung eingehalten werden. Leitungsenden mit Aderendhülsen versehen

ACHTUNG

Beschädigen Sie während der Montage nicht die sichtbaren Oberflächen des Einbauraums! De-/Montieren Sie das Dekorelement vorsichtig!

HINWEIS

Um eine einwandfreie Bedienung zu gewährleisten ist eine Montagehöhe von 1,2 bis 1,4 m über der Oberkante des fertigen Fußbodens (OKFF) einzuhalten!

- Verwenden Sie die mitgelieferten Befestigungsmaterialien.
- Die Befestigungsschrauben sind mit einem Schraubendreher anziehen, bis der Fingerscanner bzw. die Codetastatur festsitzt. Achten Sie darauf nicht zu fest anziehen, das Gehäuse könnte so zerstört werden.
- Wir empfehlen, dass Dekorelement erst nach Abschluss der Montage und einem erfolgreichen Funktionstest aufzusetzen.

HINWEIS

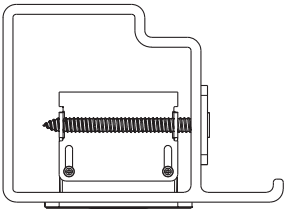
Nach Abschluss der Montage und Einschalten der Spannungsversorgung leuchten beim Fingerscanner/Codetastatur die LEDs konstant grün, rot und blau, wenn sich die Geräte im Auslieferzustand befinden. Das heißt, wenn kein Benutzer- oder Masterfinger respektive PIN-Code programmiert und der Anschluss korrekt vorgenommen wurde.

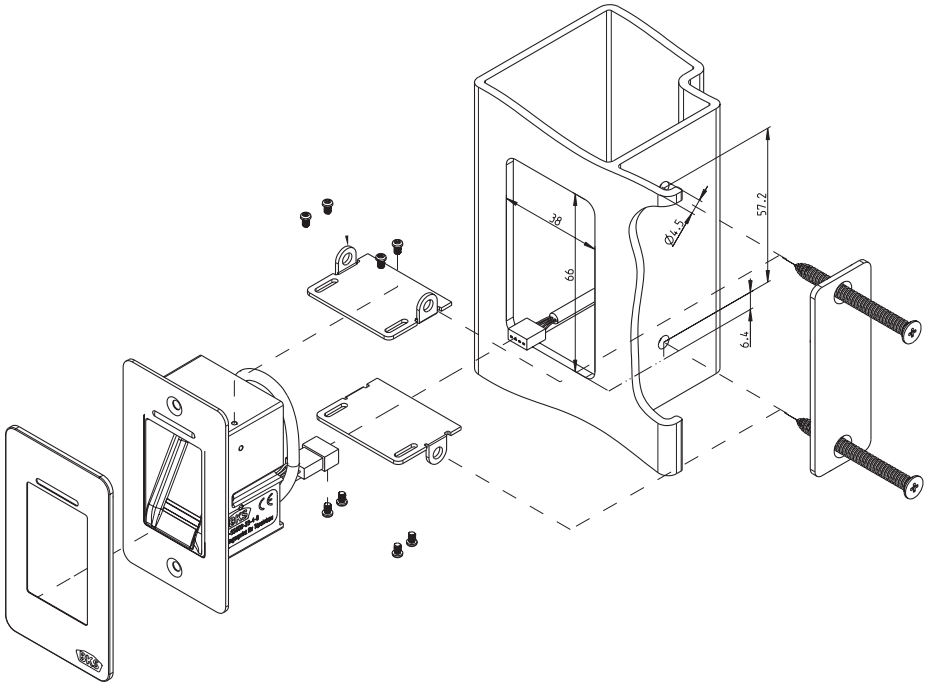
3.1 Türeinbau – B-55600-23-4-8 | B-55600-20-4-8 | B-55600-23-4-9

Diese Variante des Fingerscanners bzw. der Codetastatur ist zum Einbau in Türen als Zutrittskontrolle bestimmt. Zur Vereinfachung zeigen die Abbildungen den Einbau des Fingerscanners. Der Einbau der Codetastatur unterscheidet sich nicht.

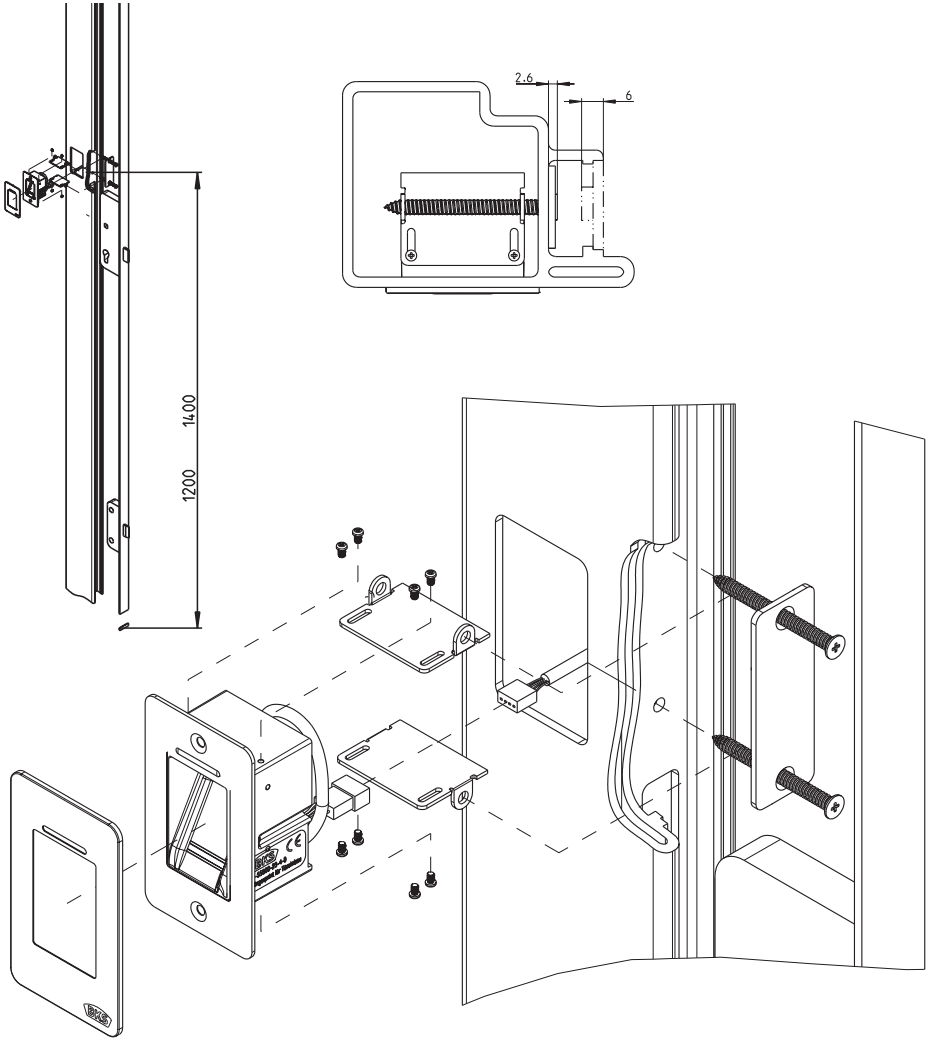
3.1.1 Montage Zutrittskontrolle in Holz- und Stahltüren

3.1.2 Montage Zutrittskontrolle in Alu- und Kunststofftüren

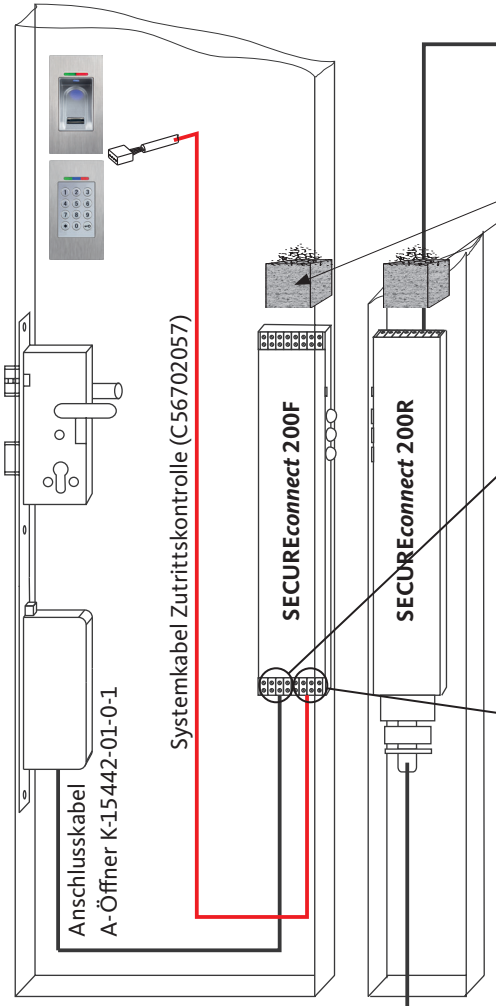




3.1.3 Montage Zutrittskontrolle mit SECURY (A-Öffner)



3.1.4 Verkabelungsplan A-Öffner



Potentialfreier Ansteuerkontakt, z. B. Taster, Sprechanlage, Zutrittskontrolle, Zeitschaltuhr.

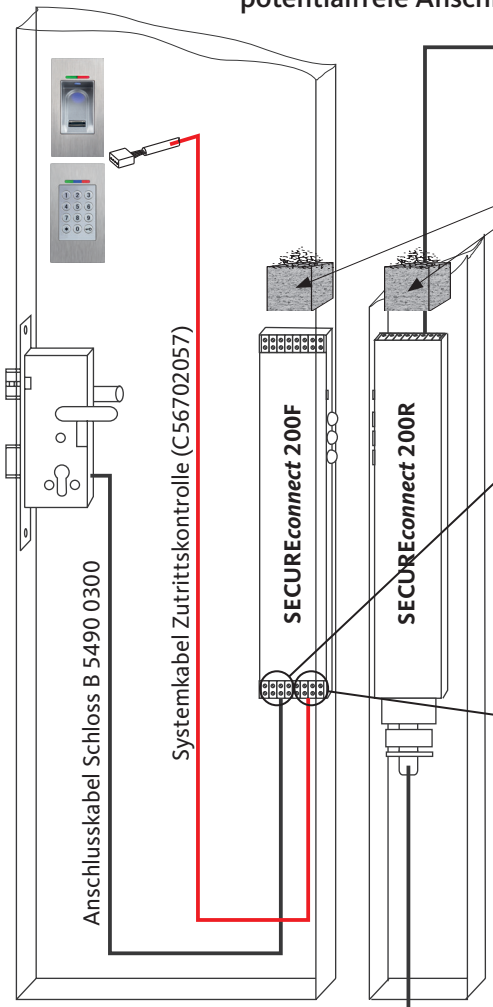
Verwenden Sie die beiliegenden Schwämme zum Schutz vor Spänen beim Einbau in Metallprofilen.

SC 200F	Anschlusskabel A-Öffner	
Klemme	Aderfarbe	Signal
GS	GY | grau	GND (minus)
VS	BN | braun	+ 24 V (plus)
90	BK |schwarz	Steuerleitung

SC 200F	Systemkabel Zutrittskontrolle	
Klemme	Aderfarbe	Signal
GS	YE | gelb	GND (minus)
96	WH | weiß	RS-485 A
95	GN | grün	RS-485 B
94	BN | braun	+ 24 V (plus)

Verwenden Sie bei Metall- und Kunststofftüren zum Leitungsauslass den beigefügten Kabelschutz.

3.1.5 Verkabelungsplan Motor- und EK-Schlösser über potentialfreie Anschlüsse



Potentialfreier Ansteuerkontakt, z. B. Taster, Sprechanlage, Zutrittskontrolle, Zeitschaltuhr.

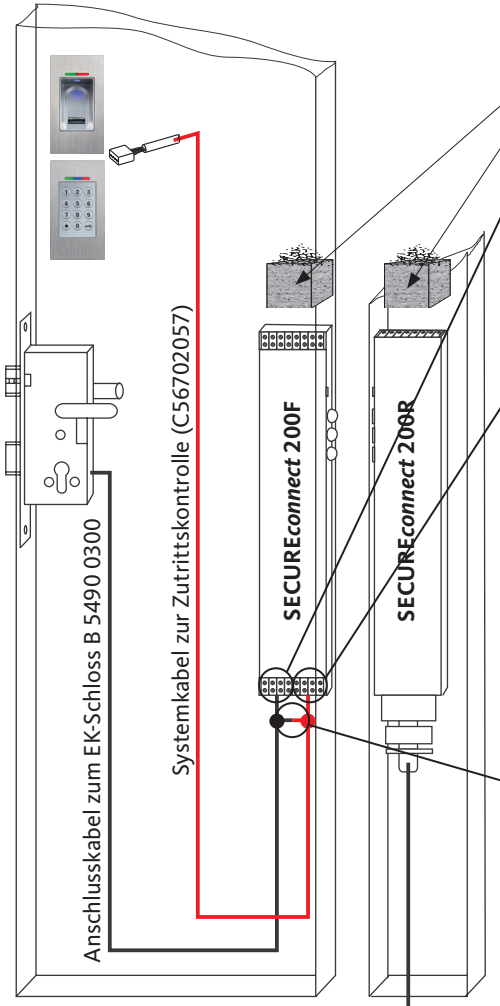
Verwenden Sie die beiliegenden Schwämme zum Schutz vor Spänen beim Einbau in Metallprofilen.

SC 200F	Anschlusskabel Schloss	
Klemme	Aderfarbe	Signal
GS	WH | weiß	GND (minus)
VS	BN | braun	+ 24 V (plus)
90	PK | rosa	Steuerleitung

SC 200F	Systemkabel Zutrittskontrolle	
Klemme	Aderfarbe	Signal
GS	YE | gelb	GND (minus)
96	WH | weiß	RS-485 A
95	GN | grün	RS-485 B
94	BN | braun	+ 24 V (plus)

Verwenden Sie bei Metall- und Kunststofftüren zum Leitungsauslass den beigefügten Kabelschutz.

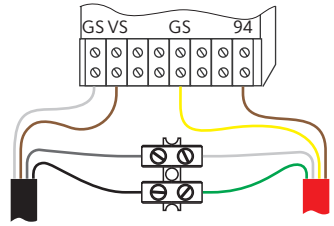
3.1.6 Verkabelungsplan EK-Schloss über RS-485 BUS



Verwenden Sie die beiliegenden Schwämme zum Schutz vor Spänen beim Einbau in Metallprofilen.

SC 200F	Anschlusskabel EK-Schloss	
Klemme	Aderfarbe	Signal
GS	WH | weiß	GND (minus)
VS	BN | braun	+ 24 V (plus)

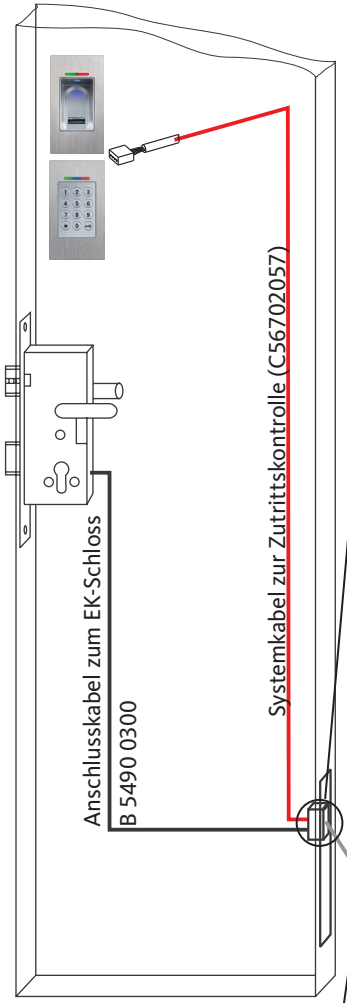
SC 200F	Systemkabel Zutrittskontrolle	
Klemme	Aderfarbe	Signal
GS	YE | gelb	GND (minus)
94	BN | braun	+ 24 V (plus)



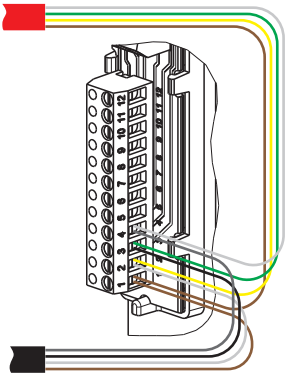
Aderfarbe		Signal
Anschlusskabel EK-Schloss	**Systemkabel Zutrittskontrolle**	
GY | Grau	WH | weiß	RS-485 A
BK | Schwarz	GN | Grün	RS-485 B

Verwenden Sie bei Metall- und Kunststofftüren zum Leitungsauslass den beigefügten Kabelschutz.

3.1.6.1 Anschluss an externe Spannungsversorgung



Aderfarbe		Nr.	Signal
Anschlusskabel EK-Schloss	**Systemkabel Zutrittskontrolle**	**Kabel-übergang**	
GY | Grau	WH | weiß	4	RS-485 A
BK | Schwarz	GN | Grün	3	RS-485 B
Anschluss an externe Spannungsversorgung			
WH | Weiß	YE | gelb	2	GND (Minus)
BN | Braun	BN | braun	1	+ 12 V – 24 V DC



Netzteil B 5570 0402

Kabelübergang
B 5527 0005

Kabelübergang	Netzteil
1	24 V DC
2	GND (Minus)

3.1.7 Manipulationsschutz mit SECURE*connect* 200

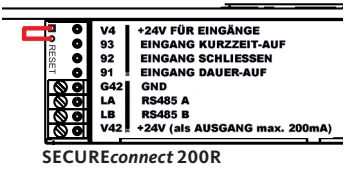
Bei der Variante Türeinbau besteht Ihr System aus 2 elektronischen Geräten

- Zutrittskontrolle: Fingerscanner oder Codetastatur
- Steuereinheit: SECURE*connect* 200

Die Zutrittskontrolle (Fingerscanner oder Codetastatur) wird in der Regel im Außenbereich (Türaußenseite) montiert. Um einer unbefugten Manipulation vorzubeugen ist Ihr System mit zahlreichen Sicherheitsfunktionen ausgestattet, die einen unbefugten Zutritt verhindern:

- Die Zutrittskontrolle ist über eine Datenleitung mit der Steuereinheit verbunden. Die Datenübertragung ist verschlüsselt.
- Die Zutrittskontrolle und die Steuereinheit werden im Rahmen der Erstinbetriebnahme eindeutig miteinander verbunden (Pairing).

Um eine Komponente (SECURE*connect* 200R, SECURE*connect* 200F oder Zutrittskontrolle) des Türsystems auszutauschen, muss an beiden Hälften des SECURE*connect* 200 eine Repairingprozedur durchgeführt werden. Hierzu muss auf der Platine des SECURE*connect* 200R oder des SECURE*connect* 200F der Zurücksetzten-Kontakt bei angeschlossener Stromversorgung für min. 3 s geschlossen werden. Verwenden Sie hierzu z. B. eine Krokodilklemme.



SECURE*connect* 200R

Danach kann die Klemme entfernt werden. Das SECURE*connect* 200R, das SECURE*connect* 200F und die Zutrittskontrolle durchlaufen nun einen erneuten Pairingvorgang. Die Zutrittskontrolle wird hierbei auf Werkseinstellung zurückgesetzt (alle gespeicherten Fingerabdrücke bzw. PIN-Codes werden gelöscht).

Schließt man eine Zutrittskontrolle an gepairtes SECURE*connect 200* an, muss ein Repairing durchgeführt werden. Dabei wird ein neuer Systemschlüssel generiert und die Fingerabdrücke bzw. die PIN-Codes werden gelöscht.

3.1.8 Pairing Fingerscanner/Codetastatur mit EK-Schloss

Ein Direktanschluss an den Fingerscanner oder Codetastatur ist mit den elektrisch kuppelbaren Schlössern (EK-Schloss) der Baureihen EK19 und EK21 in der verkabelten Ausführung möglich. Die Zutrittskontrolle und das EK-Schloss werden automatisch während der Erstinbetriebnahme über die RS-485 Schnittstelle in einer BUS-Verbindung eindeutig miteinander verbunden (Pairing).

Um nach dem Verbinden eine Komponente (Fingerscanner, Codetastatur oder Schloss) des Türsystems auszutauschen, muss vor der erneuten Verbindung der Komponenten ein Repairing durchgeführt werden. Das Repairing wird mit einer bestimmten Sequenz am EK-Schloss durchgeführt.

Diese Sequenz starten Sie mit dem Neustart des EK-Schlosses durch Trennen und Wiederherstellen der Stromversorgung. Innerhalb einer Minute nach dem Neustart, müssen nun folgende Schritte ausgeführt werden:

- Betätigen Sie den Drücker dauerhaft während Sie den Schließbartkontakt überfahren.
- Drehen Sie währenddessen mit dem Schlüssel den Schließzylinder mehrmals schnell im und gegen den Uhrzeigersinn und überfahren innerhalb von 10 s mindestens 3-mal den Schließbartkontakt.

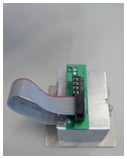
Nach erfolgreichem Abschluss des Repairings werden alle gepairten Geräte gelöscht und die Komponenten werden erneut „gepairt“.

3.2 Wandmontage UP/AP – B-55600-23-1-8 | B-55600-20-1-8

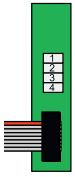
Diese Variante des Fingerscanners bzw. der Codetastatur ist zum Einbau in die Wand neben der Tür als Zutrittskontrolle bestimmt. Zur Vereinfachung zeigen die Abbildungen den Einbau des Fingerscanners. Der Einbau der Codetastatur unterscheidet sich nicht.

3.2.1 Montage Zutritskontrolle Unterputz (UP)

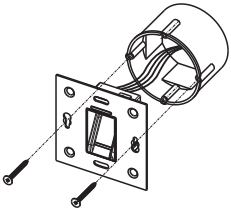
Die Montage erfolgt in einer Unterputzdose. Wir empfehlen eine Montagehöhe von 1,2 bis 1,4 m von der Oberkante Fertigfußboden (OKFF).



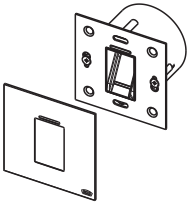
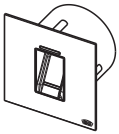
- Verbinden Sie die Zutrittskontrolle mit dem Relaismodul.



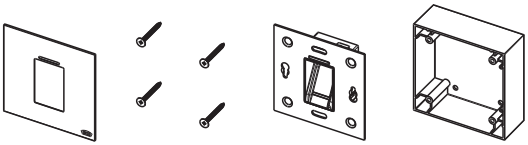
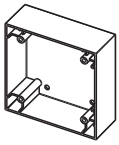
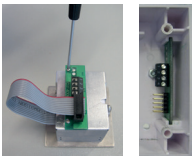
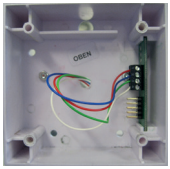
Schließen Sie die Zuleitung zur Inneneinheit entsprechend an den Klemmen 1 bis 4 an.

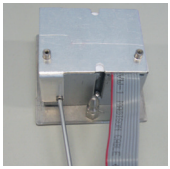


- Befestigen Sie den Tragrahmen der Zutrittskontrolle mit den beiliegenden 2 Schrauben (3,5 x 25) an der Unterputzdose.

	■ Entfernen Sie die Schutzfolie der Klebestreifen auf der Rückseite des Edelstahl-Außenrahmens. ■ Positionieren Sie den Außenrahmen auf dem Tragrahmen der Zutrittskontrolle.
	■ Überprüfen Sie die Funktion.

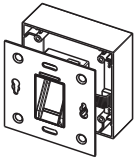
3.2.2 Montage Zutritskontrolle Aufputz (AP)

	
	Befestigen Sie das AP-Gehäuse an die Wand. Wir empfehlen eine Montagehöhe von 1,2 bis 1,4 m Oberkante Fertigfußboden (OKFF). Verwenden Sie die beiliegenden Schrauben (3,5 x 25) und Dübel.
	■ Entfernen Sie die Anschlussplatine durch lösen der beiden Schrauben. ■ Schieben Sie die Anschlussplatine in die dafür vorgerichtete Nut des AP-Gehäuses.
	■ Schließen Sie die Leitung zum Relaismodul „Whitebox“ entsprechend an den Klemmen 1 bis 4 an.

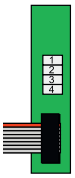


■ Entfernen Sie die Gehäuserückwand.

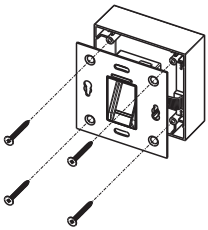
HINWEIS! Mit montierter Gehäuserückwand passt die Zutrittskontrolle nicht in das AP-Gehäuse.



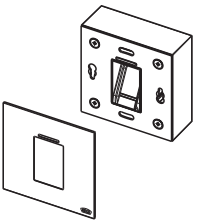
■ Stecken Sie das Flachbandkabel der Zutrittskontrolle auf die Anschlussplatine auf.



Die rote Markierung des Flachbandkabels muss in Richtung der Anschlussklemmen ausgerichtet sein.

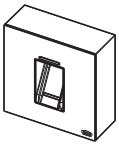


■ Befestigen Sie den Tragrahmen der Zutrittskontrolle mit den beiliegenden 4 Schrauben (3,5 x 25) am AP-Gehäuse.



■ Entfernen Sie die Schutzfolie der Klebestreifen auf der Rückseite des Edelstahl-Außenrahmens.

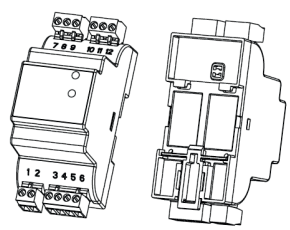
■ Positionieren Sie den Außenrahmen auf dem Tragrahmen der Zutrittskontrolle.



■ Überprüfen Sie die Funktion.

3.2.3 Verkabelungsplan mit dem Relaismodul „Whitebox“

Innen- und Außeneinheit kommunizieren über einen verschlüsselten BUS. Zur Verbindung von dem Relaismodul „Whitebox“ und Zutrittskontrolle empfehlen wir eine Telekommunikationsleitung J-Y(ST)Y 2x2x0.8.
Das Anschlussbeispiel gilt für den A-Öffner der Unternehmensgruppe Gretsch-Unitas.



Befestigung auf Hutschiene

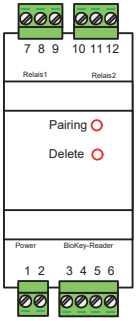
HINWEIS **Beim Aufputzeinbau muss das Flachbandkabel (rote Linie in Richtung Klemmen) richtig eingesteckt werden.**

3.2.4 Technische Daten Relaismodul „Whitebox“

Betriebsspannung:	8 bis 30 V DC oder 8 bis 12 V AC
Leistungsaufnahme:	1 W, in Spitzen 3 W (plus Leistung angeschlossener A-Öffner)
Relais-Daten:	24 V AC/DC 5,0 A
Einbauraum	Im Innenbereich zum Schutz der Relais-Steuerung
Maße Relaismodul H x B x T [mm]	86,4 x 44,9 x 52,6 (Abmessungen ohne Klemmen)

3.2.5 Manipulationsschutz mit dem Relaismodul „Whitebox“

ACHTUNG **Das Relaismodul muss im gesicherten Bereich installiert werden und darf von Außen nicht zugänglich sein!**



Bei den Unter- bzw. Aufputzgeräten zur Wandmontage sind Relaismodul „Whitebox“ und die Zutrittskontrolle ab Werk miteinander gepairt. Im Falle eines Hardware-Austauschs einer Komponente muss das Pairing neu ausgelöst werden.

- Drücken Sie zum Start des Pairings auf die Taste in der mit „Pairing“ beschrifteten und rot umrandeten Bohrung der Inneneinheit.

3.2.6 Zurücksetzten mit dem Relaismodul „Whitebox“

Bei den Unter- bzw. Aufputzgeräten zur Wandmontag können Sie mit dem Relaismodul ein Zurücksetzen auf Werkseinstellungen mit dem Löschen aller Fingerabdrücke inklusive der Masterfinger bzw. der PIN-Codes auslösen.

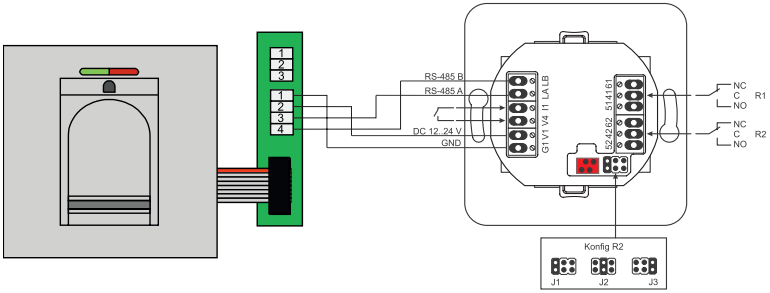
- Drücken Sie zum Start des Löschvorgangs auf die Taste in der mit „Delete“ beschrifteten und rot umrandeten Bohrung des Relaismoduls „Whitebox“.

Nach dem Zurücksetzen leuchten die grüne, rote und blaue LED konstant auf der Zutrittskontrolle.

HINWEIS **Nach dem Zurücksetzen wird der geänderte Mastercode auf den Werkscode zurückgesetzt!**

3.2.7 Anschluss an ein Funkmodul (FMIO)

Die Zutrittskontrolle kann direkt mit einem Funkmodul (FMIO) über einen verschlüsselten Bus kommunizieren.
Zur Verbindung von FMIO und Zutrittskontrolle empfehlen wir eine Telekommunikationsleitung J-Y(ST)Y 2 x 2 x 0.8.



3.2.7.1 Ausgangsfunktionen FMIO

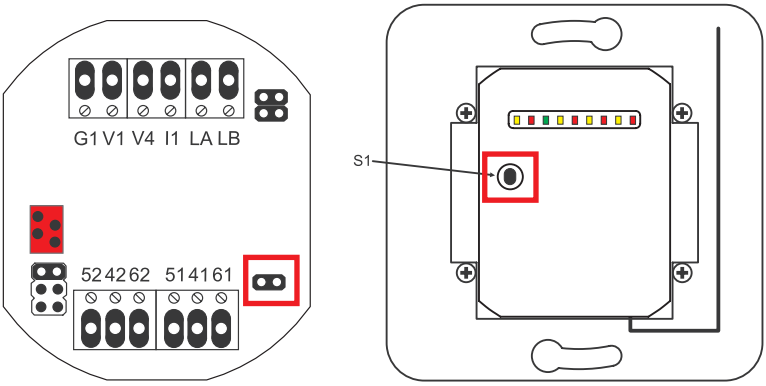
Das Relais „R1“ des FMIO wird nach dem Anschluss einer Zutrittskontrolle über die RS-485 Schnittstelle zur Anzeige eines berechtigten Zutritts verwendet. Relaisausgang „R1“ ist nicht weiter konfigurierbar. Die optische Ausgabe erfolgt über LED „L7“ an der Vorderseite des FMIO.

Das Relais „R2“ bietet die Möglichkeit, 3 unterschiedliche Signale widerzuspiegeln. Das Signal wird durch Setzen des Jumpers konfiguriert (siehe nachfolgende Tabelle). Die optische Ausgabe erfolgt über LED „L2“.

Ausgang	FMIO mit Funk-EK-Zylinder/-Schloss	FMIO mit Funk-EK-Zylinder/-Schloss und Fingerscanner/ Codetastatur
1	-	Berechtigter Zutritt
2 + J1	-	Unberechtigter Zutrittsversuch
2 + J2	Kupplung aktiv (Zylinder/ Schloss eingekuppelt)	-
2 + J3	Batteriestatus	Batteriestatus

3.2.7.2 Pairing/Repairing FMIO

Nachdem ein Zutrittskontrolle an dem FMIO angeschlossen wurde, findet ein Pairing statt. Es kann nun keine andere Zutrittskontrolle an das gleichen FMIO angeschlossen werden. Sollte dies notwendig sein, muss das Pairing mit der Zutrittskontrolle zurückgesetzt werden.



Hierzu muss der Gehäusedeckel geöffnet werden.

- Trennen Sie das Modul von der RS-485 Schnittstelle.
- Stecken Sie den Jumper neben der Klemme „51 41 61“.
- Halten Sie den Taster „S1“ gedrückt, bis ein akustisches Signal ertönt.

Die Pairing-Information wurde gelöscht.

Soll ein Pairing zwischen Funk-EK-Zylinder/Schloss und FMIO zurückgesetzt werden, darf der Jumper nicht gesteckt sein. In diesem Fall wird durch langes Drücken von „S1“ die Pairing-Information des Funk-EK-Zylinder/Schloss zurückgesetzt.

4. Bedienung Fingerscanner

Vor der Einrichtung und Benutzung des Zutrittssystems ist eine Inbetriebnahme durchzuführen. Gehen Sie dabei schrittweise vor.

- Montieren Sie den Fingerscanner wie im Kapitel 3 beschrieben.
- Führen Sie die elektrischen Anschlüsse nach Verkabelungsplan aus.

- Das erste Einschalten der Netzspannung initiiert die Verbindung (Pairing).

Zur Bedienung und Einrichtung des Fingerscanners stehen drei Betriebsmodi zur Verfügung. Mit dem Programmiergerät kann der Verwaltungsmodus umgestellt werden. **Im Auslieferungszustand ist die „Bluetoothverwaltung" aktiviert.** Weitere Modi sind die „Normalverwaltung" und „Indexverwaltung".

ACHTUNG **Der Eingang ist nicht gesichert und kann geöffnet werden, solange nicht der Masterfinger eingelernt wurden.**

4.1 Bedienhinweise

4.1.1 Umstellung der Verwaltungsart

HINWEIS **Nach dem Zurücksetzen gehen alle gespeicherten Informationen verloren, nur die Verwaltungsart bleibt erhalten.**

Der Betriebsmodus kann nur im Auslieferungszustand (alle LEDs leuchten) umgeschaltet werden. Diesen können Sie durch das Zurücksetzen Ihres Fingerscanners mit DA ›› CODE ›› OK erreichen. Der Code befindet sich auf Seite 4 und auf dem Programmiergerät.
Zur Umstellung des Verwaltungsmodus halten Sie das Programmiergerät direkt vor den Fingerscanner (blaue LED) und drücken die folgenden Tasten.

	9 » 9 » OK » 5 » 0 » OK	Normalverwaltung
	9 » 9 » OK » 5 » 1 » OK	Indexverwaltung
	9 » 9 » OK » 5 » 7 » OK	Bluetoothverwaltung (Auslieferungszustand)

Nach der Umstellung wechselt der Fingerscanner in den Auslieferungszustand (alle LEDs leuchten).

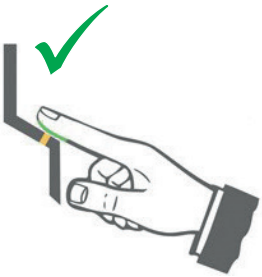
4.1.2 Fingerführung

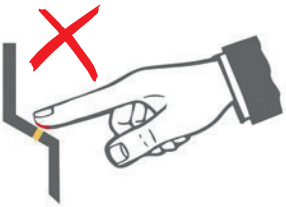
Gehen Sie bei dem Einlernen der Fingerabdrücke mit einer erhöhten Sorgfalt vor. Master- und Benutzerfinger können abgelehnt werden, wenn bei dem Einlernen Fehler gemacht werden. Je sorgfältiger ein Finger eingelernt wird, umso sicherer wird er bei der Identifikation später erkannt.

HINWEIS **Vor dem Einlernen der Master- oder Benutzerfinger empfehlen wir einmalig die Hände zu waschen.**

- Ziehen Sie zügig, gleichmäßig und mit leichtem Druck den Finger mit einem möglichst großen Teil der Fingerlinien über die Sensorzeile.

Bei der Wahl der Finger ist zu beachten, dass bei schmalen Fingern der Zeigefinger besser geeignet ist.





4.1.3 Verhalten bei Türöffnung (nur Türeinbau)

Bei den Ausführungen B-55600-23-4-8 und B-55600-23-4-9 (Fingerscanner zum Türeinbau) wird der Fingerscanner automatisch ausgeschaltet, wenn die Tür länger als 12 s geöffnet bleibt.

Die gespeicherten Fingerabdrücke zur Türöffnung bleiben bei Stromausfall erhalten. Datum und Uhrzeit zur Ereignisauswertung müssen nach einem Stromausfall neu eingestellt werden.

4.1.4 Programmiergerät, Abkürzungen

Taste	Bedeutung	Erklärung
DA	Delete All	Alle Löschen, inkl. Masterfinger
OK	OK	Funktion ausführen
R1 » B	Relay 1 » Block	Relais 1 » Benutzer-ID sperren
RT	Relay-Time	Schaltzeit
R2 » UB	Relay 2 » Unblock	Relais 2 » Benutzer-ID entsperren
D	Delete	Finger löschen
E	Enroll	Finger aufnehmen
TT	Time	Zeit (Sekunden)

Abkürzung	Bedeutung	Erklärung
MF	Masterfinger	Verwaltungsfinger
CODE	PIN-Code	Benutzer- oder Mastercode
ID	Index	Benutzer-ID
YYYY | MM | DD	Year | Month | Day	Jahr | Monat | Tag
HH | MM | TT	Hour | Minute | Time	Stunde | Minute | Sekunden (Zeit)

HINWEIS

Halten Sie das Programmiergerät direkt vor die blaue Leuchtdiode des Fingerscanners. Das Drücken der Tasten wird durch kurzes Aufleuchten der grünen LED optisch bestätigt. Leuchtet die LED nach dem Drücken nicht auf, wiederholen Sie die Eingabe.

4.2 Verwaltungsart Bluetoothverwaltung

Die Verwaltungsart „Bluetoothverwaltung“ ermöglicht es Ihnen, den Fingerscanner mit Ihrem Smartphone und der BKS BioKey-App einzurichten und zu verwalten. Nach der Autorisierung am Fingerscanner durch den Masterfinger können Sie über die Menüführung der BKS BioKey-App die gewünschte Funktion aufrufen und die notwendigen Einstellungen zur Administration Ihres Systems vornehmen.

Die Verwaltungsart „Bluetoothverwaltung“ ist im Auslieferungszustand voreingestellt. Um in einen anderen Modus zu wechseln, folgen Sie der Anleitung in Kapitel 4.1.1 [28].

- In der Verwaltungsart „Bluetoothverwaltung“ können Sie über die folgenden Funktionen den Fingerscanner einrichten.

4.2.1 Testmodus

Im Auslieferungszustand oder nach dem Zurücksetzen ist es möglich, dass zum Test mit dem Programmiergerät eine Türöffnung ausgelöst werden kann ohne den Fingerscanner vorher einzurichten. Voraussetzung ist, der Auslieferungszustand.

Beachten Sie, dass solange sich der Fingerscanner in Auslieferungszustand befindet, der Eingang nicht gesichert ist.

	■ Halten Sie das Programmiergerät direkt vor der blauen LED des Fingerscanners ■ Drücken Sie die Taste „0“ auf dem Programmiergerät ■ Die grüne LED leuchtet bei jedem Tastendruck zur optischen Kontrolle ■ Zur Bestätigung drücken Sie auf die Taste „OK“ ■ Die Türöffnung wird ausgelöst

4.2.2 Masterfinger einlernen

Aus Sicherheitsgründen wird vor jeder Konfiguration des Fingerscanners die Autorisierung über den Masterfinger geprüft. Aus diesem Grund beginnen Sie die Einrichtung mit dem Einlernen des Masterfingers und legen fest, wer später das System verwalten darf.

HINWEIS

Beginnen Sie im nächsten Schritt die Einrichtung des Fingerscanners, indem Sie den ersten Masterfinger einlernen, ohne die App zu öffnen (Fingerscanner im Auslieferungszustand).

Bei der Auswahl des Fingers ist zu beachten, dass ein Masterfinger nicht mehr als ein Benutzerfinger, mit dem die Tür geöffnet werden soll, verwendet werden kann. Deshalb wird empfohlen, dass Sie z. B. als Rechtshänder den linken Zeigefinger als Masterfinger und den rechten Zeigefinger als Benutzerfinger einlernen.

HINWEIS

Zum Einlernen des Masterfingers ziehen Sie 5-mal denselben Finger über den Sensor.

- Die grüne, rote und blaue LED leuchten dauerhaft
- Das Gerät ist initialisiert und bereit zur Einrichtung

HINWEIS! Voraussetzung ist, dass der Fingerscanner sich im Auslieferungszustand befindet oder ein Zurücksetzen durchgeführt wurde.

