Designed in Germany
C59501274 | 02 | 03.2021 | 24413E

TÜRTECHNIK | DOOR TECHNOLOGY

B-55600-13-4-6
B-55600-10-4-6

DE **Fingerabdruckscanner und Codetastatur**
Betriebsanleitung ..... SEITE | 2

EN **Fingerprint scanner and code keypad**
Operating instructions ..... PAGE | 55

FR **Lecteur d'empreintes digitales et clavier à code**
Notice d'utilisation ..... PAGE | 108

ES **Lector de huella digital y teclado de código**
Manual de instrucciones ..... PÁGINA | 161

Inhaltsverzeichnis

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 und die Codetastatur als Erfassungseinheit für motorische oder elektromechanische Verschlusssysteme entschieden haben.

Diese Betriebsanleitung enthält wichtige Hinweise und hilft, Gefahren zu vermeiden, Reparaturkosten und Ausfallzeiten zu vermindern und die Zuverlässigkeit und Lebensdauer des Fingerscanners oder der Codetastatur zu erhöhen.

Die Betriebsanleitung ist von jeder Person zu lesen und anzuwenden, die mit dem Fingerscanner oder der Codetastatur arbeitet, z. B. bei:

- Montage und Elektroinstallation
- Inbetriebnahme, Betrieb und Wartung

Die Betriebsanleitung ist nach dem Montageabschluss dem Betreiber 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/Verantwortliche 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.

Bauherren und Benutzer sind auf die Einhaltung dieser Angaben hinzuweisen um fehlerhafte Montage, sowie Fehlbedienungen zu vermeiden. Zu diesem Zweck ist diese Anleitung an Bauherren und Benutzer zu übergeben.

- 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 und 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 Betriebsmitteln beauftragt werden.
- Dabei ist sicherzustellen, dass ihnen die Unterlagen zur Aufstellung, Inbetriebnahme, Bedienung, Wartung und Reparatur des Betriebsmittels zur Verfügung stehen und sie diese beachten.
- Aus Sicherheits- und Zulassungsgründen (CE) ist das eigenmächtige Umbauen und/oder Verändern des Produkts nicht gestattet.
- Vor jeder Montage, Reparatur, Wartungs- oder Einstellarbeit sind alle zugehörigen Netzteile spannungslos zu schalten und gegen unbeabsichtigtes Wiedereinschalten abzusichern.
- Bei Schäden, die 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 Erfassungseinheiten 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.

Ihr Zutrittssystem besteht aus 2 elektronischen Geräten:

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

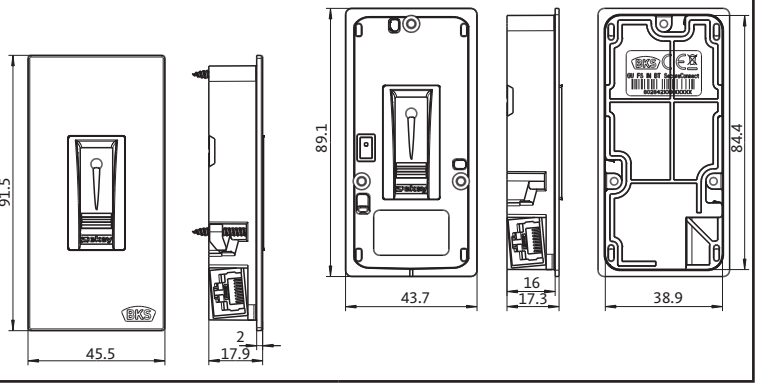
Bei Übereinstimmung der Merkmale wird durch eine verschlüsselte Übertragung an die Steuereinheit die Tür geöffnet. Das System dient primär der Öffnung von Haustüren, Wohnungstüren und Garagentoren im Heim- und Gewerbebereich.

2.1 Technische Daten

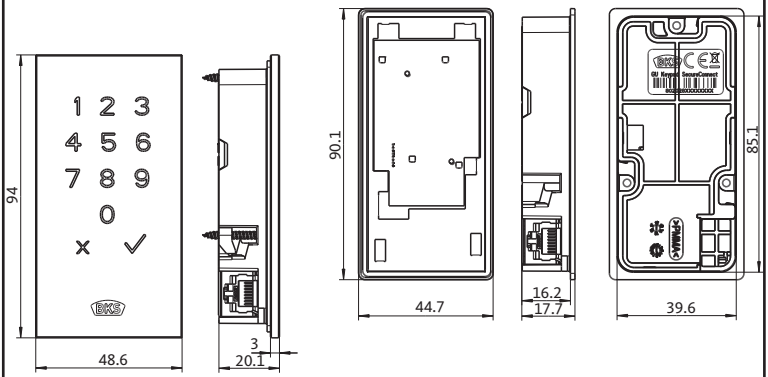
Spannungsversorgung	8....24 V DC (max. 30 V)
Leistungsaufnahme	< 1 W
Umweltbedingungen	+70 °C / –20 °C **IP54** (frontseitig)
Zertifizierungen	CE Die Zertifikate finden Sie auf www.g-u.com.

Variante	B-55600-13-4-6
Speicher	99 Fingertemplates
Template-Identifikationsdauer	1...2 s
Falschrückweisungsrate (FRR)	1:100

Falschakzeptanzrate (FAR)	1:10.000.000
Lebensdauer	max. 10 Mio. Fingerscans
Abmessungen	



Variante	B-55600-10-4-6
Speicher	99 Nutzercodes
PIN-Codelänge	4....8-stellig
Abmessungen	



2.2 Manipulationsschutz

Die Erfassungseinheit (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:

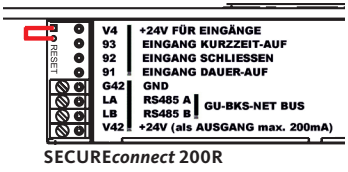
- Die Erfassungseinheit ist über eine Datenleitung mit der Steuereinheit verbunden. Die Datenübertragung ist verschlüsselt.
- Erfassungseinheit und Steuereinheit werden im Rahmen der Erstinbetriebnahme eindeutig miteinander gekoppelt (Pairing).

Beim Fingerscanner ist die Aufnahme von Benutzerfingern und die Änderung von Systeminhalten ist nur mittels vorheriger Erkennung eines Adminfingers möglich.

Die Codetastatur erfasst den PIN-Code mit dem kapazitiven Tastenfeld. Sie vergleicht die Eingabe mit den abgespeicherten Referenzcodes. Die Codetastatur verarbeitet 4- bis 8-stellige PIN-Codes. Der PIN-Code muss mindestens eine unterschiedliche Ziffer beinhalten. Es gibt 2 Arten von PIN-Codes. Den Admincode für die Konfiguration des Systems und den Nutzercode zum Öffnen der Tür.

Bei 3-maliger Falscheingabe erfolgt eine 1-minütige Sperre. Bei darauffolgender 3-maliger Falscheingabe erfolgt eine 15-minütige Sperre. Bei jeder weiteren Falscheingabe erfolgt eine 15-minütige Sperre. Durch zweimalige Eingabe eines berechtigten Nutzercodes kann die Sperre vorzeitig aufgehoben werden.

Um eine Komponente (SECURE*connect* 200R, SECURE*connect* 200F oder Erfassungseinheit) des Türsystems auszutauschen, muss an beiden Hälften des SECURE*connect* eine Repairingprozedur durchgeführt werden.



SECURE*connect* 200R

Hierzu muss auf der Platine des SECURE*connect* 200F oder des SECURE-*connect* 200R der Reset-Kontakt bei angeschlossener Stromversorgung für min. 3 s geschlossen werden. Verwenden Sie hierzu z. B. eine Krokodilklemme.

Danach kann die Klemme entfernt werden. SECURE*connect* 200R, SECURE-*connect* 200F und Erfassungseinheit (Fingerscanner oder Codetastatur) durchlaufen nun einen erneuten Pairingvorgang. Die Erfassungseinheit wird hierbei auf Werkseinstellung zurückgesetzt (alle gespeicherten Fingertemplates bzw. PIN-Codes werden gelöscht).

Wird ein Fingerscanner bzw. eine Codetastatur an einem ungepairten SECURE*connect 200* angeschlossen, wird die Erfassungseinheit hierbei auf Werkseinstellung zurückgesetzt und die Fingertemplates bzw. PIN-Codes gelöscht.

2.3 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 unser Produkt konzipiert und 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 Schlosses oder Türöffners wird ein SECURE*connect* 200 als Steuereinheit benötigt.

2.4 Nicht bestimmungsgemäße Verwendung

Ein anderer oder darüber hinausgehender Gebrauch ist nicht gestattet und für hieraus entstehende Schäden haftet BKS nicht. Eine nicht bestimmungsgemäße Verwendung ist auch gegeben, wenn die Sicherheitshinweise nicht beachtet werden. Eigenmächtige Umbauten und Veränderungen an dem Produkt sind nicht erlaubt.

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

- Der Betrieb des Zutrittssystems mit Spannungen größer 24 V + 10 % DC ist nicht zulässig und kann zu einer dauerhaften Beschädigung des Produktes führen.
- Fehler in der Polung der Anschlüsse.
- Am Produkt sind unautorisierte Modifikationen vorgenommen worden.

2.5 Lieferumfang, Transport und Lagerung

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

Die Lieferung besteht aus den folgenden Artikeln:

- Erfassungseinheit (Fingerscanner oder Codetastatur) mit Dekorelement
- Systemkabel zur Erfassungseinheit
- Anleitung

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

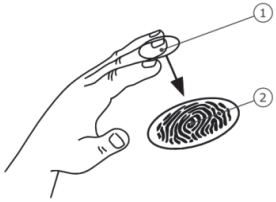
- Aufbewahrungsort nur in trockenen, sauberen und mäßig gelüfteten Innenräumen, nicht im Freien
- Lagerung ohne Bewegungen und/oder Vibrationen
- Temperaturbereich von +15 °C bis +40 °C, ohne starke Temperaturschwankungen
- Luftfeuchtigkeit mit einer relative Feuchte 30 % bis 70 %, keine Betauung
- Lagerware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

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

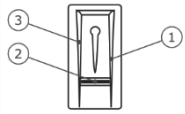
2.6 Funktion

Funktion Fingerscanner

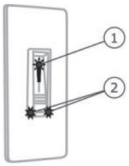
Der Fingerscanner erfasst das Fingerbild durch einen Zeilensensor und wertet es aus. Er vergleicht das Ergebnis mit den aus dem Referenz-Fingerbild gespeicherten biometrischen Informationen. Bei Übereinstimmung öffnet die Tür.



Der Fingerscanner arbeitet nur korrekt und zuverlässig mit den Papillarrillen des vorderen Fingergliedes (1).
Ziehen Sie den Finger ruhig und gleichmäßig, wie unten beschrieben, über den Sensor.



Die Fingerführung des Fingerscanners dient der richtigen Positionierung des Fingers. Sie ist das eigentliche Bedienelement und besteht aus Sensor (2), rechter (1) und linker (3) Führungskante.

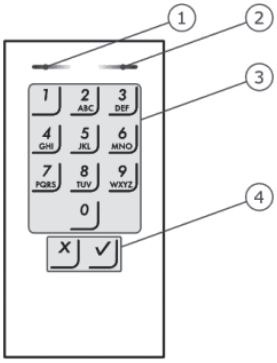


Der Fingerscanner besitzt zwei Arten von optische Signalen:

1 Status-LED für den Betriebsstatus

2 Funktions-LEDs für die Funktion des Gesamtsystems

Funktion Codetastatur



2 Status-LEDs signalisieren die Betriebszustände (PIN-Code korrekt, PIN-Code falsch, Menüpunkt...).

Ein akustischer Signalgeber signalisiert den Tastendruck und die Zutrittsfreigabe.

1 Linke Status-LED

2 Rechte Status-LED

3 Eingabetasten

4 Bestätigungstasten

Die Hintergrundbeleuchtung des Tastenfeldes ist blau, dimmbar und schaltet sich abhängig von den Lichtverhältnissen ein bzw. aus.

HINWEIS

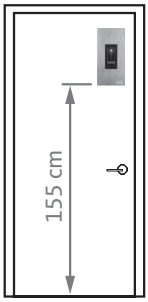
Die Codetastatur kehrt nach 10 Sekunden in den Normalbetrieb zurück, wenn keine Taste gedrückt wird. Dabei werden Eingaben und Änderungen verworfen.

3. Montage

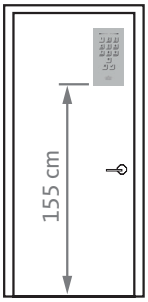
Der Fingerscanner oder die Codetastatur wird in der Regel im Außenbereich (Türaußenseite) montiert (siehe Kapitel 3.5) und über eine Datenleitung mit der Steuereinheit verbunden. Verwenden Sie BKS-Systemkabel zum Anschließen.

3.1 Montagehöhe

B-55600-13-4-6



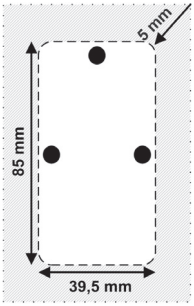
B-55600-10-4-6



- Die vorgeschriebene Montagehöhe für den Fingerscanner bzw. die Codetastatur liegt bei mindestens 155 cm oder höher!

HINWEIS **Nur bei Montage in der richtigen Höhe ist eine gute und damit eine einwandfreie Funktion gewährleistet!**

3.2 Fräsmaße

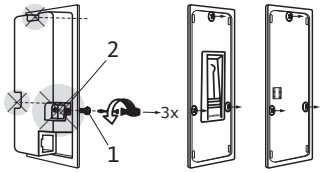


Stellen Sie in Ihrem Türprofil oder in der Holztür eine Ausfräsung mit unten stehenden Abmessungen her.

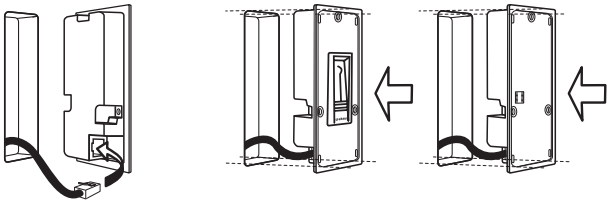
* empfohlene Fräsmaße (können je nach Werkstoff variieren), Toleranz ± 0,2 mm.

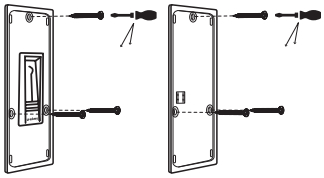
3.3 Befestigungsvarianten

3.3.1 Befestigung im Holztürblatt

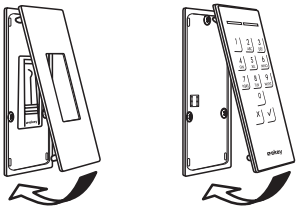


Entfernen Sie die 3 Schrauben (1) samt den Klemmnasen (2).



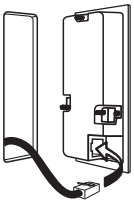


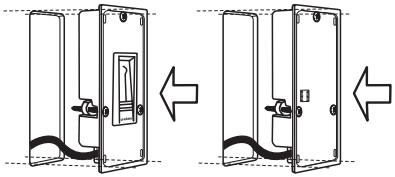
Verwenden Sie bitte die mitgelieferten Schrauben zur Befestigung im Holz.

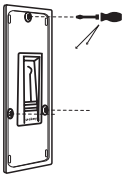


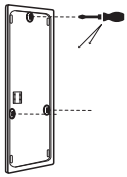
Dekorelement inklusive Dichtung für Außeneinsatz abschließend aufschnappen.

3.3.2 Befestigung in Profil, Frontplatte, Schalttafel



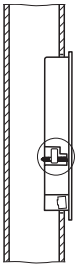


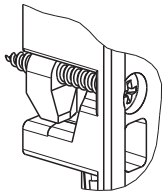


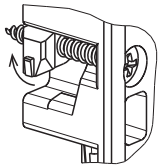


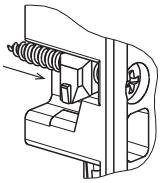
Mit Schraubendreher Schrauben anziehen bis der Fingerscanner bzw. die Codetastatur fest sitzt.

Nicht zu fest anziehen, das Gehäuse könnte so zerstört werden.







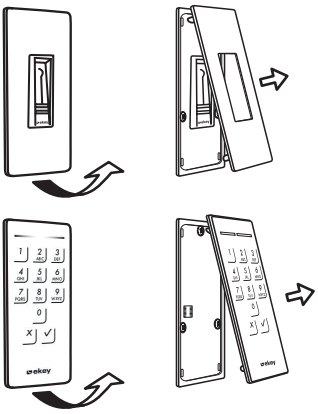


Durch das Anziehen der Schrauben bewegen sich die Klemmnasen nach außen und klemmen den Fingerscanner bzw. die Codetastatur im Profil bzw. in der Frontplatte fest.

Dekorelement inklusive Dichtung für Außeneinsatz abschließend aufschnappen.

3.4 Demontage des Dekorelementes

ACHTUNG **Beschädigen Sie nicht die Oberfläche der Tür!**
Dekorelement vorsichtig demontieren.



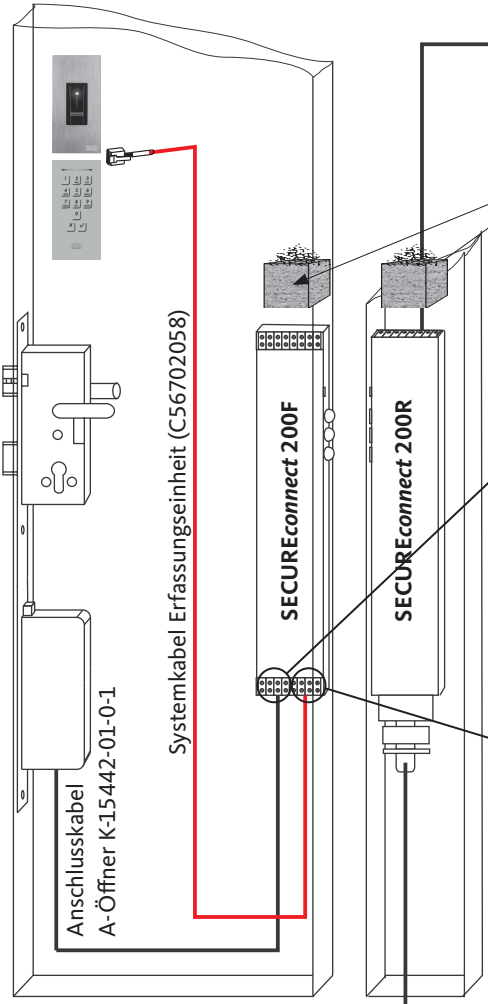
Auf der Unterseite des Dekorelementes befindet sich eine Einkerbung.

Heben Sie dort beispielsweise mit einem Schraubendreher das Dekorelement ab, bis die Rastnasen frei sind.

Drehen Sie das Dekorelement ein wenig nach oben und ziehen es schräg nach oben ab.

Dichtung gründlich reinigen und ggf. vor der Montage einfetten.

3.5 Verkabelungsplan A-Öffner



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

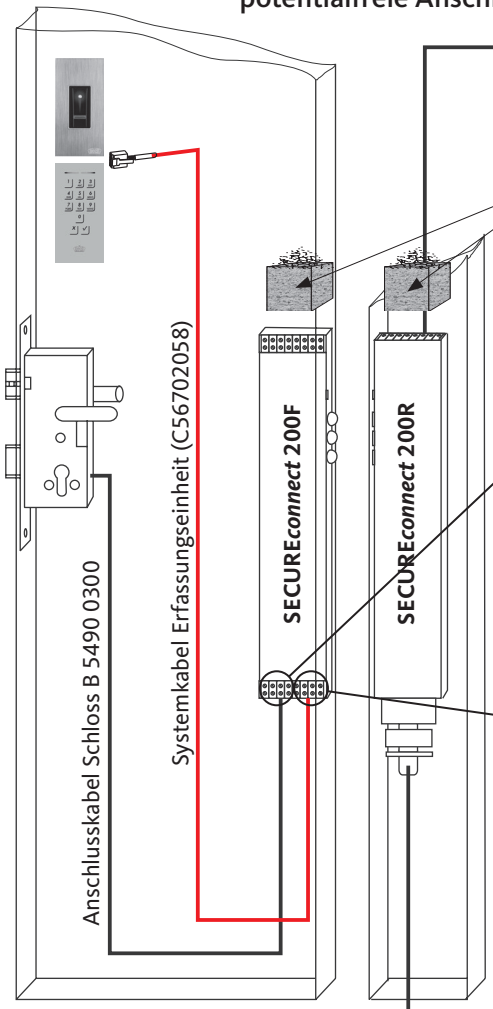
Verwenden Sie die beiliegenden Schwämme zum Schutz vor Spänen beim Einbau in Metallprofilen.

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

SC 200F	Systemkabel Erfassungseinheit	
Klemme	Litzenfarbe	Signal
GS	BN | braun	GND (minus)
96	YE | gelb	RS485 A
95	GN | grün	RS485 B
94	WH | weiß	+ 24 V (plus)

Bei Metall- und Kunststofftüren zum Leitungsauslass beigefügten Kabelschutz verwenden.

3.6 Verkabelungsplan Motor- und EK-Schlösser über potentialfreie Anschlüsse



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

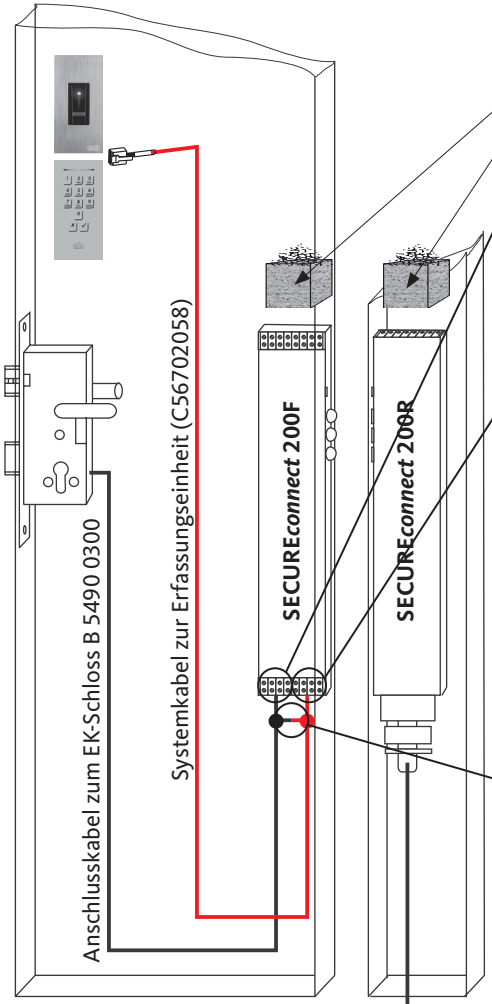
Verwenden Sie die beiliegenden Schwämme zum Schutz vor Spänen beim Einbau in Metallprofilen.

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

SC 200F	Systemkabel Erfassungseinheit	
Klemme	Litzenfarbe	Signal
GS	BN | braun	GND (minus)
96	YE | gelb	RS485 A
95	GN | grün	RS485 B
94	WH | weiß	+ 24 V (plus)

Bei Metall- und Kunststofftüren zum Leitungsauslass beigefügten Kabelschutz verwenden.

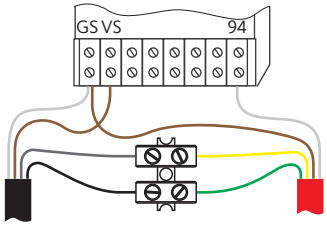
3.7 Verkabelungsplan EK-Schloss über RS485 BUS



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

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

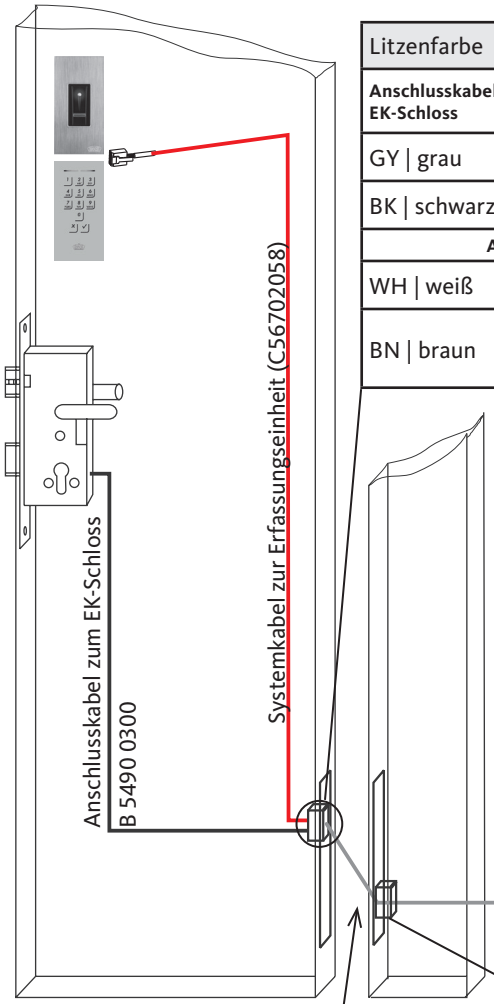
SC 200F	Systemkabel Erfassungseinheit	
Klemme	Litzenfarbe	Signal
GS	BN | braun	GND (minus)
94	WH | weiß	+ 24 V (plus)



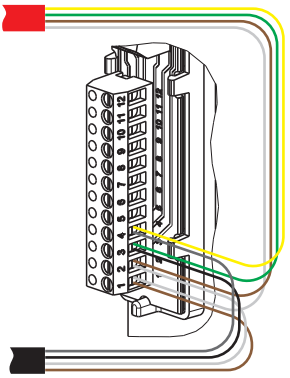
Litzenfarbe		Signal
Anschlusskabel EK-Schloss	Systemkabel Erfassungseinheit	
GY | grau	YE | gelb	RS485 A
BK | schwarz	GN | grün	RS485 B

Bei Metall- und Kunststofftüren zum Leitungsauslass beigefügten Kabelschutz verwenden.

3.7.1 Anschluss an externe Spannungsquelle



Litzenfarbe		Nr.	Signal
Anschlusskabel EK-Schloss	**Systemkabel Erfassungseinheit**	**Kabel-übergang**	
GY | grau	YE | gelb	4	RS485 A
BK | schwarz	GN | grün	3	RS485 B
Anschluss an externe Spannungsquelle			
WH | weiß	BN | braun	2	GND (minus)
BN | braun	WH | weiß	1	+ 12 V – 24 V DC



Netzteil B 5570 0402

Kabelübergang	Netzteil
1	24 V DC
2	GND (minus)

3.7.2 Pairing Fingerscanner/Codetastatur mit EK-Schloss

Erfassungseinheit und Steuereinheit werden automatisch während der Erstinbetriebnahme über die RS485 BUS-Verbindung eindeutig miteinander gekoppelt (Pairing).

Um nach dem Pairing eine Komponente (Fingerscanner, Codetastatur oder Schloss) des Türsystems auszutauschen, muss vor der erneuten Koppelung 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:

- Dauerhafte Betätigung des Drückers.
- Durch Auf- und Zuschließen mit einem mechanischen Schlüssel den Schließbartsensor 3-mal überfahren.

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

4. Inbetriebnahme

Zur Bedienung müssen die Geräte in Betrieb genommen werden. Die Inbetriebnahme des Systems koppelt die Steuereinheit mit der Erfassungseinheit. Bei Inbetriebnahme ihres Zutrittssystem gehen Sie schrittweise vor:

- Montieren Sie die Geräte wie im Kapitel 3 beschrieben.
- Der elektrische Anschluss der Komponenten ist nach dem Verkabelungsplan auszuführen.

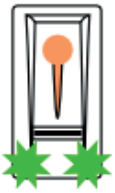
4.1 Inbetriebnahme Fingerscanner

- Verbinden Sie das Netzteil oder SECURE*connect* mit der Netzspannung.
- Nach dem ersten Einschalten führen Fingerscanner und SECURE*connect* bzw. EK-Schloss eine automatische Koppelung durch. Nach Abschluss der Koppelung blinkt die blaue LED.