HINWEIS! Nach jedem Einlesen eines Fingers (den Finger über den Sensor ziehen) sollten Sie ca. 2 Sekunden warten, bis der Abschluss des Vorgangs durch das konstante leuchten der grünen und roten LED signalisiert wird. Erst dann können Sie mit dem Einlernen fortfahren und denselben Finger wieder über den Sensor ziehen.
Zwischen den einzelnen Einlernvorgängen des Masterfingers sollten nicht mehr als 60 Sekunden verstreichen, da sonst der Vorgang abgebrochen wird.

<table>
<tr>
<td> 
 
  </td>
<td>Einlernvorgang
■ Ziehen Sie den Finger, den Sie als ersten Masterfinger verwenden wollen über den Sensor
■ Die grüne und rote LED gehen nach dem Einlesen kurz aus
■ Nach ca. 2 Sekunden leuchtet die grüne und rote LED wieder dauerhaft. Der Fingerscanner ist bereit
■ Der nächste Einlernvorgang kann durchgeführt werden, indem Sie denselben Finger erneut über den Sensor ziehen
■ Wiederholen Sie den Einlernvorgang, bis der Finger 5-mal erfolgreich eingelernt wurde</td>
</tr>
<tr>
<td>  </td>
<td>■ Das erfolgreiche Einlernen des ersten Masterfingers wird durch kurzes aufleuchten, der grünen LED signalisiert
■ In Folge von Fehlversuchen, die während des Einlernens z. B. durch nicht ausreichende Qualität auftreten können, ist der Einlernvorgang so oft zu wiederholen, bis die grüne LED kurz aufleuchtet</td>
</tr>
<tr>
<td>  </td>
<td>■ Wenn der erste Masterfinger eingelernt ist, befindet sich das Gerät im Betriebszustand
■ Die blaue LED leuchtet dauerhaft
■ Es kann mit der Einrichtung fortgefahren werden</td>
</tr>
<tr>
<td colspan="2">HINWEIS! Wurde beim Einlernvorgang ein Finger über den Sensor gezogen und nicht als Masterfinger akzeptiert, so leuchten die grüne und rote LED weiterhin. Der Einlernvorgang des Masterfingers muss wiederholt werden.</td>
</tr>
</table>

Nach Einlernen des ersten Masterfingers können Sie nachträglich noch weitere Masterfinger hinzufügen, siehe Kapitel 4.2.6 [37] bzw. 4.3.3 [46].

4.2.3 Einrichtung der BKS BioKey-App

Die BKS BioKey-App ist für Apple iOS und Google Android erhältlich. Laden Sie die App je nach verwendeter Plattform aus dem App Store oder Google Play herunter. Geben Sie im Suchfeld des Stores den Begriff „BioKey“ ein.

Available on the App Store

GET IT ON Google Play

HINWEIS

Voraussetzungen zum Verwalten der BKS BioKey-App sind:
– die Bluetooth-Schnittstelle auf dem Smartphone ist aktiv
– die App darf auf den Standort des Smartphones zugreifen
– der erste Masterfinger wurde eingelernt, siehe Kapitel 4.2.2 [32]

- Achten Sie darauf, dass sich der Fingerscanner in Bluetooth-Reichweite Ihres Smartphones befindet.
- Starten Sie die BKS BioKey-App auf Ihrem Smartphone.
- Drücken Sie auf „Gerät wählen“ in der Kopfzeile des Displays.

Die BKS BioKey-App sucht nach verfügbaren Geräten und öffnet eine Liste der gefundenen Fingerscanner.

- Wählen Sie in der Liste den gewünschten Fingerscanner aus.
- Folgen Sie der Aufforderung zur Identifizierung am Fingerscanner.

	■ Masterfinger über den Sensor ziehen ■ Die grüne und rote LED leuchten einmal kurz auf

Das Smartphone ist mit dem Fingerscanner für diese Sitzung verbunden und die Konfiguration des Scanners kann über die App durchgeführt werden.

- Nach jedem Öffnen der App oder wenn die App eine Minute nicht verwendet wurde, werden Sie aus Sicherheitsgründen aufgefordert sich über den Masterfinger zu identifizieren.

4.2.4 Benutzer hinzufügen (BKS BioKey-App)

- Starten Sie die BKS BioKey-App auf Ihrem Smartphone.
- Folgen Sie der Aufforderung zur Identifizierung am Fingerscanner.

	■ Masterfinger über den Sensor ziehen ■ Die grüne und rote LED leuchten einmal kurz auf

- Drücken Sie auf den Button „Benutzer“.
- Drücken Sie auf **„+“ rechts in der Kopfzeile** des Displays.
- Wählen Sie „Nutzername“ aus und geben diesen ein.
- Drücken Sie auf „Finger hinzufügen“ im Bereich „Finger“ aus.
- Wählen Sie „Beschreibung“ aus und geben dort an, welcher Finger des Benutzers eingelesen werden soll.
- Vergeben Sie die Rechte des neuen Fingers durch Aktivierung bzw. Deaktivierung des Schalters für das jeweilige Relais 1 und 2 im Bereich „Berechtigungen“. Relais 2 nur bei Wandmontage UP/AP mit Funktion.
- Drücken Sie auf „Neuen Finger anlernen“ im Bereich „Finger“

	■ Folgen Sie den Dialog der BKS BioKey-App ■ Ziehen Sie den Finger, der als Benutzerfinger angelegt werden soll, über den Sensor ■ Wiederholen Sie den Einlernvorgang, bis der Finger 5-mal erfolgreich eingelernt wurde ■ Der Zähler in der App zeigt Ihnen den Fortschritt an bzw. wie oft Sie den Finger noch einscannen müssen Beachten Sie, dass ein Finger, der als Masterfinger eingelernt wurde, nicht als Benutzerfinger verwendet werden.

- Ist der Finger erfolgreich gespeichert, werden eine ID und die Anzahl der Scans angezeigt.

Je Benutzer kann nur ein Fingerabdruck angelegt werden. Die Anzahl der Benutzerfinger ist durch das Limit des Speicherplatzes auf 35 Fingerabdrücke begrenzt.

- Navigieren Sie über „<- zurück“ und „<“ in die übergeordneten Menüs. In diesen wird der neue Benutzerfinger bzw. Benutzer angezeigt.

4.2.5 Benutzer bearbeiten oder löschen (BKS BioKey-App)

- Starten Sie die BKS BioKey-App auf Ihrem Smartphone.
- Folgen Sie der Aufforderung zur Identifizierung am Fingerscanner.

	■ Masterfinger über den Sensor ziehen ■ Die grüne und rote LED leuchten einmal kurz auf

- Drücken Sie auf den Button „Benutzer“.
- Wählen Sie einen Benutzer in der Liste „Benutzer“ aus, um diesen in den folgenden Schritten zu bearbeiten.
- Wählen Sie „Nutzername“ im Bereich „Allgemein“ aus und ändern bzw. korrigieren diesen.
- Zum Bearbeiten oder Hinzufügen weiterer Benutzer- oder Masterfinger wählen Sie im Bereich „Finger“ die entsprechenden Eingabefelder aus und editieren diese.

Folgen Sie bitte den Anweisungen zum Einlernen eines neuen Benutzerfingers im Kapitel 4.2.4 [35].

- Aktivieren bzw. deaktivieren Sie den Schalter „Benutzer blockieren“ im Bereich „Aktionen“, damit der Benutzer gesperrt bzw. entsperrt wird.
- Wählen Sie „Benutzer löschen“ im Bereich „Aktionen“ aus und bestätigen zur Bestätigung das Löschen.

4.2.6 Masterfinger hinzufügen (BKS BioKey-App)

- Starten Sie die BKS BioKey-App auf Ihrem Smartphone.
- Folgen Sie der Aufforderung zur Identifizierung am Fingerscanner.

	■ Masterfinger über den Sensor ziehen ■ Die grüne und rote LED leuchten einmal kurz auf

- Drücken Sie auf den Button „Benutzer“.
- Drücken Sie auf **„+“ rechts in der Kopfzeile** des Displays.
- Wählen Sie „Nutzername“ aus und geben diesen ein.
- Aktivieren Sie den Schalter „Master-Benutzer“.
- Drücken Sie auf „Finger hinzufügen“ im Bereich „Finger“.
- Drücken Sie auf „Neuen Finger anlernen“.

	■ Folgen Sie den Dialog der BKS BioKey-App ■ Ziehen Sie den Finger, der als Masterfinger angelegt werden soll, über den Sensor ■ Wiederholen Sie den Einlernvorgang, bis der Finger 5-mal erfolgreich eingelernt wurde ■ Der Zähler in der App zeigt Ihnen den Fortschritt an bzw. wie oft Sie den Finger noch einscannen müssen Beachten Sie, dass ein Finger, der als Masterfinger eingelernt wurde, nicht als Benutzerfinger verwendet werden.

4.2.7 Identifikation durch Benutzerfinger, Tür öffnen

	■ Das Gerät befindet sich im Betriebszustand ■ Die blaue LED leuchtet
	■ Den Benutzerfinger über den Sensor ziehen ■ Bei Fingererkennung leuchtet die grüne LED auf und die Tür wird geöffnet In der Verwaltungsart Normalverwaltung wird bei der AP/ UP-Variante (Wandmontage) immer das Relais 1 geschaltet.
	■ Wird der Benutzerfinger vom Fingerscanner nicht erkannt, leuchtet die rote LED auf und die Tür wird nicht geöffnet

4.2.8 Sperrmodus

	**Sperrung** ■ Wird 10-mal hintereinander ein nicht eingelernter Finger über den Sensor gezogen (rote LED leuchtet), wechselt das Gerät in einen Sperrmodus. Hierdurch wird verhindert, dass unbefugte Personen sich ungestört Zutritt verschaffen können Im Sperrmodus wird auf keine Finger und Eingaben des Programmiergeräts reagiert. Die Sperrzeit beträgt 1 Minute. Die rote LED blinkt in der Sperrzeit.
	**Entsperrung** ■ Der Sperrmodus kann vorzeitig beendet werden, indem ein eingelernter Finger (Master- oder Benutzerfinger) über den Sensor gezogen wird. Anschließend kann die Tür wie gewohnt mit einem Benutzerfinger geöffnet werden.

4.2.9 Zurücksetzen, alle Benutzer- und Masterfinger löschen

HINWEIS

Schließen Sie vor dem Zurücksetzen die BKS BioKey App auf Ihrem Smartphone.

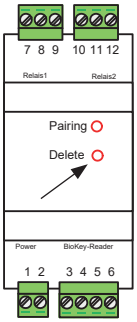
Halten Sie das Programmiergerät direkt vor die blaue Leuchtdiode des Fingerscanners.

- Taste „DA“ (Delete all) auf dem Programmiergerät drücken (die grüne LED leuchtet beim Tastendruck)
- Geben Sie bitte den Werkscode von Seite 4 bzw. den Mastercode mit dem Programmiergerät ein
- Zum Beenden des Löschvorganges drücken Sie auf die Taste „OK“
- Das Gerät ist initialisiert, die grüne, rote und blaue LED leuchten dauerhaft

HINWEIS

Der Fingerscanner wird auch durch ein Repairing zurückgesetzt. Dabei werden auch alle Benutzer- und Masterfinger gelöscht sowie der Mastercode auf den Werkscode zurückgesetzt!

4.2.9.1 Alternatives Zurücksetzen mit dem Relaismodul „Whitebox“ (AP/UP)



Bei der AP/UP-Variante zur Wandmontag können Sie mit der der Relaisbox „Whitebox“ ein Zurücksetzen auf Werkseinstellungen mit dem Löschen aller Fingerabdrücke incl. des Masterfingers auslösen.

- Drücken Sie zum Start des Löschens ca. 5 Sekunden auf die Taste in der mit „Delete“ beschrifteten und rot umrandeten Bohrung der Inneneinheit.

Nach dem Zurücksetzen leuchten die grüne, rote und blaue LED konstant.

HINWEIS

Nach dem Zurücksetzen wird der geänderter Mastercode auf den Werkscode zurückgesetzt!

4.2.9.2 Alternatives Zurücksetzen mit dem Masterfinger

	■ Der Fingerscanner befindet sich im Betriebszustand ■ Die blaue LED leuchtet
	■ Ziehen Sie den Masterfinger über den Sensor, wodurch die grüne und rote LED einmal kurz aufleuchten
	■ Nach dem zweiten Einlesen des Masterfingers wird durch wiederholtes kurzes Blinken der grünen und roten LED darauf hingewiesen, dass der Löschmodus initialisiert wird
	■ Nach dem vierten Einlesen des Masterfingers wird der Löschvorgang gestartet und durch das Aufleuchten der grünen LED signalisiert
	■ Nach dem Zurücksetzen befindet sich der Fingerscanner im Auslieferungszustand ■ Die grüne und rote LED leuchten dauerhaft

HINWEIS

Nach dem Zurücksetzen wird der geänderter Mastercode auf den Werkscode zurückgesetzt!

4.2.10 Ändern des Werkscodes zum Mastercode (BKS BioKey-App)

Der Werkscode (siehe Seite 4) kann mit der BKS BioKey-App oder dem Programmiergerät in einen 6-stelligen Mastercode geändert werden.

HINWEIS

Aus Sicherheitsgründen ist es zu empfehlen, den Werkscode durch einen neuen Mastercode zu ersetzen! Nach dem Zurücksetzen wird der Mastercode auf den Werkscode zurückgesetzt!

- Starten Sie die BKS BioKey-App auf Ihrem Smartphone.
- Folgen Sie der Aufforderung zur Identifizierung am Fingerscanner.

	■ Masterfinger über den Sensor ziehen ■ Die grüne und rote LED leuchten einmal kurz auf

- Drücken Sie auf den Button „Einstellungen“.
- Wählen Sie „Resetcode“ aus und geben einen neuen Code ein.

4.2.10.1 Ändern mit dem Programmiergerät

	■ Taste „D“ (Delete) auf dem Programmiergerät ■ Drücken Sie die Taste „E“ (Enroll) ■ Geben Sie den Werkscode bzw. „alten CODE“ ein und drücken zur Bestätigung die Taste „OK“ ■ Geben Sie den „neuen CODE“ ein und drücken zur Bestätigung die Taste „OK“ ■ Wiederholen Sie die Eingabe des Mastercodes („neuen CODE“) und drücken zum Beenden die Taste „OK“

4.2.11 Zutrittsprotokoll anzeigen (BKS BioKey-App)

- Starten Sie die BKS BioKey-App auf Ihrem Smartphone.
- Folgen Sie der Aufforderung zur Identifizierung am Fingerscanner.

	■ Masterfinger über den Sensor ziehen ■ Die grüne und rote LED leuchten einmal kurz auf

- Drücken Sie auf den Button „Zutrittsprotokoll“.

Es wird die Liste „Zutrittsprotokoll“ geöffnet und die im Fingerscanner gespeicherten Ereignisse werden angezeigt. Diese Liste beinhaltet u. a. erfolgreiche und abgelehnte Identifikationen.

4.2.12 Schaltzeiten der Relais einstellen (BKS BioKey-App)

Die Relais sind nur bei Wandmontage UP/AP über Schaltzeiten steuerbar. Bei Geräten für den Türeinbau wird diese Funktion nicht unterstützt.

- Starten Sie die BKS BioKey-App auf Ihrem Smartphone.
- Folgen Sie der Aufforderung zur Identifizierung am Fingerscanner.

	■ Masterfinger über den Sensor ziehen ■ Die grüne und rote LED leuchten einmal kurz auf

- Drücken Sie auf den Button „Relaiszeit“.
- Wählen Sie „Relais 1“ oder „Relais 2“ aus, um dieses einzustellen.
- Wählen Sie „Beschreibung“ aus, um einen neuen Namen für das Relais zu vergeben. Dieser wird im Zutrittsprotokoll bzw. Benutzervergabe angezeigt.
- Über das Eingabefeld „Zeit“ ist die Schaltzeit des jeweiligen Relais im Zeitraum zwischen 0 und 60 Sekunden einstellbar.

4.2.13 Umbenennung des Fingerscanners und Anzeige der Speichernutzung (BKS BioKey-App)

- Starten Sie die BKS BioKey-App auf Ihrem Smartphone.
- Folgen Sie der Aufforderung zur Identifizierung am Fingerscanner.

	■ Masterfinger über den Sensor ziehen ■ Die grüne und rote LED leuchten einmal kurz auf

- Drücken Sie auf den Button „Einstellungen“.
- Wählen Sie „Gerätename“ aus und ändern den Namen des Fingerscanners.

Die Anzeige dieses Menüs bietet eine Übersicht der Informationen wie z. B. der Speicherbedarf der eingelernten Fingerabdrücke, der verfügbare Speicher und die Firmware-Version etc..

4.3 Verwaltungsart Normalverwaltung

In der Verwaltungsart „Normalverwaltung“ ist es möglich, den Fingerscanner auch ohne die Verwendung einer App einzurichten und zu verwalten. Die Einrichtung des Fingerscanners wird im Modus „Normalverwaltung“ in erster Linie mit dem Masterfinger vorgenommen. Für spezielle Funktionen wird auch das Programmiergerät benötigt.

Zum Wechseln in diese Verwaltungsart folgen Sie der Anleitung in Kapitel 4.1.1 [28].

■ Die Verwaltungsart „Normalverwaltung“ bietet folgende Funktionen.

4.3.1 Funktionsübersicht

Funktion	Beschreibung | Kurzanleitung
Testmodus (nur im Auslieferungszustand möglich)	→ Kapitel 4.2.1 [31] 0 » OK
Masterfinger einlernen	→ 4.2.2 [32] Auslieferungszustand » Masterfinger 5-mal erfolgreich einlernen
Benutzerfinger einlernen	→ Kapitel 4.3.2 [45] Masterfinger scannen » Benutzerfinger 5-mal erfolgreich einlernen
Identifikation durch Benutzerfinger	→ Kapitel 4.2.7 [38] Benutzerfinger scannen
Sperrung des Fingerscanners	→ Kapitel 4.2.8 [38] Nach 10 Fehlversuchen ohne Identifikation des Fingers wird der Fingerscanner gesperrt
Entsperren des Fingerscanners	→ Kapitel 4.2.8 [38] Eingelernten Master- oder Benutzerfinger einscannen

Funktion	Beschreibung	Kurzanleitung
Zurücksetzten, alle Benutzer- und Masterfinger löschen	→ Kapitel 4.2.9 [39] DA » CODE » OK (CODE: aktueller Werks- oder Mastercode)
Werkscode ändern	→ Kapitel 4.2.10 [40] → D » E » alter CODE » OK » neuer CODE » OK » neuer CODE » OK
Masterfinger hinzufügen	→ Kapitel 4.3.3 [46] MF » E » 0 » Masterfinger 5-mal erfolgreich einlernen
Relais-Schaltzeit einstellen	→ Kapitel 4.3.4 [47] MF » RT » TT » OK *TT = Zeit in s [1...60 s], Standard = 3 s*
Datum und Zeit einstellen	→ Kapitel 4.3.5 [47] MF » E » RT » YYYY » OK » MM » OK » DD » OK » HH » OK » MM »OK

Weitere Informationen zur Tastenbelegung der Programmiergerät und Erklärung der Abkürzungen siehe Kapitel 4.1.4 [30].

4.3.2 Benutzerfinger einlernen

	■ Das Gerät befindet sich im Betriebszustand und die blaue LED leuchtet **HINWEIS!** Masterfinger dürfen nicht als Benutzerfinger eingelernt werden
	■ Masterfinger über den Sensor ziehen ■ Die grüne und rote LED leuchten kurz auf
 	**Einlernvorgang** ■ Ziehen Sie den Finger, den Sie als Benutzerfinger verwenden wollen über den Sensor ■ Das Einlesen wird durch **kurzes aufleuchten**, der **grünen LED** bestätigt ■ Der nächste Einlernvorgang kann durchgeführt werden, indem Sie denselben Finger erneut über den Sensor ziehen
	■ Wiederholen Sie den Einlernvorgang, bis der Finger 5-mal erfolgreich eingelernt wurde ■ Das erfolgreiche Einlernen des Benutzerfingers wird durch **4-maliges** kurzes **Aufleuchten** der **grünen und roten LED** signalisiert ■ Zur Signalisierung der Betriebsbereitschaft leuchtet die blaue LED dauerhaft
HINWEIS! Bei „schwierigen“ Fingern kann es notwendig sein, diesen einen Benutzerfinger öfters einzulernen. Bei zu vielen Fehlversuchen sollten Sie einen anderen Finger als Benutzerfinger verwenden.	

Die Anzahl der Benutzerfinger ist durch das Limit des Speicherplatzes auf 35 Fingerabdrücke für Master- und Benutzerfinger begrenzt.

4.3.3 Masterfinger hinzufügen

	■ Masterfinger über den Sensor ziehen ■ Die grüne und rote LED leuchten kurz auf
	■ Taste „E“ (Enroll) auf dem Programmiergerät drücken ■ Drücken Sie auf die Taste „0“
 	**Einlernvorgang** ■ Ziehen Sie den Finger, den Sie als Masterfinger hinzufügen wollen über den Sensor ■ Das Einlesen wird durch **kurzes aufleuchten**, der **grünen LED** bestätigt ■ Der nächste Einlernvorgang kann durchgeführt werden, indem Sie denselben Finger erneut über den Sensor ziehen
	■ Wiederholen Sie den Einlernvorgang, bis der Finger 5-mal erfolgreich eingelernt wurde ■ Das erfolgreiche Einlernen des Benutzerfingers wird durch **4-maliges** kurzes **Aufleuchten** der **grünen und roten LED** signalisiert ■ Zur Signalisierung der Betriebsbereitschaft leuchtet die blaue LED dauerhaft

4.3.4 Relais-Schaltzeit einstellen (nur AP/UP)

	■ Masterfinger über den Sensor ziehen ■ Die grüne und rote LED leuchten kurz auf
	■ Taste „RT“ auf dem Programmiergerät drücken ■ Geben Sie bitte eine Schaltzeit in Sekunden von 1 bis 60 über die Tastatur ein ■ Zum Beenden drücken Sie auf die Taste „OK“

In der Verwaltungsart „Normalverwaltung“ ist nur die Schaltzeit für Relais 1 einstellbar.

4.3.5 Datum und Zeit initialisieren

Im Fingerscanner gespeicherte Zutritte können mit dem Audit-Set ausgelesen werden (B-55606-00-3-0). Die gelisteten Zutritte erhalten nur einen richtigen Zeitstempel, wenn Sie initial Datum und Uhrzeit einrichten.

	■ Masterfinger über den Sensor ziehen ■ Die grüne und rote LED leuchten kurz auf
	■ Taste „E“ auf dem Programmiergerät drücken ■ Taste „RT“ drücken ■ Geben Sie Datum und Uhrzeit über die Tastatur ein und bestätigen nach jedem Schritt mit der Taste „OK“: YYYY » OK » MM » OK » DD » OK » HH » OK » MM »OK Beispiel: 23.07.2022, 12:45 Uhr: E » RT » 2022 » OK » 07 » OK » 23 » OK »12 » OK » 45 »OK

HINWEIS **Nach einem Stromausfall müssen Datum und Uhrzeit neu eingestellt werden.**

4.4 Verwaltungsart Indexverwaltung

In der Verwaltungsart „Indexverwaltung“ ist es möglich, den Fingerscanner auch ohne die Verwendung einer App einzurichten und zu verwalten. In dieser Verwaltungsart wird jeder Benutzer einer ID zugeordnet, wodurch eine verbesserte Verwaltung möglich ist. Die Einrichtung erfolgt über Masterfinger und das Programmiergerät. In der Indexverwaltung können Sie eine ID auswählen und gezielt bearbeiten wie z. B. den Benutzerfinger einer ID löschen. Es ist ratsam die Zuordnung in einer Liste zu dokumentieren, siehe Vorlage in Kapitel 4.4.9 [55].

Zum Wechseln in diese Verwaltungsart folgen Sie der Anleitung in Kapitel 4.1.1 [28].

■ Die Verwaltungsart „Indexverwaltung“ bietet folgende Funktionen.

4.4.1 Funktionsübersicht

Funktion	Beschreibung | Kurzanleitung
Testmodus (nur im Auslieferungszustand möglich)	→ Kapitel 4.2.1 [31] 0 » OK
Masterfinger einlernen	→ Kapitel 4.2.2 [32] Auslieferungszustand » Masterfinger 5-mal erfolgreich einlernen
Benutzerfinger einlernen	→ Kapitel 4.4.2 [50] MF » E » ID » OK » Benutzerfinger 5-mal erfolgreich einlernen
Identifikation durch Benutzerfinger	→ Kapitel 4.2.7 [38] Benutzerfinger scannen
Sperrung des Fingerscanners	→ Kapitel 4.2.8 [38] Nach 10 Fehlversuchen ohne Identifikation des Fingers wird der Fingerscanner gesperrt
Entsperren des Fingerscanners	→ Kapitel 4.2.8 [38] Eingelernten Master- oder Benutzerfinger einscannen

Funktion	Beschreibung | Kurzanleitung
Zurücksetzten, alle Benutzer- und Masterfinger löschen	→ Kapitel 4.2.9 [39] DA » CODE » OK (CODE: aktueller Werks- oder Mastercode)
Werkscode ändern	→ Kapitel 4.2.10 [40] D » E » alter CODE » OK » neuer CODE » OK » neuer CODE » OK
Löschen einzelner Benutzerfinger	→ Kapitel 4.4.3 [51] MF » D » ID » OK
Sperren von IDs	→ Kapitel 4.4.4 [52] MF » B » ID » OK
Entsperren von IDs	→ Kapitel 4.4.5 [52] MF » UB » ID » OK
ID kontrollieren	→ Kapitel 4.4.6 [53] OK » ID » OK
Masterfinger hinzufügen	→ Kapitel 4.3.3 [46] MF » E » 0 » Masterfinger 5-mal erfolgreich einlernen
Relais-Schaltzeit Relais 1 einstellen (nur AP/UP)	→ Kapitel 4.4.7 [53] MF » RT » R1 » TT » OK *TT = Zeit in s [1...60 s], Standard = 3 s*
Relais-Schaltzeit Relais 2 einstellen (nur AP/UP)	→ Kapitel 4.4.7 [53] MF » RT » R2 » TT » OK *TT = Zeit in s [1...60 s], Standard = 3 s*
Benutzerfinger einlernen für Relais 1	→ Kapitel 4.4.8 [54] MF » E » ID » R1 » OK » Benutzerfinger 5-mal erfolgreich einlernen
Benutzerfinger einlernen für Relais 2 (nur Wandmontage UP/AP)	→ Kapitel 4.4.8 [54] MF » E » ID » R2 » OK » Benutzerfinger 5-mal erfolgreich einlernen

Funktion	Beschreibung	Kurzanleitung
Datum und Zeit einstellen	→ Kapitel 4.3.5 [47] MF » E » RT » YYYY » OK » MM » OK » DD » OK » HH » OK » MM »OK

Weitere Informationen zur Tastenbelegung des Programmiergeräts und Erklärung der Abkürzungen siehe Kapitel 4.1.4 [30].

4.4.2 Benutzerfinger einlernen

	■ Das Gerät befindet sich im Betriebszustand und die blaue LED leuchtet **HINWEIS!** Masterfinger dürfen nicht als Benutzerfinger eingelernt werden
	■ Masterfinger über den Sensor ziehen ■ Die grüne und rote LED leuchten kurz auf
	■ Taste „E“ (Enroll) auf dem Programmiergerät drücken ■ Geben Sie eine ID zwischen 1 und 35 über die Tastatur ein ■ Taste „OK“ zur Bestätigung drücken
 	**Einlernvorgang** ■ Ziehen Sie den Finger, den Sie als Benutzerfinger verwenden wollen über den Sensor ■ Das Einlesen wird durch **kurzes aufleuchten**, der **grünen LED** bestätigt ■ Der nächste Einlernvorgang kann durchgeführt werden, indem Sie denselben Finger erneut über den Sensor ziehen

	■ Wiederholen Sie den Einlernvorgang, bis der Finger 5-mal erfolgreich eingelernt wurde ■ Das erfolgreiche Einlernen des Benutzerfingers wird durch **4-maliges** kurzes **Aufleuchten** der **grünen und roten LED** signalisiert ■ Zur Signalisierung der Betriebsbereitschaft leuchtet die blaue LED dauerhaft
HINWEIS! Bei „schwierigen" Fingern kann es notwendig sein, diesen einen Benutzerfinger öfters einzulernen. Bei zu vielen Fehlversuchen sollten Sie einen anderen Finger als Benutzerfinger verwenden.	

Die Anzahl der Benutzerfinger ist durch das Limit des Speicherplatzes auf 35 Fingerabdrücke für Master- und Benutzerfinger begrenzt.

4.4.3 Einzelne Benutzerfinger löschen

	■ Einen Masterfinger über den Sensor ziehen ■ Die grüne und rote LED leuchten kurz auf
	■ Taste „D" (Delete) des Programmiergeräts drücken, die grüne LED leuchtet auf ■ Eingabe der ID des zu löschenden Benutzerfingers ■ Mit Taste „OK" bestätigen, die grüne LED leuchtet auf Der unter der eingegebenen ID gespeicherte Benutzerfinger ist nun gelöscht und wird beim Versuch, die Tür zu öffnen, abgewiesen.

4.4.4 Sperren von IDs

	■ Masterfinger über den Sensor ziehen ■ Die grüne und rote LED leuchten kurz auf.
	■ Taste „R1 (B)“ drücken ■ ID eingeben ■ Mit Taste „OK“ bestätigen Der unter der eingegebenen ID gespeicherte Benutzerfinger ist nun gesperrt und wird beim Versuch, die Tür zu öffnen, abgewiesen.

HINWEIS

Einzelne IDs können vorübergehend gesperrt werden, ohne dass der eingelernte Fingerabdruck verloren geht. Die ID kann später entsperrt werden, ohne dass die entsprechende Person anwesend sein muss, um Ihren Abdruck nochmals einzulernen.

4.4.5 Entsperren von IDs

	■ Masterfinger über den Sensor ziehen ■ Die grüne und rote LED leuchten kurz auf
	■ Taste „R2 (UB)“ drücken ■ ID eingeben ■ Mit Taste „OK“ bestätigen Der unter der eingegebenen ID gespeicherte Benutzerfinger ist wieder freigegeben und kann die Tür öffnen.

4.4.6 ID kontrollieren

	■ Taste „OK“ drücken ■ Nummer der zu überprüfenden ID eingeben ■ Erneut Taste „OK“ drücken ■ Bei einer bereits vergebenen ID, leuchten die grüne und rote LED auf ■ Ist die ID nicht vergeben, leuchtet nur die rote LED

4.4.7 Relais-Schaltzeit pro Relais einstellen (nur AP/UP)

In der „Indexverwaltung“ wird die Schaltdauer pro Relais separat festgelegt.

	■ Einen Masterfinger über den Sensor ziehen ■ Die grüne und rote LED leuchten kurz auf
	■ Taste „RT“ des Programmiergeräts drücken ■ Auswahl des Relais über die Taste „R1“ oder „R2“ ■ Geben Sie bitte eine Schaltzeit in Sekunden von 1 bis 60 über die Tastatur ein ■ Mit Taste „OK“ bestätigen, die grüne LED leuchtet auf

4.4.8 Benutzerfinger einlernen für Relais 1/2 (nur AP/UP)

Bei der AP/UP-Variante können beide Relais getrennt geschaltet werden.

	■ Masterfinger über den Sensor ziehen ■ Die grüne und rote LED leuchten kurz auf
	■ Taste „E“ (Enroll) auf dem Programmiergerät drücken ■ Geben Sie eine ID zwischen 1 und 35 über die Tastatur ein ■ Wählen Sie über die Taste „R1“ oder „R2“ ein das Relais aus ■ Taste „OK“ zur Bestätigung drücken
 	**Einlernvorgang** ■ Ziehen Sie den Finger, den Sie als Benutzerfinger verwenden wollen über den Sensor ■ Das Einlesen wird durch **kurzes aufleuchten**, der **grünen LED** bestätigt ■ Der nächste Einlernvorgang kann durchgeführt werden, indem Sie denselben Finger erneut über den Sensor ziehen
	■ Wiederholen Sie den Einlernvorgang, bis der Finger 5-mal erfolgreich eingelernt wurde ■ Das erfolgreiche Einlernen des Benutzerfingers wird durch **4-maliges** kurzes **Aufleuchten** der **grünen und roten LED** signalisiert ■ Zur Signalisierung der Betriebsbereitschaft leuchtet die blaue LED dauerhaft

4.4.9 Zuordnung von ID und Person

ID	Person (Name)	Fingerbezeichnung (Daumen, Zeigefinger,...)

5. Bedienung der Codetastatur

Vor der Einrichtung und Benutzung des Zutrittssystems ist eine Inbetriebnahme durchzuführen. Gehen Sie dabei schrittweise vor.

- Montieren Sie die Codetastatur wie im Kapitel 3 beschrieben.
- Führen Sie die elektrischen Anschlüsse nach Verkabelungsplan aus.

- Das erste Einschalten der Netzspannung startet die Kopplung (Pairing).

Im Auslieferungszustand leuchten alle LEDs (grün/rot/ggf. blau) konstant. Die Eingaben werden über die Codetastatur direkt eingeben. Es ist kein Programmiergerät erforderlich bzw. im Lieferumfang enthalten.

	Tür öffnen
*	Eingabestart bzw. Bestätigung dieser
Mastercode	Verwaltungscode
Benutzercode	Code zur Türöffnung

HINWEIS

Jedes Drücken einer Taste wird durch kurzes Aufleuchten der grünen LED optisch angezeigt. Wiederholen Sie die Eingabe, wenn nach dem Drücken einer Taste die grüne LED nicht aufleuchtet.

Die Ziffernkombinationen für den Mastercode bzw. den Benutzercode sollte 4-6-stellige Zahlenkombination sein. Bestimmte Mastercode- bzw. Benutzercode-Kombinationen sind aus Sicherheitsgründen ausgeschlossen. Dazu gehören regelmäßige Zahlenkombinationen wie 8888, 123456, 4321 etc. Den initialen Mastercode (Werkscode) finden Sie auf der Seite 4.

Wird 5-mal hintereinander ein falscher Benutzercode eingegeben, wechselt das Gerät in einen Sperrmodus. Hierdurch wird verhindert, dass unbefugte Personen sich Zutritt verschaffen können.

Ist das Gerät im Sperrmodus, so wird dies durch Blinken der roten LED angezeigt. Der Sperrmodus ist zunächst zeitlich begrenzt. Nach weiteren 5 Fehlversuchen verlängert sich jeweils die Sperrzeit (Sperrintervalle: 1 Minute, 5 Minuten, 30 Minuten, 1 Stunde, danach Dauersperrung).

Wird zweimal hintereinander ein gültiger Benutzercode eingegeben, so wird der Sperrmodus beendet.

5.1 Testmodus

Im Auslieferungszustand kann zu Testzwecken eine Türöffnung erfolgen. Drücken Sie hierzu die Tastenfolge 0 » 🔑. Die grüne LED leuchtet zur Bestätigung.

	
0	🔑

5.2 Mastercode ändern

HINWEIS **Aus Sicherheitsgründen empfehlen wir, den Werkscode durch einen eigenen Mastercode zu ersetzen!**

				
*	Mastercode	*	1	*

			
neuer Mastercode	*	neuer Mastercode	*

5.3 Benutzercode setzen/ändern

				
*	Mastercode	*	2	*

					
Benutzer-ID [1...150]	*	Benutzer-code	*	Benutzer-code	*

HINWEIS

Bei der AP/UP-Variante können beide Relais getrennt voneinander geschaltet werden. Eine ungerade Benutzer-ID schaltet Relais 1, eine gerade ID das Relais 2.

5.4 Tür öffnen

	
Benutzer-code	

HINWEIS

Werden Ziffern zusätzlich vor dem Benutzercode eingegeben, werden diese ignoriert.

5.5 Benutzercode löschen

				
*	Mastercode	*	3	*

	
Benutzer-ID	*

Alternativ:

				
*	Mastercode	*	3	*

			
0	*	Benutzer-code	*

HINWEIS

Durch ein Repairing wird die Codetastatur zurückgesetzt. Dabei werden alle Benutzercodes gelöscht.
Nach dem Zurücksetzten wird der geänderter Mastercode auf den Werkscode zurückgesetzt!

5.6 Relais-Schaltzeit einstellen (nur AP/UP)

				
*	Mastercode	*	4	*

			
Relais [1|2]	*	Zeit [1...60 s]	*

5.7 Alle Benutzercodes und Mastercode löschen

				
*	Mastercode	*	0	*

	
Mastercode	*

6. Wartung und Pflege

- Die Betriebsbereitschaft ist regelmäßig zu prüfen.
- Ein defektes Produkt ist durch ein Neues zu ersetzen.

Die Sensorfläche des Fingerscanners ist aufgrund der immer wiederkehrenden Verwendung (Finger scannen) praktisch selbstreinigend. Falls der Fingerscanner trotzdem verschmutzt, reinigen Sie ihn mit Wattestäbchen, Mikrofaser- und Brillentücher. Nicht geeignet sind sämtliche Stoffe aus Baumwolle, Papiertücher, Küchenschwämme und Geschirrtücher. Verwenden Sie reines Wasser ohne Reinigungsmittelzusätze. Gehen Sie behutsam im Sensorflächenbereich vor.

Die Codetastatur ist zur Sicherheit von Fingerabdrücken und Verschmutzungen mit einem feuchten (nicht nassen) und nicht kratzenden Tuch zu reinigen. Verwenden Sie hierbei nur reines Wasser ohne Reinigungsmittelzusätze.

Bei Variante Türeinbau:
Bei häufiger Nutzung pflegen Sie die Kontakte des SECURE*connect* 200 mit dem Kontaktfett B-55606-00-4-0.

Die Betriebsbereitschaft des Verschlusssystems ist regelmäßig zu prüfen. Hierzu müssen die Befestigungspunkte überprüft- und die Schrauben ggf. nachgezogen werden. Die mechanischen Eigenschaften des Schlosses (Schlüssel- bzw. Drückerbedienung / Fallenriegel) dürfen nicht durch Verschmutzung beeinträchtigt werden und müssen ebenfalls regelmäßig gewartet werden.

Die Schlossmechanik ist lebensdauergeschmiert und somit wartungsfrei. Den Fallenriegelkopf 1x jährlich leicht fetten. Verwenden Sie kein Öl, dieses kann die Schlosselektronik beschädigen!

7. Fehlersuche und -behebung

Fehlerbeschreibung	Ursache	Abhilfe
Die rote LED blinkt dauerhaft mehrmals pro Sekunde	Keine Busverbindung zur Steuereinheit	Prüfen Sie die Verkabelung oder nehmen Sie das Gerät in Betrieb
	Kein Pairing bzw. Pairing fehlerhaft	Führen Sie ein Zurücksetzten des Pairings aus
Die grüne und rote LED blinken dauerhaft	Fehler in der Verkabelung des RS-485 Bus	Anschlussklemmen überprüfen und ggf. Anschlüsse korrekt anschließen
Die rote LED blinkt dauerhaft alle zwei Sekunden	Sperrmodus: System nach mehrmaligen ungültigen Identifikationen gesperrt.	Scannen Sie einen berechtigten Finger ein
Die grüne LED leuchtet bei Zutrittsversuch, aber die Tür öffnet nicht	Verbindungsproblem zwischen SC200R und SC200F	Kontakte des SC200 reinigen
		Einbauposition SC200 überprüfen
	Verbindungsproblem – zwischen Innen- und Außeneinheit – zwischen Relais und angeschlossener Komponente z. B. E-Öffner	Die Verkabelung überprüfen
		Spannungsversorgung aus und neu einschalten
		Defekte Hardware austauschen
Die rote LED leuchtet dauerhaft	Hardware Defekt	Austausch des Fingerscanners bzw. der Codetastatur notwendig

8. Instandhaltung und Ersatzteile

Wir empfehlen je nach Nutzung und Einbausituation eine regelmäßige Inspektion, Pflege und Reinigung. Störungen und Mängel sind umgehend zu beheben.

⚠ GEFAHR

Lebensgefahr durch elektrischen Strom!

Trennen Sie die Spannungsversorgung und entladen gespeicherte Restenergien.

Instandhaltungsarbeiten dürfen nur von Fachkräften ausgeführt werden, welche vom Hersteller geschult bzw. autorisiert sind.

Im Servicefall empfehlen wir, vor einer Instandsetzung vor Ort, den Service der Unternehmensgruppe Gretsch-Unitas zu kontaktieren und ggf. nach Absprache das Produkt einzuschicken.

Demontieren Sie das Produkt aus dem Bauraum. Zum Ausbau lösen Sie die Befestigungen, trennen die elektrischen Anschlüsse und entfernen das Produkt.

Werden Ersatzteile oder Erweiterungen benötigt, so dürfen ausschließlich Originalteile des Herstellers verwendet werden. Bei Verwendung von Fremdfabrikaten besteht kein Haftungs-, Gewährleistungs- oder Serviceleistungsanspruch.