Fingerscanner ist nicht mit SC200|-EK-Schloss gekoppelt.

Fingerscanner ist mit SC200|-EK-Schloss gekoppelt. Es ist kein Finger gespeichert.

Fingerscanner ist mit Bluetooth-Gerät verbunden.



Fingerscanner ist mit SC200|-EK-Schloss gekoppelt - Adminmenü.

4.1.1 Bedienkonzept

Es stehen zwei unterschiedliche Bedienkonzepte zur Verfügung:

- App – Administration des Bluetooth-Fingerscanners mittels mobilen Gerätes (Kapitel 6.1, ab Seite 27)
- Adminfinger – Administration des Fingerscanners mittels Adminfinger (Kapitel 6.3, ab Seite 34)

4.1.2 Testmodus

Verbinden Sie die Netzspannung und führen Sie innerhalb der nächsten 10 Minuten den Test durch. Sind die 10 Minuten abgelaufen, ist dieser Test erst nach einem Power-on-Reset des Fingerscanners möglich.

Fingerscanner ist mit SC200|EK-Schloss gekoppelt. Es ist kein Finger gespeichert.

Legen Sie einen Finger für 3 – 5 s auf den Sensor.

Wenn Sie den Finger entfernen, schaltet das Relais (SECURE*connect* oder EK-Schloss).

HINWEIS

Ein Test kann nur erfolgen, wenn noch keine Adminfinger eingespeichert sind bzw. noch kein mobiles Gerät gekoppelt ist.

Sie dürfen Ihren Finger insgesamt maximal 5 s auf den Sensor auflegen. Wenn Sie den Finger länger auf dem Sensor lassen, dann schaltet das Relais (SECURE*connect* oder EK-Schloss) nicht.

4.2 Inbetriebnahme Codetastatur

- Nach dem ersten Einschalten führen Codetastatur und SECURE*connect* bzw. EK-Schloss eine automatische Koppelung durch. Die Status-LEDs der Codetastatur blinken abwechselnd gelb. Nach Abschluss der Koppelung leuchtet keine Status-LED.

Codetastatur ist nicht mit SC200|EK-Schloss gekoppelt.

Codetastatur ist mit SC200|EK-Schloss gekoppelt.

ACHTUNG

Ändern Sie sofort nach der Inbetriebnahme den werkseitigen Admincode 9999 und halten Sie diesen Geheim!
Wird der Admincode nicht geändert, ermöglichen Sie unbefugten Personen Zugang zu Ihrem Adminmenü und folglich Zutritt zu Ihrem Haus.

4.2.1 Optische Signalisierung

Anzeige	Status-LED links	Status-LED rechts	Bedeutung
	aus	aus	Standby
	gelb blinkend	gelb blinkend	Werkseinstellung/ keine Koppelung mit Steuereinheit
	gelb	aus	Bereit zur Eingabe des Admincodes
	grün	aus	Adminmenü aktiv
	grün	grün	Eingabe positiv: richtiger PIN-Code, richtiger Eingabewert, ...
	rot	rot	Eingabe negativ: falscher PIN-Code, falscher Eingabewert, ...
	aus	rot	1-minütige bzw. 15-minütige Systemsperre

5. Bedienung Fingerscanner

Finger ziehen

Halten Sie den Finger gerade, legen Sie ihn mittig zwischen den Führungskanten auf. Verdrehen Sie ihn nicht.

Legen Sie das Gelenk des vorderen Fingergliedes direkt auf den Sensor. Legen Sie den Finger flach auf die Fingerführung auf.

Strecken Sie die benachbarten Finger aus.

Bewegen Sie den Finger gleichmäßig nach unten über den Sensor. Bewegen Sie die ganze Hand mit. Ziehen Sie das vordere Fingerglied vollständig über den Sensor, um optimale Ergebnisse zu erzielen.
Die Bewegung dauert ca. 1 s.

Allgemeine Tipps für eine gute Qualität des Fingerbildes

- Zeige-, Mittel- und Ringfinger funktionieren am besten. Daumen und kleiner Finger liefern schlecht auswertbare Fingerbilder.
- Bei oft feuchten Fingern speichern Sie diese im feuchten Zustand ein.
- Kinderfinger funktionieren ab ca. 5 Jahren.

Finger-Touch

Berühren Sie den Sensor kurz und schnell mit dem Finger.

6. Programmierung des Fingerscanners

6.1 Programmierung mit der open biometric-App

Der Fingerscanner muss mit dem SECURE*connect* gekoppelt sein, um mit der Programmierung starten zu können.

HINWEIS **Die open biometric-App kann nur in Verbindung mit dem Bluetooth-Fingerscanner verwendet werden.**

Die open biometric-App dient der Programmierung des Systems. Zusätzlich können Türen mittels der App geöffnet werden.

6.1.1 App herunterladen

Die App ist für Apple iOS und Google Android erhältlich. Laden Sie die open biometric-App vom App Store oder Google Play herunter. Geben Sie dazu den Suchbegriff „open biometric“ ein.

Download on the App Store GET IT ON Google Play

Für die erstmalige Koppelung benötigen Sie den Gerätekoppelungscode und den App-Sicherheitscode. **Beide Codes lauten werkseitig 9999.**

- Starten Sie die open biometric-App.
- Berühren Sie die Eingabefläche (Android) oder drücken Sie „Suchen“ (iOS). Die App sucht nach verfügbaren Bluetooth-Geräten.
- Wählen Sie Ihren Bluetooth-Fingerscanner aus (die letzen 4 Stellen der Seriennummer werden angezeigt).
- Nur Android: Drücken Sie „Anmelden“.
- Geben Sie den **werkseitigen Gerätekoppelungscode 9999** ein.
- Drücken Sie „Weiter“. Das mobile Gerät wird mit dem Bluetooth-Fingerscanner gekoppelt.

- Geben Sie einen neuen 6-stelligen Gerätekoppelungscode ein. Sie müssen den werkseitigen Gerätekoppelungscode aus Sicherheitsgründen bei der ersten Koppelung des Systems ändern. Merken Sie sich diesen, da er zum Koppeln von weiteren mobilen Geräten benötigt wird.

  Ihr Gerätekoppelungscode:

- Drücken Sie „Ändern“ (Android) oder „Weiter“ (iOS).
- Geben Sie den werkseitigen App-Sicherheitscode 9999 ein.
- Drücken Sie „Weiter“.

Die Koppelung zwischen Bluetooth-Fingerscanner und mobilem Gerät wurde durchgeführt. Das System befindet sich im Normalbetrieb.

Sie können nun das Fingerscan-Zutrittssystem mit der open biometric-App programmieren und verwalten.

HINWEIS

Zur Administration Ihres Bluetooth-Fingerscanners ist nun lediglich die intuitive open biometric-App notwendig.
Tippen Sie auf die gewünschten Funktionen in der App und folgen Sie den Anweisungen auf dem Display.

6.1.2 Sicherheitscode ändern

Sie können jederzeit sämtliche Sicherheitscodes ändern:

- App-Sicherheitscode
- Adminkoppelungscode
- Benutzerkoppelungscode

HINWEIS

Der 4- bis 6-stellige App-Sicherheitscode wird zur Sicherheitsabfrage für die App benötigt. Sie können die Abfrage des App-Sicherheitscodes unter „ADMINISTRATION“ deaktivieren, falls Ihr mobiles Gerät über gesicherte Sperrmechanismen (Fingerprint, Code usw.) verfügt.

- Wählen Sie „ADMINISTRATION“ aus.
- Wählen Sie „SICHERHEITSCODES ÄNDERN“ aus.
- Ändern Sie den gewünschten Code.
- Drücken Sie „Ändern“ (Android) oder „Fertig“ (iOS).

Der ausgewählte Sicherheitscode wurde geändert.

6.1.3 Finger einspeichern

Sie können Admin- und Benutzerfinger mit der open biometric-App einspeichern.

- Wählen Sie „ADMINISTRATION“ aus.
- Wählen Sie „BENUTZERVERWALTUNG“ aus.
- Drücken Sie  (Android) oder "+" (iOS).
- Geben Sie den Benutzernamen ein.
- Drücken Sie „Neue Adminberechtigung“ oder „Neue Zugangsberechtigung."
- Wählen Sie das zu schaltende Relais aus (für das jeweils angeschlossene SECURE*connect* oder EK-Schloss).
- Wählen Sie einen Finger aus.
- Drücken Sie „Einspeichern“.
- Lesen Sie den Hinweis und drücken Sie „Start“.
- Sobald Ihr Finger erfolgreich registriert wurde, drücken Sie „OK“.
- Drücken Sie „Fertig“.

HINWEIS **Speichern Sie mindestens einen Finger von jeder Hand pro Zutrittspunkt ein.**

6.1.4 Bluetooth deaktivieren

Sie können die Bluetooth-Funktionalität deaktivieren.
In der Werkseinstellung ist die Bluetooth-Funktionalität aktiv.

- Starten Sie die open biometric-App.
- Wählen Sie „ADMINISTRATION“ aus.
- Wählen Sie „SYSTEMSTATUS“ aus.
- Aktivieren Sie unter „BLUETOOTH-EINSTELLUNGEN“ „Bluetooth nach 15 Minuten deaktivieren“.

Mit dieser Einstellung wird Bluetooth am Fingerscanner nach 15 Minuten in einem der folgenden Fällen deaktiviert:

- kein mobiles Gerät wurde verbunden.
- mindestens ein Finger wurde eingespeichert.

Sie können Bluetooth wieder aktivieren: Steigen Sie in das Adminmenü ein und ziehen Sie einen beliebigen Adminfinger über den Sensor.

6.1.5 Weitere mobile Geräte koppeln

Sie können weitere mobile Geräte mit dem selbstgewählten 6-stelligen Admin- bzw. Benutzerkoppelungscode mit dem Bluetooth-Fingerscanner koppeln.

- Starten Sie die open biometric-App.
- Koppeln Sie das mobile Gerät mit dem Bluetooth-Fingerscanner und verwenden Sie den selbstgewählten 6-stelligen Admin- bzw. Benutzerkoppelungscode.
- Die Koppelung zwischen Bluetooth-Fingerscanner und mobilem Gerät wird durchgeführt.

Sie können nun den Fingerscanner mit der App programmieren und verwalten.

6.1.6 Mehrere Bluetooth-Fingerscanner verwenden

Die open biometric-App ermöglicht das Verwenden von mehreren Bluetooth-Fingerscannern. Um zwischen zwei Bluetooth-Fingerscannern zu wechseln, müssen Sie die Koppelung zwischen Bluetooth-Fingerscanner und mobilem Gerät zurücksetzen.

HINWEIS

Beim Zurücksetzen der Koppelung werden die gespeicherten Relaisnamen (SECURE*connect* oder EK-Schloss) und Nutzerbilder gelöscht. Die Nutzernamen und Berechtigungen bleiben am Bluetooth-Fingerscanner gespeichert.

- Starten Sie die open biometric-App.
- Wählen Sie „ADMINISTRATION“ aus.
- Wählen Sie „KOPPELUNG ZURÜCKSETZEN“ aus.
- Bestätigen Sie das Zurücksetzen mit „Fortfahren“.

Die Koppelung zwischen Bluetooth-Fingerscanner und mobilem Gerät ist jetzt zurückgesetzt. Sie können nun einen anderen Bluetooth-Fingerscanner koppeln.

6.2 Benutzerkoppelungscode einspeichern

Sie können einen Benutzerkoppelungscode einspeichern. Sie können diesen Code an einer Person Ihrer Wahl weitergeben. Mit diesem Code können folgende Aktionen ausgeführt werden:

- Tür öffnen
- App-Sicherheitscode aktivieren oder deaktivieren
- App-Sicherheitscode ändern
- Koppelung zwischen Fingerscanner und mobilem Gerät zurücksetzen

Um den Benutzerkoppelungscode einzuspeichern, führen Sie folgende Schritte aus:

- Starten Sie die open biometric-App.
- Wählen Sie „ADMINISTRATION“ aus.
- Wählen Sie „SICHERHEITSCODES ÄNDERN“ aus.
- Geben Sie den gewünschten Benutzerkoppelungscode im entsprechenden Feld ein.
- Bestätigen Sie die Eingaben mit „Ändern“ (Android) oder „Fertig“ (iOS).

Der Benutzerkoppelungscode ist nun eingespeichert.

6.2.1 App-Sicherheitscode zurücksetzen

- Starten Sie die open biometric-App.
- Tippen Sie einen falschen App-Sicherheitscode ein.
- Bestätigen Sie die Eingabe mit „Weiter“.
- Wählen Sie „KOPPELUNG ZURÜCKSETZEN“ aus.
- Bestätigen Sie das Zurücksetzen mit „Fortfahren“.

Die Koppelung zwischen Bluetooth-Fingerscanner und mobilem Gerät wird zurückgesetzt und der App-Sicherheitscode auf 9999 gesetzt.

Sie können nun den Bluetooth-Fingerscanner wieder koppeln und einen neuen App-Sicherheitscode vergeben.

6.2.2 System vor Verlust des mobilen Gerätes schützen

Wenn Sie Ihr mobiles Gerät verloren haben, können Sie mit Hilfe eines zweiten mobilen Gerätes den Admin- bzw. Benutzerkoppelungscode ändern. Durch den neuen Admin- bzw. Benutzerkoppelungscode unterbinden Sie den Verbindungsaufbau des verlorenen mobilen Gerätes.

- Starten Sie die open biometric-App am zweiten mobilen Gerät.
- Koppeln Sie das zweite mobile Gerät mit dem Bluetooth-Fingerscanner.

- Wählen Sie „ADMINISTRATION“ aus.
- Wählen Sie „SICHERHEITSCODES ÄNDERN“ aus.
- Geben Sie einen neuen 6-stelligen Admin- bzw. Benutzerkoppelungscode ein.
- Bestätigen Sie die Eingabe mit „Ändern“ (Android) oder „Fertig“ (iOS).

Der Admin- bzw. Benutzerkoppelungscode ist im System geändert.

Das verlorene mobile Gerät kann nun keine Verbindung mehr mit dem Bluetooth-Fingerscanner aufbauen. Ihr System ist vor Zugriffen unberechtigter Personen sicher.

6.2.3 System auf Werkseinstellung zurücksetzen

- Starten Sie die open biometric-App.
- Verbinden Sie sich mit dem Bluetooth-Fingerscanner.
- Wählen Sie „ADMINISTRATION“ aus.
- Wählen Sie „SYSTEM ZURÜCKSETZEN“ aus.
- Bestätigen Sie das Zurücksetzen mit „Fortfahren“.

Das System ist auf Werkseinstellung zurückgesetzt. Sie können nun das System wieder in Betrieb nehmen.

HINWEIS

Alle Benutzerfinger und Adminfinger werden gelöscht!
Die Koppelung zwischen Fingerscanner und SECURE*connect* 200 bzw. EK-Schloss bleibt erhalten!

Durch ein Repairing des SECURE*connect* 200 wird der Fingerscanner auch in den Werkszustand zurückgesetzt.

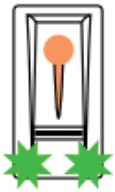
6.3 Programmierung mit Adminfingern

6.3.1 Adminfinger einspeichern

Die Adminfinger dienen zur Programmierung des Systems. Speichern Sie zu Beginn 4 unterschiedliche Adminfinger ein. Jeder Finger muss **mindestens 3-mal eingelesen** werden. Wir empfehlen von 2 verschiedenen Personen jeweils 2 Finger einzuspeichern.

Fingerscanner ist mit SC200|-EK-Schloss gekoppelt. Es ist kein Finger gespeichert.

3 Finger-Touches innerhalb von 5 s.



Admin-modus aktiv.

Ziehen Sie den ersten Adminfinger über den Sensor.

Der Finger wurde er-kannt.

System ist bereit zur Wiederho-lung.

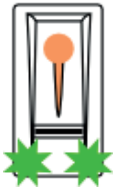
Ziehen Sie den ersten Adminfinger erneut über den Sensor.

Der Finger wurde er-kannt.

System ist bereit zur Wiederho-lung.

Ziehen Sie den ersten Adminfinger erneut über den Sensor.

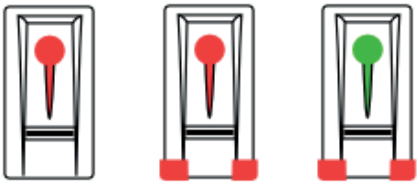
Qualität der drei Scans sehr gut.



Fingerscanner ist bereit zur Aufnahme der weiteren Adminfinger.

Weitere mögliche Anzeigen während des Einspeichervorgangs:

Qualität der Scans ausreichend.
Die Qualität kann durch weitere Scans verbessert werden.



Fehler beim Scanvorgang bzw. die Qualität ist nicht ausreichend.
Ziehen Sie diesen Finger nochmals über den Sensor.

HINWEIS

Bei einem Neustart des Fingerscanners, wenn dieser im Adminmodus ist und weniger als 4 Adminfinger vorhanden sind, werden alle bereits gespeicherten Adminfinger gelöscht.

Während des Einspeicherns der Finger dürfen zwischen den einzelnen Fingerscans maximal 10 s vergehen. Das Einspeichern des Fingers wird sonst abgebrochen.

6.3.2 Benutzerfinger einspeichern

Mit Benutzerfingern können Sie eine Türöffnung ausführen. Alle Finger, die keine Adminfinger sind, können als Benutzerfinger verwendet werden.

Normalbetrieb.

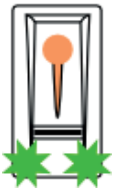
3 Finger-Touches innerhalb von 5 s.

Adminmenü

Ziehen Sie einen beliebigen Adminfinger über den Sensor.

Adminfinger wurde erkannt. Einspeichermodus aktiv.

1 Finger-Touch innerhalb von 5 s.



Aufnahmemodus ist aktiv.

Ziehen Sie den zu speichernden Finger über den Sensor.

Der Finger wurde erkannt.

System ist bereit zur Wiederholung.

Ziehen Sie den zu speichernden Finger über den Sensor.

Der Finger wurde erkannt.

System ist bereit zur Wiederholung.

Ziehen Sie den zu speichernden Finger über den Sensor.

Der Finger wurde erkannt.

Der Finger wurde erfolgreich eingespeichert.

Nach Speichern des Benutzerfingers: Normalbetrieb.

6.3.3 Benutzerfinger löschen

Einzelne Benutzerfinger können nur gelöscht werden, wenn dieser Benutzer anwesend ist.

Normal-betrieb

3 Finger-Touches innerhalb von 5 s.

Adminmenü

Ziehen Sie einen beliebiegen Adminfinger über den Sensor.

Adminfinger wurde erkannt. Ein-speichermo-dus aktiv.

5 s warten!

Löschmodus aktiv

1 Finger-Touch

Verwal-tungsmenü

Ziehen Sie den zu löschenden Finger über den Sensor.

Benutzer-finger ge-löscht!

Normal-betrieb

6.3.4 Alle Benutzerfinger löschen

Es werden alle im System gespeicherten Benutzerfinger gelöscht. Die Adminfinger bleiben erhalten.

Normalbetrieb

3 Finger-Touches innerhalb von 5 s.

Adminmenü

Ziehen Sie einen beliebiegen Adminfinger über den Sensor.

Adminfinger wurde erkannt. Einspeichermodus aktiv.

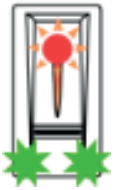
5 s warten!

Löschmodus aktiv

1 Finger-Touch

Verwaltungsmenü

Gleichen Adminfinger wie oben erneut scannen.



Alle Benutzerfinger gelöscht!

Normalbetrieb

HINWEIS **Prüfen Sie einen beliebigen Benutzerfinger. Sie dürfen keine Freigabe mehr erhalten!**

6.3.5 Werksreset Fingerscanner

Sie setzen damit den Fingerscanner in den Auslieferungszustand zurück.

HINWEIS

Alle Benutzerfinger und Adminfinger werden gelöscht! Die Koppelung zwischen Fingerscanner und SECURE*connect* 200 bzw. EK-Schloss bleibt erhalten!

Durch ein Repairing des SECURE*connect* 200 oder EK-Schloss wird der Fingerscanner auch in den Werkszustand zurückgesetzt.

Normal-betrieb

3 Finger-Touches innerhalb von 5 s.

Adminmenü

Ziehen Sie einen beliebiegen Adminfinger über den Sensor.

Adminfinger wurde er-kannt. Einspeicher-modus aktiv.

5 s warten!

Löschmodus aktiv

1 Finger-Touch

Verwal-tungsmenü

Einen anderen Adminfinger als zuvor scannen.

Alle Be-nutzer- und Adminfinger gelöscht!

Fingerscanner ist mit SC200|-EK-Schloss gekoppelt. Es ist kein Finger gespeichert.

7. Programmierung der Codetastatur

Für die Programmierung stehen verschiedene Menüpunkte im Adminmenü zur Verfügung. Diese können über die Tasten aufgerufen werden.

Taste	Menüpunkt
1	Nutzercode speichern
2 ABC	Nutzercode löschen
3 DEF	Admincode ändern
4 GHI	System auf Werkseinstellung zurücksetzen
5 JKL	Codetastatur einstellen

7.1 Admincode ändern

Diese Funktion ermöglicht das Ändern des bestehenden Admincodes. Der Admincode kann 4 bis 8-stellig sein und muss mindestens eine unterschiedliche Ziffer beinhalten. Die Änderung des Admincodes wird über das Adminmenü durchgeführt. Um ins Adminmenü zu gelangen, geben Sie den Admincode ein.

HINWEIS **Admincodes können nicht als Nutzercodes verwendet werden.**

Drücken Sie √ um die Eingabe des Admincodes zu starten.

Geben Sie den Admin-code ein (Default = 9999).

√

3

√

Geben Sie den alten Admincode ein.

√

Geben Sie den neuen Admincode ein.

√

Geben Sie den neuen Admincode erneut ein.

√

7.2 Nutzercode einspeichern

Das System erlaubt das Einlernen von maximal 99 Nutzercodes. Ein Nutzercode ist ein PIN-Code, mit dem eine Aktion auf der Steuereinheit ausgelöst wird, z. B. das Öffnen einer Tür. Der Nutzercode kann 4- bis 8-stellig sein und muss mindestens eine unterschiedliche Ziffer beinhalten.

HINWEIS

Verwenden Sie lange Nutzercodes. Verwenden Sie möglichst alle Ziffern. Verwenden Sie unterschiedliche Codes für die Berechtigten.

Drücken Sie √ um die Eingabe des Admincodes zu starten.

Geben Sie den Admincode ein.

√

1

√

Geben Sie den Nutzercode ein.

√

Geben Sie den Nutzercode erneut ein.

√

7.3 Nutzercode löschen

Sie können einzelne Nutzercodes löschen. Dazu benötigen Sie den zu löschenden Nutzercode.

Das Löschen eines Nutzercodes wird über das Adminmenü durchgeführt. Um ins Adminmenü zu gelangen, geben Sie den Admincode ein.

Drücken Sie √ um die Eingabe des Admincodes zu starten.

Geben Sie den Admincode ein.

√

2

√

Geben Sie den zu löschenden Nutzercode ein.

√

7.4 System auf Werkseinstellung zurücksetzen

Die Codetastatur wird auf Werkseinstellung zurückgesetzt. Es werden alle Nutzercodes unwiederbringlich gelöscht. Der Admincode wird auf Werkseinstellung 9999, die Helligkeitsschwelle wird auf 10 % und der Helligkeitswert auf 100 % zurückgesetzt. Die akustische und optische Signalisierung für den Tastendruck und das akustische Signal für die Türöffnung wird eingeschaltet.

Durch einen Repairing-Vorgang (siehe Kapitel 2.2) wird die Codetastatur ebenfalls auf Werkseinstellung zurückgesetzt.

Drücken Sie √ um die Eingabe des Admincodes zu starten.

Geben Sie den Admincode ein.

√

4

√

Geben Sie den Admincode ein.

√

7.5 Automatische Hintergrundbeleuchtung einstellen

Hier legen Sie die Helligkeitsschwelle fest, bei der die blaue Hintergrundbeleuchtung bei Dämmerung automatisch eingeschaltet wird.

Die Helligkeitsschwelle kann mittels Prozentwerten eingestellt werden. Werksseitig ist die Helligkeitsschwelle auf 10 % eingestellt. Geben Sie den gewünschten Prozentwert ein:

0 = automatische Hintergrundbeleuchtung aus
1 bis 100 = Helligkeitsschwelle von Einschaltung bei sehr heller Umgebung bis Einschaltung erst bei sehr dunkeler Umgebung

Drücken Sie √ um die Eingabe des Admincodes zu starten.

Geben Sie den Admincode ein.

√

51

Wert der gewünschten Helligkeitsschwelle, z. B. 70.

√

7.6 Helligkeit der Hintergrundbeleuchtung einstellen

Die Helligkeit der Hintergrundbeleuchtung kann mittels 4 vordefinierten Modi eingestellt werden. Werksseitig ist die Hintergrundbeleuchtung zu 100 % an. Geben Sie die Zahl des gewünschten Modus ein:

0 = Hintergrundbeleuchtung aus
1 = Hintergrundbeleuchtung zu 33 % an
2 = Hintergrundbeleuchtung zu 66 % an
3 = Hintergrundbeleuchtung zu 100 % an

Das Einstellen der Helligkeit der Hintergrundbeleuchtung wird über das Adminmenü durchgeführt. Um ins Adminmenü zu gelangen, geben Sie den Admincode ein.

Drücken Sie √ um die Eingabe des Admincodes zu starten.

Geben Sie den Admincode ein.

√

52

Zahl des gewünschten Modus, z. B. 2.

√

7.7 Signalisierung des Tastendrucks einstellen

Die akustische und optische Signalisierung des Tastendrucks kann mittels 4 vordefinierter Modi eingestellt werden. Werksseitig sind die akustischen und optischen Signale für den Tastendruck eingeschaltet. Geben Sie die Zahl des gewünschten Modus ein:

0 = akustische und optische Signale aus
1 = akustische Signale ein und optische Signale aus
2 = akustische Signale aus und optische Signale ein
3 = akustische und optische Signale ein

Das Einstellen der Signalisierung des Tastendrucks wird über das Adminmenü durchgeführt. Um ins Adminmenü zu gelangen, geben Sie den Admincode ein.

Drücken Sie √ um die Eingabe des Admincodes zu starten.

Geben Sie den Admincode ein.

√

54

Zahl des gewünschten Modus, z. B. 2.

√

7.8 Akustisches Signal beim Öffnen einstellen

Das akustische Signal beim Öffnen kann aus- bzw. eingeschaltet werden. Werksseitig ist das akustische Signal eingeschaltet. Geben Sie die Zahl des gewünschten Modus ein:

0 für ausschalten
1 für einschalten

Das Einstellen des akustischen Signals beim Öffnen wird über das Adminmenü durchgeführt. Um ins Adminmenü zu gelangen, geben Sie den Admincode ein.

Drücken Sie √ um die Eingabe des Admincodes zu starten.

Geben Sie den Admincode ein.

√

55

Zahl des gewünschten Modus, z. B. 0.

√

8. Öffnen der Tür

Die Türöffnung kann mit der open biometric-App, dem Fingerscanner oder der Codetastatur erfolgen.

8.1 Türöffnung mit der open biometric-App

Das System befindet sich im Normalbetrieb.

- Starten Sie die open biometric-App. Das mobile Gerät verbindet sich mit dem Bluetooth-Fingerscanner.
- Wählen Sie „ZUGÄNGE“ aus.
- Schieben Sie den Schieber des zu öffnenden Zuganges nach rechts.

Das SECURE*connect* sendet dann das Steuersignal für A-Öffner bzw. Motorschloss und Ihre Tür öffnet sich. Das EK-Schloss empfängt das Steuersignal direkt.

8.2 Türöffnung mit Fingerscan

Normalbetrieb

Ziehen Sie einen eingespeicherten Benutzer oder Adminfinger über den Sensor.