9. Entsorgung

HINWEIS

Die Abfallentsorgung ist getrennt vom Hausmüll durchzuführen. Gemäß der national und lokal geltenden Gesetze und Richtlinien ist eine ordnungsgemäße Entsorgung im entsprechenden Recycling-Prozess durchzuführen.

Das Produkt ist als Elektronikschrott an öffentlichen Rücknahmestellen und/oder Wertstoffhöfen zu entsorgen. Die Verpackung ist separat zu entsorgen.

Table of contents

Your factory code:

The factory code can also be found on an adhesive label on the back of the programming device. If you have defined your own master code, this code must be used.

Please hand this document over to the user!

1. Information and safety instructions

1.1 General information regarding theses instructions

Thank you for choosing the fingerprint scanner and code keypad as access control for motor-driven or electromechanical exit devices.

These operating instructions contain important notes which must be followed in order to prevent danger, to reduce downtimes and repair costs and to ensure reliability and long lifetime.

The operating instructions must be read and followed by every person **before** use of the product. Pay particular attention to the instructions during:

- mounting and electrical installation
- start-up, operation and maintenance

The operating instructions must be handed over to the operator/customer once the installation is complete. Please read this manual carefully before the first operation and keep it for future reference. Please instruct all operators/customers to read the operating instructions.

1.2 Safety instructions

These operating instructions are aimed at trained specialist personnel with knowledge of installing lock, door hardware and electronic components and provide information on how to install, start-up and operate these products.

The necessity to observe the instructions given in this manual must be pointed out to customers and users in order to prevent false assembly and improper usage.

- The appropriate local installation specifications, directives and regulations must be followed. This applies especially to the VDE directives and regulations, e.g., DIN VDE 0100 and IEC 60364.

- No liability is assumed for damage arising from improper use, assembly and installation, and from use of non-original parts and accessories!
- It is necessary to ensure that only trained specialists (for the definition thereof see EN 50110-1, DIN VDE 0105 or IEC 60364) are charged with jobs related to the product (planning, transport, assembly, installation, start-up, maintenance, repair, disassembly).
- Moreover, it is necessary to ensure that the documents required for installation, start-up, operation, maintenance and repair of the product are made available to the specialists and observed by them duly.
- For safety and approval reasons (CE), unauthorised conversion and/or modification of the product is not permitted.
- Before starting any installation, repair, maintenance or adjustment work, ensure that no voltage is applied to any of the power supply units and protect against unintended switch-on.
- Claims made under the warranty for damage caused by non-observance of these instructions will become invalid! No liability is assumed for consequential damages!

1.3 Warning symbols

⚠ CAUTION	**CAUTION denotes a dangerous situation which, if ignored, could lead to injuries.**
ATTENTION	**ATTENTION denotes a situation which could lead to material damage.**
NOTE	**NOTE denotes a statement which is provided for information only.**

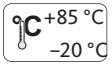
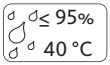
2. Product description

The fingerprint scanner and code keypad are access control systems for identification using biometric or mental characteristics. The fingerprint scanner records the characteristics (minutiae) of the fingerprint skin ridges and compares the image obtained with the biometric information stored in the reference fingerprint. The code keypad records entered PIN codes and compares them with the stored reference PIN codes.

If the characteristics match, an encrypted transmission to the control unit opens the door. The system is primarily used to open house and apartment entrance doors and garage doors in the home or commercial sector.

2.1 Technical data

Stainless steel variant	B-55600-23-4-8 B-55600-20-4-8 	B-55600-23-1-8 B-55600-20-1-8 
Black variant	B-55600-23-4-9 only fingerprint scanner	-
Version for	Installation in door	Wall mounting
Voltage supply	8 ... 24 V DC	8 ... 30 V DC
Power consumption	Max. 1 W	Max. 3 W
Relay output	Via SECURE*connect* 200	24 V DC | 5.0 A
Dimensions	44 x 75 x 29 mm	80.5 x 80.5 x 30 mm (55 x 55 x 30 mm w/o frame)
Memory	35 fingerprints 1000 events access protocol 150 PIN codes for the code keypad	

Template	Scanning duration: approx. 1 s Identification duration: approx. 10 ms per comparison
False rejection rate (FRR)	Approx. 0.5%
False acceptance rate (FAR)	Better than 1 in 1 million (at FRR 0.5%)
Fingerprint detection	Querying the capacitive/conductive electromagnetic properties of the skin contact when dragging the finger over the CMOS sensor.
Battery for programming device	CR2025
Environmental conditions	  IP65 (at the front)
Certifications	The certificates can be found at our website www.g-u.com.

2.2 Intended use

Use the product only in accordance with the product description. The use is restricted to the functions, technical data, applications and instructions described below. The use is only permitted within the usage limits described in this manual for which our product was designed for. The product was designed for these usage limits. Any other use is not permitted.

The fingerprint scanner and code keypad are designed for access control only by means of a biometric identification feature or a PIN code, at various building entrances within a locking system. The main function is the identification. A SECURY with A-opener, a SECURE*connect* 200, a relay to operate as a control unit or an electrically coupled lock is required to open the access point.

Changes made to the product or to the connections without the consent of the Gretsch-Unitas group exclude any liability of the manufacturer for any resulting damage.

2.3 Improper use

Any other use or use beyond the intended scope is not permitted and Gretsch-Unitas group will not assume liability for the resulting losses. If the safety instructions are disregarded this is also considered as 'improper use'. Unauthorised conversion or modification of the product is not permitted.

If the product is used in one of the following conditions this especially, but not conclusively, constitutes improper use.

- Incorrect polarity of connections.
- Unauthorised modifications have been made to the product.
- During operation when installed in the door with SECURE*connect*, voltages greater than 24 V +10 % DC are not permitted and lead to damage.

2.4 Function

2.4.1 Function of fingerprint scanner

The fingerprint scanner records the fingerprint via a line sensor and evaluates it. The result is compared with the biometric information of the fingerprint previously saved as reference. If they correspond, authorisation is sent and passage through the door is granted. For safety reasons, a line sensor is used in the fingerprint scanner which automatically removes the fingerprint and cleans the sensor surface each time the scanner is used by swiping the finger.

2.4.2 Function of the code keypad

The code keypad compares the input on the keypad with the user code you assigned as reference. If they correspond, authorisation is sent and passage through the door is granted.

2.5 Scope of delivery, transport and storage

The scope of delivery must be checked to make sure it is complete and undamaged. In the event of damage, inform the specialist dealer. Only install and commission products that are in perfect technical condition.

The delivery consists of the following products/document:

- Access control (fingerprint scanner or code keypad)
- Programming device (only with fingerprint scanner)
- System cable to control unit (only with unit for door installation)
- "Whitebox" relay module (only with wall-mounted unit)
- Fixing material
- Operating instructions

Only store the product in its original packaging and under the following conditions:

- Only store in dry, clean and moderately ventilated spaces indoors, and not outdoors. The storage location must be free of movements and vibrations.
- Temperature range of +15 °C to +40 °C, without strong temperature fluctuations
- Relative air humidity of 30% to 70%, non-condensing
- Regularly inspect the general condition of the product during longer storage periods

Only transport the product in its original packaging. Make sure the goods are secured during transportation to prevent them from falling and ensure protection against moisture. Also avoid hard impacts.

2.6 Accessories

- Substitute assembly frame (on-wall/in-wall) B-55606-00-0-1 2
- Stainless steel front panel with BKS logo B-55606-00-1-1 3
- Stainless steel front panel with BKS logo, black B-55606-00-7-1 3
- Stainless steel front panel without BKS logo B-55606-00-2-1 4

3. Installation

The fingerprint scanner or the code keypad are generally mounted on the external door side (outdoor). Depending on the version, it is installed in the door or in the wall. The connection to the control unit at the access point is established with the data line (SECURE*connect*/electrically coupled lock or "Whitebox" relay box). For connection use the BKS system cables.

ATTENTION

The standards and regulations for safety extra-low voltage (SELV) during installation and laying of cables must be observed. To this end, provide the cable ends with ferrules.

ATTENTION

Be careful not to damage the visible surfaces of the installation space during the installation! Carefully dismount/mount the decorative element!

NOTE

To guarantee problem-free operation, the installation height must be 1.2 to 1.4 m above finished floor level (FFL)!

- Use the fixing material provided.
- Tighten the fixing screws with a screwdriver until the fingerprint scanner or the code keypad is secure. Do not tighten too much, otherwise the housing may be destroyed.
- We recommend you only fit the decorative element once the installation is complete and the function test has been successfully carried out.

NOTE

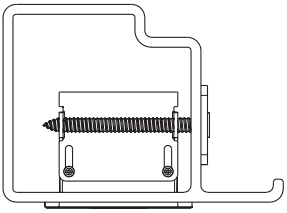
After completing the installation and switching on the power supply, the LEDs on the fingerprint scanner/code keypad light up solid green, red and blue when the units are in the delivery condition. In other words, if no user or master finger and/or PIN code has been programmed and the connection has been established correctly.

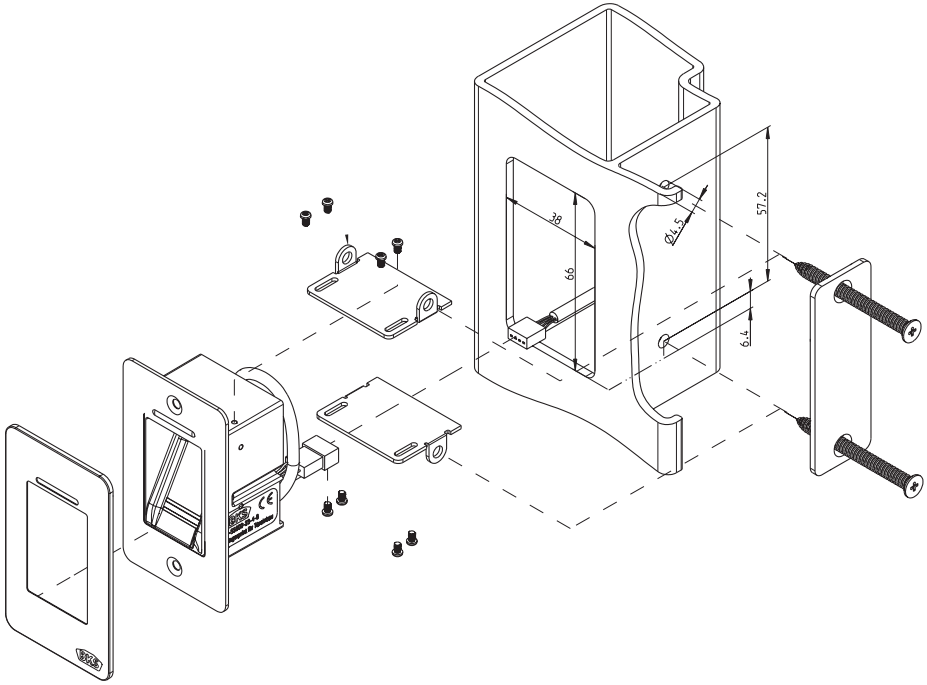
3.1 Installation in door – B-55600-23-4-8 | B-55600-20-4-8 | B-55600-23-4-9

This variant of the fingerprint scanner or code keypad is intended as an access control for installation in doors. For the sake of simplicity, the illustrations show the installation of the fingerprint scanner. The installation of the code keypad is no different.

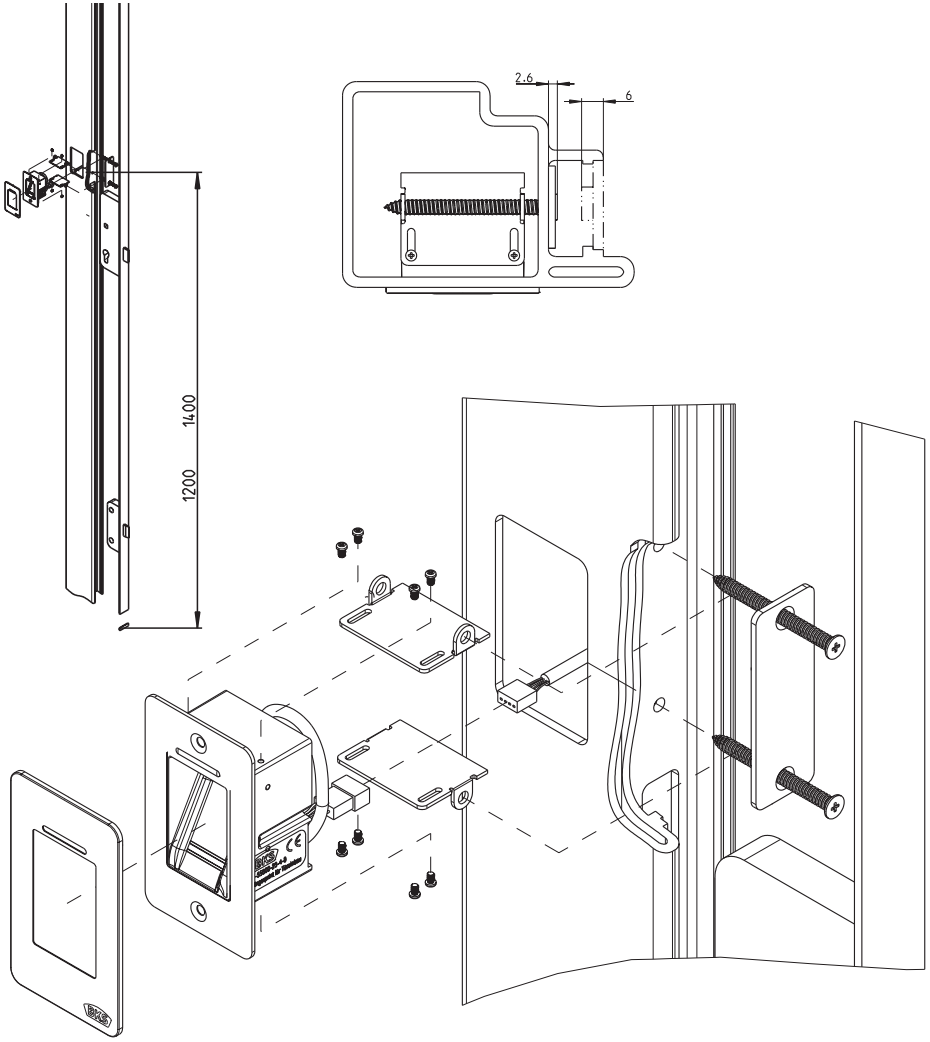
3.1.1 Installation in timber and steel doors

3.1.2 Installation in aluminium and PVC doors

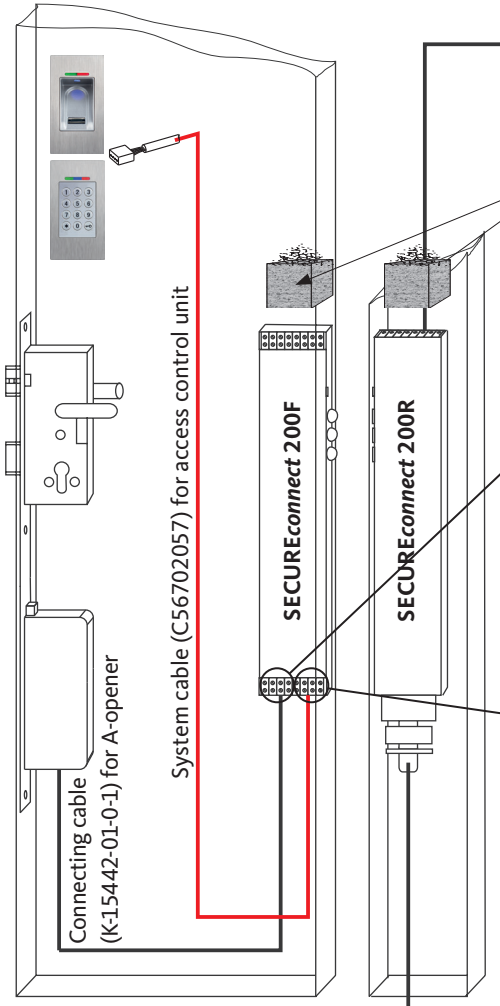




3.1.3 Installation with SECURY (A-opener)



3.1.4 Wiring diagram for A-opener



Potential-free control contact, e.g. push-button, intercom, access control, time switch.

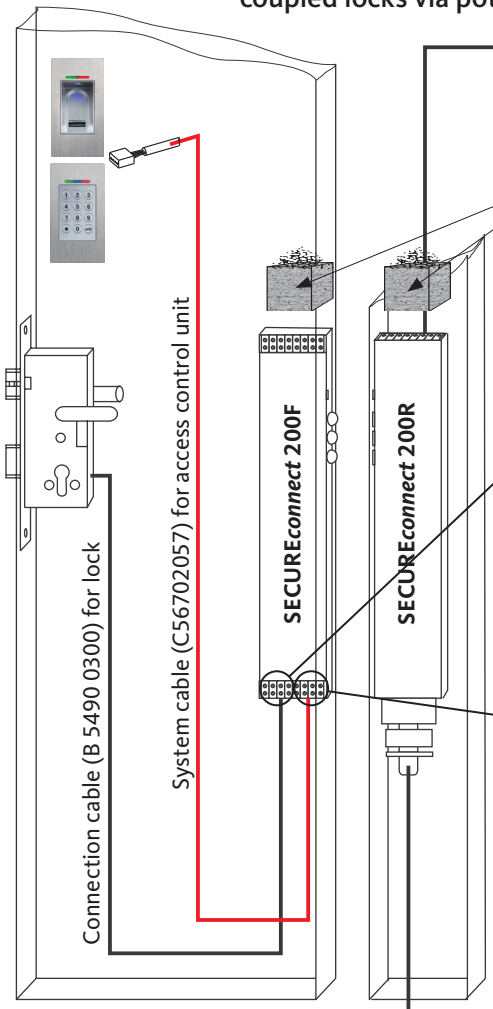
During installation in metal profiles, we recommend using the provided foam pieces to prevent swarf interfering the function.

SC 200F	Connecting cable for A-opener	
Terminal	Wire colour	Signal
GS	GY | Grey	GND (minus)
VS	BN | Brown	24 V (plus)
90	BK | Black	Control line

SC 200F	System cable for access control unit	
Terminal	Wire colour	Signal
GS	YE | Yellow	GND (minus)
96	WH | White	RS-485 A
95	GN | Green	RS-485 B
94	BN | Brown	24 V (plus)

For metal and PVC doors, use the cable protection provided for cable outlet.

3.1.5 Wiring diagram for motor-driven and electrically coupled locks via potential-free connections



Potential-free control contact, e.g. push-button, intercom, access control, time switch.

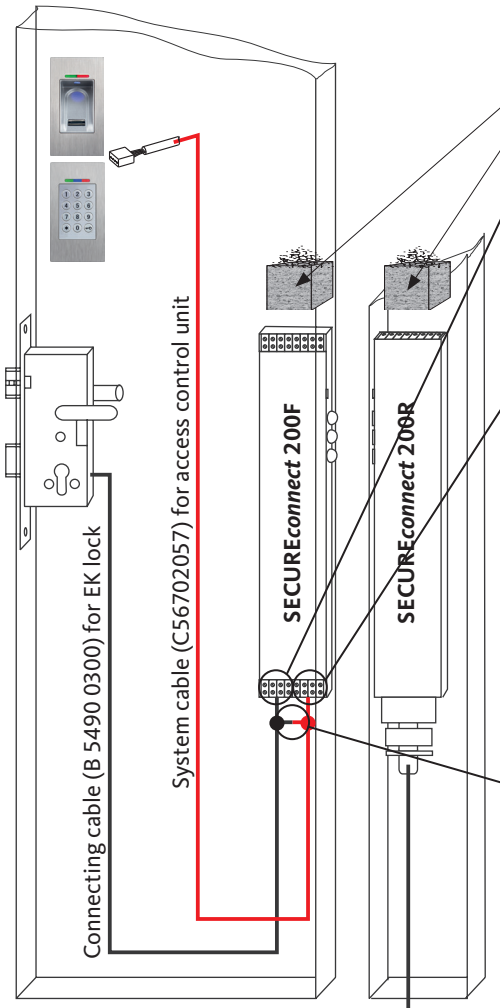
During installation in metal profiles, we recommend using the provided foam pieces to prevent swarf interfering the function.

SC 200F	Connecting cable for lock	
Terminal	Wire colour	Signal
GS	WH | White	GND (minus)
VS	BN | Brown	+24 V (plus)
90	PK | Pink	Control line

SC 200F	System cable for access control unit	
Terminal	Wire colour	Signal
GS	YE | Yellow	GND (minus)
96	WH | White	RS-485 A
95	GN | Green	RS-485 B
94	BN | Brown	24 V (plus)

For metal and PVC doors, use the cable protection provided for cable outlet.

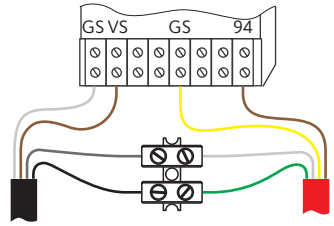
3.1.6 Wiring diagram for electrically coupled lock via RS-485 bus



During installation in metal profiles, we recommend using the provided foam pieces to prevent swarf interfering the function.

SC 200F	Connecting cable for EK lock	
Terminal	Wire colour	Signal
GS	WH | White	GND (minus)
VS	BN | Brown	24 V (plus)

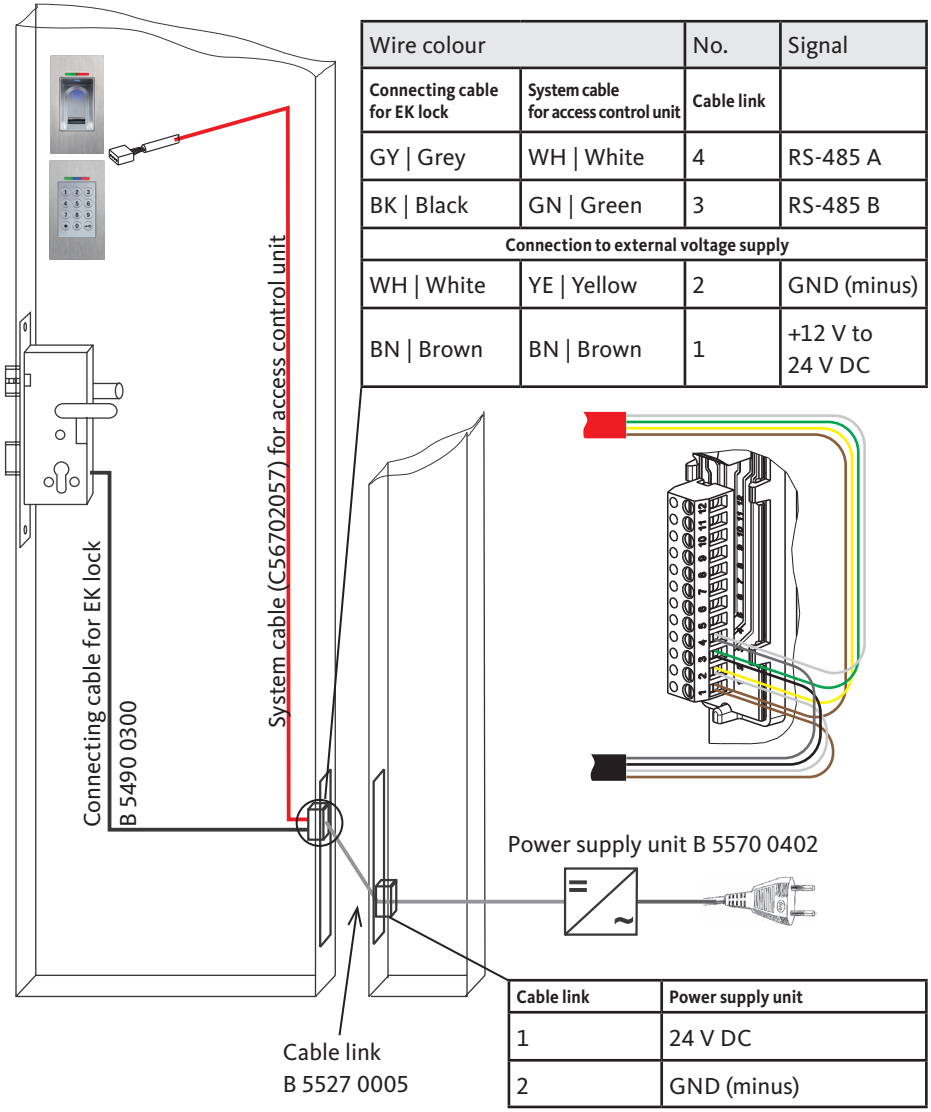
SC 200F	System cable for access control unit	
Terminal	Wire colour	Signal
GS	YE | Yellow	GND (minus)
94	BN | Brown	24 V (plus)



Wire colour		Signal
Connecting cable for EK lock	System cable for access control unit	
GY | Grey	WH | White	RS-485 A
BK | Black	GN | Green	RS-485 B

For metal and PVC doors, use the cable protection provided for cable outlet.

3.1.6.1 Connection to external voltage supply



Wire colour		No.	Signal
Connecting cable for EK lock	**System cable for access control unit**	**Cable link**	
GY | Grey	WH | White	4	RS-485 A
BK | Black	GN | Green	3	RS-485 B
Connection to external voltage supply			
WH | White	YE | Yellow	2	GND (minus)
BN | Brown	BN | Brown	1	+12 V to 24 V DC

Cable link	Power supply unit
1	24 V DC
2	GND (minus)

3.1.7 Pairing with SECURE*connect* 200

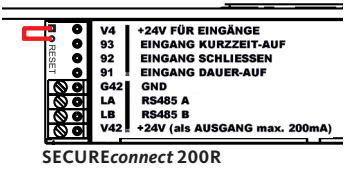
With the door installation variant, your system consists of 2 electronic devices.

- Access control: fingerprint scanner and code keypad
- Control unit: SECURE*connect* 200

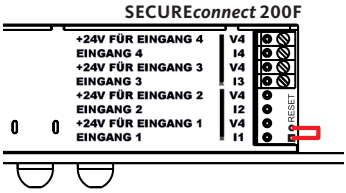
The access control (fingerprint scanner or code keypad) are generally mounted outside (external door side). To prevent unauthorised access, your system is equipped with numerous security functions:

- The access control is connected to the control unit using a data cable. Data transmission is encrypted.
- The access control and control unit are clearly coupled together for initial commissioning (pairing).

In order to exchange a component of the door system (SECURE*connect* 200R, SECURE*connect* 200F or access control), you have to start a re-pairing procedure for the power and data transmission unit. To do so, close the reset contact on the board of the SECURE*connect* 200F or SECURE*connect* 200R for a minimum of 3 seconds with the power supply connected. We recommend to use an alligator clip.



SECURE*connect* 200R



The terminal can be removed. The pairing process for the SECURE*connect* 200R, SECURE*connect* 200F and the access control now restarts. The access control is reset to the factory setting (all saved finger prints and PIN codes are deleted).

If an access control is connected to a paired SECURE*connect 200*, a re-pairing must be carried out. This involves generating a new system key and erasing the fingerprints or the PIN code.

3.1.8 Pairing of fingerprint scanner/code keypad with electrically coupled lock

A direct connection can be established between the fingerprint scanner or code keypad using the wired version of the electrically coupled locks (EK locks) in the EK19 and EK21 series. The access control and the electrically coupled lock are automatically paired with each other via the RS-485 bus connection during initial start-up.

When a component (fingerprint scanner, code keypad or lock) of the door system is replaced following pairing, the re-pairing must be performed before pairing the components again. The re-pairing at the electrically coupled lock is carried out in a specific sequence.

Start this sequence by disconnecting, then reconnecting the power supply to the electrically coupled lock in order to restart it. The following steps must now be performed within a minute after restarting.

- Continuously operate the lever handle while overrunning the cylinder cam monitoring contact.
- As you do so, turn the key in the locking cylinder several times quickly clockwise and anticlockwise and overrun the cylinder cam monitoring contact at least 3 times within 10 s.

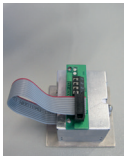
Once the repairing has been successfully concluded, all paired devices are deleted and the components are "paired" again.

3.2 In-wall/on-wall mounting – B-55600-23-1-8 | B-55600-20-1-8

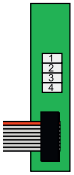
This variant of the fingerprint scanner or code keypad is intended as access control for in-wall installation next to the door. For the sake of simplicity, the illustrations show the installation of the fingerprint scanner. The installation of the code keypad is no different.

3.2.1 In-wall installation of access control system

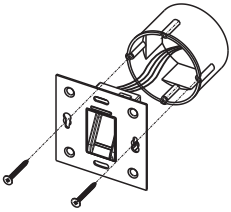
These are installed in a flush box. We recommend an installation height of between 1.2 and 1.4 m above finished floor level (FFL).



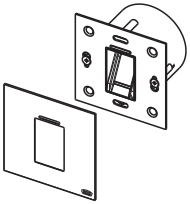
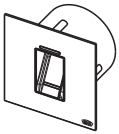
- Connect the access control to the relay module.



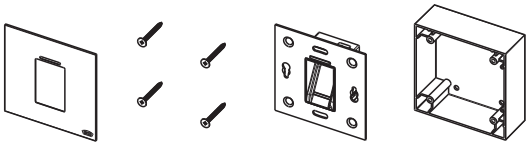
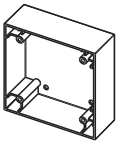
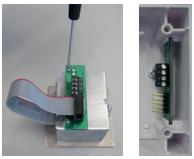
Connect the supply line to the internal unit accordingly at terminals 1 to 4.

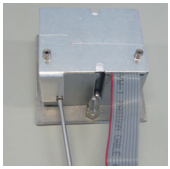


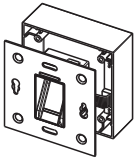
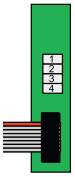
- Fasten the supporting frame using the 2 enclosed screws (3.5 x 25) to the flush box.

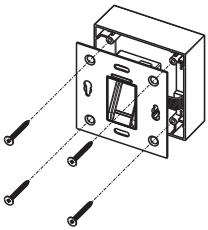
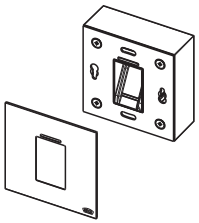
	■ Remove the protective film of the adhesive strip on the back of the stainless steel outer frame. ■ Position the outer frame on the supporting frame of the access control.
	■ Check the functioning.

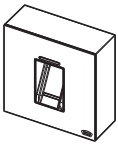
3.2.2 On-wall installation of access control system

	
	Fasten the on-wall housing to the wall. We recommend an installation height of between 1.2 and 1.4 m above finished floor level (FFL). You can use the enclosed screws (3.5 x 25) and plugs for this.
	■ Remove the terminal board by undoing the two screws. ■ Push the terminal board into the groove of the on-wall housing that has been prepared for this.
	■ Connect the supply line to the "Whitebox" relay module" accordingly at terminals 1 to 4.

<table>
<tr><td>  </td><td>■ Remove the back of the housing.

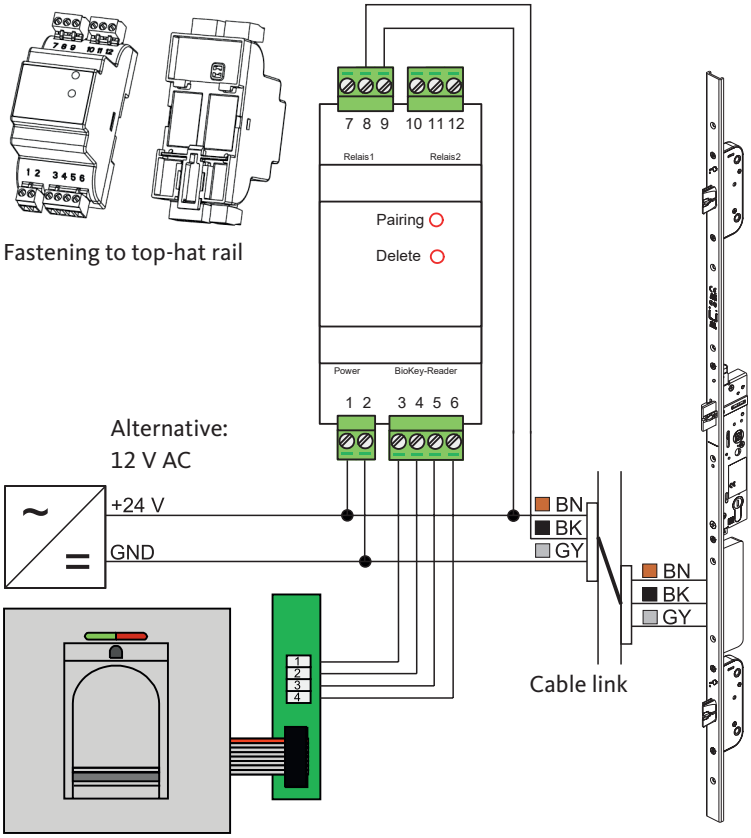
NOTE! The access control will not fit into the on-wall housing with the back of the housing attached.</td></tr>
<tr><td rowspan="2">  </td><td>■ Plug the flat ribbon cable of the access control onto the terminal board.</td></tr>
<tr><td> 

The red mark on the flat ribbon cable must face in the direction of the terminal clamps.</td></tr>
<tr><td>  </td><td>■ Fasten the supporting frame using the 4 enclosed screws (3.5 x 25) to the on-wall housing.</td></tr>
<tr><td>  </td><td>■ Remove the protective film of the adhesive strip on the back of the stainless steel outer frame.

■ Position the outer frame on the supporting frame of the access control.</td></tr>
<tr><td>  </td><td>■ Check the functioning.</td></tr>
</table>

3.2.3 Wiring diagram with "Whitebox" relay module

The inside and outside units communicate via an encoded bus. We recommend using a telecommunication cable type J-Y(ST)Y 2x2x0.8 to connect the "Whitebox" relay module and access control.
The connection example applies for the GU A-opener of the Gretsch-Unitas group.



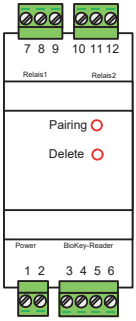
NOTE **When installing on the wall, the flat ribbon cable must be correctly inserted (red line must be directed to the terminals).**

3.2.4 Technical data for "Whitebox" relay module

Operating voltage:	8 to 30 V DC or 8 to 12 V AC
Power consumption:	1 W, at peak times 3 W (plus rating of connected A-opener)
Relay data:	24 V AC/DC 5.0 A
Installation space	To protect the relay controller at the interior
Dimension of relay module H x W x D [mm]	86.4 x 44.9 x 52.6 (dimensions without terminals)

3.2.5 Pairing with "Whitebox" relay module

ATTENTION **The relay module must be installed in the secured area and must not be accessible from the outside!**



In the case of the in-wall or on-wall units, the "Whitebox" relay module and access control are paired at the factory. If a hardware component is replaced, the pairing must be triggered again by pressing the "Pairing" button on the inside unit.

- To start the pairing, press the recessed button in the drill hole edged in red in the indoor unit labelled "Pairing".

3.2.6 Resetting with "Whitebox" relay module

You can use the relay module to restore the factory settings of the in-wall or on-wall units and erase all fingerprints, including the master finger or PIN code.

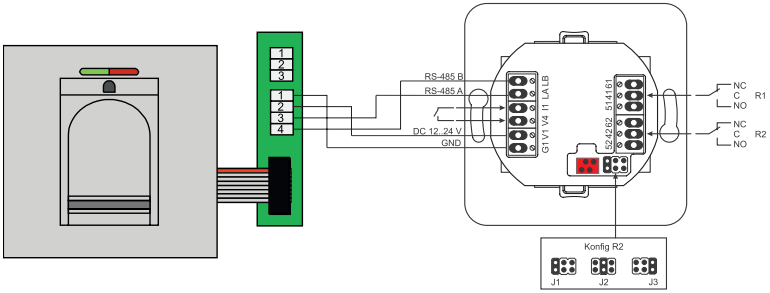
- To start the deletion operation, press the recessed button in the drill hole edged in red in the "Whitebox" relay module labelled "Delete".

After resetting, the green, red and blue LEDs light up continuously on the access control.

NOTE **After resetting, the modified master code is reset to the factory code!**

3.2.7 Connection to a radio module (FMIO)

The access control can communicate directly with a radio module (FMIO) via an encoded bus.
We recommend using a telecommunication cable type J-Y(ST)Y 2x2x0.8 to connect the radio module (FMIO) and access control.



3.2.7.1 Output functions of wall-mounted radio module I/O

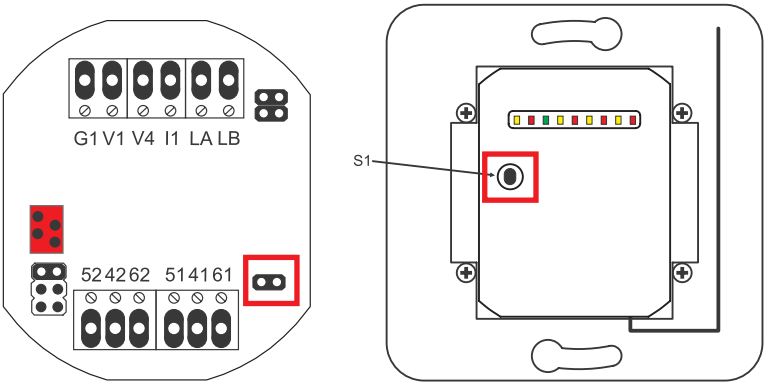
The relay "R1" of the wall-mounted radio module I/O is used to display an authorised access after connecting an access control via the RS-485 interface. Further configuration of relay output "R1" is not possible. The status is indicated visually by LED "L7" at the front of the FMIO.

The relay "R2" provides the option of reflecting 3 different signals. The signal is configured as follows by setting the jumper (see below table). The status is indicated visually via LED "L2".

Output	FMIO with radio-controlled electrically coupled cylinder/lock	FMIO with radio-controlled electrically coupled cylinder/lock and fingerprint scanner/code keypad
1	-	Authorised access
2 + J1	-	Unauthorised access attempt
2 + J2	Coupling active (cylinder/lock engaged)	-
2 + J3	Battery status	Battery status

3.2.7.2 Pairing/Repairing of wall-mounted radio module I/O

Once an access control has been connected to the wall-mounted radio module I/O, the pairing procedure occurs. It is now not possible to connect any other access control to the same wall-mounted radio module I/O. If this is necessary, the access control pairing can be reset.



The housing cover must be opened to do this.

- Disconnect the module from the RS-485 interface.
- Insert the jumper next to the terminal "51 41 61".
- Now press push-button "S1" until an acoustic signal is heard.

The pairing information has been deleted.

If you wish to reset the pairing between the radio-controlled electrically coupled cylinder/lock and radio module I/O, the jumper must not be plugged in. In this case press and hold down "S1" to reset the pairing information of the radio-controlled electrically coupled cylinder/lock.

4. Operation of fingerprint scanner

Commissioning must be carried out before setting up and using the access system. Proceed step by step.

- Install the fingerprint scanner as described in Chapter 3.
- For electrical connections, refer to wiring diagram.

- The connection (pairing) is initiated the first time the mains voltage is switched on.

Three operation modes are available for operating and configuring the fingerprint scanner. Use the programming device to change the administration mode.
"Bluetooth administration" mode is activated in the delivery condition.
Other modes are "Standard administration" and "Index administration".

ATTENTION **The entrance is not secure and can be opened if the master finger has not been taught-in.**

4.1 Operating advices

4.1.1 Changing the administration mode

NOTE **After resetting, all saved information is lost, only the administration mode is retained.**

The operating mode can only be changed over in the delivery condition (all LEDs light up). You can do this by resetting your fingerprint scanner DA >> CODE >> OK. The code can be found on page 66 and in addition on the programming device.
To change over to administration mode, hold the programming device directly in front of the fingerprint scanner (blue LED) and press the following buttons:

	9 » 9 » OK » 5 » 0 » OK	Standard administration
	9 » 9 » OK » 5 » 1 » OK	Index administration
	9 » 9 » OK » 5 » 7 » OK	Bluetooth administration (delivery condition)

Following the changeover, the finger scanner changes to the delivery condition (all LEDs light up).

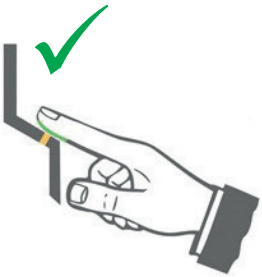
4.1.2 Finger guidance

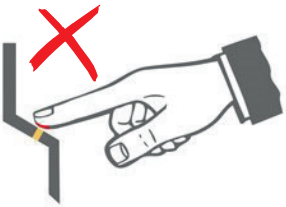
When teaching-in the fingerprints, proceed particularly carefully. The master and user finger may be rejected if errors are made when teaching-in. The more careful a finger is taught-in, the better it will be detected during identification later.