Der Finger wurde erfolgreich erkannt.

Nach Türöffnung: Normalbetrieb.

HINWEIS

Bei Verwendung des Fingerscanners mit einem SC200 wird, wenn Sie die Tür länger als 12 s geöffnet lassen, der Fingerscanner spannungslos geschaltet. Nach dem Schließen und folgender Wiederkehr der Spannungsversorgung zeigt der Fingerscanner kurzzeitig „Keine Busverbindung “ bis der Normalbetrieb automatisch wieder hergestellt ist.

8.3 Türöffnung mit Codetastatur

Geben Sie einen eingespeicherten Nutzercode ein.

Drücken Sie √ und die Tür öffnet sich.

Der Nutzercode wurde nicht erkannt.

HINWEIS

Bei 3-maliger Falscheingabe erfolgt eine Sperrung für eine Minute. Bei darauffolgender 3-maliger Falscheingabe erfolgt eine Sperrung für weitere 15 Minuten. Bei weiterer Falscheingabe erfolgt eine Sperrung für weitere 15 Minuten.
Durch zweimalige Eingabe eines berechtigten Nutzercodes kann die Sperre vorzeitig aufgehoben werden. Eine Signalisierung erfolgt hierbei nicht.

HINWEIS

Bei Verwendung der Codetastatur mit einem SC200 wird, wenn Sie die Tür länger als 12 s geöffnet lassen, die Codetastatur spannungslos geschaltet.
Nach dem Schließen und folgender Wiederkehr der Spannungsversorgung zeigt die Codetastatur kurzzeitig „Keine Busverbindung “ bis der Normalbetrieb automatisch wieder hergestellt ist.

---

9. Wartung | Pflege

Die Sensorfläche des Fingerscanners ist aufgrund der immer wiederkehrenden Verwendung (Finger scannen) praktisch selbstreinigend. Falls der Fingerscanner trotzdem verschmutzt, reinigen Sie ihn mit einem feuchten (nicht nassen), nicht kratzenden Tuch. Geeignet sind 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 Zeit zu Zeit von Fingerabdrücken und Verschmutzungen mit einem feuchten (nicht nassen) und nicht kratzenden Tuch zu reinigen. Verwenden Sie hierbei nur reines Wasser ohne Reinigungsmittelzusätze.

Bei häufiger Nutzung pflegen Sie die Kontakte des SECURE*connect* 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!

10. Fehlersuche und -behebung

Anzeige und Behebung des Fehlers

Fingerscanner Anzeige		Ursache	Abhilfe
	Status-LED leuchtet rot.	Der Finger wurde nicht erkannt.	Ziehen Sie den Finger nochmals über den Sensor.
	Alle LEDs leuchten 1 Minute rot.	Systemsperre. Es wurde 10-mal hintereinander ein unbekannter Finger erkannt.	Warten Sie 1 Minute ab. Das System befindet sich dann im Normalbetrieb.
	Status-LED blinkt orange.	Keine Busverbindung zum SECURE*connect*|EK-Schloss.	Prüfen Sie die Verkabelung oder führen Sie einen Pairing-Reset durch.
	Status-LED blinkt rot/grün.	Der Sensor des Fingerscanners ist verschmutzt bzw. defekt.	Reinigen Sie den Sensor oder trocknen Sie ihn ab.

Codetastatur Anzeige		Ursache	Abhilfe
	Beide Status-LEDs leuchten rot.	Der Nutzercode wurde nicht erkannt.	Geben Sie den Nutzercode erneut ein.
		Der gewünschte Nutzercode besteht ausschließlich aus gleichen Ziffern, z. B. 1111, 3333	Verwenden Sie Nutzercodes mit verschiedenen Ziffern.
		Der gewünschte Nutzercode ist zu kurz bzw. zu lang, z.B: 321, 987654321	Beachten Sie die Länge des Nutzercodes: min. 4 Stellen, max. 8 Stellen.
		Bei der Eingabe von Menüpunkten bzw. Werten ist ein Fehler aufgetreten.	Wiederholen Sie die Eingabe.
	Status-LED leuchtet rechts rot	3-malige Eingabe eines falschen Nutzercodes. Systemsperre für 1 bzw. 15 Minuten.	Geben Sie zwei Mal einen berechtigten Nutzercode ein. Danach lässt sich die Tür vor Ablauf der Sperre mit einem berechtigten Nutzercode öffnen.
	Status-LEDs blinken abwechselnd gelb.	Keine Busverbindung zur Steuereinheit.	Prüfen Sie die Verkabelung oder nehmen Sie das Gerät in Betrieb.
		kein Pairing bzw. Pairing fehlerhaft.	Führen Sie einen Pairing-Reset aus (siehe Kapitel 2.2).

11. Instandhaltung | Ersatzteile

Das Produkt ist grundsätzlich wartungsfrei. 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 gesamte Stromversorgung 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 BKS-Service zu kontaktieren und ggf. nach Absprache das Gerät 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 keinerlei Haftungs-, Gewährleistungs- oder Serviceleistungsanspruch.

12. 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.

Der Fingerscanner und die Codetastatur sind als Elektronikschrott an öffentlichen Rücknahmestellen und Wertstoffhöfen zu entsorgen. Die Verpackung ist separat zu entsorgen.

Table of contents

Please hand this document over to the user!

1. Information and safety instructions

1.1 General note regarding theses instructions

Thank you for choosing the fingerprint scanner and code keypad as a detection unit for motor-driven or electromechanical exit devices.

These instructions contains important advice which must be followed in order to prevent hazard, to ensure the opening system's reliable functioning and long service life of the fingerprint scanner and code keypad, and to reduce downtimes and repair cost.

The operating instructions must be read and applied by every person who works with the fingerprint scanner or code keypad, e.g. during:

- Electrical installation
- Start-up, operation and maintenance

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

1.2 Safety instructions

These 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 building contractors and users in order to prevent false installation and improper usage. Therefore, this manual must be delivered to building contractors and end users.

- 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 refer to EN 50110-1, DIN VDE 0105 or IEC 60364) are charged with any work (planning, transport, assembly, installation, start-up, maintenance, repair, disassembly) on the equipment.
- It must be ensured that the documents for installation, start-up, operation, maintenance and repair of the equipment are made available to the specialists and that they observe them.
- 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 damage!

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 property damage.**
NOTE	**NOTE denotes a statement which is provided for information only.**

2. Product description

The fingerprint scanner and code keypad are detection units 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.

The access system consists of two electronic devices:

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

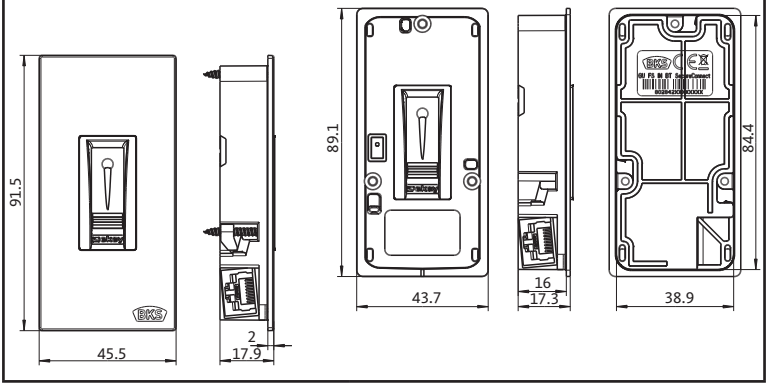
If the characteristics match, an encrypted transmission to the control unit opens the door. The system is primarily used to open house and apartment entrance doors and garage doors in the home and commercial sector.

2.1 Technical data

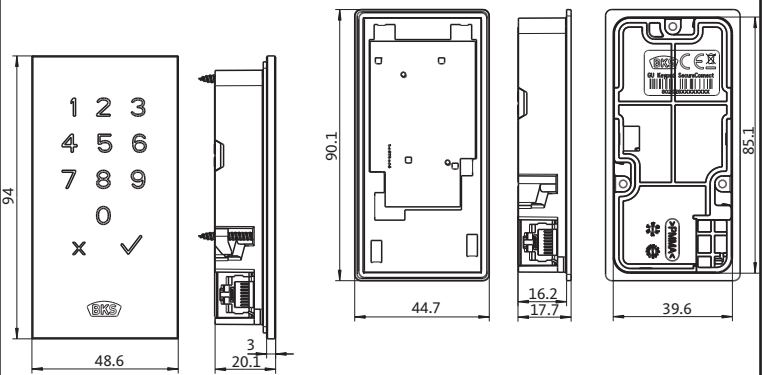
Voltage supply	8–24 V DC (max. 30 V)
Power consumption	< 1 W
Environmental conditions	°C +70 °C / –20 °C **IP54** (at the front)
Certifications	CE The certificates can be found at our website www.g-u.com.

Variant	B-55600-13-4-6
Memory	99 finger templates
Template identification duration	1–2 seconds
False rejection rate (FRR)	1:100

False acceptance rate (FAR)	1:10 000 000
Lifetime	Max. 10 million finger scans
Dimensions	



Variant	B-55600-10-4-6
Memory	99 user codes
PIN code length	4–8 digits
Dimensions	



2.2 Protection against manipulation

The detection unit (fingerprint scanner and code keypad) are generally installed externally (external door side). To prevent unauthorised access, your system is equipped with numerous security functions:

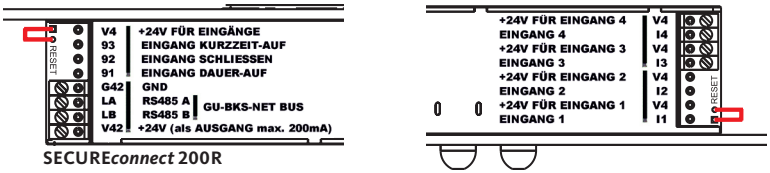
- The detection unit is connected to the control unit using a data cable. Data transmission is encrypted.
- The detection unit and the control unit are paired with each other during initial start-up.

With the fingerprint scanner, recording of the user finger and the modification of the system content is only possible if the master finger has already been detected by the system.

The code keypad records the PIN code with the capacitive keypad and compares the entered data with the stored reference codes. The code keypad can process PIN codes comprising 4 up to 8 digits. The PIN code must include at least one number different from the rest. There are two types of PIN codes. The master code for configuring the system and the user code for opening the door.

If you enter the code incorrectly 3 times, you will be locked out of the system for 1 minute. If you enter the code incorrectly 3 times again, you will be locked out for 15 minutes. Subsequently, you will be locked out for 15 minutes each time you enter the code incorrectly. The lock can be reversed before it is due to end by entering an authorised user code twice.

In order to exchange a component of the door system (SECURE*connect* 200R, SECURE*connect* 200F or detection unit), 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.

The terminal can then be removed.
The pairing process for the SECURE*connect* 200R, SECURE*connect* 200F and the detection unit (fingerprint scanner or code keypad) now restarts. The detection unit is reset to the factory setting (all saved finger templates and PIN codes are deleted).

If a fingerprint scanner and a code keypad are connected to an unpaired SECURE*connect* 200, the detection unit is reset to the factory settings and the finger templates and the PIN codes are deleted.

2.3 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. 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 SECURE*connect* 200 control unit is required to open the lock or electric strike.

2.4 Improper use

Any other use or use beyond the intended scope is not permitted and BKS 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.

- Operation of the access system with voltages greater than 24 V +10% DC is not permitted and could permanently damage the product.
- Incorrect polarity of connections.
- Unauthorised modifications have been made to the product.

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 dealer. Only install and commission products that are in perfect technical condition.

The delivery consists of the following products:

- Detection unit (fingerprint scanner or code keypad) with decorative element
- System cable of detection unit
- Instructions

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

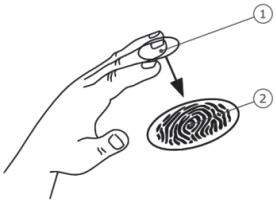
- Only store in dry, clean and moderately ventilated spaces indoors, and not outdoors
- The storage location must be free of movements and/or vibrations
- Temperature range of +15 °C to +40 °C, without strong temperature fluctuations
- Relative air humidity of 30% to 70%, non-condensing
- Do not expose the goods stored to aggressive media or sunlight
- 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 and vibrations.

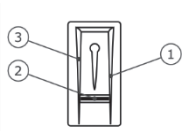
2.6 Function

Function of the fingerprint scanner

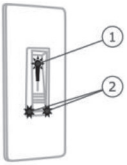
The fingerprint scanner records the fingerprint via a line sensor and evaluates it. It compares the image obtained with the biometric information stored in the reference fingerprint. If these correspond, the door opens.



The fingerprint scanner only works correctly and reliably with the papillary lines of the distal phalanx (1).
Drag the finger smoothly and evenly over the sensor as described below.



The finger guide on the fingerprint scanner serves to position the finger correctly. It is the underlying operating element and consists of the sensor (2) and the right (1) and left (3) guide edges.

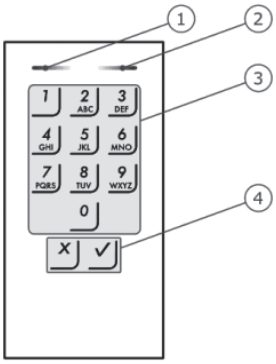


The fingerprint scanner features two different signals:

1 Status LED for the operating state

2 Functions LEDs for the function of the entire system

Function of the code keypad



2 status LEDs indicate the operating status (correct PIN code, incorrect PIN code, menu item etc.).

An acoustic signal transmitter indicates the keystrokes and when access is granted.

1 Left status LED

2 Right status LED

3 Input buttons

4 Confirmation buttons

The keypad backlight is blue, can be dimmed and switches on and off depending on the available light.

NOTE

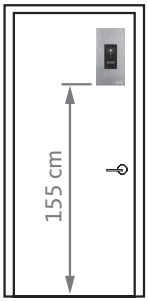
If no keys are pressed for a period of 10 seconds, the code keypad switches back to normal mode. Any data or changes entered are discarded.