NOTE **Before teaching-in the master or user fingers, we recommend washing your hands once.**

- Drag finger quickly and evenly, applying light pressure with as many fingerprint ridges as possible over the sensor line.

When choosing a finger, bear in mind that the index finger is more suitable if your fingers are slender.





4.1.3 Door opening behaviour (only door installation)

With the versions B-55600-23-4-8 and B-55600-23-4-9 (fingerprint scanner for door installation), the fingerprint scanner is automatically switched off if the door remains open for longer than 12 s.

The saved fingerprints for opening the door are retained in the event of a power failure. After a power failure, the date and time must be set again in order to evaluate events.

4.1.4 Programming device, abbreviations

Button	Meaning	Explanation
DA	Delete All	Delete all, including master finger
OK	OK	Perform function
R1 » B	Relay 1 » Block	Relay 1 » Block user ID
RT	Relay-Time	Switching time
R2 » UB	Relay 2 » Unblock	Relay 2 » Unblock user ID
D	Delete	Delete finger prints
E	Enroll	Record finger prints
TT	Time	Time (seconds)

Abbreviation	Meaning	Explanation
MF	Master finger	Administration finger
CODE	PIN code	User or master code
ID	Index	User ID
YYYY | MM | DD	Year | Month | Day	Year | Month | Day
HH | MM | TT	Hour | Minute | Time	Hour | Minute | Seconds (time)

NOTE

Hold the programming device directly in front of the blue LED of the module. Each time a button is pressed, the green LED lights up briefly to confirm this. If the LED does not light up once a button has been pressed, repeat the input.

4.2 Bluetooth administration mode

The "Bluetooth administration" mode enables you to set up and administer the fingerprint scanner with your smartphone and the BKS BioKey app. Once authorised to do so at the fingerprint scanner via the master finger, you can call up the required function by navigating to the relevant menu item in the BioKey app then make the necessary settings for administration of your system.

"Bluetooth administration" mode is activated in the delivery condition. To switch to another mode, follow the instructions in Section 4.1.1 [90].

- You can configure the fingerprint scanner in the "Bluetooth administration" mode via the following functions.

4.2.1 Test mode

It is possible to trigger a door opening in the delivery condition or after resetting without configuring the fingerprint scanner beforehand in order to perform a test with the programming device. Prerequisite is the delivery condition.

Bear in mind that while the fingerprint scanner is in the delivery condition, the entrance is not secure.

	■ Hold the programming device directly in front of the blue LED of the module ■ Press the "0" button on the programming device ■ As visual confirmation, the green LED lights up each time the button is pressed ■ Press "OK" to confirm ■ The door is unlocked

4.2.2 Teaching-in master fingers

For security reasons, when the fingerprint scanner is configured the authorisation via the master finger is checked beforehand. This is why you start the configuration by teaching-in the master finger and deciding who will subsequently be permitted to administer the system.

NOTE

In the next step, start the configuration of the fingerprint scanner by teaching-in the first master finger without opening the app (fingerprint scanner in delivery condition).

When choosing the finger, bear in mind that a master finger cannot be used more than the user finger which will be used to open the door. It is therefore recommended that if you are right-handed for example, you teach-in the left index finger as the master finger and the right index finger as the user finger.

NOTE

Drag the same finger 5 times across the sensor to teach-in the master finger.

- The green, red and blue LED light up permanently
- The device is initialised and ready for set-up

NOTE! The prerequisite is that the fingerprint scanner is in the delivery condition or a reset has been carried out.

NOTE! Each time you have read-in a finger (by dragging the finger over the sensor) you should wait roughly 2 seconds until the green and red LEDs light up continuously to signal that the procedure is complete.
Only then will you be able to continue teaching-in by dragging the same finger over the sensor again.
Do not allow more than 60 s to elapse between the master finger teach-in operations, otherwise the procedure will be interrupted.

<table>
<tr>
<td> 
 
  </td>
<td>Teach-in operation
■ Drag the finger you want to use as master finger across the sensor
■ The green and red LED go out briefly after reading-in
■ After approx. 2 seconds, the green and red LED light up permanently again. The fingerprint scanner is ready
■ You can perform the next teach-in operation by dragging the same finger over the sensor again
■ Repeat the teach-in operation until the finger has been successfully taught-in 5 times</td>
</tr>
<tr>
<td>  </td>
<td>■ The green LED lights up briefly to signal successful teaching-in of the first master finger
■ Following a failed teach-in attempt, which can occur due to insufficient quality for example, the teach-in operation should be repeated as often as possible until the green LED lights up briefly</td>
</tr>
<tr>
<td>  </td>
<td>■ Once the first master finger has been taught-in, the device is operational
■ The blue LED lights up permanently
■ The configuration can continue</td>
</tr>
<tr>
<td colspan="2">NOTE! If a finger is dragged across the sensor during the teach-in operation and is not accepted as master finger, the green and red LEDs remain lit. The master finger teach-in operation must be repeated.</td>
</tr>
</table>

After teaching-in the first master finger, you can then add other master fingers, see Section 4.2.6 [99] or 4.3.3 [108].

4.2.3 Installing the BKS BioKey app

The BKS BioKey app is available for Apple iOS and Google Android. Download the app from the App Store or Google Play. Enter the term "BioKey" in the search field of the App store.

Available on the App Store

GET IT ON Google Play

NOTE

The prerequisites for administering the BKS BioKey app are:
– Bluetooth interface on the smartphone is active
– the app can access the location of the smartphone
– the first master finger has been taught-in, see Section 4.2.2 [94]

- Make sure that the fingerprint scanner is within Bluetooth range of your smartphone.
- Start the BKS BioKey app on your smartphone.
- Press "Select device" in the header of the display.

The BKS BioKey app searches for available units and opens a list of the available fingerprint scanners.

- Select the required fingerprint scanner from the list.
- Follow the prompt for identification at the fingerprint scanner.

- Drag the master finger across the sensor
- The green and red led light up briefly once

The smartphone is now connected for this session and the scanner can be configured via the app.

- Each time you open the app or if the app has not been used for one minute, you will then be prompted for security reasons to identify yourself via the master finger.

4.2.4 Adding user (BKS BioKey app)

- Start the BKS BioKey app on your smartphone.
- Follow the prompt for identification at the fingerprint scanner.

	■ Drag the master finger across the sensor ■ The green and red led light up briefly once

- Tap on the "Users" button.
- Press "**+**" **on the right in the header** of the display.
- Select "Name" and enter this.
- Tap "Add finger" in the "Fingers" area.
- Select "Description" and enter which finger of the user should be read-in here.
- Assign the rights of the new finger by activating or deactivating the switch for the corresponding relay 1 and 2 in the "Permissions" area. Relay 2 only with in-wall/on-wall mounting with function.
- Tap on "Enroll finger..." in the "Action" area.

	■ Follow the instructions in the dialogue of the BKS BioKey app ■ Drag the finger which is to be created as user finger across the sensor ■ Repeat the teach-in operation until the finger has been successfully taught-in 5 times ■ The counter in the app indicates the progress, or how often you still have to scan in your finger Note that once you have scanned in a finger as the master finger, it cannot be used as user finger.

- Once the finger has been successfully saved, an ID and the number of scans is displayed.

Only one fingerprint can be created per user. The number of user fingers is restricted to 35 fingerprints due to limited space in the memory.

- Navigate to the higher-level menus via "<- back“ and "<". The new user finger or user is displayed in these menus.

4.2.5 Editing and deleting user (BKS BioKey app)

- Start the BKS BioKey app on your smartphone.
- Follow the prompt for identification at the fingerprint scanner.

	■ Drag the master finger across the sensor ■ The green and red led light up briefly once

- Tap on the "Users" button.
- Select a user from the list "Users" to edit it in the following steps.
- Select "Name" in the "General" area and change or correct this.
- To edit or add further users or master fingers, select and edit the relevant input fields in the "Fingers" area.

Please follow the instructions for teaching-in a new user finger in the Section 4.2.4 [97].

- Activate or deactivate the "Block user" switch in the "Actions" area to block or unblock the user.
- Select "Delete user" in the "Actions" area and confirm the confirmation prompt.

4.2.6 Adding master finger (BKS BioKey app)

- Start the BKS BioKey app on your smartphone.
- Follow the prompt for identification at the fingerprint scanner.

	■ Drag the master finger across the sensor ■ The green and red led light up briefly once

- Tap on the "Users" button.
- Press "**+**" **on the right in the header** of the display.
- Select "Name" and enter this.
- Activate the "Master user" switch.
- Tap "Add finger" in the "Fingers" area.
- Tap on "Enroll finger...".

	■ Follow the instructions in the dialogue of the BKS BioKey app ■ Drag the finger which is to be created as master finger over the sensor ■ Repeat the teach-in operation until the finger has been successfully taught-in 5 times ■ The counter in the app indicates the progress, or how often you still have to scan in your finger Note that once you have scanned in a finger as the master finger, it cannot be used as user finger.

4.2.7 Identification through user finger, door opening

	■ The device is operational ■ The blue LED lights up
	■ Drag the user finger across the sensor ■ If the finger is detected, the green LED lights up and the door is opened Relay 1 is always enabled in the Standard administration mode with the on-wall/in-wall variant (wall mounting).
	■ If the finger is not detected, the red LED lights up and the door is not opened

4.2.8 Blocking mode

	**Blocking** ■ If a finger that has not been taught-in is dragged across the sensor 10 times in succession (red LED lights up), the device enters the blocking mode. This prevents unauthorised persons from gaining unhindered access In blocking mode, the system does not respond to fingers and the input of the programming device. The blocking time is 1 minute. The red LED flashes during the blocking time.
	**Unblocking** ■ Blocking mode can be cancelled earlier by dragging a taught-in finger (master or user finger) across the sensor. Subsequently, the door can be opened with a user finger

4.2.9 Resetting, deleting all user and master fingers

NOTE

Close the BKS BioKey app on your smartphone before resetting.

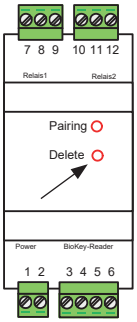
Hold the programming device directly in front of the blue LED of the module.

- Press the "DA" (Delete all) button on the programming device (the green LED lights up pressing the button)
- Please enter the factory code from page 66 or the master code with the programming device
- Confirm with "OK" to finish the delete operation
- The device is initialised and the green, red and blue LED light up permanently

NOTE

The fingerprint scanner can also be restored by re-pairing. During this process, all user and master fingers are deleted and the master code is reset to the factory code!

4.2.9.1 Alternative resetting with "Whitebox" relay module (on-wall/in-wall)



With the on-wall/in-wall variant, you can use the "Whitebox" relay box to trigger a reset to the factory settings when deleting all fingerprints incl. the master finger.

- To start the deletion, press the recessed button in the drill hole edged in red in the indoor unit labelled "Delete" for roughly 5 seconds.

After resetting, the green, red and blue LEDs light up continuously.

NOTE

After resetting, the modified master code is reset to the factory code!

4.2.10.1 Alternative resetting through master finger

	■ The fingerprint scanner is operational ■ The blue LED lights up
	■ Drag the master finger across the sensor, the red and green LEDs light up briefly once
	■ Once the master finger has been scanned twice, repeated brief flashing of the red and green LEDs indicates that deletion mode is being initialised
	■ After the master finger has been read-in for the fourth time, the deletion operation starts and the green LED lights up to confirm this
	■ After resetting, the fingerprint scanner is in delivery condition ■ The green and red LED light up permanently

NOTE

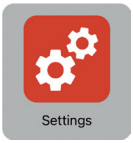
After resetting, the modified master code is reset to the factory code!

4.2.10 Changing the factory code to master code (BKS BioKey app)

The factory code (see page 66) can be changed to a 6-digit master code with the BKS BioKey app.

NOTE

For security reasons, we recommend to replace the factory code by new master code! After resetting, the master code is reset to the factory code!



- Start the BKS BioKey app on your smartphone.
- Follow the prompt for identification at the fingerprint scanner.

	■ Drag the master finger across the sensor ■ The green and red led light up briefly once

- Press the "Settings" button.
- Select "Reset code" and enter a new code.

4.2.10.2 Changing with programming device

	■ Button "D" (Delete) on the programming device ■ Press the button "E" (Enroll) ■ Enter the factory code or "old CODE" and press the "OK" button to confirm ■ Enter the "new CODE" and press "OK" to confirm ■ Enter the master code again ("new CODE") and press the "OK" button to finish

4.2.11 Displaying the access protocol (BKS BioKey app)

- Start the BKS BioKey app on your smartphone.
- Follow the prompt for identification at the fingerprint scanner.

	■ Drag the master finger across the sensor ■ The green and red led light up briefly once

- Press the "Access log" button.

The "Access log" list opens and the events saved in the fingerprint scanner are displayed. This list includes successful and rejected identifications.

4.2.12 Setting the relay module switching time (BKS BioKey app)

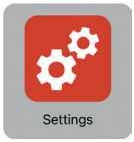
The relays can only be controlled via switching times with in-wall/on-wall versions. Units installed in the door do not support this function.

- Start the BKS BioKey app on your smartphone.
- Follow the prompt for identification at the fingerprint scanner.

	■ Drag the master finger across the sensor ■ The green and red led light up briefly once

- Press the "Relay times" button.
- Select "Relay 1" or "Relay 2" to set this.
- Select "Description" to assign a new name for the relay. This is displayed in the access log or user assignment.
- The switching time of the relevant relay can be set to between 0 and 60 seconds via the "Time" input field.

4.2.13 Renaming the fingerprint scanner and displaying the memory usage (BKS BioKey app)



- Start the BKS BioKey app on your smartphone.
- Follow the prompt for identification at the fingerprint scanner.

	■ Drag the master finger across the sensor ■ The green and red led light up briefly once

- Press the "Settings" button.
- Select the "Device name" and change the name of the fingerprint scanner.

Displaying this menu provides an overview of information, e.g. the memory space required for the taught-in fingerprints, the available memory and the firmware version, etc.

4.3 Standard administration mode

In the "Normal administration" mode, the fingerprint scanner can also be configured and administered without using the app. The fingerprint scanner is configured in the first instance in the "Standard administration" mode with the master finger. The programming device is also required for special functions.

To switch to this administration mode, follow the instructions in Section 4.1.1 [90].

- The following functions are available with the "Standard administration" mode.

4.3.1 Overview of functions

Function	Description | Quick guide
Test mode (only possible in the delivery condition)	→ Section 4.2.1 [93] 0 » OK
Teaching-in master fingers	→ Section 4.2.2 [94] Delivery condition » Teach-in master finger successfully 5 times
Teaching-in user fingers	→ Section 4.3.2 [107] Scan master finger » Teach-in user finger successfully 5 times
Identification through user finger	→ Section 4.2.7 [100] Scanning the user finger
Blocking the fingerprint scanner	→ Section 4.2.8 [100] The fingerprint scanner is blocked after 10 unsuccessful attempts without the finger being identified
Unblocking the fingerprint scanner	→ Section 4.2.8 [100] Scanning a taught-in master or user finger

Function	Description | Quick guide
Reset, delete all user and master fingers	→ Section 4.2.9 [101] DA » CODE » OK (CODE: current factory or master code)
Changing the factory code	→ Section 4.2.10 [102] → D » E » old CODE » OK » new CODE » OK » new CODE » OK
Adding master finger	→ Section 4.3.3 [108] MF » E » 0 » Teach-in master finger successfully 5 times
Setting the relay switching time	→ Section 4.3.4 [109] MF » RT » TT » OK *TT = Time in s [1...60 s], standard = 3 s*
Setting the date and time	→ Section 4.3.5 [109] MF » E » RT » YYYY » OK » MM » OK » DD » OK » HH » OK » MM »OK

For more information on the key assignment of the programming device and explanation of the abbreviations, see Section 4.1.4 [92].

4.3.2 Teaching-in user fingers

	■ The device is operational and the blue LED lights up **NOTE!** The master fingers must not be taught-in as user fingers.
	■ Drag the master finger across the sensor ■ The green and red LEDs light up briefly
 	**Teach-in operation** ■ Drag the finger you want to use as user finger across the sensor ■ The **green LED** lights up briefly to indicate the reading-in ■ You can perform the next teach-in operation by dragging the same finger over the sensor again
	■ Repeat the teach-in operation until the finger has been successfully taught-in 5 times ■ The **green and red LEDs light up briefly 4 times** to signal that the user finger has been successfully taught-in ■ The blue LED lights up continuously to signal operational readiness
NOTE! With "problematic" fingers, it may be necessary to teach-in the concerned user finger more often. If there have been too many unsuccessful attempts, you should use a different finger to the user finger.	

The number of user fingers is restricted to 35 fingerprints for master and user fingers due to limited space in the memory.

4.3.3 Adding master finger

	■ Drag the master finger across the sensor ■ The green and red LEDs light up briefly
	■ Press the "E" (Enroll) button on the programming device ■ Press the "0" button
 	**Teach-in operation** ■ Drag the finger you want to add as master finger across the sensor ■ The **green LED** lights up briefly to indicate the reading-in ■ You can perform the next teach-in operation by dragging the same finger over the sensor again
	■ Repeat the teach-in operation until the finger has been successfully taught-in 5 times ■ The **green and red LEDs light up briefly 4 times** to signal that the user finger has been successfully taught-in ■ The blue LED lights up continuously to signal operational readiness

4.3.4 Setting the relay switching time (only on-wall/in-wall version)

	■ Drag the master finger across the sensor ■ The green and red LEDs light up briefly
	■ Press the "RT" button on the programming device ■ Please enter a switching time of between 1 and 60 seconds via the keypad ■ Confirm with "OK" to complete

In the "Standard administration" mode, only the switching time for relay 1 can be adjusted.

4.3.5 Initialising the date and time

Use the audit set (B-55606-00-3-0) to read out the accesses saved in the fingerprint scanner. The listed accesses are only given a correct time stamp if you initially configure the date and time.

	■ Drag the master finger across the sensor ■ The green and red LEDs light up briefly
	■ Press the "E" button on the programming device ■ Press "RT" ■ Enter the date and time via the keypad and confirm with the "OK" button after each step: YYYY » OK » MM » OK » DD » OK » HH » OK » MM »OK Example: 2022-07-23, 12:45 a.m. E » RT » 2022 » OK » 07 » OK » 23 » OK »12 » OK » 45 »OK

NOTE **After a power failure, the date and time must be set again.**

4.4 Index administration mode

In the "Index administration" mode, the fingerprint scanner can also be configured and administered without using an app. In this administration mode, every user is assigned an ID, which improves the administration efficiency. This is configured via the master finger and the programming device. In the Index administration you can select and systematically edit an ID, e.g. delete the user finger of an ID. It is advisable to document the assignment in a list, see template in Section 4.4.9 [117].

To switch to this administration mode, follow the instructions in Section 4.1.1 [90].

- The following functions are available with the "Index administration" mode.

4.4.1 Overview of functions

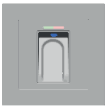
Function	Description | Quick guide
Test mode (only possible in the delivery condition)	→ Section 4.2.1 [93] 0 » OK
Teaching-in master fingers	→ Section 4.2.2 [94] Delivery condition » Teach-in master finger successfully 5 times
Teaching-in user fingers	→ Section 4.4.2 [112] MF » E » ID » OK » Teach-in user finger successfully 5 times
Identification through user finger	→ Section 4.2.7 [100] Scanning the user finger
Blocking the fingerprint scanner	→ Section 4.2.8 [100] The fingerprint scanner is blocked after 10 unsuccessful attempts without the finger being identified
Unblocking the fingerprint scanner	→ Section 4.2.8 [100] Scanning a taught-in master or user finger

Function	Description | Quick guide
Reset, delete all user and master fingers	→ Section 4.2.9 [101] DA » CODE » OK (CODE: current factory or master code)
Changing the factory code	→ Section 4.2.10 [102] D » E » old CODE » OK » new CODE » OK » new CODE » OK
Deleting individual user fingers	→ Section 4.4.3 [113] MF » D » ID » OK
Blocking IDs	→ Section 4.4.4 [114] MF » B » ID » OK
Unblocking IDs	→ Section 4.4.5 [114] MF » UB » ID » OK
Checking ID	→ Section 4.4.6 [115] OK » ID » OK
Adding master finger	→ Section 4.3.3 [108] MF » E » 0 » Teach-in master finger successfully 5 times
Set the relay switching time of relay 1 (only on-wall/in-wall version)	→ Section 4.4.7 [115] MF » RT » R1 » TT » OK *TT = time in s [1...60 s], standard = 3 s*
Set the relay switching time of relay 2 (only on-wall/in-wall version)	→ Section 4.4.7 [115] MF » RT » R2 » TT » OK *TT = time in s [1...60 s], standard = 3 s*
Teaching-in user finger for relay 1	→ Section 4.4.8 [116] MF » E » ID » R1 » OK » Teach-in user finger successfully 5 times
Teaching-in user finger for relay 2 (only on-wall/ in-wall version)	→ Section 4.4.8 [116] MF » E » ID » R2 » OK » Teach-in user finger successfully 5 times

Function	Description | Quick guide
Setting the date and time	→ Section 4.3.5 [109] MF » E » RT » YYYY » OK » MM » OK » DD » OK » HH » OK » MM »OK

For more information on the key assignment of the programming device and explanation of the abbreviations, see Section 4.1.4 [92].

4.4.2 Teaching-in user fingers

	■ The device is operational and the blue LED lights up **NOTE!** The master fingers must not be taught-in as user fingers.
	■ Drag the master finger across the sensor ■ The green and red LEDs light up briefly
	■ Press the "E" (Enroll) button on the programming device ■ Enter an ID between 1 and 35 via the keypad ■ Press "OK" to confirm
 	**Teach-in operation** ■ Drag the finger you want to use as user finger across the sensor ■ The **green LED** lights up briefly to indicate the reading-in ■ You can perform the next teach-in operation by dragging the same finger over the sensor again

	■ Repeat the teach-in operation until the finger has been successfully taught-in 5 times ■ The **green and red LEDs light up briefly 4 times** to signal that the user finger has been successfully taught-in ■ The blue LED lights up continuously to signal operational readiness
NOTE! With "problematic" fingers, it may be necessary to teach-in the concerned user finger more often. If there have been too many unsuccessful attempts, you should use a different finger to the user finger.	

The number of user fingers is restricted to 35 fingerprints for master and user fingers due to limited space in the memory.

4.4.3 Deleting individual user fingers

	■ Drag a master finger across the sensor ■ The green and red LEDs light up briefly
	■ Press the"D" (Delete) button on the programming device, the green LED lights up ■ Enter the ID of the user finger to be deleted ■ Confirm with "OK", the green LED lights up The user finger saved under the entered ID has now been deleted and will not be recognised when an attempt is made to open the door.

4.4.4 Blocking IDs

	■ Drag the master finger across the sensor ■ The green and red LEDs light up briefly
	■ Press „R1 (B)“ button ■ Enter ID ■ Confirm with "OK" The user finger saved under the entered ID has now been blocked and will not be recognised when an attempt is made to open the door.

NOTE

Individual IDs can be disabled provisionally without the taught-in fingerprint being discarded. The ID can subsequently be enabled without the relevant person having to be present in order to teach-in your fingerprint again.

4.4.5 Unblocking IDs

	■ Drag the master finger across the sensor ■ The green and red LEDs light up briefly
	■ Press "R2 (UB)" button ■ Enter ID ■ Confirm with "OK" The user finger saved under the entered ID has been enabled once again and can open the door.

4.4.6 Checking ID

	■ Press "OK" ■ Enter the ID number to be checked ■ Press again "OK" ■ If an ID has already been assigned, the green and red LEDs light up ■ If the ID is not assigned, only the red LED lights up

4.4.7 Setting the relay switching time per relay (only on-wall/in-wall version)

In the “Index administration” mode, you can specify the switching duration per relay separately.

	■ Drag a master finger across the sensor ■ The green and red LEDs light up briefly
	■ Press the "RT" button of the programming device ■ Select the relay via "R1" or "R2" buttons ■ Please enter a switching time of between 1 and 60 seconds via the keypad ■ Confirm with "OK", the green LED lights up

4.4.8 Teaching-in user fingers for relay 1/2 (only on-wall/in-wall version)

With the in-wall/on-wall version, the two relays can be switched separately.

	■ Drag the master finger across the sensor ■ The green and red LEDs light up briefly
	■ Press the "E" (Enroll) button on the programming device ■ Enter an ID between 1 and 35 via the keypad ■ Select the relay via the "R1" or "R2" button ■ Press "OK" to confirm
 	**Teach-in operation** ■ Drag the finger you want to use as user finger across the sensor ■ The **green LED** lights up briefly to indicate the reading-in ■ You can perform the next teach-in operation by dragging the same finger over the sensor again
	■ Repeat the teach-in operation until the finger has been successfully taught-in 5 times ■ The **green and red LEDs light up briefly 4 times** to signal that the user finger has been successfully taught-in ■ The blue LED lights up continuously to signal operational readiness

4.4.9 Assigning of ID and person

ID	Person (name)	Finger designation (thumb, index finger,...)

5. Operation of code keypad

Commissioning must be carried out before setting up and using the access system. Proceed step by step.

- Install the code keypad as described in Chapter 3.
- For electrical connections, refer to wiring diagram.

- The connection (pairing) is initiated the first time the mains voltage is switched on.

In the delivery condition all LEDs (green/red/blue if applicable) light up continuously. The information is entered directly via the code keypad. A programming device is not required or included in the delivery scope.

	Open the door
*	Start input or confirm it
Master code	Administration code
User code	Code for door opening

NOTE

Each time a button is pressed, the green LED lights up briefly to indicate this. If the green LED does not light up once a button has been pressed, repeat the input.

The master code or user code should be a combination of 4–6 numbers. Certain master code or user code combinations are excluded for security reasons. This includes regular number combinations such as 8888, 123456, 4321, etc. You can find the initial master code (factory code) on the page 66.

If an incorrect user code is entered 5 times in succession, the device switches to the blocking mode. This prevents unauthorised persons from gaining access.

If the device is in blocking mode, the red LED flashes to indicate this. The blocking mode initially has a time limit. The blocking time extends up to five times (blocking intervals: 1 minute, 5 minutes, 30 minutes, 1 hour, permanently blocked after that) following each subsequent failed attempt.

If a valid user code is entered two times in succession, the blocking mode is cancelled.

5.1 Test mode

In the delivery condition a door opening can been performed for test purposes. To do so, press the buttons 0 » The green LED lights up in confirmation.

	
0	

5.2 Changing master code

NOTE

For security reasons, we always recommend to replace the factory code by your own master code!

				
*	Master code	*	1	*

			
New master code	*	New master code	*

5.3 Setting/changing user code

				
*	Master code	*	2	*

					
User ID [1...150]	*	User code	*	User code	*

NOTE

With the in-wall/on-wall version, the two relays can be switched separately from each other. An odd user ID switches relay 1, an even ID switches relay 2.

5.4 Open the door

	
User code	

NOTE

If digits are entered before the user code, these are ignored.

5.5 Deleting user code

				
*	Master code	*	3	*

	
User ID	*

Alternative:

				
*	Master code	*	3	*

			
0	*	User code	*

NOTE

Carrying out a re-pairing procedure will reset the code keypad. This deletes all user codes.
After resetting, the modified master code is reset to the factory code!

5.7 Setting the relay switching time (only on-wall/in-wall version)

				
*	Master code	*	4	*

			
Relay [1|2]	*	Time [1...60 s]	*

5.6 Deleting all user and master codes

				
*	Master code	*	0	*

	
Master code	*

6. Maintenance and care

- The operational availability must be verified at regular intervals.
- A defective product must be replaced by a new one.

The surface of the fingerprint scanner is more or less self-cleaning because it is repeatedly used (for finger scanning). If the fingerprint scanner is still soiled, clean it with cotton buds, a microfibre cloth and glasses cloth. All fabrics made of cotton, paper towels, kitchen sponges and dishcloths are unsuitable. Use clean water with no cleaning additives. Proceed carefully in the area of the sensor.

However, as a precautionary measure clean any fingerprints or dirt from the code keypad using a soft, damp (not wet) cloth. Use clean water with no cleaning additives.

With version installed in door:
If frequently used, apply contact grease B-55606-00-4-0 to the contacts of the SECURE*connect* 200.

The operational availability of the locking system must be verified at regular intervals. To do so, check all fastening points and retighten screws, if required. The mechanical properties of the lock (key or lever handle operation/latchbolt) must not be impaired by dirt and must also be regularly maintained.

The lock mechanism is lubricated for life and is therefore maintenance-free. Lightly grease the latchbolt head 1x annually. Do not use oil, as this could damage lock electronics!

7. Troubleshooting

Error description	Cause	Remedy
The red LED flashes permanently several times per second	No bus connection to the control unit	Check the wiring or bring the device into operation
	No pairing or faulty pairing	Perform the pairing reset
The green and red LED flash permanently	Error in the wiring of the RS-485 bus	Check the connecting terminals and make sure the connections are correct
The red LED flashes permanently every two seconds	Blocking mode: system is blocked after several invalid identifications	Scan an authorised finger
The green LED lights up when an access attempt is made, but the door does not open	Connection problem between SC200R and SC200F	Clean the contacts of the SC200
		Check installation position of the SC200
	Connection problem – between zwischen inside and outside unit – between relay and connected components, e.g. electric strike	Check the wiring
		Switch the power supply off and back on
		Replace defective hardware
The red LED lights up permanently	Defective hardware	Replacement of fingerprint scanner or code keypad necessary

8. Maintenance and spare parts

Depending on the use and installation situation, we recommend regular inspection, care and cleaning. Faults and defects must be rectified immediately.

DANGER

Danger to life due to electric current!

Disconnect the power supply and discharge stored residual energy.

Repair work may only be carried out by qualified personnel who have been trained or authorised by the manufacturer.

If a service is due, before carrying out repairs on-site we recommend contacting the Technical Service of Gretsch-Unitas group in order to have the product sent in if necessary.

Remove the product from the installation space. To disassemble the product, release the fastenings, disconnect the electrical connections and remove.

Only use spare parts supplied by the manufacturer to carry out repairs. If other than original products are used, all product liability, warranty, and service claims will expire.

9. Disposal

NOTE

The products must not be disposed of as household waste. Instead, it must be disposed of properly by recycling it appropriately in accordance with national and local laws and regulations.

The products must be disposed of as electronic waste at special waste disposal sites. Packaging must be disposed of separately.

Table des matières

Votre code usine :

Vous le trouverez aussi sur l'autocollant placé au dos de l'appareil de programmation. Si un propre code maître a été défini, celui-ci doit être utilisé.

Remettez ce document à l'utilisateur !

1. Informations et consignes de sécurité

1.1 Remarques générales concernant la notice

Merci d'avoir choisi le lecteur d'empreintes digitales et le clavier à code comme contrôle d'accès pour systèmes de portes motorisés ou électromécaniques.

La présente notice comporte des indications importantes et vous permettra d'éviter d'éventuelles situations dangereuses, de réduire les frais de réparation ainsi que les temps d'arrêt, et d'augmenter la fiabilité et la durée de vie.

La notice d'utilisation doit être lue et employée par chaque personne **avant** l'utilisation. Conformez-vous à la notice en particulier dans les cas suivants :

- Montage et installation électrique
- Mise en service, fonctionnement et entretien

Une fois le montage effectué, la notice d'utilisation doit être remise à l'installateur/au donneur d'ordre. Lisez attentivement cette notice avant la première utilisation de l'appareil et la conserver précieusement pour tout usage ultérieur. Précisez à tous les installateurs/les donneurs d'ordre de lire la notice d'utilisation.

1.2 Consignes de sécurité

Cette notice s'adresse à un personnel technique formé, ayant des connaissances sur l'installation de composants de portes, de garnitures de porte et de composants électriques et également formé sur le montage, la mise en service et le maniement de ce produit.

Les donneurs d'ordre et les installateurs doivent également respecter ces informations pour éviter un mauvais montage ou de fausses manœuvres.

- Il est impératif d'observer les instructions d'installation et de montage, les directives et les réglementations locales en vigueur. Ceci s'applique particulièrement aux réglementations et aux directives suivantes : DIN VDE 0100 et IEC 60364.

- Nous déclinons toute responsabilité en cas d'utilisation, de montage ou d'installation incorrects et en cas d'utilisation d'accessoires non originaux !
- Il doit être garanti que seul un personnel qualifié (définition, voir EN 50110-1, DIN VDE 0105 et CEI 60364) peut être mandaté pour tout type de travaux (planification, transport, montage, installation, mise en service, maintenance, réparations, démontage) sur les différents produits.
- Il convient donc de s'assurer que les documents nécessaires pour l'installation, la mise en service, l'exploitation, la maintenance et les réparations du produits se trouvent à votre disposition et soient pris en considération.
- Pour des raisons de sécurité et d'autorisation (CE), toute modification arbitraire sur le produit est interdite.
- Avant chaque montage, travaux de réparation, de maintenance ou de réglage, il faut mettre hors tension tous les blocs d'alimentation correspondants et les sécuriser contre toute mise en route indésirable.
- La garantie expire en cas de dommages dus au non-respect de cette notice ! Nous déclinons toute responsabilité pour les dommages qui en résulteraient.

1.3 Symboles d'avertissement

⚠ PRUDENCE	**PRUDENCE indique une situation dangereuse, susceptible d'entraîner des blessures si elle n'est pas respecté.**
ATTENTION	**ATTENTION indique une situation pouvant entraîner des dommages matériels.**
REMARQUE	**REMARQUE indique un renseignement purement informatif.**

2. Description du produit

Le lecteur d'empreintes digitales et le clavier à code sont des contrôles d'accès permettant l'identification au moyen de caractéristiques biométriques ou intellectuelles. Le lecteur d'empreintes digitales saisit les caractéristiques (minuties) des lignes papillaires et les compare avec les informations biométriques enregistrées dans l'empreinte de référence. Le clavier à code saisit le code PIN entré et le compare avec le code PIN de référence enregistré.

Lorsque les caractéristiques concordent, une transmission cryptée à l'unité de commande entraîne l'ouverture de la porte. Le système est destiné en premier lieu à l'ouverture de portes d'entrée, de portes d'appartement et de portes de garage dans le domaine privé ou commercial.

2.1 Caractéristiques techniques

Version en acier inoxydable	B-55600-23-4-8 B-55600-20-4-8 	B-55600-23-1-8 B-55600-20-1-8 
Version en noir	B-55600-23-4-9 uniquement le lecteur d'empreintes digitales	-
Variante pour	montage sur porte	montage mural
Tension d'alimentation	8 ... 24 V CC	8 ... 30 V CC
Puissance absorbée	max. 1 W	max. 3 W
Sortie de relais	sur SECURE*connect* 200	24 V CC | 5,0 A
Dimensions	44 x 75 x 29 mm	80,5 x 80,5 x 30 mm (55 x 55 x 30 mm sans cadre)
Mémoire	35 empreintes digitales 1000 événements dans le protocole d'accès 150 codes PIN pour le clavier à code	

Modèle	Durée d'enregistrement : environ 1 s Durée d'identification : environ 10 ms par comparaison
Taux de faux rejets (TFR)	Environ 0,5 %
Taux de fausses acceptations (TFA)	Supérieur à 1 pour 1 million (pour TFR 0,5 r%)
Identification de l'empreinte	Interrogation des propriétés électromagnétiques capacitives/conductrices du contact avec la peau lors du passage du doigt sur le capteur CMOS.
Pile pour l'appareil de programmation	CR2025
Conditions environnantes	+ 85 °C -20 °C ≤ 95 % + 40 °C IP65 (face devant)
Certifications	Vous trouverez les certificats sur notre site web www.g-u.com.

2.2 Utilisation conforme

Utilisez le produit uniquement conformément à la description qui en est fournie. L'utilisation se limite aux fonctions, caractéristiques techniques, applications et instructions décrites ci-après. L'utilisation est uniquement autorisée dans les limites définies dans la présente notice. Le produit a été conçu dans ce but. Toute utilisation excédant ce cadre n'est pas autorisée.

Le lecteur d'empreintes digitales ekey et le clavier à code ekey servent uniquement au contrôle d'accès aux différents points d'entrée d'un édifice, au moyen d'une caractéristique d'identification biométrique ou d'un code PIN dans le cadre d'un système de fermeture. Leur fonction principale est l'identification. Un SECURY avec dispositif de déverrouillage motorisé, un SECURE*connect* 200,un relais en tant qu'unité de commande ou une serrure à béquille contrôlée est nécessaire pour ouvrir le point d'accès.

Le fabricant se dégage de toute responsabilité en cas de dommages

provenant de modifications effectuées sur le produit ou au niveau des raccords, sans l'autorisation du groupe Gretsch-Unitas.

2.3 Utilisation non conforme

Une utilisation autre ou excédant ce cadre n'est pas autorisée et le groupe Gretsch-Unitas n'assume aucune responsabilité pour les dommages en résultant. L'utilisation est également considérée comme non conforme lorsque les consignes de sécurité ne sont pas respectées. Les transformations et/ou les modifications effectuées en propre sur le produit ne sont pas autorisées.

Une utilisation non conforme est notamment donnée lorsque le produit est utilisé dans l'une des conditions énumérées ci-dessous, dont la liste n'est toutefois pas exhaustive.

- Erreur de polarité des branchements.
- Modifications non autorisées effectuées sur le produit.
- Pour un fonctionnement dans le montage sur porte avec SECURE*connect*, des tensions supérieures à 24 V + 10 % CC ne sont pas autorisées et entraînent des dommages.

2.4 Fonctionnement

2.4.1 Fonctionnement du lecteur d'empreintes digitales

Le lecteur d'empreintes digitales enregistre l'empreinte grâce à un capteur linéaire et analyse celle-ci. Le résultat est comparé avec les informations biométriques enregistrées dans l'empreinte de référence. En cas de correspondance, l'autorisation est envoyée, permettant d'autoriser l'accès par la porte. Pour des raisons de sécurité, le lecteur d'empreintes digitales utilise un capteur linéaire qui élimine automatiquement la trace de l'empreinte laissée par le glissement du doigt et nettoie la surface du capteur à chaque utilisation.

2.4.2 Fonctionnement du clavier à code

Le clavier à code compare la saisie au clavier avec le code utilisateur attribué comme référence. En cas de correspondance, l'autorisation est envoyée, permettant d'autoriser l'accès par la porte.

2.5 Contenu de la livraison, transport et stockage

Le caractère complet et l'absence de détériorations de la livraison doivent être contrôlés. Informez le distributeur en cas de dommage. Ne montez et ne mettez en service que des produits en parfait état technique.

La livraison est composée des articles/du document suivants :

- Lecteur d'empreintes digitales ou clavier à code (contrôle d'accès)
- Appareil de programmation (uniquement pour le lecteur d'empreintes digitales)
- Câble d'interconnexion vers l'unité de commande (uniquement pour appareil à montage sur porte)
- Module relais « Whitebox » (uniquement pour appareil à montage mural)
- Matériaux de fixation
- Notice d'utilisation

Stockez toujours le produit dans son emballage d'origine et dans les conditions suivantes :

- Stockage uniquement dans des pièces intérieures sèches, propres et modérément ventilées, pas en extérieur. Stockage sans mouvements et vibrations.
- Plage de température de + 15 °C à + 40 °C, sans variations importantes
- Humidité relative de l'air de 30 % à 70 %, sans condensation
- Effectuez régulièrement une inspection de l'état général en cas de stockage prolongé

Transportez le produit uniquement dans son emballage d'origine. Prévoyez lors du transport une sécurité contre la chute de même qu'une protection contre l'humidité. Les chocs violents doivent également être évités.

2.6 Accessoires

- Cadre de montage de remplacement (en applique/encastré) B-55606-00-0-1 2
- Panneau avant en acier inoxydable avec logo BKS B-55606-00-1-1 3
- Panneau avant en noir avec logo BKS B-55606-00-7-1 3
- Panneau avant en acier inoxydable sans logo BKS B-55606-00-2-1 4

3. Montage

Le lecteur d'empreintes digitales ou le clavier à code est en général montée à l'extérieur (face extérieure de la porte). Suivant le modèle, il est monté dans la porte ou dans le mur. Un câble de données permet d'établir la connexion avec la commande du point d'accès (SECURE*connect*/serrure à béquille contrôlée ou boîtier relais « Whitebox »). Utilisez les câbles d'interconnexion BKS pour le branchement.

ATTENTION **Lors de l'installation et de la pose des câbles, respecter les directives et les normes relatives à la tension TBTS. Équipez à cet effet les extrémités de câble d'embouts.**

ATTENTION **N'endommagez pas les surfaces visibles de l'espace de montage pendant le montage ! Montez/démontez la plaque d'habillage avec précaution !**

REMARQUE **Pour garantir une bonne utilisation, il convient respecter une hauteur de montage de 1,2 à 1,4 m au-dessus du bord supérieur du sol fini (HSF) !**

- Utilisez les matériaux de fixation fournis.
- Serrez les vis de fixation à l'aide d'un tournevis jusqu'à ce que le lecteur d'empreintes digitales ou le clavier à code soit bien fixé. Ne pas serrez trop fort pour ne pas endommager le boîtier.
- Nous conseillons de ne poser la plaque d'habillage qu'une fois le montage terminé et un test de fonctionnement réussi.