3. Installation

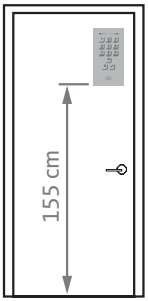
The fingerprint scanner and code keypad are generally installed externally (external door side) (see Section 3.5) and are connected to the control unit using a data cable. For connection use the BKS system cable.

3.1 Installation height

B-55600-13-4-6



B-55600-10-4-6

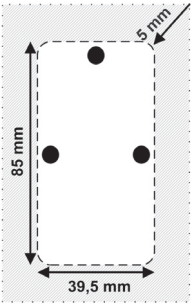


- The prescribed installation height for the fingerprint scanner is at least 155 cm or higher!

NOTE

The proper functioning can only be guaranteed if the fingerprint scanner is installed at the correct height!

3.2 Milling dimensions

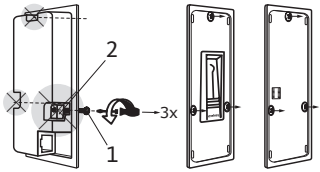


Make a milled recess to match the dimensions below in your door profile or in the timber door.

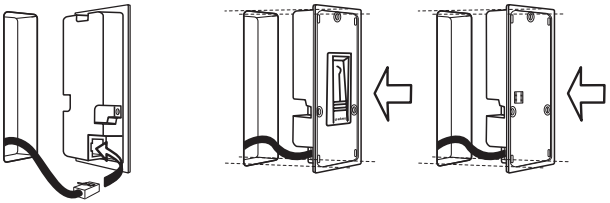
* recommended milling dimensions (may vary according to material), tolerance of ± 0.2 mm.

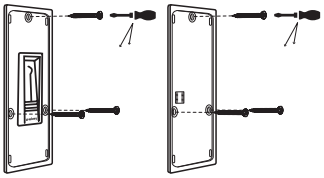
3.3 Fastening versions

3.3.1 Fastening in the timber door leaf

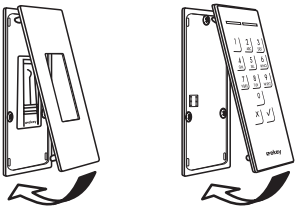


Take out the three screws (1) including the snap-pin noses (2).



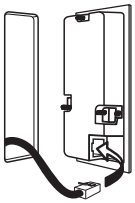


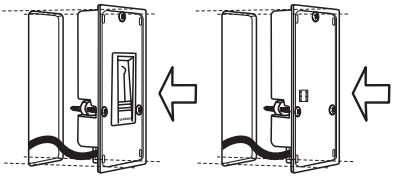
Please use the screws provided for fastening the fingerprint scanner in timber.

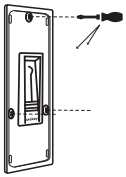


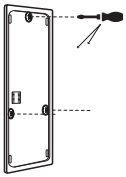
Finally, snap the decorative element, including gasket for outdoor use, into place.

3.3.2 Fastening in the profile, front panel, control panel



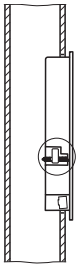


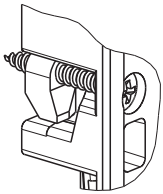


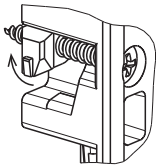


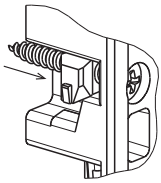
Tighten the screws with a screwdriver until the fingerprint scanner or the code keypad is secure.

Do not tighten too much, otherwise the housing may be destroyed.









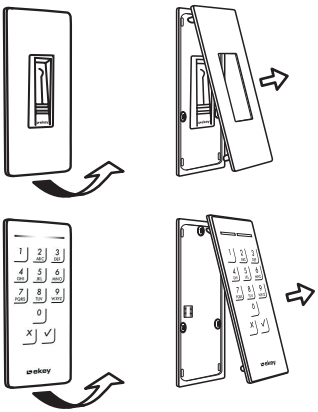
When the screws are tightened, the snap-in noses move outwards and snap the fingerprint scanner or code keypad into place in the profile and the front panel.

Finally, snap the decorative element, including gasket for outdoor use, into place.

3.4 Disassembly of the decorative element

ATTENTION

Be careful not to damage the surface of the door!
Carefully disassemble the decorative element.



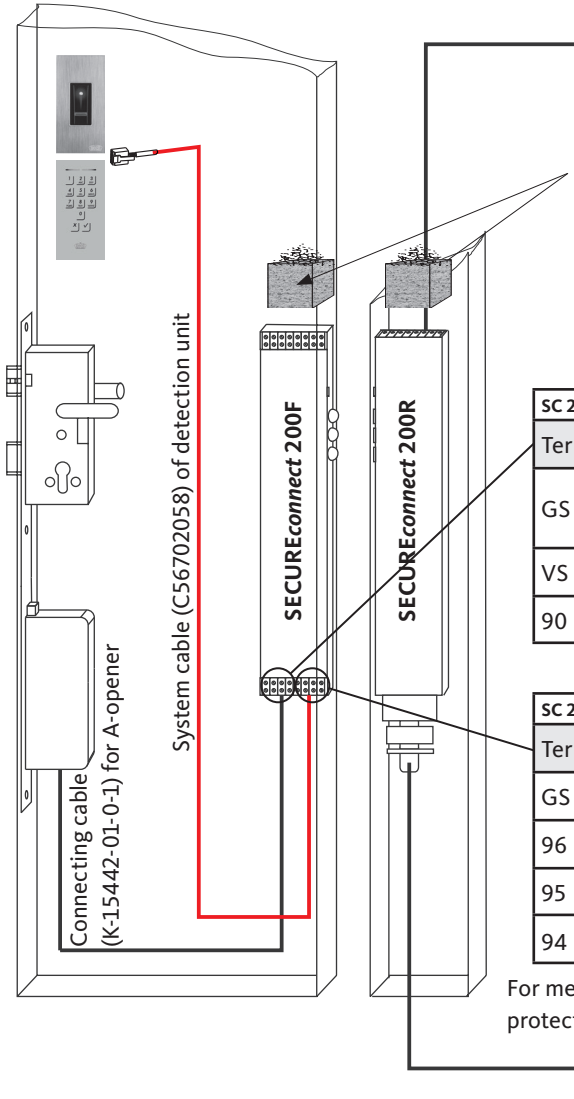
A notch is located on the underside of the decorative element.

Lift up the decorative element using a screwdriver, for example, until the locking catches are released.

Tilt the decorative element up slightly and pull it up at an angle.

Clean the gasket thoroughly and, if necessary, grease it before installation.

3.5 Wiring diagram for A-opener



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

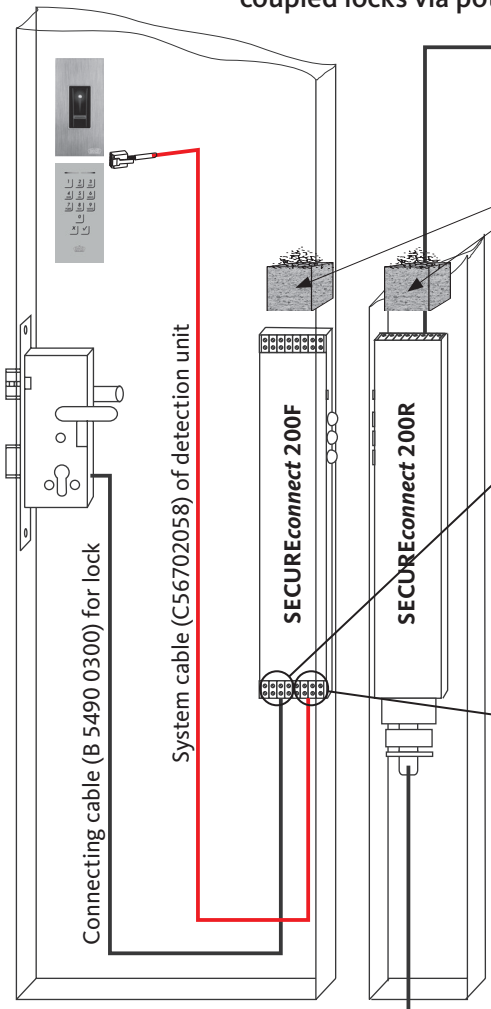
When installing the SECURE*connect* in aluminium profiles, we recommend using the provided foam pieces to prevent swarf interfering the function.

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

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

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

3.6 Wire 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.

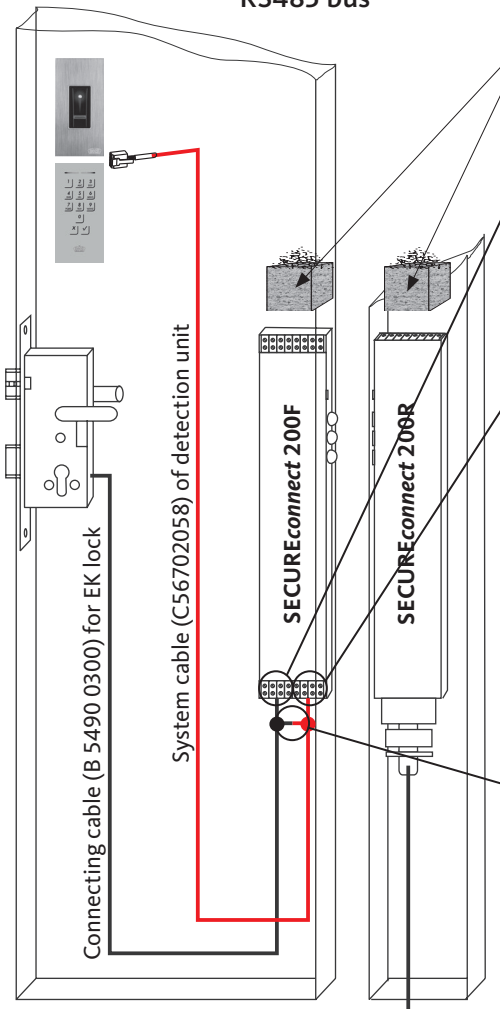
When installing the SECURE*connect* in aluminium profiles, we recommend using the provided foam pieces to prevent swarf interfering the function.

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 detection unit	
Terminal	Wire colour	Signal
GS	BN | Brown	GND (minus)
96	YE | Yellow	RS-485 A
95	GN | Green	RS-485 B
94	WH | White	24 V (plus)

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

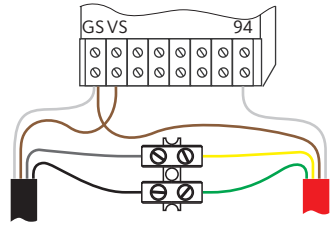
3.7 Wiring diagram for electrically coupled lock via RS485 bus



When installing the SECURE*connect* in aluminium profiles, we recommend using the provided foam pieces to prevent swarf interfering the function.

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

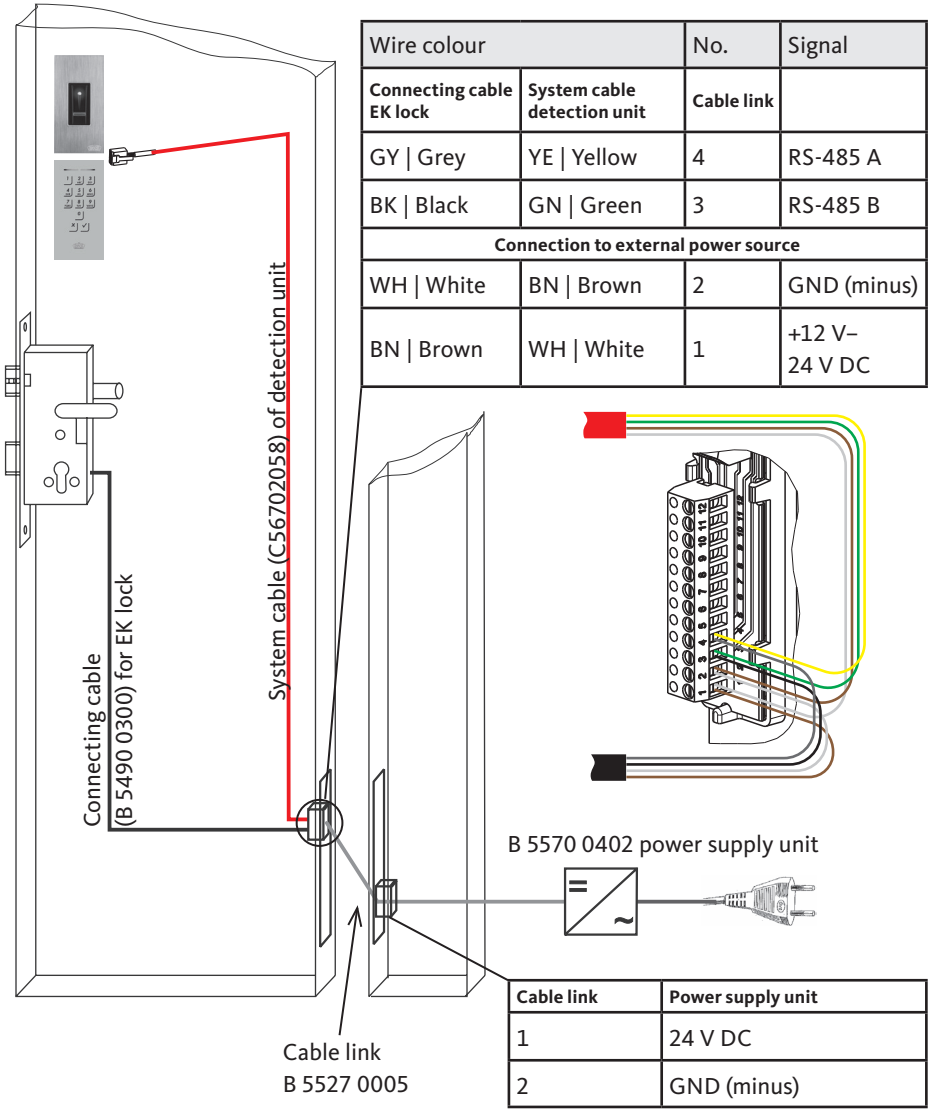
SC 200F	System cable for detection unit	
Terminal	Wire colour	Signal
GS	BN | Brown	GND (minus)
94	WH | White	24 V (plus)



Wire colour		Signal
Connecting cable EK lock	**System cable detection unit**	
GY | Grey	YE | Yellow	RS-485 A
BK | Black	GN | Green	RS-485 B

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

3.7.1 Connection to external power source



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

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

3.7.2 Pairing of fingerprint scanner/code keypad with EK lock

The detection unit and the control unit are automatically paired with each other via the RS485 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 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.

- Permanent actuation of the lever handle.
- Override the lock-bit sensor 3 times by unlocking and locking with a mechanical key.

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

4. Start-up

The devices must be brought into operation in order to use them. When the system is commissioned, the control unit couples with the detection unit. Follow these steps to commission your access system:

- Install the devices as described in Chapter 3.
- The electrical connection of the components is established as specified in the wiring diagram.

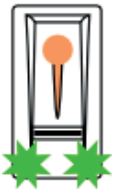
4.1 Start-up of fingerprint scanner

- Connect the power supply unit or SECURE*connect* to the mains voltage.
- When switched on for the first time, the fingerprint scanner and SECURE*connect* or the EK lock perform an automatic pairing. Once the pairing is complete, the blue LED flashes.

Finger scanner is not paired with SC200/EK lock.

Fingerprint scanner is paired with SC200/EK lock. No fingerprint stored.

Fingerprint scanner is connected to Bluetooth device.



Fingerprint scanner is paired with SC200/EK lock – admin menu.

4.1.1 Operating concept

Two different operating concepts exist:

- App – administration of the Bluetooth fingerprint scanner using a mobile device (Section 6.1, from page 80)
- Master finger – administration of fingerprint scanner via master finger (Section 6.3, from page 87)

4.1.2 Test mode

Connect the mains voltage and perform the test within the next 10 minutes. Once the 10 minutes have elapsed, this test can only be carried out following a power-on reset of the fingerprint scanner.

Fingerprint scanner is paired with SC200/ EK lock. No fingerprint stored.

Put a finger on the sensor for 3–5 seconds.

If you take the finger off, the relay (SECURE*connect* or EK lock) switches.

NOTE

A test can only be performed if a master finger has not yet been stored or if a mobile device has not yet been paired.

You can place your finger on the sensor for a maximum of 5 seconds. If you leave your finger on the sensor for longer, the relay (SECURE*connect* or EK lock) will not switch.

4.2 Start-up of code keypad

- When switched on for the first time, the code keypad and SECURE*connect* or the EK lock perform an automatic pairing. The status LEDs of the code keypad alternately flash yellow. Once the pairing is complete, no LED flashes.

Code keypad is not paired with SC200/ EK lock.

Code keypad is paired with SC200/EK lock.

ATTENTION

Change the default admin code 9999 immediately after start-up and keep it confidential!
If you do not change the admin code, unauthorised individuals will be able to access your admin menu and thus enter your house.

4.2.1 Visual signalling

Display	Left status LED	Right status LED	Meaning
	Off	Off	Standby
	Flashing yellow	Flashing yellow	Factory setting/no pairing with control unit
	Yellow	Off	Ready to enter the admin code
	Green	Off	Admin menu active
	Green	Green	Positive data entry: correct PIN code, correct input value etc.
	Red	Red	Negative data entry: incorrect PIN code, incorrect input value etc.
	Off	Red	System locked for 1 minute or 15 minutes

5. Operation of fingerprint scanner

Drag finger

Holding the finger straight, position it centrally between the guide edges. Do not turn it.

Place the joint of the distal phalanx directly on the sensor. Place the finger flat on the finger guidance.

Stretch out the fingers next to it.

Move the the finger evenly down over the sensor. Move the entire hand with the finger. For the best results, drag the distal phalanx completely over the sensor. The movement takes roughly 1 seconds.

General tips on how to obtain a good quality fingerprint

- The best results can be obtained using the index, middle or ring finger. The images obtained from scanning the thumb or little finger cannot be easily analysed.
- If fingers are often wet, store these when they are wet.
- The fingers of children aged around 5 years or older will work.

Finger touch

Touch the sensor briefly and quickly with the finger.

6. Programming the fingerprint scanner

6.1 Programming with the open biometric app

The fingerprint scanner must be paired with the SECURE*connect* to be able to start programming.

NOTE

The open biometric app can only be used in combination with the Bluetooth fingerprint scanner.

The open biometric app is used for programming of the system. The app can also be used to open doors.

6.1.1 Downloading the app

The app is available for Apple iOS and Google Android. Download the open biometric app from the App Store or Google Play. To find the app, enter the search term "open biometric".

Download on the App Store

GET IT ON Google Play

To pair the device for the first time, you need the device coupling code and the app security code. **The default code in both cases is 9999.**

- Start the open biometric app.
- Touch the input surface (Android) or press "Search" (iOS). The app searches for available Bluetooth devices.
- Select your Bluetooth fingerprint scanner (the last 4 digits of the serial number are displayed).

- Android only: press "Log in".
- Enter the **default device coupling code 9999**.
- Click on "Next". The mobile device is paired with the Bluetooth fingerprint scanner.

- Enter a new 6-digit device coupling code. For security reasons, you must change the default device coupling code when pairing the system for the first time. Make a note of this you will need it to pair further mobile devices.

  Your device coupling code:

- Press "Change“ (Android) or "Next" (iOS).
- Enter the default app security code 9999.
- Click on "Next".

The Bluetooth fingerprint scanner has been paired with the mobile device. The system is in normal mode.

You can now program and administer the fingerprint scanner access system with the open biometric app.

NOTE

All you need now to administer your Bluetooth fingerprint scanner is the intuitive open biometric app.
Touch the required functions in the app and follow the instructions on the display.

6.1.2 Changing security code

You can change all security codes at any time:

- App security code
- Admin coupling code
- User coupling code

NOTE

The 4 to 6-digit app security code is required for the app security question. You can deactivate the request for the app security code under "ADMINISTRATION" if your mobile device is equipped with secured locking mechanisms (fingerprint, code, etc.).

- Select "ADMINISTRATION".
- Select "CHANGE SECURITY CODES".
- Change the required code.
- Press "Change“ (Android) or "Done" (iOS).

The selected security code was changed.

6.1.3 Storing the finger prints

You can store the master and user finger using the open biometric app.

- Select "ADMINISTRATION".
- Select "USER ADMINISTRATION“.
- Press  (Android) or "+" (iOS).
- Enter the user name.
- Press "New admin authorisation“ or "New access authorisation".
- Select the relay to be switched (for the next connected SECURE*connect* or EK lock).
- Select a finger.
- Press "Store".
- Read the note and press "Start".
- Once your finger has been successfully registered, press "OK".
- Press "Done".

NOTE **Store at least one fingerprint on each hand per access point.**

6.1.4 Disabling Bluetooth

You can disable the Bluetooth functionality.
The Bluetooth functionality is active by default.

- Start the open biometric app.
- Select "ADMINISTRATION".
- Select "SYSTEM STATUS“ off.
- Under "BLUETOOTH SETTINGS", activate "Deactivate Bluetooth after 15 minutes".

With this setting, Bluetooth is deactivated at the fingerprint scanner after 15 minutes in one of the following cases:

- no mobile device was connected
- at least one finger was stored

You can reactivate Bluetooth: select the admin menu and drag any finger over the sensor.

6.1.5 Pairing further mobile devices

You can pair additional mobile devices with the Bluetooth fingerprint scanner using your chosen 6-digit admin or user coupling code.

- Start the open biometric app.
- Pair the mobile device with the Bluetooth fingerprint scanner and use your chosen 6-digit admin or user coupling code.
- The Bluetooth fingerprint scanner is paired with the mobile device.

You can now program and administer the fingerprint scanner with the app.

6.1.6 Using several Bluetooth fingerprint scanners

The open biometric app allows several Bluetooth fingerprint scanners to be used. To switch between two Bluetooth fingerprint scanners, you must reset the pairing between the Bluetooth fingerprint scanner and mobile device.

NOTE

When the pairing is reset, the stored relay names (SECURE*connect* or EK lock) and user images are deleted. The user names and authorisations are stored in the memory of the Bluetooth fingerprint scanner.

- Start the open biometric app.
- Select "ADMINISTRATION".
- Select "RESET PAIRING“.
- Select "Continue" to confirm the reset.

The pairing between the Bluetooth fingerprint scanner and mobile device is now reset. You can now pair another Bluetooth fingerprint scanner.

6.2 Storing the user coupling code

You can store a user coupling code. You can pass on this code to a person of your choice. The following actions can be performed with this code:

- Open the door.
- Activate or deactivate app security code.
- Change app security code.
- Reset pairing between Bluetooth fingerprint scanner and mobile device.

Follow these steps to save the user coupling code:

- Start the open biometric app.
- Select "ADMINISTRATION".
- Select "CHANGE SECURITY CODES".
- Enter the required user coupling code in the respective field.
- Confirm your entries with "Change" (Android) or "Done" (iOS).

The user coupling code is now stored.

6.2.1 Resetting the app security code

- Start the open biometric app.
- Enter an incorrect app security code.
- Confirm your entry with "Next".
- Select "RESET PAIRING“.
- Select "Continue" to confirm the reset.

The pairing between the Bluetooth fingerprint scanner and mobile device is reset and the app security code is set to 9999.

You can now pair the Bluetooth fingerprint scanner again and assign a new app security code.

6.2.2 Protecting the system against loss of the mobile device

If you have lost your mobile device, you can change the admin or user coupling code using a second mobile device. You can use the new admin or user coupling code to prevent a connection from being established with the lost mobile device.

- Start the open biometric app at the second mobile device.
- Pair the second mobile device with the Bluetooth fingerprint scanner.

- Select "ADMINISTRATION".
- Select "CHANGE SECURITY CODES".
- Enter a new 6-digit admin or user coupling code.
- Confirm your entry with "Change" (Android) or "Done" (iOS).

The admin or user coupling code is changed in the system.

The lost mobile device can no longer establish a connection with the Bluetooth fingerprint scanner. Your system is safe from access by unauthorised persons.

6.2.3 Resetting the system to factory settings

- Start the open biometric app.
- Connect to the Bluetooth fingerprint scanner.
- Select "ADMINISTRATION".
- Select "RESET SYSTEM".
- Select "Continue" to confirm the reset.

The system factory setting is restored. You can now bring the system back into operation.

NOTE

All user and master fingers are deleted!
The pairing between the fingerprint scanner and SECURE*connect* 200 or the EK lock is maintained!

The factory settings of the fingerprint scanner can also be restored by re-pairing the SECURE*connect* 200.

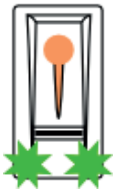
6.3 Programming with master finger

6.3.1 Storing the master finger

The master fingers are used for programming the system. To start with, store 4 different master fingers. Every finger must be **scanned at least 3 times**. We recommend storing two fingers of 2 different people.

Fingerprint scanner is paired with SC200/EK lock. No finger stored.

Three finger touches within 5 seconds.



Admin mode is active.

Drag the first master finger over the sensor.

The fingerprint has been detected.

The system is ready to retry.

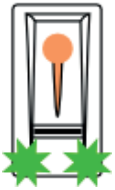
Drag the first master finger across the sensor again.

The fingerprint has been detected.

The system is ready to retry.

Drag the first master finger across the sensor again.

The quality of the three scans is very good.



The fingerprint scanner is ready to record the next master finger.

Further possible displays during the saving process:

Quality of the scan is sufficient.
The quality could be improved by carrying out further scans.

An error occurred during the scanning operation or the quality is insufficient.
Drag this finger over the sensor once again.

NOTE

If the fingerprint scanner is restarted when in admin mode and fewer than 4 master fingers exist, all master fingers that have already been stored are deleted.

When storing the finger, no more than 10 seconds can elapse between the individual finger scans. Otherwise the fingerprint storing operation will be aborted.

6.3.2 Storing the user finger

You can open a door with user fingers. All fingers which are not master fingers can be used as user fingers.

Normal mode

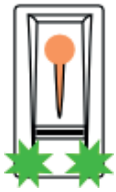
Three finger touches within 5 seconds.

Admin menu

Drag any master finger over the sensor.

Master finger has been detected. Saving mode active.

One finger touch within 5 seconds.



Recording mode is active.

Drag the finger to be stored over the sensor.

The finger-print has been detected.

The system is ready to retry.

Drag the finger to be stored over the sensor.

The finger-print has been detected.

The system is ready to retry.

Drag the finger to be stored over the sensor.

The fingerprint has been detected.

The fingerprint has been stored successfully.

After storing the user finger: normal mode.

6.3.3 Deleting the user finger

Individual user fingers can only be deleted if this user is present.

Normal mode

Three finger touches within 5 seconds.

Admin menu

Drag any master finger over the sensor.

Master finger detected. Saving mode active.

Wait 5 seconds!

Deletion mode active

1 finger touch

Administration menu

Drag the finger to be deleted over the sensor.

User finger deleted!

Normal mode

6.3.4 Deleting all user fingers

All user fingers stored in the system are deleted. The master fingers remain stored in the system.

Normal mode

Three finger touches within 5 seconds.

Admin menu

Drag any master finger over the sensor.

Master finger detected. Saving mode active.

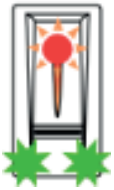
Wait 5 seconds!

Deletion mode active.

1 finger touch

Administration menu

Rescan the same master finger as shown above.



All user fingers deleted!

Normal mode

NOTE **Check any user finger. You are no longer able to obtain release!**

6.3.5 Resetting fingerprint scanner to factory settings

The fingerprint scanner is reset to the delivery condition as described below.

NOTE

All user fingers and master fingers are deleted! The pairing between the fingerprint scanner and SECURE*connect* 200 or the EK lock is maintained!

The factory settings of the fingerprint scanner can also be restored by re-pairing the SECURE*connect* 200 or the EK lock.

Normal mode

Three finger touches within 5 seconds.

Admin menu

Drag any master finger over the sensor.

Master finger detected. Saving mode active.

Wait 5 seconds!

Deletion mode active.

1 finger touch

Administration menu

Scan a different master finger to the previous one.