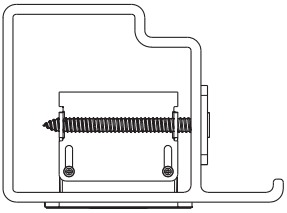
REMARQUE **Une fois le montage terminé et la tension d'alimentation activée, les LED du lecteur d'empreintes digitales/du clavier à code s'allument en vert, rouge et bleu de manière constante lorsque les appareils se trouvent dans leur état de livraison. Ce qui signifie qu'aucune empreinte utilisateur ou maître ou encore code PIN n'a été programmé et que le raccordement a été effectué correctement.**

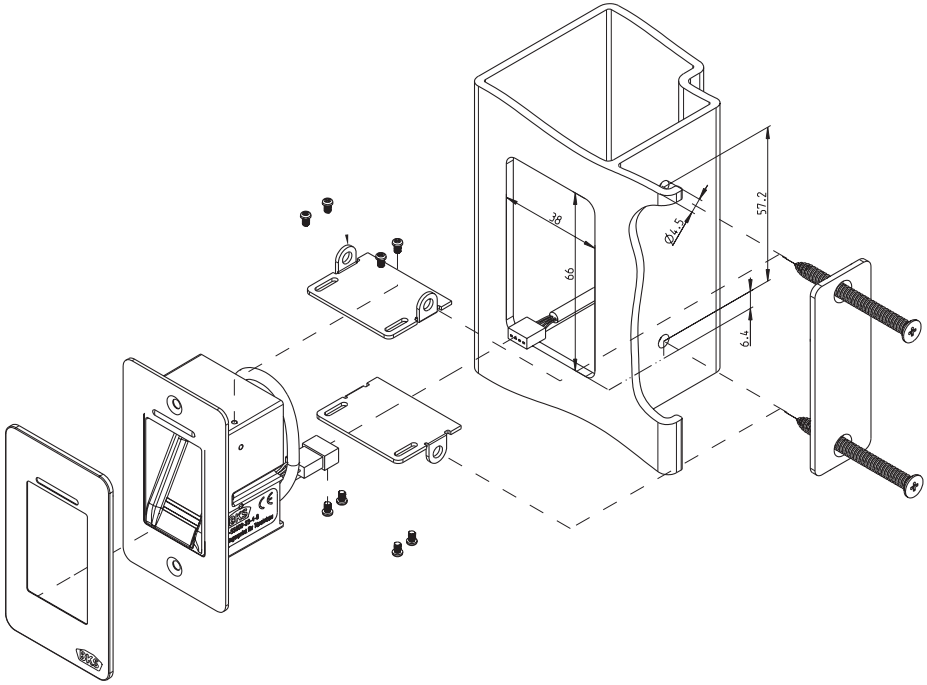
3.1 Montage sur porte – B-55600-23-4-8 | B-55600-20-4-8 | B-55600-23-4-9

Cette variante du lecteur d'empreintes digitales ou du clavier à code est destinée à être installée dans les portes comme contrôle d'accès. Pour simplifier, les figures illustrent le montage du lecteur d'empreintes digitales. Le montage du clavier à code n'est pas différent.

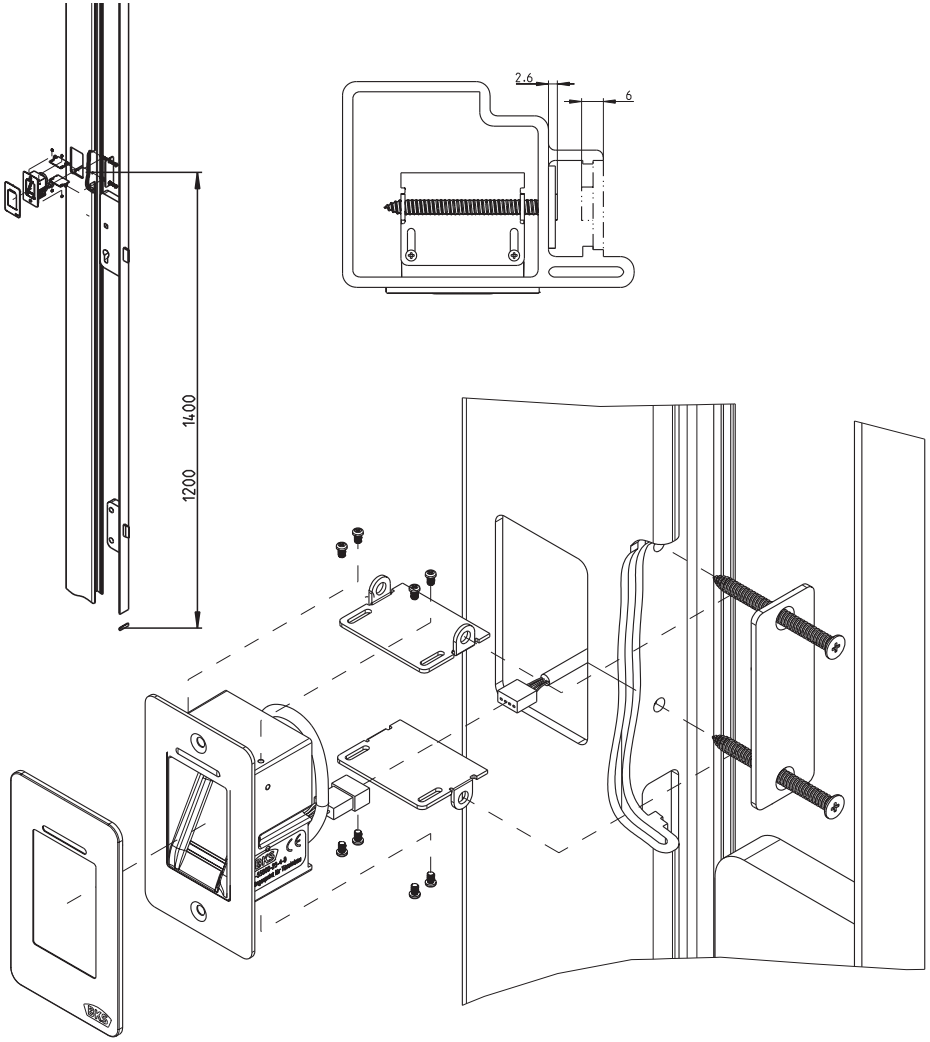
3.1.1 Montage dans des portes en bois et acier

3.1.2 Montage dans des portes en alu et PVC

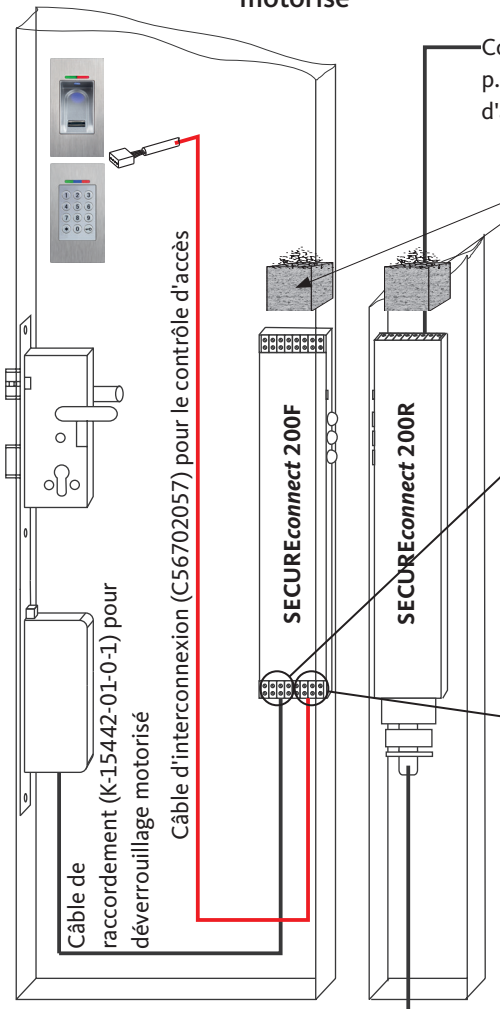




3.1.3 Montage avec SECURY (déverrouillage motorisé)



3.1.4 Schéma de câblage pour le dispositif de déverrouillage motorisé



Contact d'amorçage sans potentiel
p. ex. bouton-poussoir, interphone, contrôle d'accès, horloge de programmation.

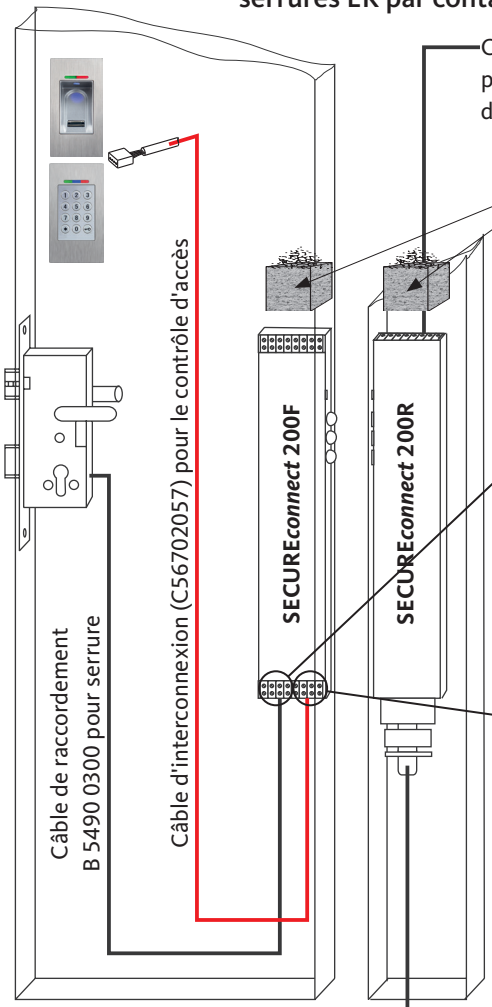
Utilisez les éponges fournies comme protection contre les copeaux lors du montage dans des profilés métalliques.

SC 200F	Câble de raccordement pour déverrouillage motorisé	
Borne	Couleur du fil	Signal
GS	GY | Gris	GND (moins)
VS	BN | Brun	+ 24 V (plus)
90	BK | Noir	Câble de commande

SC 200F	Câble d'interconnexion pour le contrôle d'accès	
Borne	Couleur du fil	Signal
GS	YE | Jaune	GND (moins)
96	WH | Blanc	RS-485 A
95	GN | Vert	RS-485 B
94	BN | Brun	+ 24 V (plus)

Sur les portes en métal et PVC, utilisez le protège-câble fourni au niveau de la sortie de câble.

3.1.5 Schéma de câblage pour les serrures motorisés et les serrures EK par contacts sans potentiel



Contact d'amorçage sans potentiel
p. ex. bouton-poussoir, interphone, contrôle d'accès, horloge de programmation.

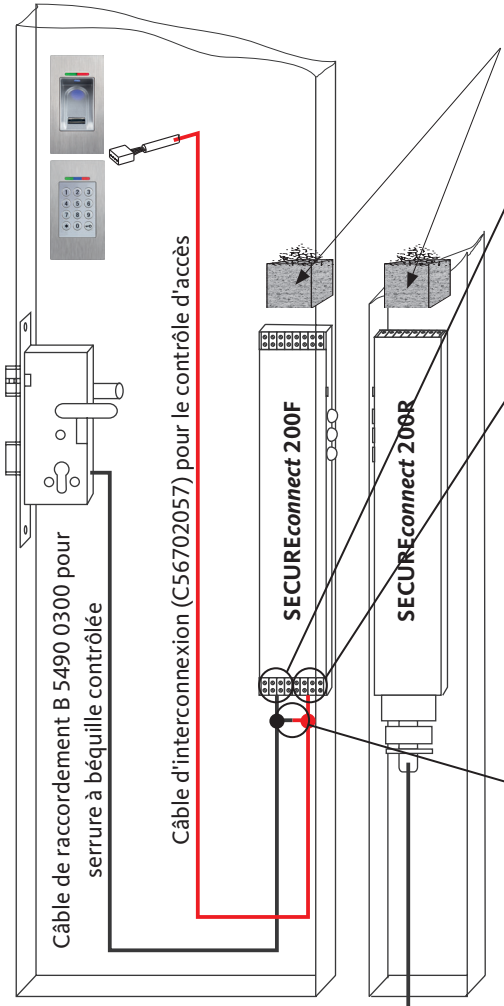
Utilisez les éponges fournies comme protection contre les copeaux lors du montage dans des profilés métalliques.

SC 200F	Câble de raccordement pour serrure	
Borne	Couleur du fil	Signal
GS	WH | Blanc	GND (moins)
VS	BN | Brun	+ 24 V (plus)
90	PK | Rose	Câble de commande

SC 200F	Câble d'interconnexion pour le contrôle d'accès	
Borne	Couleur du fil	Signal
GS	YE | Jaune	GND (moins)
96	WH | Blanc	RS-485 A
95	GN | Vert	RS-485 B
94	BN | Brun	+ 24 V (plus)

Sur les portes en métal et PVC, utilisez le protège-câble fourni au niveau de la sortie de câble.

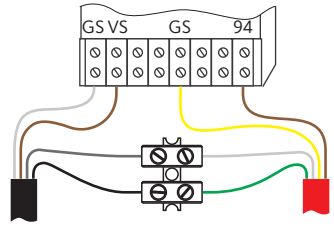
3.1.6 Schéma de câblage pour les serrures EK par bus RS-485



Utilisez les éponges fournies comme protection contre les copeaux lors du montage dans des profilés métalliques.

SC 200F	Câble de raccordement pour serrure EK	
Borne	Couleur du fil	Signal
GS	WH | Blanc	GND (moins)
VS	BN | Brun	+ 24 V (plus)

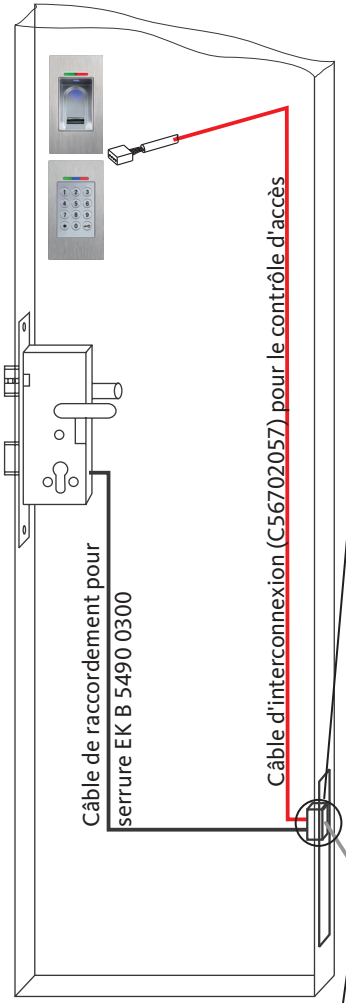
SC 200F	Câble d'interconnexion pour le contrôle d'accès	
Borne	Couleur du fil	Signal
GS	YE | Jaune	GND (moins)
94	BN | Brun	+ 24 V (plus)



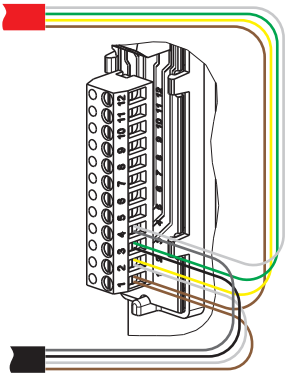
Couleur du fil		Signal
Câble de raccordement pour serrure EK	Câble d'interconnexion pour le contrôle d'accès	
GY | Gris	WH | Blanc	RS-485 A
BK | Noir	GN | Vert	RS-485 B

Sur les portes en métal et PVC, utilisez le protège-câble fourni au niveau de la sortie de câble.

3.1.6.1 Raccordement à la tension d'alimentation externe



Couleur du fil		N°	Signal
Câble de raccordement pour serrure EK	**Câble d'inter-connexion pour le contrôle d'accès**	**Passe-câble**	
GY | Gris	WH | Blanc	4	RS-485 A
BK | Noir	GN | Vert	3	RS-485 B
Raccordement à la tension d'alimentation externe			
WH | Blanc	YE | Jaune	2	GND (moins)
BN | Brun	BN | Brun	1	+ 12 V– 24 V CC



Bloc d'alimentation B 5570 0402

Passe-câble	Bloc d'alimentation
1	24 V CC
2	GND (moins)

3.1.7 Protection contre les manipulations avec SECURE*connect* 200

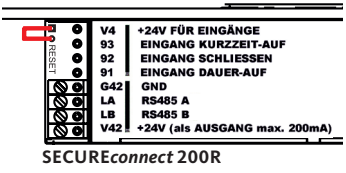
Lors de montage sur porte, votre système est composé de 2 appareils électroniques

- Contrôle d'accès : lecteur d'empreintes digitales ou clavier à code
- Unité de commande : SECURE*connect* 200

Le lecteur d'empreintes digitales ou le clavier à code est en général montée à l'extérieur (face extérieure de la porte). Pour éviter toute manipulation non autorisée, votre système est équipé de nombreuses fonctions de sécurité qui empêchent un accès illicite :

- Le contrôle d'accès est reliée à l'unité de commande par un câble de données. La transmission des données est cryptée.
- Le contrôle d'accès et l'unité de commande sont couplés entre eux de manière univoque lors de la première mise en service (appairage).

Pour remplacer un composant (SECURE*connect* 200R, SECURE*connect* 200F ou le contrôle d'accès) du système de porte, une procédure de ré-appairage doit être effectuée sur le transmetteur de courant et de données du SECURE*connect* 200. À cet effet, le contact de réinitialisation sur la platine du SECURE*connect* 200F ou du SECURE*connect* 200R doit être fermé pendant 3 secondes au moins, avec alimentation électrique branchée. Utilisez pour cela p. ex. une pince crocodile.



SECURE*connect* 200R

La pince peut ensuite être retirée. Le SECURE*connect* 200R, le SECURE*connect* 200F et le contrôle d'accès entament alors une nouvelle procédure d'appairage. Le contrôle d'accès est remis à la configuration d'usine (tous les empreintes digitales et les codes PIN sont effacés).

Si un contrôle d'accès est connecté à un SECURE*connect 200* appairé, il convient de procéder à un reset d'appairage. Une nouvelle clé système est alors générée et les empreintes digitales ou les codes PIN sont effacés.

3.1.8 Appairage du lecteur d'empreintes digitales/clavier à code avec la serrure EK

Un raccordement direct au lecteur d'empreintes digitales ou au clavier à code est possible avec les serrures à béquille contrôlée des séries EK19 et EK21 dans la version câblée. Le contrôle d'accès et la serrure à béquille contrôlée sont automatiquement reliés entre eux de manière univoque lors de la première mise en service par l'intermédiaire de l'interface RS-485 dans une connexion de bus (appairage).

Pour remplacer après l'appairage un composant du système de porte (lecteur d'empreintes digitales, clavier à code ou serrure), un ré-appairage doit être effectué avant de coupler à nouveau les composants. Le ré-appairage est effectué sur la serrure à béquille contrôlée suivant une séquence donnée.

Cette séquence commence par le redémarrage de la serrure à béquille contrôlée par coupure et restauration de l'alimentation électrique. En l'espace d'une minute après le redémarrage, les étapes suivantes doivent être effectuées :

- Maintenez la béquille appuyée tout en déclenchant le contact du panneton.
- En même temps, faites plusieurs fois rapidement tourner le cylindre avec la clé dans le sens des aiguilles d'une montre et dans le sens cxontraire et passez au moins 3 fois sur le contact du panneton en 10 secondes.

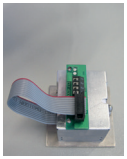
Une fois le ré-appairage effectué avec succès, tous les appareils appairés sont effacés et les composants sont à nouveau « appairés ».

3.2 Montage mural appliqué/encastré – B-55600-23-1-8 | B-55600-20-1-8

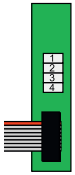
Cette variante du lecteur d'empreintes digitales ou du clavier à code est destinée à être montée dans le mur à côté de la porte comme contrôle d'accès. Pour simplifier, les figures illustrent le montage du lecteur d'empreintes digitales. Le montage du clavier à code n'est pas différent.

3.2.1 Montage encastré du système d'accès

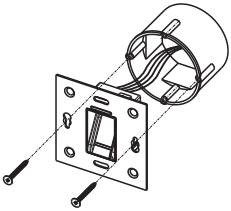
Le montage se fait dans une boîte d'encastrement. Nous recommandons une hauteur de montage de 1,2 à 1,4 m à partir du bord supérieur du sol fini.



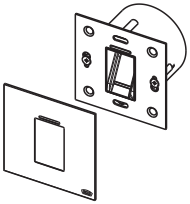
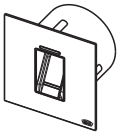
- Connectez le contrôle d'accès au module relais.



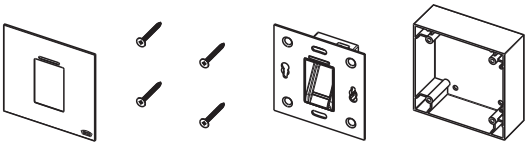
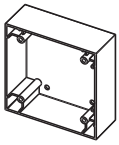
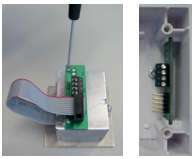
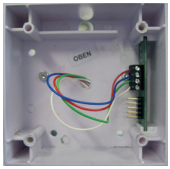
Raccordez comme il se doit le câble d'amenée vers l'unité interne aux bornes 1 à 4.

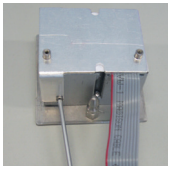


- Fixez le cadre porteur avec les 2 vis (3,5 x 25) fournies sur la boîte d'encastrement.

	■ Retirez la feuille de protection des bandes adhésives au dos du cadre extérieur en acier inoxydable. ■ Positionnez le cadre extérieur sur le cadre porteur du contrôle d'accès.
	■ Vérifiez le bon fonctionnement.

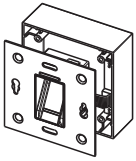
3.2.2 Montage en applique du système de contrôle d'accès

	
	Fixez le boîtier d'applique au mur. Nous recommandons une hauteur de montage de 1,2 à 1,4 m à partir du bord supérieur du sol fini. Utilisez à cet effet les vis (3,5 x 25) et les chevilles fournies.
	■ Retirez la platine de connexion en desserrant les deux vis. ■ Poussez la platine de connexion dans la rainure prévue à cet effet sur le boîtier d'applique.
	■ Raccordez le câble au module relais « Whitebox » correspondant aux bornes de 1 à 4.

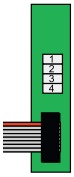


■ Retirez la paroi arrière.

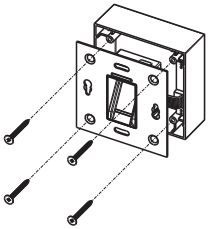
REMARQUE ! Le contrôle d'accès ne rentre pas dans le boîtier d'applique lorsque la paroi arrière est montée.



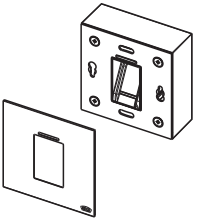
■ Connectez le câble plat du contrôle d'accès sur la platine de connexion.



Le repère rouge sur le câble plat doit être orienté en direction des bornes de connexion.

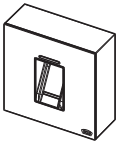


■ Fixez le cadre porteur avec les 4 vis (3,5 x 25) fournies sur le boîtier d'applique.



■ Retirez la feuille de protection des bandes adhésives au dos du cadre extérieur en acier inoxydable.

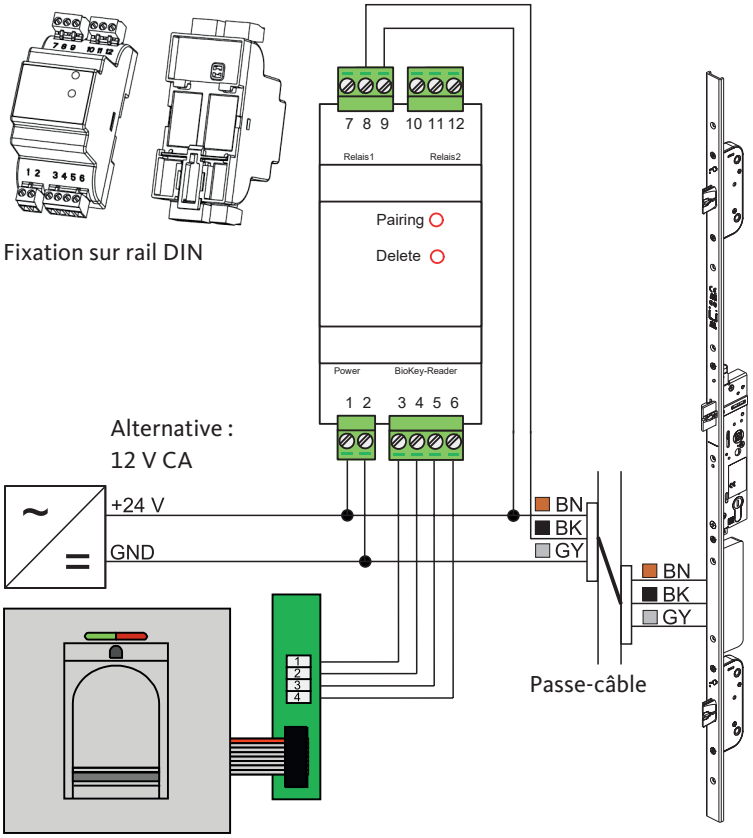
■ Positionnez le cadre extérieur sur le cadre porteur du contrôle d'accès.



■ Vérifiez le bon fonctionnement.

3.2.3 Schéma de câblage avec le module relais « Whitebox »

Les unités internes et externes communiquent par le biais d'un bus crypté. Pour la connexion entre le module relais « Whitebox » et le contrôle d'accès, nous recommandons une conduite de télécommunication J-Y(ST) Y2 x 2 x 0.8. L'exemple de connexion vaut pour le dispositif de déverrouillage motorisé de la groupe Gretsch-Unitas.



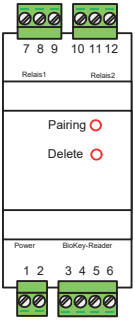
REMARQUE **Pour le montage appliqué, le câble plat (ligne rouge en direction des bornes) doit être correctement connecté.**

3.2.4 Caractéristiques techniques – module relais « Whitebox »

Tension de service :	8 à 30 V CC ou 8 à 12 V CA
Puissance absorbée :	1 W, en pointe 3 W (plus puissance du dispositif de déverrouillage motorisé connecté)
Données de relais :	24 V CA/CC 5,0 A
Espace de montage	En intérieur pour protéger la commande des relais
Dimensions de module relais H x l x P [mm]	86,4 x 44,9 x 52,6 (dimensions sans bornes)

3.2.5 Protection contre les manipulations avec le module relais « Whitebox »

ATTENTION **Le module relais doit être installé dans une zone sécurisée et ne doit pas être accessible de l'extérieur !**



Pour les appareils encastrés ou en applique pour montage mural, le module relais « Whitebox » et le contrôle d'accès sont appairés entre eux en usine. En cas de remplacement d'un composant de matériel, l'appairage doit être à nouveau déclenché.

- Pour démarrer l'appairage, appuyez sur le bouton situé dans le perçage entouré de rouge de l'unité intérieure et libellé « Pairing ».

3.2.6 Réinitialisation avec le module relais « Whitebox »

Pour les appareils encastrés ou en applique pour montage mural, vous pouvez déclencher, à l'aide du module relais, une réinitialisation aux réglages d'usine avec effacement de toutes les empreintes digitales, y compris les empreintes maître ou les codes PIN.

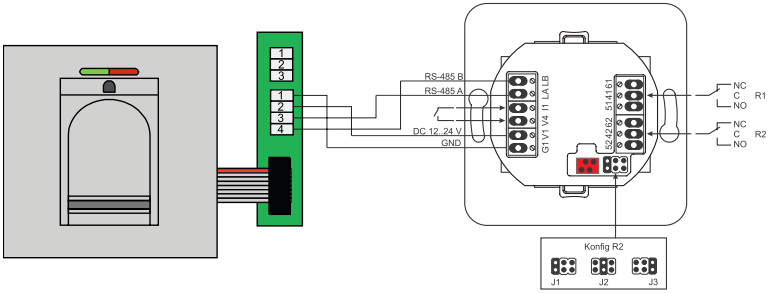
- Pour lancer le processus de suppression, appuyez sur le bouton situé dans le perçage libellé « Delete » et entouré de rouge du module relais « Whitebox ».

Après la réinitialisation, les LED verte, rouge et bleue sont allumées en permanence sur le contrôle d'accès.

REMARQUE **Après la réinitialisation, le code maître modifié sera remplacé par le code usine !**

3.2.7 Connexion au module radio (FMIO)

Le contrôle d'accès peut communiquer directement avec un module radio (FMIO) par le biais d'un bus crypté.
Pour la connexion entre le module mural radio I/O et le contrôle d'accès, nous recommandons un câble de télécommunication J-Y(ST) Y2 x 2 x 0.8.



3.2.7.1 Fonctions de sortie du FMIO

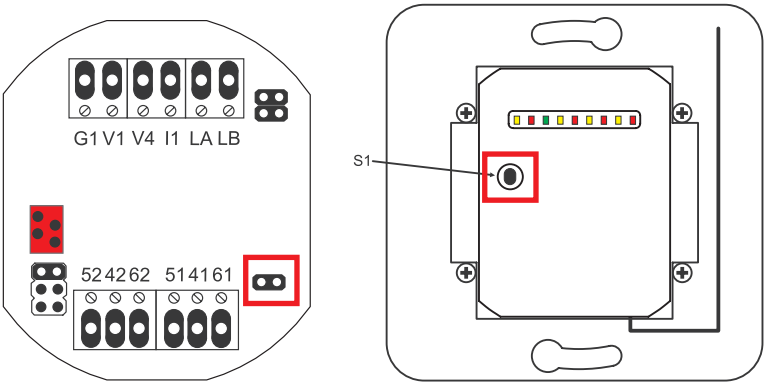
Le relais « R1 » du module mural radio I/O est utilisé après le raccordement d'un contrôle d'accès via l'interface RS-485 pour indiquer un accès autorisé. La sortie de relais « R1 » n'est plus configurable. L'affichage optique sera effectué via LED « L7 » sur la face du module mural radio I/O.

Le relais « R2 » offre la possibilité de refléter 3 signaux différents. Le signal est configuré par la mise en place du cavalier (voir le tableau ci-après). L'affichage optique s'effectue via LED « L2 ».

Sortie	FMIO avec cylindre avec commande radio à couplage électronique/serrure radio à béquille contrôlée	FMIO avec cylindre avec commande radio à couplage électrique/serrure radio à béquille contrôlée et lecteur d'empreintes digitales/clavier à code
1	-	Accès autorisé
2 + J1	-	Tentative d'accès non autorisée
2 + J2	Embrayage actif (cylindre/serrure embrayé)	-
2 + J3	Niveau de charge de la pile	Niveau de charge de la pile

3.2.7.2 Appairage et reset d'appairage du FMIO

Une fois qu'un contrôle d'accès a été raccordé au module mural radio I/O a lieu, ce qu'on appelle, un appairage. Aucun autre contrôle d'accès ne peut désormais être connecté au même FMIO. Si cela devait s'avérer nécessaire, l'appairage avec le contrôle d'accès doit être réinitialisé.



À cet effet, il faut ouvrir le couvercle du boîtier.

- Séparez le module de l'interface RS-485.
- Fichez le cavalier à côté de la borne « 51 41 61 ».
- Il faut maintenant presser la touche « S1 » jusqu'à ce qu'un signal acoustique se fasse entendre.

L'information d'appairage a été effacée.

Si un appairage entre le cylindre avec commande radio à couplage électrique, entre la serrure radio à béquille contrôlée et le module mural radio I/O doit être annulé, le cavalier ne doit pas être enfoncé. Dans ce cas, une pression longue sur « S1 » annule l'information d'appairage du cylindre électrique radio/de la serrure radio à béquille contrôlée.

4. Utilisation du lecteur d'empreintes digitales

Une mise en service doit être effectuée avant l'installation et l'utilisation du système d'accès. Procédez par étapes.

- Montez le lecteur d'empreintes digitales comme décrit au Chapitre 3.
- Effectuez les raccordements électriques conformément au schéma de câblage.

- La première mise sous tension initie la connexion (appairage).

Trois modes de fonctionnement sont disponibles pour l'utilisation et la configuration du lecteur d'empreintes digitales. L'appareil de programmation permet de changer de mode d'administration. **À la livraison, le mode d'administration Bluetooth est activé.** Les autres modes sont le « Mode d'administration normal » et le « Mode d'administration par liste ».

ATTENTION **L'entrée n'est pas sécurisée et peut être ouverte tant que l'empreinte maître n'a pas été programmée.**

4.1 Consignes d'utilisation

4.1.1 Conversion du mode d'administration

REMARQUE **Après la réinitialisation, toutes les informations enregistrées sont perdues, seul le mode d'administration est conservé.**

Le mode de fonctionnement ne peut être converti qu'à l'état de livraison (toutes les LED sont allumées). Vous retournez à cet état en réinitialisant votre lecteur d'empreintes digitales avec DA » CODE » OK. Le code se trouve sur la page 128 et sur l'appareil de programmation. Pour changer de mode d'administration, tenez l'appareil de programmation directement devant le lecteur d'empreintes digitales (LED bleue) et pressez les touches suivantes :

	9 » 9 » OK » 5 » 0 » OK	Mode d'administration normal
	9 » 9 » OK » 5 » 1 » OK	Mode d'administration par liste
	9 » 9 » OK » 5 » 7 » OK	Mode d'administration Bluetooth (état de livraison)

Après la conversion, le lecteur d'empreintes digitales passe à l'état de livraison (toutes les LED sont allumées).

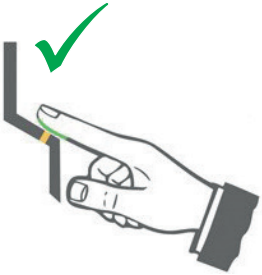
4.1.2 Positionnement du doigt

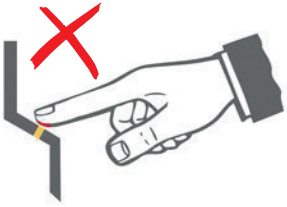
Procédez avec très grand soin pendant la programmation des empreintes digitales. Les empreintes maître et utilisateur peuvent être refusées si des erreurs ont été commises au cours de programmation. Plus l'empreinte est programmée correctement, plus il sera facile de la reconnaître ultérieurement lors de l'identification.

REMARQUE **Avant de programmer les empreintes maître ou utilisateur, nous recommandons de se laver au moins une fois les mains.**

- Faites glisser votre doigt rapidement, régulièrement et avec une légère pression sur la ligne du capteur en utilisant la plus grande partie possible du doigt.

Pour choisir un doigt, il faut savoir que l'index est plus approprié si les doigts sont fins.





4.1.3 Comportement à l'ouverture de la porte (uniquement pour le montage sur porte)

Pour les versions B-55600-23-4-8 et B-55600-23-4-9 (lecteur d'empreintes digitales à monter sur porte), le lecteur d'empreintes digitales est automatiquement désactivé si la porte reste ouverte pendant plus de 12 secondes.

Les empreintes digitales enregistrées pour l'ouverture de la porte sont conservées en cas de panne de courant. La date et l'heure pour l'analyse des événements doivent être reprogrammées après une coupure de courant.

4.1.4 Appareil de programmation, abréviations

Touche	Signification	Explication
DA	Delete All	Effacer tout, y compris l'empreinte maître
OK	OK	Exécuter fonction
R1 » B	Relay 1 » Block	Relais 1 » Bloquer ID utilisateur
RT	Relay-Time	Temps de commutation
R2 » UB	Relay 2 » Unblock	Relais 2 » Débloquer ID utilisateur
D	Delete	Effacer l'empreinte enregistrée
E	Enroll	Enregistrement de l'empreinte
TT	Time	Temps (secondes)

Abréviation	Signification	Explication
MF	Master Finger	Empreinte maître
CODE	PIN code	Code d'utilisateur ou code maître
ID	Index	ID utilisateur
YYYY | MM | DD	Year | Month | Day	Année | Mois | Jour
HH | MM | TT	Hour | Minute | Time	Heure | Minute | Secondes (temps)

REMARQUE

Tenez l'appareil de programmation directement devant la diode électroluminescente bleue du lecteur d'empreintes digitales. La pression des touches est indiquée visuellement par un bref allumage de la LED verte. Si la LED ne s'allume pas après la pression, répétez l'entrée.

4.2 Mode d'administration Bluetooth

Le mode d'administration Bluetooth vous permet de configurer et de gérer le lecteur d'empreintes digitales avec votre smartphone et l'application BKS BioKey. Après l'autorisation sur le lecteur d'empreintes digitales à l'aide de l'empreinte maître, vous pouvez appeler la fonction souhaitée suivant le menu de l'application BKS BioKey et effectuer les réglages nécessaires à l'administration de votre système.

Le mode d'administration Bluetooth est préréglé à l'état de livraison. Pour passer à un autre mode, suivez les instructions de la Section 4.1.1 [152].

- Dans le mode d'administration Bluetooth, vous pouvez configurer le lecteur d'empreintes digitales à l'aide des fonctions suivantes.

4.2.1 Mode test

Dans l'état de livraison ou après la réinitialisation, il est possible qu'une ouverture de porte puisse être déclenchée à titre de test avec l'appareil de programmation sans que le lecteur d'empreintes digitales ne soit configuré au préalable. Condition : l'appareil est en état de livraison.

Notez que tant que le lecteur d'empreintes digitales est en état de livraison, l'entrée n'est pas sécurisée.

	■ Tenez l'appareil de programmation directement devant la LED bleue du lecteur d'empreintes digitales ■ Pressez la touche « 0 » sur l'appareil de programmation ■ La LED verte s'allume à chaque pression de touche pour contrôle visuel ■ Pressez la touche « OK » pour confirmer. ■ L'ouverture de la porte est déclenchée

4.2.2 Programmer l'empreinte maître

Pour des raisons de sécurité, l'autorisation par l'empreinte maître est vérifiée avant chaque configuration du lecteur d'empreintes digitales. Raison pour laquelle vous commencez la configuration par la programmation de l'empreinte maître et en définissant qui sera autorisé à gérer le système par la suite.

REMARQUE

Dans l'étape suivante de la configuration du lecteur d'empreintes digitales, commencez par programmer la première empreinte maître sans ouvrir l'application (lecteur d'empreintes digitales à l'état de livraison).

Dans le choix du doigt, il convient de considérer qu'une empreinte maître ne peut plus être utilisée comme empreinte utilisateur pour ouvrir une porte. Il est ainsi conseillé, pour un droitier par exemple, d'utiliser l'index gauche comme empreinte maître et l'index droit comme empreinte utilisateur.

REMARQUE

Pour programmer l'empreinte maître, faites glisser 5 fois le même doigt sur le capteur.

- Les LED verte, rouge et bleue sont allumées en permanence
- L'appareil est initialisé et prêt à être configuré

REMARQUE ! La condition préalable est que le lecteur d'empreintes digitales se trouve dans l'état de livraison ou qu'une réinitialisation ait été effectuée.

REMARQUE ! Après chaque lecture d'une empreinte digitale (en passant le doigt sur le capteur), vous devez attendre environ 2 secondes pour que la fin de l'opération soit signalée par l'allumage constant des LED verte et rouge.
Ce n'est qu'alors que vous pouvez poursuivre la programmation et passer à nouveau le même doigt sur le capteur.
Ne pas laisser s'écouler plus de 60 s entre les différentes étapes de saisie de l'empreinte maître, faute de quoi la procédure est annulée.

<table>
<tr>
<td> 
 
  </td>
<td>Programmation
■ Vous faites glisser le doigt que vous voulez utiliser comme première empreinte maître sur le capteur
■ Les LED verte et rouge s'éteignent brièvement après la lecture
■ Après environ 2 secondes, les LED verte et rouge s'allument à nouveau en permanence. Le lecteur d'empreintes digitales est prête
■ La programmation peut être poursuivi en faisant à nouveau glisser le même doigt sur le capteur
■ Répétez la programmation jusqu'à ce que le doigt soit enregistré 5 fois avec succès</td>
</tr>
<tr>
<td>  </td>
<td>■ La programmation réussie est indiquée par la LED verte qui s'allume brièvement
■ En cas d'échec de la programmation, par manque de qualité par exemple, il convient de répéter la procédure jusqu'à ce que la LED verte s'allume brièvement</td>
</tr>
<tr>
<td>  </td>
<td>■ Lorsque le premier empreinte maître a été programmée, l'appareil est en état de fonctionnement
■ La LED bleue s'allume en permanence
■ La configuration peut alors être poursuivie</td>
</tr>
<tr>
<td colspan="2">REMARQUE ! Si pendant la procédure de programmation une empreinte a été passée sur le capteur et n'a pas été acceptée comme empreinte maître, les LED verte et rouge demeurent allumées. La procédure de programmation de l'empreinte maître doit être répétée.</td>
</tr>
</table>

Après avoir programmé la première empreinte maître,
vous pouvez encore ajouter d'autres empreintes maître ultérieurement,
voir la Section 4.2.6 [161] ou 4.3.3 [170].

4.2.3 Configuration de l'application BKS BioKey

L'appli BKS BioKey est disponible pour les systèmes d'exploitation Apple iOS et Google Android. Téléchargez l'appli sur l'App Store ou Google Play. Saisissez le terme « BioKey » dans le champ de recherche du store.

Available on the App Store

GET IT ON Google Play

REMARQUE

Les conditions préalables à la gestion de l'application BKS BioKey sont les suivantes :
- l'interface Bluetooth est activée sur le smartphone
- l'application est autorisée à accéder à l'emplacement du smartphone
- la première empreinte maître a été programmée, voir Section 4.2.2 [156]

- Veillez à ce que le lecteur d'empreintes digitales se trouve à portée Bluetooth de votre smartphone.
- Démarrez l'appli BKS BioKey.
- Appuyez sur « Select device » (sélectionner un apparail) en haut de l'écran.

L'application BKS BioKey recherche les appareils disponibles et ouvre une liste des lecteurs d'empreintes digitales trouvés.

- Sélectionnez le lecteur d'empreintes digitales souhaité dans la liste.
- Suivez l'invitation à vous identifier avec le lecteur d'empreintes digitales.

- Passez l'empreinte maître sur le capteur
- Les LED verte et route s'allument une fois brièvement

L'appareil mobile est maintenant connecté avec le lecteur d'empreintes digitales pour cette séance et la configuration du lecteur peut être effectuée par le biais de l'appli.

- Après chaque ouverture de l'application, ou si l'application n'a pas été utilisée pendant une minute, il vous est demandé, pour des raisons de sécurité, de vous identifier avec votre empreinte maître.

4.2.4 Ajouter utilisateur (appli BKS BioKey)

- Démarrez l'appli BKS BioKey.
- Suivez l'invitation à vous identifier avec le lecteur d'empreintes digitales.

	■ Passez l'empreinte maître sur le capteur ■ Les LED verte et route s'allument une fois brièvement

- Appuyez sur le bouton « Users » (utilisateurs).
- Appuyez sur « + » **en haut à droite** l'écran.
- Sélectionnez « Name » (nom d'utilisateur) et saisissez-le.
- Appuyez sur « Add finger... » (ajouter un doigt) dans la zone « Fingers » (doigts).
- Sélectionnez « Description » et indiquez quel doigt de l'utilisateur doit être lu.
- Attribuez les droits du nouveau doigt en activant ou en désactivant le commutateur pour les relais 1 et 2 respectifs dans la zone « Permissions » (autorisations). Relais 2 uniquement pour montage mural encastré/en applique avec fonction.
- Appuyez sur « Enroll finger... » (programmer l'empreinte) dans la zone « Actions » (actions).

	■ Suivez le dialogue de l'application BKS BioKey ■ Faites glisser sur le capteur le doigt qui doit être utilisé comme empreinte utilisateur ■ Répétez la programmation jusqu'à ce que le doigt soit enregistré 5 fois avec succès ■ Le compteur de l'application vous indique la progression ou le nombre de fois où vous devez encore scanner le doigt Notez qu'un doigt qui a été programmé comme empreinte maître ne peut pas être utilisé comme empreinte utilisateur.

- Lorsqu'une empreinte a été enregistrée avec succès, un ID et le nombre de lectures sont affichés.

Une seule empreinte digitale peut être créée par utilisateur. Le nombre d'empreintes utilisateur est limité à 35 empreintes digitales en raison des capacités de l'espace mémoire.

- Naviguez dans les menus du haut à l'aide de « <- retour » et de « < ». La nouvelle empreinte utilisateur ou l'utilisateur y est affiché.

4.2.5 Traiter et effacer utilisateur (appli BKS BioKey)

- Démarrez l'appli BKS BioKey.
- Suivez l'invitation à vous identifier avec le lecteur d'empreintes digitales.

	■ Passez l'empreinte maître sur le capteur ■ Les LED verte et route s'allument une fois brièvement

- Appuyez sur le bouton « Users » (utilisateurs).
- Sélectionnez un utilisateur dans la liste « Users » (utilisateurs) pour le modifier d'après les étapes suivantes.
- Sélectionnez « Name » (nom d'utilisateur) dans la section « General » (généralités) et modifiez-le ou corrigez-le.
- Pour modifier ou ajouter d'autres empreintes utilisateur ou maître, sélectionnez dans la zone « Fingers » (doigts) les champs de saisie correspondants et éditez-les.

Veuillez suivre les instructions pour l'apprentissage d'une nouvelle empreinte utilisateur dans la Section 4.2.4 [159].

- Activez ou désactivez le bouton « Block finger » (bloquer l'empreinte) dans la zone « Actions » pour bloquer ou débloquer l'utilisateur.
- Sélectionnez « Delete user...» (supprimer l'utilisateur) dans la zone « Actions » et confirmez la suppression.

4.2.6 Ajouter empreinte maître (appli BKS BioKey)

- Démarrez l'appli BKS BioKey.
- Suivez l'invitation à vous identifier avec le lecteur d'empreintes digitales.

	■ Passez l'empreinte maître sur le capteur ■ Les LED verte et route s'allument une fois brièvement

- Appuyez sur le bouton « Users » (utilisateurs).
- Appuyez sur « + » **en haut à droite** l'écran.
- Sélectionnez « Name » (nom d'utilisateurs) et saisissez-le.
- Activez le bouton « Master user » (maître-utilisateur).
- Appuyez sur « Add finger... (ajouter un doigt) dans la zone « Fingers » (doigts).
- Appuyez sur « Enroll finger...» (programmer l'empreinte).

	■ Suivez le dialogue de l'application BKS BioKey ■ Faites glisser sur le capteur le doigt qui doit être utilisé comme empreinte maître ■ Répétez la programmation jusqu'à ce que le doigt soit enregistré 5 fois avec succès ■ Le compteur de l'application vous indique la progression ou le nombre de fois où vous devez encore scanner le doigt Notez qu'un doigt qui a été programmé comme empreinte maître ne peut pas être utilisé comme empreinte utilisateur.

4.2.7 Identification par empreinte utilisateur, Ouvrir porte

	■ L'appareil est en état de service ■ La LED bleu s'allume
	■ Passez l'empreinte utilisateur sur le capteur ■ En cas d'identification de l'empreinte, la LED verte s'allume et la porte s'ouvre Dans le mode d'administration normal, c'est toujours le relais 1 qui est activé pour la variante en applique/encastré (montage mural).
	■ Si le lecteur d'empreintes digitales ne reconnaît pas l'empreinte utilisateur, la LED rouge s'allume et la porte ne s'ouvre pas

4.2.8 Mode de blocage

	**Blocage** ■ Lorsqu'une empreinte non programmée est passée à dix reprises consécutives sur le capteur (la LED rouge s'allume), l'appareil commute sur le mode de blocage. Ceci empêche des personnes non autorisées de parvenir à se frayer librement un accès En mode de blocage, l'appareil de programmation ne réagit à aucune empreinte ni à aucune entrée. La période de blocage est de 1 minute. La LED rouge s'allument pendant la période de blocage.
	**Déblocage** ■ Le mode de blocage peut être supprimé avant terme par le passage d'une empreinte programmée (empreinte maître ou utilisateur) sur le capteur. Ensuite la porte peut être ouverte comme habituellement avec l'empreinte d'un utilisateur

4.2.9 Réinitialiser, effacer toutes les empreintes d'utilisateurs et maîtres

REMARQUE

Avant la réinitialisation, fermez l'application BKS BioKey sur votre smartphone.

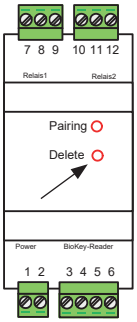
Tenez l'appareil de programmation directement devant la diode électroluminescente bleue du lecteur d'empreintes digitales.

- Pressez la touche « DA » (Delete all) sur l'appareil de programmation. La LED verte s'allume
- Saisissez le code usine de la page 128 ou le code maître avec l'appareil de programmation
- Pour terminer, clicquez sur la touche « OK »
- L'appareil est initialisé. La LED verte, rouge et bleue s'allument en permanence

REMARQUE

Un reset d'appairage permet de réinitialiser le lecteur d'empreintes digitales. Toutes les empreintes utilisateur et maître sont alors également effacées et le code maître est réinitialisé au code usine !

4.2.9.1 Réinitialisation alternative avec le module relais « Whitebox » (en applique/encastré)



Pour la variante en applique/encastré à montage mural, vous pouvez utiliser le boîtier de relais « Whitebox » pour déclencher une réinitialisation aux paramètres d'usine avec effacement de toutes les empreintes digitales, y compris l'empreinte maître.

- Pour lancer la suppression, appuyez pendant environ 5 secondes sur le bouton situé dans le perçage libellé « Delete » de l'unité intérieure.

Après la réinitialisation, les LED verte, rouge et bleue sont allumées en permanence.

REMARQUE

Après la réinitialisation, le code maître modifié sera remplacé par le code usine !

4.2.9.2 Réinitialisation alternative avec l'empreinte maître

	■ Le lecteur d'empreintes digitales est en état de service ■ La LED bleu s'allume
	■ Passez l'empreinte maître sur le capteur, les LED verte et rouge s'allument brièvement une seule fois
	■ Après la deuxième lecture de l'empreinte maître, un bref clignotement des LED verte et rouge indique que le mode d'effacement est initialisé
	■ Après la quatrième lecture de l'empreinte maître, le processus d'effacement est lancé. Ceci est indiqué par l'éclairage de la LED verte
	■ Après la réinitialisation, le lecteur d'empreintes digitales est en état de livraison ■ Les LED verte et rouge s'allument en permanence

REMARQUE

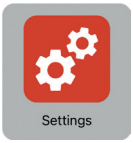
Après la réinitialisation, le code maître modifié sera remplacé par le code usine !

4.2.10 Modification du code usine en code maître (application BKS BioKey)

Le code usine (voir page 128) peut être modifié en un code maître à 6 chiffres à l'aide de l'application BKS BioKey ou de l'appareil de programmation.

REMARQUE

Pour raisons de sécurité, nous recommandons de remplacer le code usine par un nouveau code maître. Après la réinitialisation, le code maître sera remplacé par le code usine !



- Démarrez l'appli BKS BioKey.
- Suivez l'invitation à vous identifier avec le lecteur d'empreintes digitales.

	■ Passez l'empreinte maître sur le capteur ■ Les LED verte et route s'allument une fois brièvement

- Appuyez sur le bouton « Settings » (réglages).
- Sélectionnez « Reset code » (code de réinitialisation) et saisissez un nouveau code.

4.2.10.1 Modifier à l'aide de l'appareil de programmation

	■ Touche « D » (Delete) sur l'appareil de programmation ■ Appuyez sur la touche « E » (Enroll) ■ Saisissez le code usine ou « ancien CODE » et appuyez sur la touche « OK » pour confirmer ■ Entrez le « nouveau CODE » et confirmez avec « OK » ■ Répétez la saisie du code maître (« nouveau CODE ») et appuyez sur la touche « OK » pour terminer

4.2.11 Afficher protocole d'accès (appli BKS BioKey)

- Démarrez l'appli BKS BioKey.
- Suivez l'invitation à vous identifier avec le lecteur d'empreintes digitales.

	■ Passez l'empreinte maître sur le capteur ■ Les LED verte et route s'allument une fois brièvement

- Appuyez sur le bouton « Access log » (protocole d'accès).

La liste « Access log » (protocole d'accès) s'ouvre et les événements enregistrés dans le lecteur d'empreintes digitales s'affichent. Cette liste comprend notamment les identifications réussies et les identifications refusées.

4.2.12 Régler les temps de commutation du module relais (appli BKS BioKey)

Les relais ne peuvent être commandés par des temps de commutation que dans le cas d'un montage mural encastré/en applique. Cette fonction n'est pas prise en charge pour les appareils destinés au montage sur porte.

- Démarrez l'appli BKS BioKey.
- Suivez l'invitation à vous identifier avec le lecteur d'empreintes digitales.

	■ Passez l'empreinte maître sur le capteur ■ Les LED verte et route s'allument une fois brièvement

- Appuyez sur le bouton « Relay times » (temps de relais).
- Sélectionnez « Relais 1 » ou « Relais 2 » pour le régler.
- Sélectionnez « Description » pour attribuer un nouveau nom au relais. Ce dernier est affiché dans le protocole d'accès ou dans l'attribution des utilisateurs.
- Le champ de saisie « Time » (temps) permet de régler le temps de commutation de chaque relais dans une plage comprise entre 0 et 60 secondes.

4.2.13 Renommer le lecteur d'empreintes digitales et afficher l'utilisation de la mémoire (application BKS BioKey)

- Démarrez l'appli BKS BioKey.
- Suivez l'invitation à vous identifier avec le lecteur d'empreintes digitales.

	■ Passez l'empreinte maître sur le capteur ■ Les LED verte et route s'allument une fois brièvement

- Appuyez sur le bouton « Settings » (réglages).
- Sélectionnez « Device name » (nom de l'appareil) et modifiez le nom du lecteur d'empreintes digitales

L'affichage de ce menu offre une vue d'ensemble des informations telles que la mémoire utilisée pour les empreintes digitales enregistrées, la mémoire disponible et la version firmware, etc.

4.3 Mode d'administration normal

Dans le mode d'administration normal, il est possible de configurer et de gérer le lecteur d'empreintes digitales sans utiliser d'application. La configuration du lecteur d'empreintes digitales s'effectue en « mode d'administration normal » en premier lieu avec l'empreinte maître. L'appareil de programmation est également nécessaire pour des fonctions spéciales.

Pour passer à ce mode d'administration, suivez les instructions de la Section 4.1.1 [152].

■ Le mode d'administration normal offre les fonctions suivantes.

4.3.1 Vue d'ensemble des fonctions

Fonctionnement	Déscription | Notice succincte
Mode test (n'est possible qu'à l'état de livraison)	→ Section 4.2.1 [155] 0 » OK
Programmer l'empreinte maître	→ Section 4.2.2 [156] État de livraison » Programmer avec succès l'empreinte maître à cinq reprises
Programmer l'empreinte utilisateur	→ Section 4.3.2 [169] Scanner l'empreinte maître » Programmer avec succès l'empreinte utilisateur à cinq reprises
Identification par empreinte utilisateur	→ Section 4.2.7 [162] Scanner l'empreinte utilisateur
Blocage du lecteur d'empreintes digitales	→ Section 4.2.8 [162] Après 10 tentatives infructueuses sans identification du doigt, le lecteur d'empreintes digitales est bloqué.
Déblocage du lecteur d'empreintes digitales	→ Section 4.2.8 [162] Scanner l'empreinte maître et l'empreinte utilisateur programmées

Fonctionnement	Déscription	Notice succincte
Réinitialiser, effacer toutes les empreintes d'utilisateurs et maîtres	→ Section 4.2.9 [163] DA » CODE » OK (CODE : code usine ou code maître actuel)
Modifier le code usine	→ Section 4.2.10 [164] → D » E » ancien CODE » OK » nouveau CODE » OK » nouveau CODE » OK
Ajouter l'empreinte maître	→ Section 4.3.3 [170] MF » E » 0 » Programmer avec succès l'empreinte maître à cinq reprises
Régler le temps de commutation	→ Section 4.3.4 [170] MF » RT » TT » OK *TT = temps en secondes [1...60 s], standard = 3 s*
Régler la date et l'heure	→ Section 4.3.5 [171] MF » E » RT » YYYY » OK » MM » OK » DD » OK » HH » OK » MM »OK

Pour plus d'informations sur l'affectation des touches de l'appareil de programmation et l'explication des abréviations, voir la Section 4.1.4 [154].

4.3.2 Programmer l'empreinte utilisateur

	■ L'appareil est en état de service et la LED bleue s'allume **REMARQUE !** Les empreintes maîtres ne peuvent pas être programmées comme empreintes utilisateur.
	■ Passez l'empreinte maître sur le capteur ■ Les LED verte et rouge s'éclairent brièvement
 	**Programmation** ■ Vous faites glisser le doigt que vous voulez utiliser comme empreinte utilisateur sur le capteur ■ La programmation est indiquée par un **bref allumage** de la **LED verte** ■ La programmation peut être poursuivi en faisant à nouveau glisser le même doigt sur le capteur
	■ Répétez la programmation jusqu'à ce que le doigt soit enregistré 5 fois avec succès ■ La réussite de programmation de l'empreinte utilisateur est signalée par **4 brefs allumages des LED verte et rouge** ■ L'état opérationnel est indiqué par la LED bleue en continu
REMARQUE ! Pour les empreintes « difficiles », il peut être nécessaire de programmer la même empreinte à plusieurs reprises. Si le nombre d'échecs est trop élevé, vous devriez utiliser un autre doigt comme empreinte utilisateur.	

Le nombre d'empreintes utilisateur est limité à 35 empreintes digitales en raison des capacités de l'espace mémoire pour les empreintes maître et utilisateur.

4.3.3 Ajouter l'empreinte maître

	■ Passez l'empreinte maître sur le capteur ■ Les LED verte et rouge s'éclairent brièvement
	■ Pressez la touche « E » (Enroll) sur l'appareil de programmation ■ Appuyez sur la touche « 0 »
 	**Programmation** ■ Vous faites glisser le doigt que vous voulez ajouter comme empreinte maître sur le capteur ■ La programmation est indiquée par un **bref allumage** de la **LED verte** ■ La programmation peut être poursuivi en faisant à nouveau glisser le même doigt sur le capteur
	■ Répétez la programmation jusqu'à ce que le doigt soit enregistré 5 fois avec succès ■ La réussite de programmation de l'empreinte utilisateur est signalée par **4 brefs allumages des LED verte et rouge** ■ L'état opérationnel est indiqué par la LED bleue en continu

4.3.4 Régler le temps de commutation des relais (uniquement pour variante appliquée/encastrée)

	■ Passez l'empreinte maître sur le capteur ■ Les LED verte et rouge s'éclairent brièvement

	■ Pressez la touche « RT » sur l'appareil de programmation ■ Saisissez au clavier un temps de commutation en secondes de 1 à 60 ■ Pour terminer, cliquez sur la touche « OK »

Dans le mode d'administration normal, seul le temps de commutation du relais 1 est réglable.

4.3.5 Initialiser la date et l'heure

Les accès enregistrés dans le lecteur d'empreintes digitales peuvent être lus à l'aide du kit d'audit (B-55606-00-3-0). Les accès répertoriés ne reçoivent un horodatage correct que si vous définissez initialement la date et l'heure.

	■ Passez l'empreinte maître sur le capteur ■ Les LED verte et rouge s'éclairent brièvement
	■ Pressez la touche « E » sur l'appareil de programmation ■ Appuyez la touche « RT » ■ Saisissez la date et l'heure sur le clavier et confirmez chaque étape avec la touche « OK » : YYYY« OK » MM « OK » DD « OK » HH « OK » MM « OK » Exemple : 23.07.2022, 12 h 45 : E » RT » 2022 » OK » 07 » OK » 23 » OK »12 » OK » 45 »OK

REMARQUE **Après une coupure de courant, la date et l'heure doivent être reprogrammées.**

4.4 Mode d'administration par liste

Dans le mode d'administration par liste, il est possible de configurer et de gérer le lecteur d'empreintes digitales sans utiliser d'application. Dans ce mode d'administration, chaque utilisateur se voit attribuer un identifiant, permettant une meilleure administration. La configuration se fait par le biais de l'empreinte maître et de l'appareil de programmation. Dans le mode d'administration par liste, vous pouvez sélectionner un identifiant et le traiter de manière ciblée, pour supprimer l'empreinte utilisateur d'un identifiant par exemple. Il est conseillé de documenter l'attribution dans une liste, voir un modèle dans la Section 4.4.9 [179].

Pour passer à ce mode d'administration, suivez les instructions de la Section 4.1.1 [152].

■ Le mode d'administration par liste offre les fonctions suivantes.

4.4.1 Vue d'ensemble des fonctions

Fonctionnement	Déscription | Notice succincte
Mode test (n'est possible qu'à l'état de livraison)	→ Section 4.2.1 [155] 0 » OK
Programmer l'empreinte maître	→ Section 4.2.2 [156] État de livraison » Programmer avec succès l'empreinte maître à cinq reprises
Programmer l'empreinte utilisateur	→ Section 4.4.2 [174] MF » E » ID » OK » Programmer avec succès l'empreinte utilisateur à cinq reprises
Identification par empreinte utilisateur	→ Section 4.2.7 [162] Scanner l'empreinte utilisateur
Blocage du lecteur d'empreintes digitales	→ Section 4.2.8 [162] Après 10 tentatives infructueuses sans identification du doigt, le lecteur d'empreintes digitales est bloqué.
Déblocage du lecteur d'empreintes digitales	→ Section 4.2.8 [162] Scanner l'empreinte maître et l'empreinte utilisateur programmées

Fonctionnement	Déscription | Notice succincte
Réinitialiser, effacer toutes les empreintes d'utilisateurs et maîtres	→ Section 4.2.9 [163] DA » CODE » OK (CODE : code usine ou code maître actuel)
Modifier le code usine	→ Section 4.2.10 [164] D » E » ancien CODE » OK » nouveau CODE » OK » nouveau CODE » OK
Suppression de certaines empreintes utilisateur	→ Section 4.4.3 [175] MF » D » ID » OK
Bloquer ID	→ Section 4.4.4 [176] →MF » B » ID » OK
Débloquer ID	→ Section 4.4.5 [176] →MF » UB » ID » OK
Contrôler ID	→ Section 4.4.6 [177] → OK » ID » OK
Ajouter l'empreinte maître	→ Section 4.3.3 [170] MF » E » 0 » Programmer avec succès l'empreinte maître à cinq reprises
Régler le temps de commutation du relais 1 (uniquement pour variante appliquée/encastrée)	→ Section 4.4.7 [177] MF » RT » R1 » TT » OK *TT = temps en secondes [1...60 s], standard = 3 s*
Régler le temps de commutation du relais 2 (uniquement pour variante appliquée/encastrée)	→ Section 4.4.7 [177] MF » RT » R2 » TT » OK *TT = temps en secondes [1...60 s], standard = 3 s*
Programmer l'empreinte utilisateur pour relais 1	→Section 4.4.8 [178] MF » E » ID » R1 » OK » Programmer avec succès l'empreinte utilisateur à cinq reprises
Programmer l'empreinte utilisateur pour relais 2 (uniquement pour le montage mural encastré/appliqué)	→ Section 4.4.8 [178] MF » E » ID » R2 » OK » Programmer avec succès l'empreinte utilisateur à cinq reprises

Fonctionnement	Déscription	Notice succincte
Régler la date et l'heure	→ Section 4.3.5 [171] MF » E » RT » YYYY » OK » MM » OK » DD » OK » HH » OK » MM »OK

Pour plus d'informations sur l'affectation des touches de l'appareil de programmation et l'explication des abréviations, voir la Section 4.1.4 [154].

4.4.2 Programmer l'empreinte utilisateur

	■ L'appareil est en état de service et la LED bleue s'allume **REMARQUE !** Les empreintes maîtres ne peuvent pas être programmées comme empreintes utilisateur.
	■ Passez l'empreinte maître sur le capteur ■ Les LED verte et rouge s'éclairent brièvement
	■ Pressez la touche « E » (Enroll) sur l'appareil de programmation ■ Saisissez un ID entre 1 et 35 à l'aide du clavier ■ Appuyez sur la touche « OK » pour confirmer
 	**Programmation** ■ Vous faites glisser le doigt que vous voulez utiliser comme empreinte utilisateur sur le capteur ■ La programmation est indiquée par un **bref allumage** de la **LED verte** ■ La programmation peut être poursuivi en faisant à nouveau glisser le même doigt sur le capteur

	■ Répétez la programmation jusqu'à ce que le doigt soit enregistré 5 fois avec succès ■ La réussite de programmation de l'empreinte utilisateur est signalée par **4 brefs allumages des LED verte et rouge** ■ L'état opérationnel est indiqué par la LED bleue en continu
REMARQUE ! Pour les empreintes « difficiles », il peut être nécessaire de programmer la même empreinte à plusieurs reprises. Si le nombre d'échecs est trop élevé, vous devriez utiliser un autre doigt comme empreinte utilisateur.	

Le nombre d'empreintes utilisateur est limité à 35 empreintes digitales en raison des capacités de l'espace mémoire pour les empreintes maître et utilisateur.

4.4.3 Effacer les empreintes utilisateurs individuelles

	■ Passez un empreinte maître sur le capteur ■ Les LED verte et rouge s'éclairent brièvement
	■ Pressez la touche « D » (Delete) de l'appareil de programmation. La LED verte s'allume ■ Entrée l'ID de l'empreinte utilisateur à effacer ■ Confirmez avec la touche « OK », la LED verte s'allume L'empreinte utilisateur enregistrée sous l'ID saisi est maintenant supprimée et sera rejetée à l'occasion d'une tentative d'ouverture de la porte.

4.4.4 Bloquer ID

	■ Passez l'empreinte maître sur le capteur ■ Les LED verte et rouge s'éclairent brièvement
	■ Pressez la touche « R1 (B) » ■ Entrer ID ■ Confirmer avec touche « OK » L'empreinte utilisateur enregistrée sous l'ID saisi est maintenant bloquée et sera rejetée à l'occasion d'une tentative d'ouverture de la porte.

REMARQUE

Certaines ID peuvent être bloquées provisoirement sans que l'empreinte digitale programmée ne soit supprimée. L'ID peut être débloqué ultérieurement sans nécessité de reprogrammer l'empreinte.

4.4.5 Débloquer ID

	■ Passez l'empreinte maître sur le capteur ■ Les LED verte et rouge s'éclairent brièvement
	■ Presser la touche « R2 (UB) » ■ Entrer ID ■ Confirmer avec touche « OK » L'empreinte utilisateur enregistrée sous l'ID saisi est à nouveau libérée et peut ouvrir la porte.

4.4.6 Contrôler ID

	■ Pressez la touche « OK » ■ Saisissez le numéro de l'ID à vérifier ■ Appuyez à nouveau sur la touche « OK » ■ Si un ID a déjà été attribué, les LED verte et rouge s'allument ■ Si l'ID n'a pas été attribuée, seule la LED rouge s'allume

4.4.7 Régler le temps de commutation par relais (uniquement pour variante appliquée/encastrée)

En « Mode d'administration par liste », la durée d'activation de chaque relais est déterminée séparément.

	■ Passez un empreinte maître sur le capteur ■ Les LED verte et rouge s'éclairent brièvement
	■ Presser la touche « R » de l'appareil de programmation ■ Sélectionner le relais avec la touche « R1 » ou « R2 » ■ Saisissez au clavier un temps de commutation en secondes de 1 à 60 ■ Confirmez avec la touche « OK », la LED verte s'allume

4.4.8 Programmer l'empreinte utilisateur pour relais 1/2 (uniquement pour variante appliquée/encastrée)

Avec la variante en applique/encastré, les deux relais peuvent être activés séparément l'un de l'autre.

	■ Passez l'empreinte maître sur le capteur ■ Les LED verte et rouge s'éclairent brièvement
	■ Pressez la touche « E » (Enroll) sur l'appareil de programmation ■ Saisissez un ID entre 1 et 35 à l'aide du clavier ■ Sélectionnez le relais avec la touche « R1 » ou « R2 » ■ Appuyez sur la touche « OK » pour confirmer
 	**Programmation** ■ Vous faites glisser le doigt que vous voulez utiliser comme empreinte utilisateur sur le capteur ■ La programmation est indiquée par un **bref allumage** de la **LED verte** ■ La programmation peut être poursuivi en faisant à nouveau glisser le même doigt sur le capteur
	■ Répétez la programmation jusqu'à ce que le doigt soit enregistré 5 fois avec succès ■ La réussite de programmation de l'empreinte utilisateur est signalée par **4 brefs allumages des LED verte et rouge** ■ L'état opérationnel est indiqué par la LED bleue en continu

4.4.9 Attribuer ID à une personne

ID	Nom de la personne	Désignation de l'empreinte (pouce, index,...)

5. Utilisation du clavier à code

Une mise en service doit être effectuée avant l'installation et l'utilisation du système d'accès. Procédez par étapes.

- Montez le clavier à code comme décrit au Chapitre 3.
- Effectuez les raccordements électriques conformément au schéma de câblage.

- La première mise sous tension établit la connexion (appairage).

À la livraison, toutes les LED (verte, rouge et bleue (le cas échéant)) sont allumées en permanence. Les entrées sont saisies directement au moyen du clavier à code. Un appareil de programmation n'est pas nécessaire et pas compris dans la livraison.

	Ouvrir la porte
*	Début ou confirmation de la saisie
Code maître	Code d'administration
Code utilisateur	Code pour l'ouverture de porte

REMARQUE

Chaque pression d'une touche est indiquée visuellement par un bref allumage de la LED verte. Répétez la saisie si, après avoir appuyé sur une touche, le voyant vert ne s'allume pas.

Les combinaisons de chiffres pour le code maître ou le code utilisateur doivent être des combinaisons de 4 à 6 chiffres. Certaines combinaisons de codes maître ou utilisateur sont exclues pour des raisons de sécurité. Il s'agit notamment de combinaisons de chiffres comme 8888, 123456, 4321, etc. Le code maître initial (code usine) se trouve à la page 128.

Lorsqu'un code utilisateur erroné est entré à cinq reprises consécutives, l'appareil commute sur le mode de blocage. Ceci empêche des personnes non autorisées de parvenir à se frayer librement un accès.

Lorsque l'appareil est en mode de blocage, cet état est indiqué par le clignotement de la LED rouge. Le mode de blocage est tout d'abord limité dans le temps. Après cinq autres tentatives infructueuses, la période de

blocage est à chaque fois prolongée (intervalle de blocage : 1 minute, 5 minutes, 30 minutes, 1 heure, puis blocage permanent).

Si un code d'utilisateur valide est entré à deux reprises consécutives, le mode de blocage est supprimé.

5.1 Mode test

À la livraison, il est possible de tester l'ouverture de la porte. Entrez la suite de touches 0 » 🔑. La LED verte s'allume.

	
0	🔑

5.2 Modifier le code maître

REMARQUE **Pour raisons de sécurité, nous recommandons de remplacer le code usine par votre propre code maître !**

				
*	Code maître	*	1	*

			
Nouveau code maître	*	Nouveau code maître	*

5.3 Déterminer/modifier code utilisateur

				
*	Code maître	*	2	*

					
ID utilisateur [1...150]	*	Code utilisateur	*	Code utilisateur	*

REMARQUE

Avec la variante appliquée/encastrée, les deux relais peuvent être activés séparément l'un de l'autre. Un identifiant utilisateur impair active le relais 1, un identifiant pair active le relais 2.

5.4 Ouvrir la porte

	
Code utilisateur	

REMARQUE

Si des chiffres supplémentaires sont saisis avant le code utilisateur, ceux-ci seront ignorés.

5.5 Effacer code utilisateur

				
*	Code maître	*	3	*

	
ID utilisateur	*

Alternative :

				
*	Code maître	*	3	*

			
0	*	Code utilisateur	*

REMARQUE

Une procédure de reset d'appairage remet le clavier à code à la configuration d'usine. Tous les codes utilisateurs sont alors effacés.
Après la réinitialisation, le code maître modifié sera remplacé par le code usine !

5.7 Régler le temps de commutation des relais (uniquement pour variante appliquée/encastrée)

				
*	Code maître	*	4	*

			
Relais [1|2]	*	Temps [1...60 s]	*

5.6 Effacer tous les codes utilisateurs et le code maître

				
*	Code maître	*	0	*

	
Code maître	*

6. Entretien et maintenance

- La disponibilité opérationnelle doit être régulièrement contrôlée.
- Remplacez un produit défectueux par un nouveau.

La surface du capteur du lecteur d'empreintes digitales s'auto nettoie grâce à son utilisation répétitive (scan des empreintes). Si le lecteur d'empreintes digitales se salit malgré tout, nettoyez-le avec des cotons-tiges, des microfibres ou des chiffons pour lunettes. Tous les matériaux comme le coton, les sopalins, les éponges de cuisine et les torchons pour essuyer la vaisselle ne conviennent pas. Utilisez de l'eau claire sans addition de produit nettoyant. Procédez avec précaution dans la zone de la surface du capteur.

Nettoyez le clavier à code par mesure de précaution avec un chiffon légèrement humide et non abrasif pour éliminer les marques de doigt et les impuretés. A cet effet, n'utilisez que de l'eau claire sans addition de produit nettoyant.

Variante montage dans la porte :
en cas d'utilisation fréquente, entretenez les contacts du SECURE*connect* 200 à l'aide de la graisse de contact B-55606-00-4-0.

La disponibilité opérationnelle du système de fermeture doit être régulièrement contrôlée. Pour ce faire, il convient de vérifier les points de fixation et de resserrer les vis, si nécessaire. Les caractéristiques mécaniques de la serrure (l'actionnement par clé ou par béquille / pêne demi-tour/dormant) ne doivent pas être altérées par un éventuel encrassement et les composants correspondants doivent faire l'objet d'un entretien à intervalles réguliers.

Le mécanisme de la serrure est lubrifié pour toute sa durée de vie et ne demande donc pas de maintenance. Graissez légèrement le pêne demi-tour/dormant une fois par an au minimum. N'utilisez pas de l'huile pour ne pas endommager l'électronique de la serrure !

7. Défauts et solutions

Description des erreurs	Cause	Solution
La LED rouge clignote en continu plusieurs fois par seconde	Pas de connexion bus à l'unité de commande	Vérifiez le câblage ou mettez l'appareil en service
	Pas d'appairage ou appairage défaillant	Effectuez une réinitialisation de l'appairage
Les LED verte et rouge clignotent en permanence	Erreur dans le câblage de bus RS-485	Vérifiez les bornes de raccordement et, le cas échéant, raccorder correctement les connexions
La LED rouge clignote en continu toutes les deux secondes	Mode de blocage : le système se bloque au bout de plusieurs tentatives d'identification invalides	Scanner une empreinte autorisée
La LED verte s'allume en cas de tentative d'accès mais la porte ne s'ouvre pas	Problème de connexion entre SC200R et SC200F	Nettoyez les contacts du SC200
		Vérifiez la position de montage du SC200
	Problème de connexion - entre l'unité intérieure et l'unité extérieure - entre le relais et le composant raccordé, par ex. gâche électrique	Contrôlez le câblage
		Coupez la tension d'alimentation et la remettre en marche
		Remplacez le matériel défectueux
La LED rouge s'allume en permanence	Matériel défectueux	Remplacement du lecteur d'empreintes digitales ou du clavier à code nécessaire

8. Entretien et pièces de rechange

En fonction de l'utilisation et de la situation de montage, nous recommandons une inspection, un entretien et un nettoyage réguliers. Éliminez immédiatement les défaillances et les défauts.

⚠ DANGER

Danger de mort par électrocution !

Coupez l'alimentation électrique et déchargez les énergies résiduelles accumulées.

Les travaux de maintenance ne peuvent être effectués que par un personnel spécialisé autorisé et formé par le fabricant.

En cas de problème, nous recommandons de contacter le service après-vente du groupe d'entreprises Gretsch-Unitas avant une réparation sur place et, si nécessaire et après accord, de renvoyer le produit.

Démontez le produit hors de sa mortaise. Pour le démontage, desserrez les fixations, détachez les branchements électriques et extrayez le produit.

Si des pièces de rechange ou des extensions sont requises, seules des pièces d'origine du fabricant peuvent être utilisées. En cas d'utilisation de composants tiers, le fabricant décline toute garantie, toute responsabilité ou tout droit aux prestations.

9. Mise au rebut

REMARQUE

Les déchets ne doivent pas être éliminés avec les ordures ménagères. Conformément aux lois et directives nationales et locales, l'élimination correcte des déchets doit être effectuée selon le processus de recyclage applicable.

En tant que rebut électronique, le produit doit être remis aux points de collecte publics et/ou aux déchetteries de tri sélectif. L'emballage doit être éliminé séparément.

Índice de contenido

Su código de fábrica:

También hay un adhesivo con el código de fábrica en el lado posterior del dispositivo de programación. Si ha asignado un código maestro propio, debe utilizar este.

¡Entregue este documento al usuario!

1. Informaciones e instrucciones de seguridad

1.1 Indicaciones generales sobre el manual

Gracias por haber escogido el lector de huella digital y el teclado de código como sistema de control de acceso para los dispositivos de salida motorizados o electromecánicos.

Este manual de instrucciones incluye notas importantes y contribuye a evitar peligros, costes de reparación y tiempos de inactividad, además de aumentar la fiabilidad y la vida útil.

Todos los usuarios deben leer y aplicar el manual de instrucciones **antes** del uso del producto. Tenga especialmente en cuenta las instrucciones para:

- Montaje e instalación eléctrica
- Puesta en servicio, funcionamiento y mantenimiento

Una vez finalizado el montaje, hay que entregar el manual de instrucciones al titular/cliente. Por favor, lea atentamente este manual antes de usar nuestro producto y consérvelo para posteriores usos. Indique a todos los titulares/clientes que deben leer el manual de instrucciones.

1.2 Instrucciones de seguridad

Este manual de instrucciones está dirigido al personal técnico especializado con conocimientos sobre la instalación de componentes electrónicos, componentes para puertas y herrajes. El manual ofrece indicaciones sobre el montaje, la puesta en marcha y el manejo de este producto.

Para evitar montajes erróneos y maniobras incorrectas, recuerde a los clientes y usuarios la necesidad de cumplir lo indicado en el presente manual.

- Se deben cumplir las correspondientes disposiciones, directivas y reglamentos localmente vigentes sobre montajes e instalaciones. Esto se aplica especialmente a las directivas y reglamentos VDE, por ejemplo, DIN VDE 0100 e IEC 60364.

- ¡No se acepta responsabilidad alguna en caso de utilización, montaje o instalación inadecuados o en el caso de no utilizarse repuestos originales!
- Es importante que solo el personal especializado (véase definición en EN 50110-1, DIN VDE 0105 o IEC 60364) se encargue de cualquier tipo de trabajo (planificación, transporte, montaje, instalación, puesta en marcha, mantenimiento, reparación, desmontaje) que se realice en los productos.
- Para ello, debe asegurarse de que dispone de los documentos para la colocación, puesta en marcha, manejo, mantenimiento y reparación del producto y de que se tengan en cuenta.
- Por motivos de seguridad y de homologación (CE) no se permite transformar ni modificar el producto por propia mano.
- Antes de realizar cualquier trabajo de montaje, reparación, mantenimiento o ajuste, deberá desconectar de la red todos los bloques de alimentación correspondientes y asegurarlos contra una reconexión involuntaria.
- ¡En el caso de producirse daños por la inobservancia de estas instrucciones, expirará cualquier derecho a garantía! ¡No se asume responsabilidad alguna por los daños derivados!

1.3 Símbolos de advertencia

⚠ PRECAUCIÓN	**PRECAUCIÓN indica una situación de peligro que, en caso de no evitarse, podría provocar lesiones.**
ATENCIÓN	**ATENCIÓN indica una situación que podría causar daños materiales.**
NOTA	**NOTA indica un enunciado puramente informativo.**

2. Descripción del producto

El lector de huella digital y el teclado de código son sistemas de control de acceso para la identificación mediante características biométricas o psíquicas. El lector de huella digital genera las características (puntos característicos) de las líneas de los dedos, las compara con la información biométrica almacenada en la huella dactilar de referencia. El teclado de código registra el código PIN tecleado y lo compara con el código PIN de referencia.

En caso de coincidencia de las características se abre la puerta mediante una transmisión encriptada a la unidad de control. El sistema sirve principalmente para la apertura de puertas para el hogar, puertas de apartamentos y puertas de garaje en el ámbito doméstico o el industrial.

2.1 Datos técnicos

Variante Acero inoxidable	B-55600-23-4-8 B-55600-20-4-8 	B-55600-23-1-8 B-55600-20-1-8 
Variante Nero	B-55600-23-4-9 sólo lector de huella digital	-
Versión	Encastrada en puerta	Montaje en pared
Fuente de alimentación	8 ... 24 V CC	8 ... 30 V CC
Potencia absorbida	Máx. 1 W	Máx. 3 W
Salida de relés	A través de SECURE*connect* 200	24 V CC | 5,0 A
Dimensiones	44 x 75 x 29 mm	80,5 x 80,5 x 30 mm (55 x 55 x 30 mm sin marco)
Memoria	35 huellas dactilares 1000 eventos en el protocolo de acceso 150 códigos PIN para el teclado para la introducción de código	

Plantilla	Tiempo de registro: aprox. 1 s Tiempo de identificación: aprox. aprox. 10 ms por comparación
Cuota de denegación errónea	Aprox. 0,5 %
Cuota de aceptación errónea	Mejor que 1 entre 1 millón (en la FRR, 0,5 %)
Reconocimiento del dedo	Consulta de las propiedades electromagnéticas capacitivas/conductivas del contacto con la piel al deslizar el dedo sobre el sensor CMOS.
Batería para dispositivo de programación	CR2025
Condiciones ambientales	+85 °C –20 °C ≤ 95 % 40 °C IP65 (parte frontal)
Certificaciones	Los certificados se pueden encontrar en nuestra página web www.g-u.com.

2.2 Uso previsto

Utilice el producto únicamente de acuerdo con la descripción del producto. El uso se limita a las funciones, los datos técnicos, las aplicaciones y las indicaciones descritas a continuación. Se permite el uso establecido dentro de los límites de uso descritos en estas instrucciones. El producto ha sido concebido para este uso y no está permitida cualquier otra aplicación.

El lector de huella digital y el teclado de código sirve exclusivamente para el control de acceso mediante características de identificación biométricas o un código PIN, junto a los diversos accesos al edificio en un sistema de cierre. La función principal es la identificación. Para abrir el punto de acceso, es necesario SECURY con el motor tipo A, SECURE*connect* 200, relé como unidad de control o una cerradura con acoplamiento eléctrico.

El fabricante no se responsabiliza de los daños que pudieran derivarse de cualquier modificación realizada en el producto o en las conexiones sin la expresa autorización del grupo de empresas Gretsch-Unitas.

2.3 Uso no previsto

No está permitida cualquier otra aplicación, por lo que el grupo de empresas Gretsch-Unitas no se haría responsable de los daños causados. El uso no previsto también incluye la inobservancia de las instrucciones de seguridad. Las transformaciones y modificaciones por cuenta propia en el producto no están permitidas.

El uso no previsto se refiere, especialmente, aunque no de forma exclusiva, al uso del producto en las condiciones descritas a continuación.

- Fallo en la polaridad de las conexiones.
- En el producto se han realizado modificaciones no autorizadas.
- Al operar en la versión encastrada en puerta con SECURE*connect*, los voltajes que superen los 24 V + 10 % CC no están permitidos y producen daños.

2.4 Funcionamiento

2.4.1 Funcionamiento del escáner de huella digital

El escáner de huella digital captura la imagen del dedo mediante un sensor lineal y la analiza. El resultado se compara con la información biométrica de la huella dactilar almacenada previamente como referencia. En caso de coincidencia, se envía la autorización, lo cual concede el acceso a través de la puerta. Por motivos de seguridad, en el lector de huella digital se utiliza un sensor lineal que elimina automáticamente el rastro de la huella y limpia la superficie del sensor cada vez que se desliza el dedo.

2.4.2 Funcionamiento del teclado de código

El teclado para la introducción de código compara la entrada en el teclado con el código de usuario que ha asignado como referencia. En caso de coincidencia, se envía la autorización, lo cual concede el acceso a través de la puerta.

2.5 Volumen de suministro, transporte y almacenamiento

Es necesario comprobar si el suministro está completo y si presenta daños. En caso de presentar daños, informe al distribuidor. Monte y ponga en funcionamiento únicamente los productos que se encuentren en perfecto estado.

La entrega se compone de los artículos/del documento siguientes:

- Sistema de control de acceso (lector de huella digital o teclado para la introducción de código)
- Dispositivo de programación (sólo para lector de huella digital)
- Cable del sistema para la unidad de control (solo en el dispositivo para el montaje en la puerta)
- Módulo de relé "Whitebox" (solo en el dispositivo con montaje en pared)
- Materiales de fijación
- Manual de instrucciones

Almacene el producto únicamente en el embalaje original y en las siguientes condiciones:

- Almacenar exclusivamente en un habitáculo seco, limpio y con ventilación suficiente, nunca al aire libre. Almacenar en un lugar sin movimientos ni vibraciones.
- Rango de temperatura de +15 °C a +40 °C, sin cambios bruscos en la temperatura
- Humedad del aire con una humedad relativa de 30 % a 70 %, sin condensación
- Inspeccionar periódicamente el estado general cuando se den periodos de almacenamiento prolongados

Transporte el producto únicamente en el embalaje original. Para el transporte, proteja el producto ante posibles caídas y use también una protección frente a la humedad. También hay que evitar los golpes fuertes.

2.6 Accesorios

- Marco de montaje de recambio en superficie/empotrable B-55606-00-0-1 2
- Panel frontal de acero inoxidable con logotipo BKS B-55606-00-1-1 3
- Panel frontal de acero inoxidable con logotipo BKS negro B-55606-00-7-1 3
- Panel frontal de acero inoxidable sin logotipo BKS B-55606-00-2-1 4

3. Montaje

El lector de huella digital o el teclado de código se monta por lo general en la zona exterior (lado exterior de la puerta). Según la versión, se monta en la puerta o en la pared. Se utiliza una línea de datos para establecer la conexión con el control del punto de acceso (SECURE*connect*/cerradura con acoplamiento eléctrico o caja de relés "Whitebox"). Utilice los cables del sistema BKS para establecer la conexión.

ATENCIÓN

Durante la instalación y el tendido de cables se deben respetar los reglamentos y las normas sobre tensión MBTS. En los extremos de los cables deben colocarse punteras de cable.

ATENCIÓN

¡No dañe las superficies visibles del lugar de instalación durante el montaje! ¡Montar/desmotar con cuidado el elemento decorativo!

NOTA

¡Para garantizar un funcionamiento correcto, debe mantenerse una altura de montaje de 1,2 a 1,4 m por encima del borde superior del nivel suelo acabado (NSA)!

- Utilice los materiales de fijación suministrados.
- Apriete los tornillos de fijación con un destornillador hasta que el lector de huella digital y el teclado para la introducción de código esté fijo. Tenga cuidado de no apretar demasiado, ya que la caja podría dañarse.
- Le recomendamos que no coloque el elemento decorativo hasta que se haya completado el montaje y se haya realizado una prueba de funcionamiento satisfactoria.

NOTA

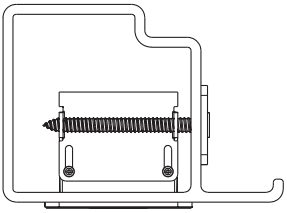
Una vez finalizado el montaje y conectada la fuente de alimentación, los LED del lector de huella digital/teclado de código se iluminan de forma constante en verde, rojo y azul cuando los dispositivos están en estado de suministro. Es decir, si no se ha programado ningún dedo de usuario o maestro o código PIN y la conexión se ha realizado correctamente.

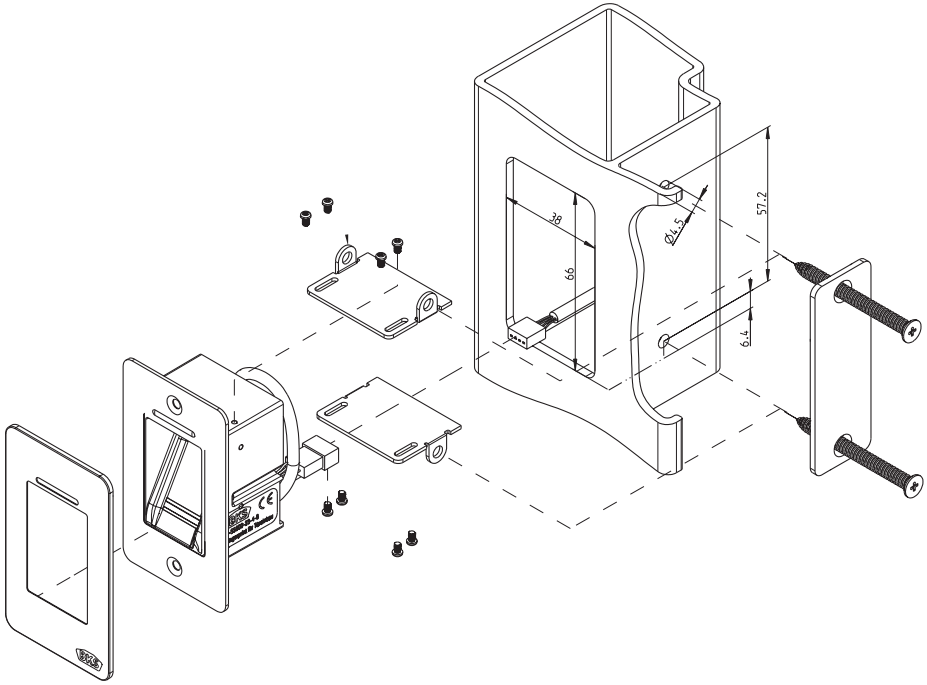
3.1 Encastrada en puerta – B-55600-23-4-8 | B-55600-20-4-8 | B-55600-23-4-9

Esta variante del lector de huella digital o del teclado para la introducción de código está pensada para su montaje en puertas como control de acceso. Para simplificar, las ilustraciones muestran el montaje del lector de huella digital. El montaje del teclado para la introducción de código no difiere.

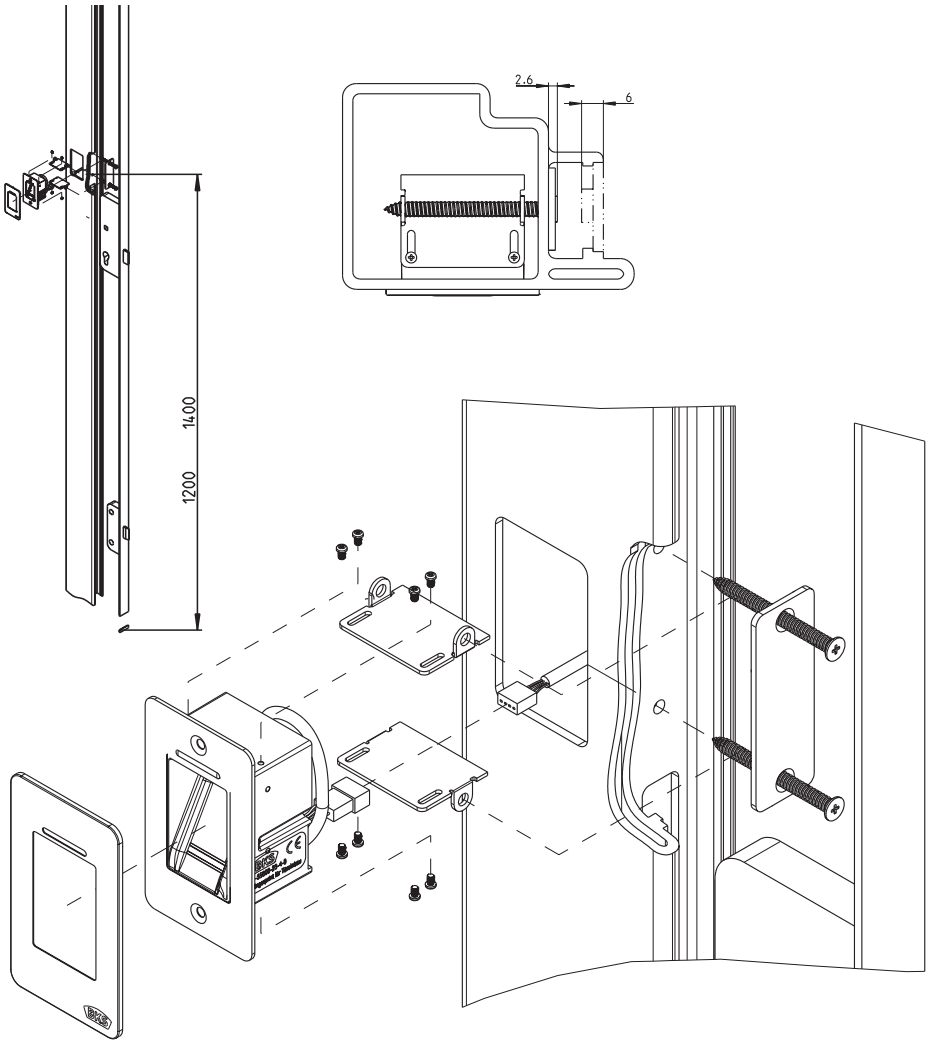
3.1.1 Montaje en puertas de madera/acero

3.1.2 Montaje en puertas de aluminio/PVC

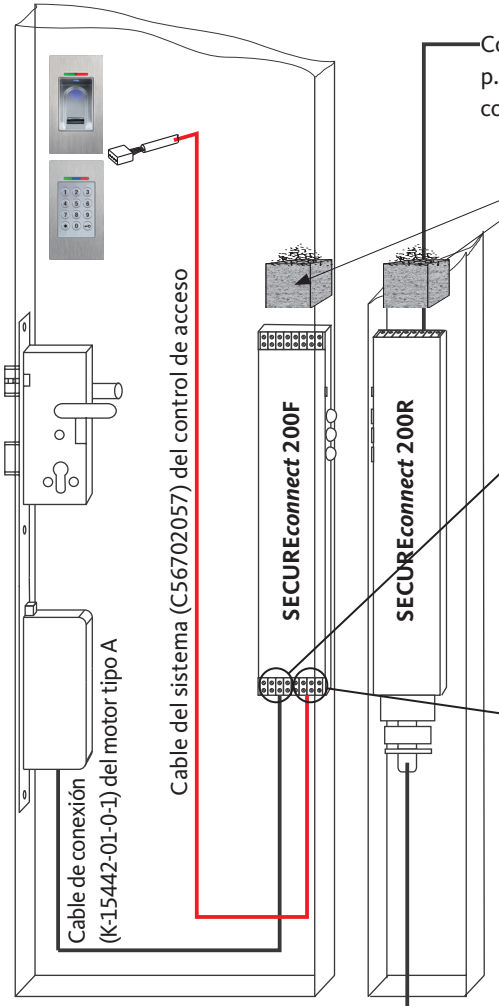




3.1.3 Montaje con SECURY (motor tipo A)



3.1.4 Esquema de conexión del motor tipo A



Contacto de acceso **sin potencial**, p. ej., botón pulsador, interfono, control de acceso, interruptor temporizador.

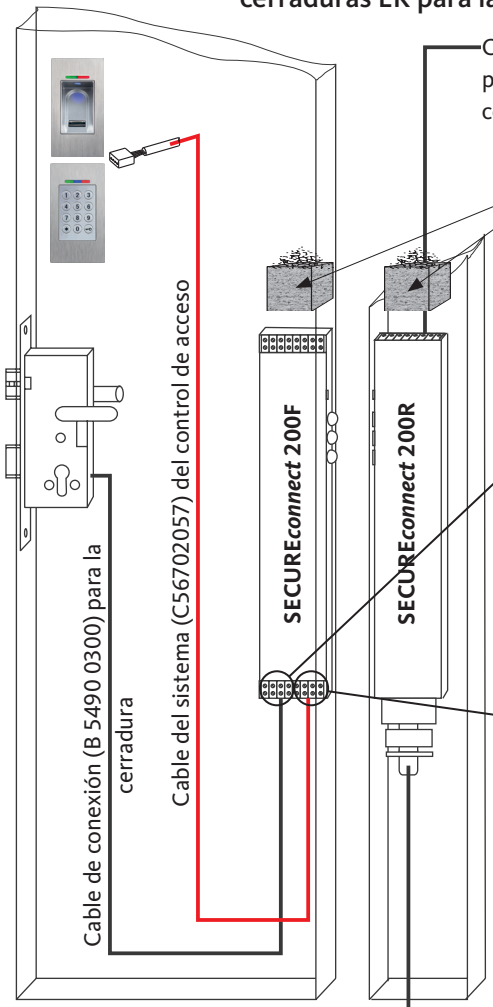
Utilice las esponjas adjuntas como protección contra virutas al realizar el montaje en perfiles metálicos.

SC 200F	Cable de conexión del motor tipo A	
Borne	Color del hilo	Señal
GS	GY | Gris	GND (negativo)
VS	BN | Marrón	+ 24 V (positivo)
90	BK | Negro	Conductor de control

SC 200F	Cable del sistema – sistema de control de acceso	
Borne	Color del hilo	Señal
GS	YE | Amarillo	GND (negativo)
96	WH | Blanco	RS-485 A
95	GN | Verde	RS-485 B
94	BN | Marrón	+ 24 V (positivo)

En puertas de metal y de PVC, usar la protección de cables incluida para la salida del cable.

3.1.5 Esquema de conexión de los bloqueos del motor y las cerraduras EK para las conexiones sin potencial

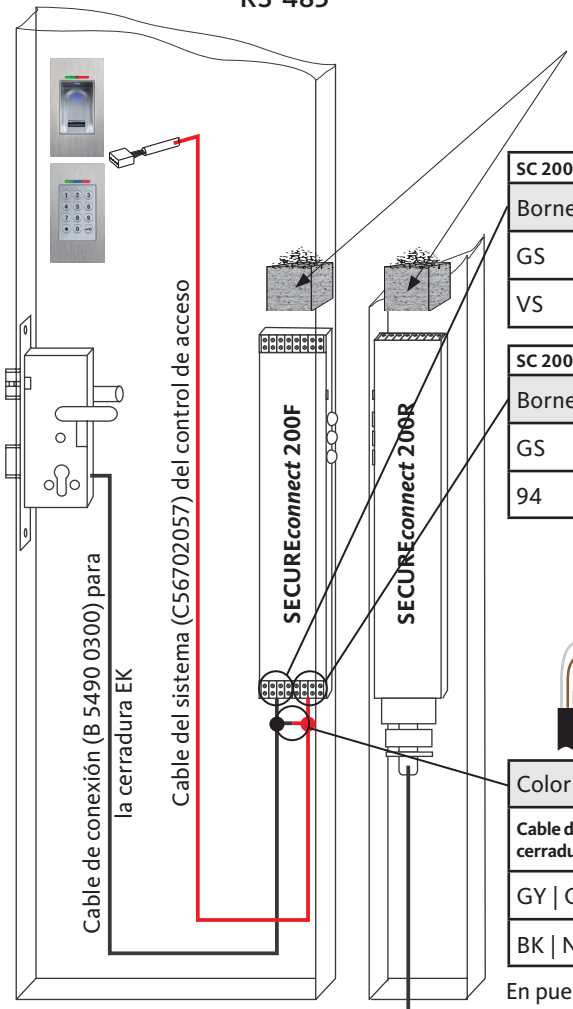


SC 200F	Cable de conexión – cerradura	
Borne	Color del hilo	Señal
GS	WH | Blanco	GND (negativo)
VS	BN | Marrón	+ 24 V (positivo)
90	PK | Rosa	Conductor de control

SC 200F	Cable del sistema – sistema de control de acceso	
Borne	Color del hilo	Señal
GS	YE | Amarillo	GND (negativo)
96	WH | Blanco	RS-485 A
95	GN | Verde	RS-485 B
94	BN | Marrón	+ 24 V (positivo)

En puertas de metal y de PVC, usar la protección de cables incluida para la salida del cable.

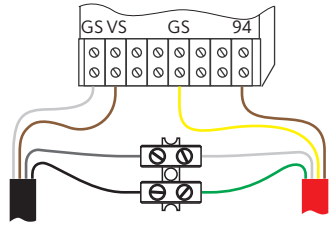
3.1.6 Esquema de conexión de la cerradura EK para el bus RS-485



Utilice las esponjas adjuntas como protección contra virutas al realizar el montaje en perfiles metálicos.

SC 200F	Cable de conexión de la cerradura EK	
Borne	Color del hilo	Señal
GS	WH | Blanco	GND (negativo)
VS	BN | Marrón	+ 24 V (positivo)

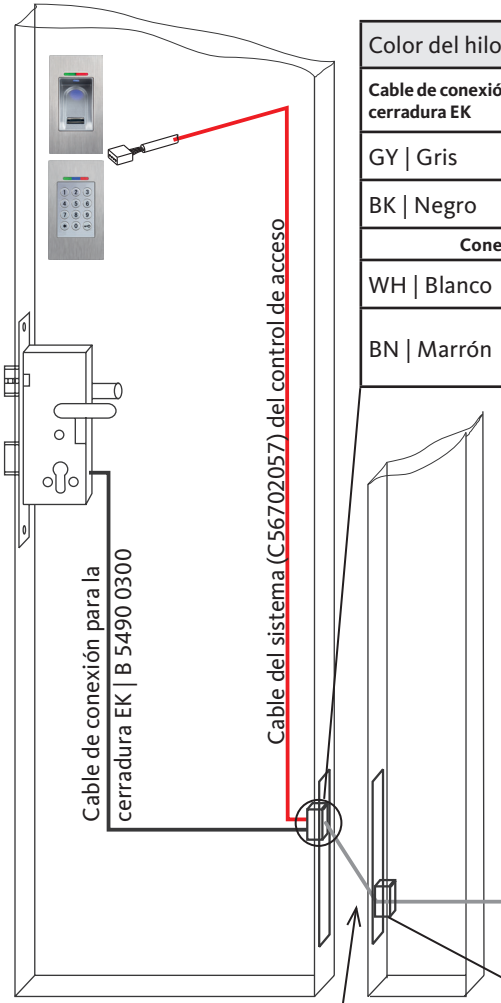
SC 200F	Cable del sistema – sistema de control de acceso	
Borne	Color del hilo	Señal
GS	YE | Amarillo	GND (negativo)
94	BN | Marrón	+ 24 V (positivo)



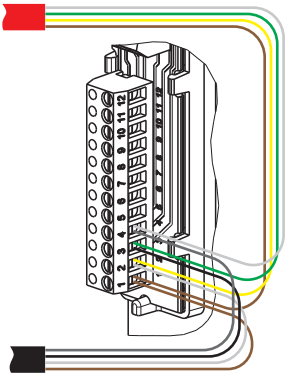
Color del hilo		Señal
Cable de conexión cerradura EK	**Cable del sistema – sistema de control de acceso**	
GY | Gris	WH | Blanco	RS-485 A
BK | Negro	GN | Verde	RS-485 B

En puertas de metal y de PVC, usar la protección de cables incluida para la salida del cable.

3.1.6.1 Conexión a la fuente de alimentación externa



Color del hilo		N.°	Señal
Cable de conexión cerradura EK	**Cable del sistema – sistema de control de acceso**	**Pasacables**	
GY | Gris	WH | Blanco	4	RS-485 A
BK | Negro	GN | Verde	3	RS-485 B
Conexión a la fuente de alimentación externa			
WH | Blanco	YE | Amarillo	2	GND (negativo)
BN | Marrón	BN | Marrón	1	+12 V – 24 V CC



Bloque de alimentación B 5570 0402

Pasacables	Bloque de alimentación
1	24 V CC
2	GND (negativo)

3.1.7 Protección contra la manipulación con SECURE*connect* 200

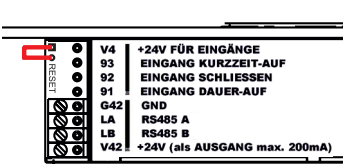
En la variante encastrada en puerta, su sistema consta de 2 aparatos electrónicos

- Control de acceso: lector de huella digital o teclado para la introducción de código
- Unidad de control: SECURE*connect* 200

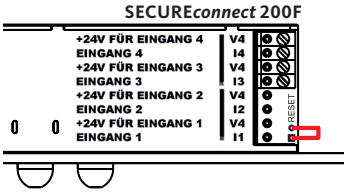
El sistema de control de acceso (lector de huella digital o el teclado de código) se monta por lo general en la zona exterior (lado exterior de la puerta). Para prevenir una manipulación ilícita, su sistema cuenta con numerosas funciones de seguridad que evitan accesos no autorizados:

- El sistema de control de acceso está conectada a la unidad de control a través de una línea de datos. La transmisión de datos está codificada.
- El sistema de control de acceso y la unidad de control se acoplan de forma unívoca (emparejamiento) durante la primera puesta en marcha.

Para cambiar un componente (SECURE*connect* 200R, SECURE*connect* 200F o sistema de control de acceso) del sistema de la puerta, es necesario realizar un procedimiento de reemparejamiento en ambas partes de SECURE*connect* 200. Para ello, en la placa del SECURE*connect* 200F o del SECURE*connect* 200R, se debe cerrar el contacto de reset con suministro eléctrico conectado durante un mínimo de 3 segundos. Utilice por ejemplo una pinza de cocodrilo para hacerlo.



SECURE*connect* 200R



Después puede retirarse la pinza. SECURE*connect* 200R, SECURE*connect* 200F y el control de acceso se someten ahora a un nuevo proceso de emparejamiento. El sistema de control de acceso se restablece con ello a la configuración de fábrica (se borran todas las huellas dactilares y códigos PIN guardados).

Si un control de acceso está conectado a un SECURE*connect* 200 emparejado, debe realizarse un reemparejamiento. Se genera una nueva clave del sistema y se borran las huellas digitales o los códigos PIN.

3.1.8 Emparejamiento del escáner de huella digital/ teclado de código con cerradura EK

La conexión directa al lector de huella digital o al teclado para la introducción de código es posible con las cerraduras con acoplamiento eléctrico (cerradura EK) de las series EK19 y EK21 en la versión con cable. El control de acceso y la cerradura con acoplamiento eléctrico se acoplan automáticamente de forma unívoca (emparejamiento) durante la primera puesta en servicio mediante la interfaz RS-485 en una conexión bus.

Para cambiar un componente (lector de huella digital, teclado para la introducción de código o cerradura) del sistema de la puerta tras la conexión, es necesario realizar el reemparejamiento antes de volver a conectar los componentes. El reemparejamiento se realiza con una secuencia determinada en la cerradura con acoplamiento eléctrico.

Comience esta secuencia con el reinicio de la cerradura EK desconectando y volviendo a conectar el suministro de corriente. Transcurrido un minuto tras el reinicio, hay que dar los pasos siguientes:

- Mantenga accionada la manilla mientras activa el contacto de excéntrica.
- Mientras tanto, utilice la llave para girar rápidamente el cilindro de cierre en sentido horario y antihorario varias veces y active el contacto de excéntrica al menos 3 veces en 10 segundos.

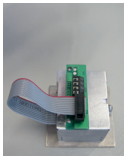
Una vez concluido el reemparejamiento, se eliminan todos los dispositivos emparejados y los componentes volver a «emparejarse» de nuevo.

3.2 Montaje en pared (empotrable/en superficie) – B-55600-23-1-8 | B-55600-20-1-8

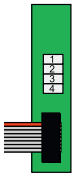
Esta variante del lector de huella digital o del teclado para la introducción de código está pensada para su montaje en la pared al lado de la puerta como control de acceso. Para simplificar, las ilustraciones muestran el montaje del lector de huella digital. El montaje del teclado para la introducción de código no difiere.

3.2.1 Montaje versión empotrada

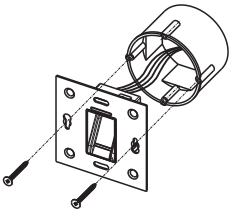
El montaje se efectúa en cajas empotrables. Le recomendamos una altura de montaje de 1,2 hasta 1,4 m desde el nivel de suelo acabado.



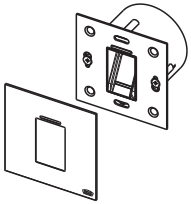
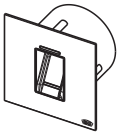
- Conecte el control de acceso con el módulo de relé.



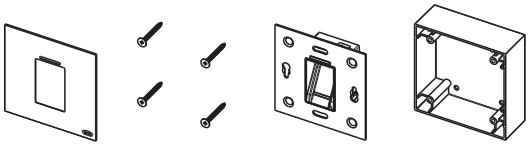
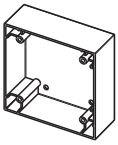
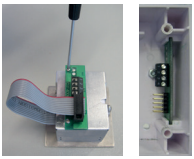
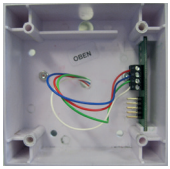
Conecte el cable de alimentación a la unidad interior correspondientemente en los bornes 1 a 4.

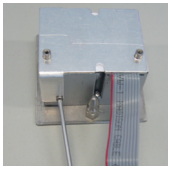
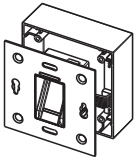
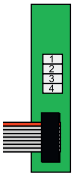
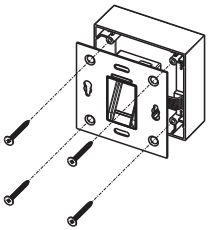
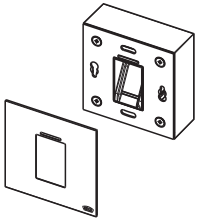
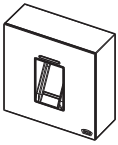


- Fije el marco de soporte del control de acceso en la caja empotrable con los 2 tornillos incluidos (3,5 x 25).

	■ Retire la lámina protectora de las tiras adhesivas en el envés del marco exterior de acero inoxidable. ■ Coloque el marco exterior sobre el marco de soporte del control de acceso.
	■ Compruebe el funcionamiento.

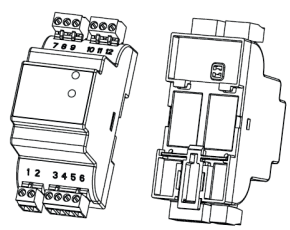
3.2.2 Montaje versión en superficie

	
	Fije la caja en superficie en la pared. Le recomendamos una altura de montaje de 1,2 hasta 1,4 m desde el nivel de suelo acabado. Puede utilizar los tornillos y tacos (3,5 x 25) incluidos.
	■ Retire la placa de conexión aflojando los dos tornillos. ■ Deslice la placa de conexión en la ranura a tal efecto de la caja en superficie.
	■ Conecte el cable al módulo de relé "Whitebox" correspondientemente en los bornes 1 a 4.

	■ Retire la parte posterior de la caja. ¡**NOTA!** Si la parte posterior de la caja está montada, el sistema de control de acceso no cabe en la caja en superficie.
	■ Inserte el cable de cinta plana del sistema de control de acceso en el placa de conexión.  La marca roja del cable de cinta plana debe dirigirse hacia los bornes de conexión.
	■ Fije el marco de soporte del control de acceso en la caja en superficie con los 4 tornillos (3,5 x 25).
	■ Retire la lámina protectora de las tiras adhesivas en el envés del marco exterior de acero inoxidable. ■ Coloque el marco exterior sobre el marco de soporte del control de acceso.
	■ Compruebe el funcionamiento.

3.2.3 Esquema de conexiones con el módulo de relé "Whitebox"

La unidad interior y la exterior se comunican a través de un bus codificado. Para conectar el módulo de relé "Whitebox" y el control de acceso le recomendamos un cable de telecomunicaciones J-Y(ST)Y 2x2x0.8.
El ejemplo de conexión es válido para el motor tipo A del grupo de empresas Gretsch-Unitas.



Fijación en el carril DIN simétrico

NOTA

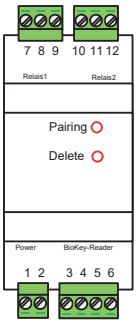
Para el montaje versión en superficie se debe introducir correctamente el cable de cinta plana (línea roja en dirección a los bornes).

3.2.4 Datos técnicos del módulo de relé "Whitebox"

Tensión de servicio:	8 a 30 V CC o 8 a 12 V CA
Potencia absorbida:	1 W, en picos de 3 W (más la potencia de los motores tipo A conectados)
Datos de relé:	24 V CA/CC 5,0 A
Espacio de montaje	En el interior para proteger el control del relé
Medidas del módulo de relé An x Al x Pr [mm]	86,4 x 44,9 x 52,6 (dimensiones sin bornes)

3.2.5 Protección contra la manipulación con el módulo de relé "Whitebox"

ATENCIÓN **¡El módulo de relé debe instalarse en la zona asegurada y no debe ser accesible desde el exterior!**



En el caso de los dispositivos empotrados o en superficie para el montaje en pared, el módulo de relé "Whitebox" y el control de acceso se emparejan entre sí de fábrica. Si se sustituye el hardware de un componente, es necesario cancelar dicho emparejamiento.

- Para iniciar el emparejamiento, pulse la tecla situada en el taladrado de la unidad interna etiquetado como "Whitebox" y marcado en rojo.

3.2.6 Restablecimiento con el módulo de relé "Whitebox"

En el caso de los dispositivos empotrados o en superficie para el montaje en pared, puede utilizar el módulo de relé para activar un restablecimiento de los ajustes de fábrica con la eliminación de todas las huellas dactilares, incluidos los dedos maestros o los códigos PIN.

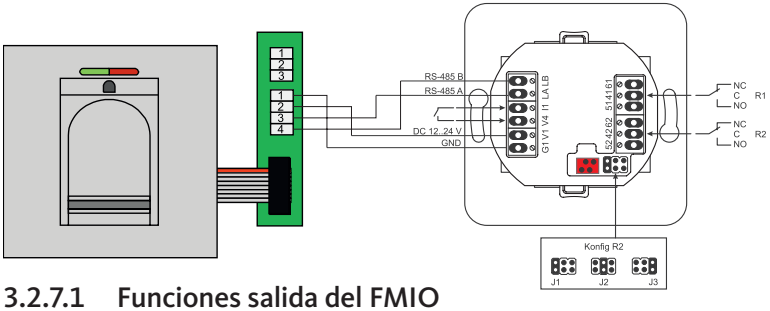
- Para iniciar el proceso de borrado, pulse la tecla situada en el taladrado del módulo de relé "Whitebox" etiquetado como "Delete" y marcado en rojo.

Tras el restablecimiento, los LED verde, rojo y azul se iluminan de forma constante en el control de acceso.

NOTA **¡Tras el restablecimiento, se restablecerá el código maestro modificado al código de fábrica!**

3.2.7 Conexión a un módulo de radio (FMIO)

El sistema de control de acceso puede comunicar directamente con un módulo de radio (FMIO) a través de un bus codificado.
Para conectar el módulo de pared radio I/O y el sistema de control de acceso le recomendamos un cable de telecomunicaciones J-Y(ST)Y 2x2x0.8.



3.2.7.1 Funciones salida del FMIO

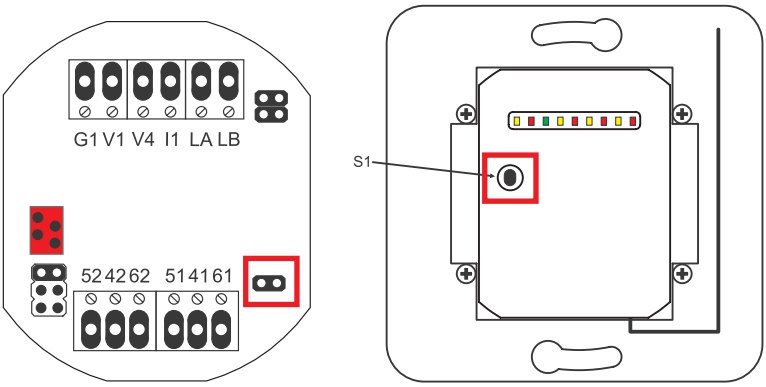
El relé "R1" del módulo de pared radio I/O se utiliza para la visualización de un acceso autorizado tras la conexión de un control de acceso a través de la interfaz RS-485. La salida de relés "R1“ no tiene más opciones de configuración. La salida óptica tiene lugar a través del LED "L7" situado en el frontal del módulo de pared radio I/O.

El relé "R2" ofrece la posibilidad de reflejar 3 señales diferentes. La señal se configura mediante la colocación de un puente (jumper) (véase la siguiente tabla). La salida óptica tiene lugar a través del LED "L2".

Salida	FMIO con cilindro/cerradura electrónica inalámbrica	FMIO con cilindro/cerradura electrónica inalámbrica y lector de huella digital/teclado de código
1	-	Acceso autorizado
2 + J1	-	Intento de acceso no autorizado
2 + J2	Acoplamiento activado (cilindro/ cerradura está acoplado/a)	-
2 + J3	Estado de la batería	Estado de la batería

3.2.7.2 Emparejamiento/reemparejamiento FMIO

Una vez se haya conectado un sistema de control de acceso al módulo de pared radio I/O, se produce el denominado emparejamiento. Ningún otro control de acceso puede ahora conectarse al mismo módulo de pared radio I/O. Si fuera necesario hacerlo, se debe restablecer el emparejamiento con el control de acceso.



Para ello debe abrirse la tapa de la caja.

- Separe el módulo del interfaz RS-485.
- Inserte el puente junto al borne "51 41 61".
- Pulsar el pulsador "S1" hasta que se produzca una señal acústica.

La información de emparejamiento se ha borrado.

Si es necesario restablecer un emparejamiento entre el cilindro/la cerradura inalámbrico/a con acoplamiento eléctrico y el módulo de pared radio I/O, el puente no debe estar insertado. En este caso, pulsando "S1" durante más tiempo se restablece la información de emparejamiento del cilindro/de la cerradura inalámbrico/a con acoplamiento eléctrico.

4. Manejo del lector de huella digital

Antes de configurar y utilizar el sistema de acceso, hay que llevar a cabo una puesta en marcha. Proceda paso a paso.

- Monte el lector de huella digital tal y como se describe en el capítulo 3.
- Realice las conexiones eléctricas de acuerdo con el esquema de conexiones.

- La primera vez que se enciende la tensión de red, se inicia la conexión (emparejamiento).

Existen tres modos de funcionamiento para operar y configurar el lector de huella digital. El dispositivo de programación puede utilizarse para cambiar el modo de gestión. **El modo de "gestión de Bluetooth" se activa en el estado de suministro.** Otros modos son "gestión normal" y "gestión de índice".

ATENCIÓN **La entrada no está asegurada y puede abrirse mientras el dedo maestro no se haya asignado.**

4.1 Instrucciones de funcionamiento

4.1.1 Cambio del modo de gestión

NOTA **Tras el restablecimiento, se perderá toda la información memorizada, solo se conserva el modo de gestión.**

El modo de funcionamiento solo puede conmutarse en el estado de suministro (todos los LED iluminados). Puede hacerlo restableciendo el lector de huella digital con DA ›› CODE ›› OK. El código está en la página 190 y en el dispositivo de programación.
Para cambiar el modo de gestión, mantenga el dispositivo de programación directamente frente al lector de huella digital (LED azul) y pulse las siguientes teclas.

	9 » 9 » OK » 5 » 0 » OK	Modo de gestión normal
	9 » 9 » OK » 5 » 1 » OK	Modo de gestión de índice
	9 » 9 » OK » 5 » 7 » OK	Modo de gestión de Bluetooth (estado de suministro)

Tras el cambio, el lector de huella digital pasa al estado de suministro (todos los LED iluminados).

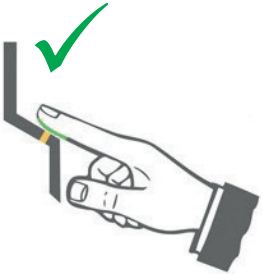
4.1.2 Colocación del dedo

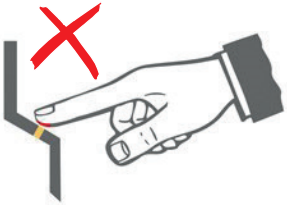
Proceda con mucho cuidado al asignar las huellas dactilares. Los dedos maestros y de usuario pueden ser rechazados si se cometen errores durante la asignación. Cuanto más cuidadosamente se programe un dedo, más fiable será su reconocimiento posterior durante la identificación.

NOTA **Antes de asignar los dedos maestros o de usuario, le recomendamos que se lave las manos una vez.**

- Deslice el dedo por la línea del sensor de forma rápida, uniforme y con una ligera presión utilizando la mayor parte posible de las líneas del dedo.

Al elegir los dedos, tenga en cuenta que el dedo índice es más adecuado en el caso de dedos estrechos.





4.1.3 Comportamiento en caso de apertura de puerta (sólo versión encastrada en puerta)

En las versiones B-55600-23-4-8 y B-55600-23-4-9 (lector de huella digital para la variante encastrada en puerta), el lector de huella digital se desconecta automáticamente si la puerta permanece abierta durante más de 12 s.

Las huellas digitales memorizadas para la apertura de puerta no se pierden en caso de corte de corriente. La fecha y la hora para el análisis de eventos deben volver a ajustarse tras un corte de corriente.

4.1.4 Dispositivo de programación, abreviaturas

Tecla	Significado	Explicación
DA	Delete All	Borrar todo, incl. dedo maestro
OK	OK	Ejecutar función
R1 » B	Relay 1 » Block	Relé 1 » Desbloquear ID de usuario
RT	Relay-Time	Tiempo de conmutación
R2 » UB	Relay 2 » Unblock	Relé 2 » Desbloquear ID de usuario
D	Delete	Borrar huella dactilar
E	Enroll	Registrar huella dactilar
TT	Time	Tiempo (segundos)

Abreviatura	Significado	Explicación
MF	Master Finger	Dedo maestro
CODE	PIN code	Código de usuario o maestro
ID	Index	ID de usuario
YYYY | MM | DD	Year | Month | Day	Año | Mes | Día
HH | MM | TT	Hour | Minute | Time	Hora | Minuto | Segundos (tiempo)

NOTA

Mantenga el dispositivo de programación directamente frente al diodo luminoso azul del lector de huella digital. Cuando se pulsen las teclas, se encenderá brevemente el LED verde a modo de confirmación visual. Si tras pulsar una tecla no se ilumina el LED, repita la pulsación.

4.2 Modo de gestión de Bluetooth

El modo de "gestión de Bluetooth" le permite configurar y gestionar el lector de huella digital con su smartphone y la app BKS BioKey. Tras la autorización en el lector de huella digital mediante el dedo maestro, puede llamar a la función deseada a través del menú de navegación de la aplicación BKS BioKey y realizar los ajustes necesarios para administrar su sistema.

El modo de "gestión de Bluetooth" está preconfigurado en el estado de suministro. Para cambiar a otro modo, siga las instrucciones del manual, en el capítulo 4.1.1 [214].

- En el modo de "gestión de Bluetooth", puede configurar el lector de huella digital mediante las siguientes funciones.

4.2.1 Modo de prueba

En el estado de suministro o tras el restablecimiento, es posible que se active la apertura de puerta para realizar una prueba con el dispositivo de programación sin necesidad de configurar previamente el lector de huella digital. El requisito es el estado de suministro.

Tenga en cuenta que mientras el lector de huella digital esté en estado de suministro, la entrada no está asegurada.

	■ Mantenga el dispositivo de programación directamente frente al LED azul del lector de huella digital ■ Pulse la tecla "0" en el dispositivo de programación ■ El LED verde se ilumina para el control visual cada vez que se pulsa una tecla ■ Pulsar la tecla "OK" para confirmar ■ La apertura de la puerta se activa

4.2.2 Asignar dedo maestro

Por motivos de seguridad, la autorización mediante el dedo maestro se comprueba antes de cada configuración del lector de huella digital. Por esta razón, se comienza la configuración asignando el dedo maestro y se determina quién podrá gestionar el sistema posteriormente.

NOTA

En el siguiente paso, comience a configurar el lector de huella digital asignando el primer dedo maestro sin abrir la aplicación (lector de huella digital en estado de suministro).

Al seleccionar el dedo, tenga en cuenta que un dedo maestro no puede utilizarse más que un dedo de usuario con el que se vaya a abrir la puerta. Por ello, se recomienda que, por ejemplo, como diestro, asigne el dedo índice izquierdo como dedo maestro y el derecho como dedo de usuario.

NOTA

Para asignar el dedo maestro, deslice el mismo dedo sobre el sensor 5 veces.

	■ Los LED verde, rojo y azul están iluminados permanentemente ■ El dispositivo se ha inicializado y está listo para la configuración **¡NOTA!** El requisito previo es que el lector de huella digital esté en estado de suministro o se haya reiniciado.

¡NOTA! Después de la programación de cada dedo (deslizando el dedo sobre el sensor), debe esperar aprox. 2 segundos hasta que se indique que el proceso ha finalizado mediante los LED verde y rojo iluminados de forma constante.
Solo entonces podrá continuar con la asignación y volver a deslizar el mismo dedo sobre el sensor.
No deje que transcurran más de 60 s entre cada proceso de asignación del dedo maestro, de lo contrario el proceso se interrumpirá.

<table>
<tr>
<td> 
 
  </td>
<td>Proceso de asignación
■ Deslice el dedo que desea utilizar como primer dedo maestro sobre el sensor
■ Los LED verde y rojo se apagan tras la lectura
■ Después de unos 2 segundos, los LED verde y rojo se iluminan de nuevo de forma permanente. El lector de huella digital está preparado
■ El siguiente proceso de asignación puede realizarse deslizando de nuevo el mismo dedo sobre el sensor
■ Repita el proceso de asignación hasta que el dedo haya sido asignado con éxito 5 veces</td>
</tr>
<tr>
<td>  </td>
<td>■ La asignación correcta del primer dedo maestro se indica con el LED verde que se enciende brevemente
■ Como consecuencia de los intentos fallidos que pueden producirse durante la asignación, por ejemplo, debido a una calidad insuficiente, el proceso de asignación debe repetirse hasta que el LED verde se encienda brevemente</td>
</tr>
<tr>
<td>  </td>
<td>■ Una vez asignado el primer dedo maestro, el dispositivo se encontrará en estado de funcionamiento
■ El LED azul se enciende permanentemente
■ Se puede continuar con la configuración</td>
</tr>
<tr>
<td colspan="2">¡NOTA! Si durante el proceso de asignación se deslizara un dedo sobre el sensor y no fuera aceptado como dedo maestro, los LED verde y rojo seguirían iluminándose. Se deberá repetir el proceso de asignación del dedo maestro.</td>
</tr>
</table>

Una vez asignado el primer dedo maestro, puede añadir posteriormente otros dedos maestros, véase el capítulo 4.2.6 [223] o 4.3.3 [232].

4.2.3 Configuración de la app BKS BioKey

La aplicación BKS BioKey está disponible para Apple iOS y Google Android. Descargue la aplicación BioKey desde la App Store o Google Play. Introduzca el término "BioKey" en el campo de búsqueda de la Store.

Available on the App Store

GET IT ON Google Play

NOTA

Los requisitos previos para la gestión de la app BKS BioKey son:
– la interfaz Bluetooth del smartphone está activa
– la app tiene permiso para acceder a la ubicación del smartphone
– se ha asignado el primer dedo maestro, véase el capítulo 4.2.2 [218]

- Asegúrese de que el lector de huella digital está dentro del alcance del Bluetooth de su smartphone.
- Inicie la app BKS BioKey en su smartphone.
- Pulse “Select device” (seleccionar dispositivo) en la cabecera de la pantalla.

La app BKS BioKey busca los dispositivos disponibles y abre una lista de los lectores de huella digital encontrados.

- Seleccione en la lista el lector de huella digital.
- Siga la indicación de identificación en el lector de huella digital.

	■ Deslizar el dedo maestro sobre el sensor ■ Los LED verde y rojo se iluminan brevemente una vez

El smartphone está conectado ahora para esta sesión y la configuración del escáner puede realizarse a través de la aplicación.

- Después de cada apertura de la app o si esta no se ha utilizado durante un minuto, se le pedirá que se identifique con el dedo maestro por motivos de seguridad.

4.2.4 Añadir usuario (app BKS BioKey)

- Inicie la app BKS BioKey en su smartphone.
- Siga la indicación de identificación en el lector de huella digital.

	■ Deslizar el dedo maestro sobre el sensor ■ Los LED verde y rojo se iluminan brevemente una vez

- Pulse el botón “Users” (usuarios).
- Pulse "+" **a la derecha de la cabecera** de la pantalla.
- Seleccione “Name” (nombre de usuario) e introdúzcalo.
- Pulse “Add finger...”(añadir dedo) en el área “Fingers” (dedos).
- Seleccione “Description” (descripción) y especifique allí qué dedo del usuario se debe leer.
- Asigne los derechos del nuevo dedo activando o desactivando el interruptor de los respectivos relés 1 y 2 en el área de “Permissions” (permisos). Relé 2 solo en el caso de montaje en pared en superficie/empotrada con función.
- Pulse “Enroll finger” (añadir dedo) en el área “Actions” (acciones).

	■ Siga las indicaciones del cuadro de diálogo de la app BKS BioKey ■ Deslice el dedo que se debe crear como dedo de usuario sobre el sensor ■ Repita el proceso de asignación hasta que el dedo haya sido asignado con éxito 5 veces ■ El contador de la app le muestra el progreso o cuántas veces tiene que escanear el dedo todavía Tenga en cuenta que un dedo que se ha asignado como dedo maestro no puede ser utilizado como dedo de usuario.

- Si el dedo se memoriza correctamente, se muestra una ID y el número de escaneos.

Solo se puede crear una huella digital por usuario. El número de dedos de usuario está limitado a 35 huellas dactilares debido al límite de espacio de memoria.

- Vaya a los menús de nivel superior a través de "<- atrás" y "<". En ellos aparece el nuevo dedo o usuario.

4.2.5 Editar o eliminar usuarios (app BKS BioKey)

- Inicie la app BKS BioKey en su smartphone.
- Siga la indicación de identificación en el lector de huella digital.

	■ Deslizar el dedo maestro sobre el sensor ■ Los LED verde y rojo se iluminan brevemente una vez

- Pulse el botón “Users” (usuarios).
- Seleccione un usuario en la lista de “Users” (usuarios) para editarlo en los siguientes pasos.
- Seleccione “Name” (nombre de usuario) en el área "General" y modifíquelo o corríjalo.
- Para editar o añadir más dedos maestros o de usuario, seleccione los campos de entrada correspondientes en el área “Fingers” (dedo) y edítelos.

Siga las instrucciones para asignar un nuevo dedo de usuario en el capítulo 4.2.4 [221].

- Active o desactive el interruptor “Block user” (bloquear usuario) en el área “Actions” (acciones) para bloquear o desbloquear el usuario.
- Seleccione “Delete user...”(borrar usuario) en el área de “Actions” (acciones) y confirme la eliminación.

4.2.6 Añadir dedo maestro (app BKS BioKey)

- Inicie la app BKS BioKey en su smartphone.
- Siga la indicación de identificación en el lector de huella digital.

	■ Deslizar el dedo maestro sobre el sensor ■ Los LED verde y rojo se iluminan brevemente una vez

- Pulse el botón “Users” (usuarios).
- Pulse "+" **a la derecha de la cabecera** de la pantalla.
- Seleccione “Name” (nombre de usuario) e introdúzcalo.
- Active el interruptor de “Master user” (usuario maestro).
- Pulse “Add finger...” (añadir dedo) en el área “Fingers” (dedos).
- Pulse “Enroll finger...”(asignar dedo).

	■ Siga las indicaciones del cuadro de diálogo de la app BKS BioKey ■ Deslice el dedo que se debe crear como dedo maestro sobre el sensor ■ Repita el proceso de asignación hasta que el dedo haya sido asignado con éxito 5 veces ■ El contador de la app le muestra el progreso o cuántas veces tiene que escanear el dedo todavía Tenga en cuenta que un dedo que se ha asignado como dedo maestro no puede ser utilizado como dedo de usuario.

4.2.7 Identificación con el dedo de usuario, abrir la puerta

	■ El dispositivo se encuentra en estado de funcionamiento ■ El LED azul se ilumina
	■ Deslizar el dedo de usuario sobre el sensor ■ Si se reconoce el dedo, el LED verde se ilumina y la puerta se abre En el modo de gestión normal, el relé 1 siempre está conmutado en la versión en superficie/empotrada (montaje en pared).
	■ Si el lector de huella digital no reconoce el dedo de usuario, el LED rojo se enciende y la puerta no se abre

4.2.8 Modo de bloqueo

	**Bloqueo** ■ Si se desliza 10 veces consecutivas sobre el sensor un dedo no asignado (LED rojo se ilumina), el dispositivo cambiará a un modo de bloqueo. De este modo se impide el libre acceso a personas no autorizadas En el modo de bloqueo, no se produce ninguna reacción a ningún dedo o entrada del dispositivo de programación. El tiempo de bloqueo es de 1 minuto. El LED rojo parpadea en el tiempo de bloqueo.
	**Desbloqueo** ■ El modo de bloqueo se puede detener antes si se desliza un dedo asignado (dedo maestro o de usuario) sobre el sensor A continuación, la puerta puede abrirse con un dedo de usuario como habitualmente

4.2.9 Restablecer, borrar todos los dedos de usuario y maestros

NOTA

Cierre la app BKS BioKey en su smartphone antes de reiniciar.

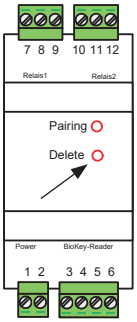
Mantenga el dispositivo de programación directamente frente al diodo luminoso azul del lector de huella digital.

- Pulse la tecla "DA" ("Delete all") en el dispositivo de programación (el LED verde se ilumina al pulsar la tecla)
- Introduzca el código de fábrica de la página 190 o el código maestro con el dispositivo de programación
- Para finalizar el proceso de borrado, pulse la tecla "OK"
- El dispositivo se ha iniciado, los LED verde, rojo y azul están iluminados permanentemente

NOTA

El lector de huella digital también se restablece mediante un reemparejamiento. Esto también borra todos los dedos maestros y de usuario y restablece el código maestro al código de fábrica.

4.2.9.1 Restablecimiento alternativo con el módulo de relé "Whitebox" (versión en superficie/empotrada)



Con la versión en superficie/empotrada para el montaje en pared, puede utilizar la caja de relés "Whitebox" para activar un restablecimiento de los ajustes de fábrica con el borrado de todas las huellas dactilares, incluido el dedo maestro.

- Para iniciar el borrado, pulse durante aprox. 5 segundos la tecla situada en el taladrado de la unidad interna etiquetado con "Delete" y marcado en rojo.

Tras el restablecimiento, los LED verde, rojo y azul se iluminan de forma constante.

NOTA

¡Tras el restablecimiento, se restablecerá el código maestro modificado al código de fábrica!

4.2.9.2 Restablecimiento alternativo con el dedo maestro

	■ El lector de huella digital se encuentra en estado de funcionamiento ■ El LED azul se ilumina
	■ Deslice el dedo maestro sobre el sensor, como consecuencia los LED verde y rojo se encienden una vez brevemente
	■ Una vez leído el dedo maestro dos veces, un breve parpadeo de los LED rojo y verde indica que se ha inicializado el modo de borrado
	■ Después de la cuarta lectura del dedo maestro, el proceso de borrado se inicia y se señala con el encendido del LED verde
	■ Tras el restablecimiento, el lector de huella digital se encuentra en estado de suministro ■ Los LED verde y rojo están iluminados permanentemente

NOTA

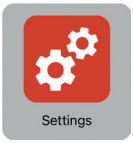
¡Tras el restablecimiento, se restablecerá el código maestro modificado al código de fábrica!

4.2.10 Modificación del código de fábrica por el código maestro (app BKS BioKey)

El código de fábrica (ver página 190) se puede cambiar por un código maestro de 6 dígitos con la app BKS BioKey o el dispositivo de programación.

NOTA

Por motivos de seguridad, se recomienda sustituir el código de fábrica por un nuevo código maestro. ¡Tras el restablecimiento, se restablecerá el código maestro al código de fábrica!



- Inicie la app BKS BioKey en su smartphone.
- Siga la indicación de identificación en el lector de huella digital.

	■ Deslizar el dedo maestro sobre el sensor ■ Los LED verde y rojo se iluminan brevemente una vez

- Pulse el botón “Settings” (ajustes).
- Seleccione “Reset code” (reiniciar código) e introduzca un nuevo código.

4.2.10.1 Modificación con el dispositivo de programación

	■ Tecla "D" ("Delete") en el dispositivo de programación ■ Pulsar la tecla "E“ (Enroll) ■ Introduzca el código de fábrica o el "CÓDIGO antiguo" y pulse la tecla "OK" para confirmar ■ Introduzca el "CÓDIGO nuevo" y pulse la tecla "OK" para confirmar ■ Repita la introducción del código maestro “CÓDIGO nuevo” y pulse la tecla "OK" para finalizar

4.2.11 Mostrar protocolo de acceso (app BKS BioKey)

- Inicie la app BKS BioKey en su smartphone.
- Siga la indicación de identificación en el lector de huella digital.

	■ Deslizar el dedo maestro sobre el sensor ■ Los LED verde y rojo se iluminan brevemente una vez

- Pulse el botón “Access log” (protocolo de acceso).

Se abre la lista “Access log” (protocolo de acceso) y se muestran los eventos almacenados en el lector de huella digital. Esta lista incluye las identificaciones exitosas y las rechazadas, entre otras cosas.

4.2.12 Ajustar tiempos de conmutación del módulo de relé (app BKS BioKey)

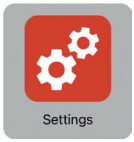
Los relés solo pueden ser controlados a través de los tiempos de conmutación en el caso de montaje en pared en superficie/empotrada. Esta función no es compatible con los dispositivos para la variante encastrada en puerta.

- Inicie la app BKS BioKey en su smartphone.
- Siga la indicación de identificación en el lector de huella digital.

	■ Deslizar el dedo maestro sobre el sensor ■ Los LED verde y rojo se iluminan brevemente una vez

- Pulse el botón “Relay times” (tiempo de relé).
- Seleccione “Relay 1” (relé 1) o “Relay 2” (relé 2) para ajustarlo.
- Seleccione “Description” (descripción) para asignar un nuevo nombre al relé. Este se muestra en el protocolo de acceso o en la asignación de usuarios.
- El tiempo de conmutación del relé correspondiente puede ajustarse entre 0 y 60 segundos a través del campo de entrada “Time” (tiempo).

4.2.13 Cambio de denominación del lector de huella digital e indicador del uso de la memoria (app BKS BioKey)



- Inicie la app BKS BioKey en su smartphone.
- Siga la indicación de identificación en el lector de huella digital.

	■ Deslizar el dedo maestro sobre el sensor ■ Los LED verde y rojo se iluminan brevemente una vez

- Pulse el botón “Settings” (ajustes).
- Seleccione “Device name” (nombre del dispositivo) y cambie el nombre del lector de huella digital.

La pantalla de este menú ofrece una visión general de la información, como la necesidad de memoria de las huellas dactilares asignadas, la memoria disponible y la versión del firmware, etc.

4.3 Modo de gestión normal

En el modo de "gestión normal", es posible configurar y gestionar el lector de huella digital incluso sin utilizar una app. El lector de huella digital se configura principalmente con el dedo maestro en el modo de "gestión normal". El dispositivo de programación también es necesario para las funciones especiales.

Para pasar a este modo de gestión, siga las instrucciones del manual, en el capítulo 4.1.1 [214].

■ El modo de "gestión normal" ofrece las siguientes funciones.

4.3.1 Resumen de funciones

Funcionamiento	Descripción | Instrucciones abreviadas
Modo de prueba (sólo posible en estado de suministro)	→ Capítulo 4.2.1 [217] 0 » OK
Asignar dedo maestro	→ 4.2.2 [218] Estado de suministro » asignar 5 veces el dedo maestro de forma correcta
Asignar dedo de usuario	→ Capítulo 4.3.2 [231] Escanear dedo maestro » asignar 5 veces el dedo de usuario de forma correcta
Identificación con el dedo de usuario	→ Capítulo 4.2.7 [224] Escanear dedo de usuario
Bloqueo del lector de huella digital	→ Capítulo 4.2.8 [224] Después de 10 intentos fallidos sin identificación del dedo, el lector de huella digital se bloquea
Desbloqueo del lector de huella digital	→ Capítulo 4.2.8 [224] Deslizar un dedo asignado (dedo maestro o de usuario) sobre el sensor

Funcionamiento	Descripción | Instrucciones abreviadas
Restablecer, borrar todos los dedos de usuario y maestros	→ Capítulo 4.2.9 [225] DA » CODE » OK (CODE: código de fábrica o maestro actual)
Cambiar el código de fábrica	→ Capítulo 4.2.10 [226] → D » E » CÓDIGO anterior » OK » CÓDIGO nuevo » OK » CÓDIGO nuevo » OK
Añadir dedo maestro	→ Capítulo 4.3.3 [232] MF » E » 0 » asignar 5 veces el dedo maestro de forma correcta
Ajustar el tiempo de conmutación del relé	→ *Capítulo* 4.3.3 [232] MF » RT » TT » OK *TT = tiempo en segundos [1...60 s], default = 3 s*
Ajustar fecha y hora	→ Capítulo 4.3.5 [109] MF » E » RT » YYYY » OK » MM » OK » DD » OK » HH » OK » MM »OK

Para más información sobre la asignación de teclas del dispositivo de programación y la explicación de las abreviaturas, véase el capítulo 4.1.4 [216].

4.3.2 Asignar dedo de usuario

	■ El dispositivo se encuentra en estado de funcionamiento y el LED azul está iluminado **¡NOTA!** No se pueden asignar dedos maestros como dedos de usuario
	■ Deslizar el dedo maestro sobre el sensor ■ Los LED verde y rojo se iluminan brevemente
 	**Proceso de asignación** ■ Deslice el dedo que desea utilizar como dedo usuario sobre el sensor ■ La lectura se confirma al **encenderse brevemente el LED verde** ■ El siguiente proceso de asignación puede realizarse deslizando de nuevo el mismo dedo sobre el sensor
	■ Repita el proceso de asignación hasta que el dedo haya sido asignado con éxito 5 veces ■ La asignación correcta del primer dedo de usuario se indica con los **LED verde y rojo** que se **encienden** brevemente **4 veces** ■ Para señalar la disponibilidad operativa, el LED azul se enciende de forma permanente
¡NOTA! En caso de dedos "difíciles" puede ser necesario asignar el dedo de usuario en cuestión más a menudo. Si hay demasiados intentos fallidos, deberá utilizar un dedo distinto al del usuario.	

El número de dedos de usuario está limitado a 35 huellas dactilares para el dedo maestro y de usuario debido al límite de espacio de la memoria.

4.3.3 Añadir dedo maestro

	■ Deslizar el dedo maestro sobre el sensor ■ Los LED verde y rojo se iluminan brevemente
	■ Pulse la tecla "E" ("Enroll") en el dispositivo de programación ■ Pulse la tecla "0"
 	**Proceso de asignación** ■ Deslice el dedo que desea añadir como dedo maestro sobre el sensor ■ La lectura se confirma al **encenderse brevemente el LED verde** ■ El siguiente proceso de asignación puede realizarse deslizando de nuevo el mismo dedo sobre el sensor
	■ Repita el proceso de asignación hasta que el dedo haya sido asignado con éxito 5 veces ■ La asignación correcta del primer dedo de usuario se indica con los **LED verde y rojo** que se **encienden** brevemente **4 veces** ■ Para señalar la disponibilidad operativa, el LED azul se enciende de forma permanente

4.3.4 Ajustar el tiempo de conmutación del relé (sólo para versión en superficie/empotrada)

	■ Deslizar el dedo maestro sobre el sensor ■ Los LED verde y rojo se iluminan brevemente
	■ Pulse la tecla "RT" en el dispositivo de programación ■ Introduzca un tiempo de conmutación en segundos de 1 a 60 mediante el teclado ■ Para finalizar, pulse la tecla "OK"

En el modo "gestión normal", solo se puede ajustar el tiempo de conmutación del relé 1.

4.3.5 Inicializar fecha y hora

Los accesos almacenados en el lector de huella digital pueden leerse con el Audit-Set (B-55606-00-3-0). Los accesos listados solo reciben una marca de tiempo correcta si la fecha y la hora se han fijado inicialmente.

	■ Deslizar el dedo maestro sobre el sensor ■ Los LED verde y rojo se iluminan brevemente
	■ Pulse la tecla "E" en el dispositivo de programación ■ Pulsar la tecla "RT" ■ Introduzca la fecha y la hora con el teclado y confirme después de cada paso con la tecla "OK": YYYY » OK » MM » OK » DD » OK » HH » OK » MM »OK Ejemplo: 23.07.2022, 12:45 h: E » RT » 2022 » OK » 07 » OK » 23 » OK »12 » OK » 45 »OK

NOTA **La fecha y la hora deben volver a ajustarse tras un corte de corriente.**

4.4 Modo de gestión de índice

En el modo de "gestión de índica", es posible configurar y gestionar el lector de huella digital incluso sin utilizar una app. En este modo de gestión, a cada usuario se le asigna una ID, lo que permite mejorar la gestión. La configuración se realiza mediante el dedo maestro y el dispositivo de programación. En el modo de gestión de índice, puede seleccionar una ID y editarla específicamente, por ejemplo, borrar el dedo de usuario de una ID. Es aconsejable documentar la asignación en una lista, véase la plantilla en el capítulo 4.4.9 [241].

Para pasar a este modo de gestión, siga las instrucciones del manual, en el capítulo 4.1.1 [214].

■ El modo de "gestión de índice" ofrece las siguientes funciones.

4.4.1 Resumen de funciones

Funcionamiento	Descripción | Instrucciones abreviadas
Modo de prueba (sólo posible en estado de suministro)	→ Capítulo 4.2.1 [217] 0 » OK
Asignar dedo maestro	→ Capítulo 4.2.2 [218] Estado de suministro » asignar 5 veces el dedo maestro de forma correcta
Asignar dedo de usuario	→ Capítulo 4.4.2 [236] MF » E » ID » OK » asignar 5 veces el dedo de usuario de forma correcta
Identificación con el dedo de usuario	→ Capítulo 4.2.7 [224] Escanear dedo de usuario
Bloqueo del lector de huella digital	→ Capítulo 4.2.8 [224] Después de 10 intentos fallidos sin identificación del dedo, el lector de huella digital se bloquea
Desbloqueo del lector de huella digital	→ Capítulo 4.2.8 [224] Deslizar un dedo asignado (dedo maestro o de usuario) sobre el sensor

Funcionamiento	Descripción | Instrucciones abreviadas
Restablecer, borrar todos los dedos de usuario y maestros	→ Capítulo 4.2.9 [225] DA » CODE » OK (CODE: código de fábrica o maestro actual)
Cambiar el código de fábrica	→ Capítulo 4.2.10 [226] D » E » CÓDIGO anterior » OK » CÓDIGO nuevo » OK » CÓDIGO nuevo » OK
Borrar dedos de usuario individuales	→ Capítulo 4.4.3 [237] MF » D » ID » OK
Bloqueo de ID	→ Capítulo 4.4.4 [238] MF » B » ID » OK
Desbloqueo de ID	→ Capítulo 4.4.5 [238] MF » UB » ID » OK
Controlar ID	→ Capítulo 4.4.6 [239] OK » ID » OK
Añadir dedo maestro	→ Capítulo 4.3.3 [232] MF » E » 0 » asignar 5 veces el dedo maestro de forma correcta
Ajustar el tiempo de conmutación del relé 1 (sólo para versión en superficie/empotrada)	→ *Capítulo* 4.4.7 [239] MF » RT » R1 » TT » OK *TT = tiempo en segundos [1...60 s], default = 3 s*
Ajustar el tiempo de conmutación del relé 2 (sólo para versión en superficie/empotrada)	→ *Capítulo* 4.4.7 [239] MF » RT » R2 » TT » OK *TT = tiempo en segundos [1...60 s], default = 3 s*
Asignar dedo de usuario para relé 1	→ Capítulo 4.4.8 [240] MF » E » ID » R1 » OK » asignar 5 veces el dedo de usuario de forma correcta
Asignar dedo de usuario para relé 2 (sólo para montaje en pared en superficie/empotrada)	→ Capítulo 4.4.8 [240] MF » E » ID » R2 » OK » asignar 5 veces el dedo de usuario de forma correcta

Funcionamiento	Descripción | Instrucciones abreviadas
Ajustar fecha y hora	→ Capítulo 4.3.5 [109] MF » E » RT » YYYY » OK » MM » OK » DD » OK » HH » OK » MM »OK

Para más información sobre la asignación de teclas del dispositivo de programación y la explicación de las abreviaturas, véase el capítulo 4.1.4 [216].

4.4.2 Asignar dedo de usuario

	■ El dispositivo se encuentra en estado de funcionamiento y el LED azul está iluminado **¡NOTA!** No se pueden asignar dedos maestros como dedos de usuario.
	■ Deslizar el dedo maestro sobre el sensor ■ Los LED verde y rojo se iluminan brevemente
	■ Pulse la tecla "E" ("Enroll") en el dispositivo de programación ■ Introduzca una ID entre 1 y 35 mediante el teclado ■ Pulsar la tecla "OK" para confirmar
 	**Proceso de asignación** ■ Deslice el dedo que desea utilizar como dedo usuario sobre el sensor ■ La lectura se confirma al **encenderse brevemente el LED verde** ■ El siguiente proceso de asignación puede realizarse deslizando de nuevo el mismo dedo sobre el sensor

	■ Repita el proceso de asignación hasta que el dedo haya sido asignado con éxito 5 veces ■ La asignación correcta del primer dedo de usuario se indica con los **LED verde y rojo** que se **encienden** brevemente **4 veces** ■ Para señalar la disponibilidad operativa, el LED azul se enciende de forma permanente
¡NOTA! En caso de dedos "difíciles" puede ser necesario asignar el dedo de usuario en cuestión más a menudo. Si hay demasiados intentos fallidos, deberá utilizar un dedo distinto al del usuario.	

El número de dedos de usuario está limitado a 35 huellas dactilares para el dedo maestro y de usuario debido al límite de espacio de la memoria.

4.4.3 Borrar dedo de usuario individual

	■ Deslizar un dedo maestro sobre el sensor ■ Los LED verde y rojo se iluminan brevemente
	■ Pulsar la tecla "D" (Delete) del dispositivo de programación, el LED verde se ilumina ■ Introducir la ID del dedo de usuario que desea borrar ■ Confirmar con la tecla "OK", el LED verde se ilumina El dedo de usuario memorizado con la ID indicada se borrará ahora y será rechazado al intentar abrir la puerta.

4.4.4 Bloqueo de ID

	■ Deslizar el dedo maestro sobre el sensor ■ Los LED verde y rojo se iluminan brevemente
	■ Pulsar la tecla "R1" (B) ■ Introducir ID ■ Confirmar con la tecla "OK" El dedo de usuario memorizado con la ID indicada se bloqueará ahora y será rechazado al intentar abrir la puerta.

NOTA

Es posible bloquear ID particulares temporalmente sin perder por ello las huellas dactilares asignadas. La ID se podrá desbloquear posteriormente sin necesidad de que la persona correspondiente vuelva a asignar sus huellas dactilares.

4.4.5 Desbloqueo de ID

	■ Deslizar el dedo maestro sobre el sensor ■ Los LED verde y rojo se iluminan brevemente
	■ Pulsar la tecla "R2" (UB) ■ Introducir ID ■ Confirmar con la tecla "OK" El dedo de usuario memorizado con la ID indicada vuelve a estar autorizado y puede abrir la puerta.

4.4.6 Controlar ID

	■ Pulsar la tecla "OK" ■ Introduzca el número de la ID que se tiene que comprobar ■ Volver a pulsar la tecla "OK" ■ Si ya se ha asignado una ID, los LED verde y rojo se iluminan ■ Si la ID no está asignada, sólo se ilumina el LED rojo

4.4.7 Ajustar el tiempo de conmutación del relé por relé (sólo para versión en superficie/empotrada)

En el modo de "gestión de índice", la duración de la conmutación se ajusta por separado para cada relé.

	■ Deslizar un dedo maestro sobre el sensor ■ Los LED verde y rojo se iluminan brevemente
	■ Pulsar la tecla „RT" del dispositivo de programación ■ Selección del relé mediante la tecla "R1" o "R2" ■ Introduzca un tiempo de conmutación en segundos de 1 a 60 mediante el teclado ■ Confirmar con la tecla "OK", el LED verde se ilumina

4.4.8 Asignar dedo de usuario para relé 1/2 (sólo para versión en superficie/empotrada)

En la versión en superficie/empotrada se pueden conmutar ambos relés de forma separada entre sí.

	■ Deslizar el dedo maestro sobre el sensor ■ Los LED verde y rojo se iluminan brevemente
	■ Pulse la tecla "E" ("Enroll") en el dispositivo de programación ■ Introduzca una ID entre 1 y 35 mediante el teclado ■ Seleccione el relé mediante la tecla "R1" o "R2" ■ Pulsar la tecla "OK" para confirmar
 	**Proceso de asignación** ■ Deslice el dedo que desea utilizar como dedo usuario sobre el sensor ■ La lectura se confirma al **encenderse brevemente el LED verde** ■ El siguiente proceso de asignación puede realizarse deslizando de nuevo el mismo dedo sobre el sensor
	■ Repita el proceso de asignación hasta que el dedo haya sido asignado con éxito 5 veces ■ La asignación correcta del primer dedo de usuario se indica con los **LED verde y rojo** que se **encienden** brevemente **4 veces** ■ Para señalar la disponibilidad operativa, el LED azul se enciende de forma permanente

4.4.9 Asignación de ID y persona

ID	Persona (nombre)	Dedo (pulgar, índice,...)

5. Manejo del teclado de código

Antes de configurar y utilizar el sistema de acceso, hay que llevar a cabo una puesta en marcha. Proceda paso a paso.

- Monte teclado de código y como se describe en el Capítulo 3.
- Realice las conexiones eléctricas de acuerdo con el esquema de conexiones.

- La primera vez que se enciende la tensión de red, se inicia el emparejamiento (pairing).

En estado de suministro, se iluminan de forma constante todos los LED (rojo/verde/dado el caso, azul). Las entradas se introducen directamente a través del teclado para la introducción de código. No se requiere ningún dispositivo de programación ni se incluye en el volumen de suministro.

	Abrir puerta
*	Inicio o confirmación de introducción de datos
Código maestro	Código de gestión
Código de usuario	Código para abrir la puerta

NOTA

Cada vez que pulse una tecla, el LED verde se iluminará brevemente para mostrarlo de forma visual. Si tras pulsar una tecla no se ilumina el LED verde, repita la pulsación.

Las combinaciones para el código maestro o de usuario deben ser combinaciones de 4-6 dígitos. Por motivos de seguridad, se excluyen determinadas combinaciones de código maestro o código de usuario. Esto incluye combinaciones de números regulares como 8888, 123456, 4321, etc. El código maestro inicial (código de fábrica) se encuentra en la página 190.

Si se introduce 5 veces consecutivas un código de usuario erróneo, el dispositivo cambia a modo de bloqueo. De este modo se impide el acceso a personas no autorizadas.

Si el dispositivo se encuentra en el modo de bloqueo, el LED rojo parpadea. Al principio, el modo de bloqueo está temporalmente limitado. Tras 5 intentos

fallidos, el tiempo de bloqueo se va prolongando (intervalo de bloqueo: 1 minuto, 5 minutos, 30 minutos, 1 hora, después bloqueo permanente).

Si se introduce dos veces consecutivas un código de usuario válido, el modo de bloqueo finaliza.

5.1 Modo de prueba

En estado de suministro se puede realizar una apertura de puerta para realizar una prueba. Para ello, pulse la secuencia de teclas 0 » 🔑. El LED verde se ilumina para confirmar.

	
0	🔑

5.2 Cambiar código maestro

NOTA

Por motivos de seguridad, se recomienda sustituir el código de fábrica por un código maestro propio.

				
*	Código maestro	*	1	*

			
Nuevo código maestro	*	Nuevo código maestro	*

5.3 Establecer/cambiar código de usuario

				
*	Código maestro	*	2	*

					
ID de usuario [1...150]	*	Código de usuario	*	Código de usuario	*

NOTA

En la versión en superficie/empotrada se pueden conmutar ambos relés de forma separada entre sí. Una ID de usuario impar conmuta el relé 1; una ID par, el relé 2.

5.4 Abrir puerta

	
Código de usuario	

NOTA

Si se introducen cifras adicionales antes del código de usuario, estas se ignoran.

5.5 Borrar código de usuario

				
*	Código maestro	*	3	*

	
ID de usuario	*

Alternativa:

				
*	Código maestro	*	3	*

			
0	*	Código de usuario	*

NOTA

A través de un reemparejamiento se reinicia el teclado para la introducción de código. Al hacerlo se borrarán todos los códigos de usuario. ¡Tras el restablecimiento, se restablece el código maestro modificado al código de fábrica!

5.6 Ajustar el tiempo de conmutación del relé (sólo para versión en superficie/empotrada)

				
*	Código maestro	*	4	*

			
Relé [1|2]	*	Tiempo [1...60 s]	*

5.7 Borrar todos los códigos de usuario y maestro

				
*	Código maestro	*	0	*

	
Código maestro	*

6. Mantenimiento y cuidado

- La disponibilidad operativa se tiene que comprobar con regularidad.
- Un producto defectuoso debe sustituirse por uno nuevo.

La superficie del sensor del escáner de huella digital se limpia prácticamente por sí sola, debido al uso recurrente (escaneo de dedos). En caso de que el lector de huella digital se ensucie de todos modos, límpielo con bastoncillos de algodón, paños de microfibra y paños de gafas. No están indicados todos los tejidos de algodón, toallitas de papel, bayetas de cocina y trapos de cocina. Utilice agua limpia sin añadirle agentes limpiadores. Limpie con cuidado la superficie del sensor.

Por seguridad, limpie las impresiones dactilares y la suciedad del teclado de código con un trapo húmedo (no mojado) y que no raye el sistema. Utilice agua limpia sin añadirle agentes limpiadores.

Con la variante de montaje en puerta:
en caso de uso frecuente, trate los contactos del SECURE*connect* 200 con la grasa de contacto B-55606-00-4-0.

La disponibilidad del dispositivo de cierre se tiene que comprobar con regularidad. Para ello, se deberán comprobar los puntos de fijación y, en caso necesario, reapretar los tornillos. Las propiedades mecánicas de la cerradura (accionando la llave o manilla / resbalón-cerrojo) no deben verse perjudicadas por la suciedad y esta también debe mantenerse regularmente.

El mecanismo de la cerradura dispone de una lubricación de por vida, por lo que está exento de mantenimiento. Engrasar ligeramente la cabeza del resbalón-cerrojo 1 vez al año. ¡No utilizar aceite, pues éste podría dañar la electrónica de la cerradura!

7. Búsqueda y subsanación de fallos

Descripción del error	Causa	Solución
El LED rojo parpadea de forma duradera varias veces por segundo	No hay ninguna conexión de bus a la unidad de control	Compruebe el cableado o ponga el equipo en marcha
	Sin emparejamiento o emparejamiento erróneo	Realice un reinicio del emparejamiento
Los LED verde y rojo parpadean permanentemente	Error en el cableado del bus RS-485	Compruebe los bornes de conexión y conéctelos correctamente si es necesario
El LED rojo parpadea de forma duradera cada dos segundos	Modo de bloqueo: Sistema bloqueado tras varias identificaciones no válidas	Escanee un dedo autorizado
El LED verde se ilumina al intentar acceder, pero la puerta no se abre	Problema de conexión entre SC200R y SC200F	Limpiar el contacto del SC200
		Comprobar la posición de montaje del SC200
	Problema de conexión – entre la unidad interior y la exterior – entre el relé y el componente conectado, p. ej., el cerradero eléctrico	Compruebe el cableado
		Desconecte la fuente de alimentación y vuelva a conectarla
		Reemplace el hardware defectuoso
El LED rojo se enciende permanentemente	Hardware defectuoso	Es necesario sustituir el lector de huella digital o el teclado para la introducción de código

8. Mantenimiento y piezas de recambio

Recomendamos realizar la inspección, el mantenimiento y la limpieza regulares tras cada uso y según la situación de montaje. Subsane inmediatamente los fallos y los defectos.

⚠ PELIGRO

¡Peligro de muerte por corriente eléctrica!

Desconecte el suministro eléctrico y descargue la energía restante acumulada.

Los trabajos de mantenimiento solo deben realizarlos los especialistas formados o autorizados por el fabricante.

En el caso de requerir asistencia técnica, le recomendamos ponerse en contacto con el servicio de asistencia del grupo de empresas Gretsch-Unitas antes de realizar la reparación in situ y, en caso necesario, acordar el envío la cerradura.

Desmonte el producto de la caja de cerradura. Para desmontarlo, afloje las fijaciones, desconecte las tomas eléctricas y retire el producto.

Cuando sean necesarias piezas de repuesto o ampliaciones, hay que utilizar exclusivamente las piezas originales del fabricante. En caso de utilizar piezas de otros fabricantes, no existe ningún tipo de reclamación de responsabilidad, garantía o prestación de servicio.

9. Eliminación

NOTA

La recogida de los desechos se realiza por separado del resto de la basura doméstica. De acuerdo con la legislación y las directivas nacionales y locales vigentes, es necesario realizar una correcta eliminación en el proceso de reciclaje correspondiente.

El producto se debe desechar como basura electrónica en los puntos de recogida públicos y en los puntos de selección de residuos reciclables. El embalaje se debe eliminar por separado.

Notizen | Notes | Notes | Notas

09.2022 | | Printed in Germany

Notizen | Notes | Notes | Notas

Herausgeber | Editor:
BKS GmbH
Heidestr. 71
42549 Velbert
Germany
Tel. +49 2051 201-0
Fax +49 2051 201-9733

www.g-u.com

Vorsprung mit System
Securing technology for you