All user and master fingers deleted!

Fingerprint scanner is paired with SC200/EK lock. No fingerprint stored.

7. Programming of code keypad

A number of different menu items are provided in the admin menu for programming the device. They can be accessed using the buttons.

Button	Menu item
1	Save user code
2 ABC	Delete user code
3 DEF	Change admin code
4 GHI	Reset the system to factory settings
5 JKL	Set code keypad

7.1 Changing admin code

This function allows you to change the existing admin code. The admin code can have 4 to 8 digits and must contain at least one different digit. Use the admin menu to change the admin code. Enter the admin code to access the admin menu.

NOTE **Admin codes cannot be used as user codes.**

Press √ to start entering the admin code.

Enter the admin code (default = 9999).

√

3

√

Enter the old admin code.

√

Enter the new admin code.

√

Enter the new admin code again.

√

7.2 Storing the user code

The system allows a maximum of 99 user codes to be stored. A user code is a PIN code used to trigger a particular action in the control unit, e.g. opening a door. The user code can have 4 to 8 digits and must contain at least one different digit.

NOTE

Use long user codes. Use as many different digits as possible. Use different codes for the authorised users.

Press √ to start entering the admin code.

Enter the admin code.

√

1

√

Enter the user code.

√

Enter the user code again.

√

7.3 Deleting the user code

You can delete individual user codes. To do so, you will need the user code to be deleted.

Use the admin menu to delete a user code. Enter the admin code to access the admin menu.

Press √ to start entering the admin code.

Enter the admin code.

√

2

√

Enter the user code to be deleted.

√

7.4 Resetting the system to factory settings

The code keypad is reset to the factory setting. All user codes will be permanently deleted. The admin code is reset to factory setting 9999, the brightness threshold to 10% and the brightness value to 100%. The acoustic and visual signalling for the keystrokes and the acoustic signal for opening the door is switched on.

Carrying out a re-pairing procedure (see Section 2.2) will also reset the code keypad to the factory setting.

Press √ to start entering the admin code.

Enter the admin code.

√

4

√

Enter the admin code.

√

7.5 Setting the automatic backlight

Define the brightness threshold at which the blue backlight is automatically switched on during twilight hours here.

The brightness threshold can be set using percentage values. The brightness threshold is set to 10% by default. Enter the required percentage:

0 = automatic backlight from
1 to 100 = threshold switch-on range from very bright conditions to only in very dark conditions

Press √ to start entering the admin code.

Enter the admin code.

√

51

Desired brightness threshold value, e.g. 70.

√

7.6 Setting the backlight brightness

The backlight brightness can be set using 4 predefined modes. The backlight brightness is set to 100% by default. Enter the number for the required mode:

0 = Backlight brightness off
1 = Backlight brightness 33% on
2 = Backlight brightness 66% on
3 = Backlight brightness 100% on

Use the admin menu to set the backlight brightness. Enter the admin code to access the admin menu.

Press √ to start entering the admin code.

Enter the admin code.

√

52

Enter the number for the required mode, e.g. 2.

√

7.7 Setting the signalling for the keystrokes

The acoustic and visual signalling for the keystrokes can be set using four predefined modes. The acoustic and visual signals for the keystrokes are switched on by default. Enter the number for the required mode:

0 = Acoustic and visual signals off
1 = Acoustic signals on and visual signals off
2 = Acoustic signals off and visual signals on
3 = Acoustic and visual signals on

The admin menu is required to adjust the signalling of the key press. Enter the admin code to access the admin menu.

Press √ to start entering the admin code.

Enter the admin code.

√

54

Enter the number for the required mode, e.g. 2.

√

7.8 Setting the acoustic signal when opening

The acoustic signal, when opening the door, can be switched on or off. The acoustic signal is switched on by default. Enter the number for the required mode:

0 for switched off
1 for switched on

Use the admin menu to set the acoustic signal when opening the door. Enter the admin code to access the admin menu.

Press √ to start entering the admin code.

Enter the admin code.

√

55

Enter the number for the required mode, e.g. 0.

√

8. Door opening

The door can be opened with the open biometric app, fingerprint scanner or the code keypad.

8.1 Door opening with open biometric app

The system is in normal mode.

- Start the open biometric app. The mobile device connects to the Bluetooth fingerprint scanner.
- Select "ACCESSES".
- Slide the slider of the access to be opened to the right.

The SECURE*connect* then sends a control signal to the A-opener and the motor-driven lock and your door will open. The EK lock receives the control signal directly.

8.2 Door opening with the fingerprint scanner

Normal mode

Drag a user or master finger that has already been stored over the sensor.

The finger has been detected successfully.

After door opening: normal mode.

NOTE

When using the fingerprint scanner with an SECURE*connect* 200 and you open your door for longer than 12 seconds, the finger scanner will switch to idle mode. Once the door has been closed and the voltage supply has been restored, the fingerprint scanner will briefly display the following message: "No bus connection", until normal mode is automatically re-established.

8.3 Door opening with code keypad

Enter a stored user code.

Press √ and the door opens.

The user code has not been detected.

NOTE

If you enter the code incorrectly three times, the system is blocked for 1 minute. If you enter the code incorrectly 3 times again, the system is blocked for a further 15 minutes. Subsequently, the system will be blocked for 15 minutes each time you enter the code incorrectly.
The lock can be reversed prematurely by entering an authorised user code twice. No signalling is activated in this case.

NOTE

When using the code keypad with an SECURE*connect* 200 and you open your door for longer than 12 seconds, the finger scanner will switch to idle mode.
Once the door has been closed and the voltage supply has been restored, the code keypad will briefly display the following message: "No bus connection", until normal mode is automatically re-established.

9. Maintenance and care

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 a damp (not wet), non-scratching cloth. Cotton buds, microfibre cloths and glasses cloths are suitable. 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 from time to time using a soft, damp (not wet) cloth. Use clean water with no cleaning additives.

If frequently used, apply contact grease B-55606-00-4-0 to the contacts of the *SECUREconnect*.

The operational availability of the exit device 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!

10. Troubleshooting and elimination of error

Display and elimination of error

Fingerprint scanner Display		Cause	Remedy
	Status LED lights up red.	The finger has not been detected.	Drag the finger over the sensor once again.
	All LEDs light up red for 1 minute.	System is locked. An unknown finger was detected 10 times in a row.	Wait for 1 minute. The system then reverts to normal mode.
	Status LED flashes orange.	No bus connection with SC200/ EK lock.	Check the wiring or perform a pairing reset.
	Status LED flashes red/ green.	The sensor of the fingerprint scanner is soiled or defective.	Clean or dry off the sensor.

Code keypad Display		Cause	Remedy
	Both status LEDs light up red.	The user code has not been detected.	Enter the user code again.
		The required user code consists only of identical digits, e.g. 1111, 3333.	Use a user code with at least one different digit.
		The required user code is too short or too long, e.g 321, 987654321.	Note the of the user code: min. 4 digits, max. 8 digits.
		An error occurred when selecting menu items or entering values.	Repeat your entry.
	Right status LED lights up red	You have entered an incorrect user code 3 times. The system is blocked for 1 minute or 15 minutes.	Enter an authorised user code twice. The door can then be opened before the lock is due to end by entering an authorised user code again.
	The status LEDs flash alternately yellow.	No bus connection to the control unit.	Check the wiring or bring the device into operation.
		No pairing or incorrect pairing.	Perform a pairing reset (see Section 2.2).

11. Maintenance and spare parts

The product is maintenance-free. 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!

Fully disconnect the power supply and discharge stored residual energy.

Repair work must only be carried out by experts trained and authorised by the manufacturer.

If a service is due, before carrying out repairs on-site we recommend contacting BKS Service in order to have the unit sent in if necessary.

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

If replacement parts or extensions are required, orignial parts may be used exclusively. If other than original products are used, all product liability, warranty, and service claims will expire.

12. Disposal

NOTE

The product 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 disused fingerprint scanner and code keypad must be disposed of as electronic waste at special waste disposal sites. Packaging must be disposed of separately.

Table des matières

Remettre 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 unité de saisie 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 du lecteur d'empreintes digitales ou du clavier à code.

La notice d'utilisation doit être lue et employée par chaque personne amenée à manipuler le lecteur d'empreintes digitales ou le clavier à code, p. ex. lors :

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

Une fois le montage effectué, la notice d'utilisation doit être remise à l'exploitant. Lire attentivement cette notice avant la première utilisation de l'appareil et la conserver précieusement pour tout usage ultérieur. Préciser à tous les exploitants/les responsables 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 et de ferrures et également formé sur le montage, la mise en service et le maniement de ce produit.

Les installateurs d'ouvrages ou utilisateurs doivent également respecter ces informations pour éviter un mauvais montage ou de fausses manœuvres. Cette notice doit donc être remise aux installateurs d'ouvrages et aux utilisateurs.

- 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 moyens d'exploitation.
- 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 moyen d'exploitation se trouvent à 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 évitée.**
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 unités de saisie 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.

Votre système d'accès est composé de deux appareils électroniques :

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

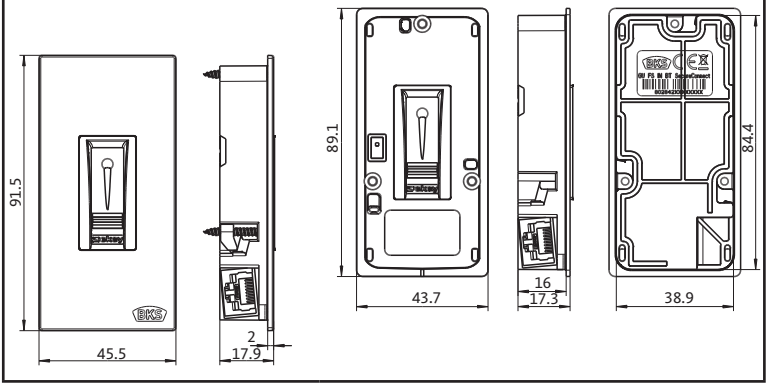
Lorsque les caractéristiques concordent, une transmission cryptée à l'unité de commande entraîne l'ouverture de la porte. Le système est destiné en premier lieu à l'ouverture de portes d'entrée, de portes d'appartement et de portes de garage dans le domaine privé et commercial.

2.1 Caractéristiques techniques

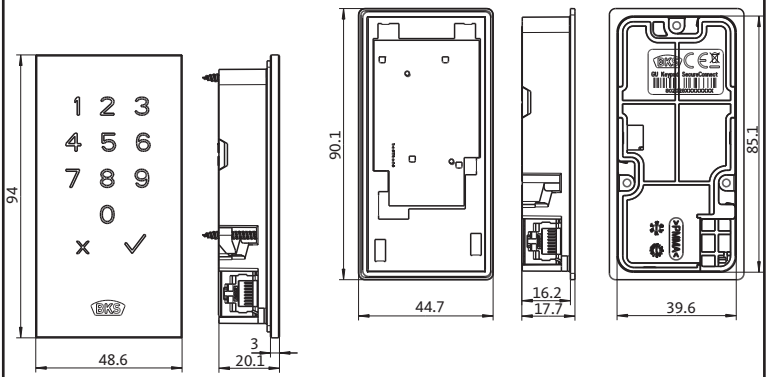
Tension d'alimentation	8–24 V CC (max. 30 V)
Puissance absorbée	< 1 W
Conditions environnantes	+ 70 °C – 20 °C IP54 (face devant)
Certifications	CE Vous trouverez les certificats sur notre site web www.g-u.com.

Variante	B-55600-13-4-6
Mémoire	99 modèles d'empreintes
Durée d'identification d'empreintes digitales	1 à 2 secondes
Taux de faux rejets (TFR)	1:100

Taux de fausses acceptations (TFA)	1:10.000.000
Durée de vie	Max. 10 millions de lectures d'empreintes digitales
Dimensions	



Variante	B-55600-10-4-6
Mémoire	99 codes utilisateurs
Longueur du code PIN	4 à 8 positions
Dimensions	



2.2 Protection contre les manipulations

L'unité de saisie (lecteur d'empreintes digitales ou 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 :

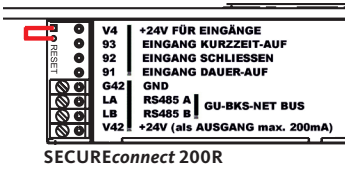
- L'unité de saisie est reliée à l'unité de commande par un câble de données. La transmission des données est cryptée.
- L'unité de saisie et l'unité de commande sont couplées entre elles de manière univoque lors de la première mise en service (appairage).

L'acceptation des empreintes utilisateurs et la modification des contenus du système ne sont possibles qu'avec identification préalable d'une empreinte maître.

Le clavier à code saisit le code PIN par la zone des touches capacitives. Il compare le code entré avec le code de référence mémorisé. Le clavier à code traite des codes PIN de 4 à 8 positions. Le code PIN doit contenir au moins deux chiffres différents. Il existe deux types de codes PIN. Le code administrateur pour la configuration du système et le code utilisateur pour l'ouverture de la porte.

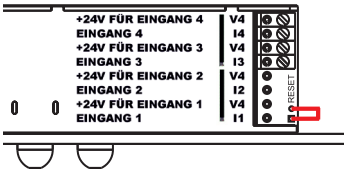
Après 3 entrées erronées consécutives a lieu un blocage de 1 minute. Après 3 autres entrées erronées consécutives a lieu un blocage de 15 minutes. Chaque nouvelle entrée erronée donne lieu à un blocage de 15 minutes. L'entrée à deux reprises d'un code utilisateur autorisé permet de mettre fin prématurément au blocage.

Pour remplacer un composant (SECURE*connect* 200R, SECURE*connect* 200F ou unité de saisie) du système de porte, une procédure de ré-appairage doit être effectuée sur les deux moitiés du SECURE*connect*.



SECURE*connect* 200R

SECURE*connect* 200F



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.

La pince peut ensuite être retirée. Le SECURE*connect* 200R, le SECURE*connect* 200F et l'unité de saisie (lecteur d'empreintes digitales ou clavier à code) entament alors une nouvelle procédure d'appairage. L'unité de saisie est remise à la configuration d'usine (tous les modèles d'empreintes et les codes PIN sont effacés).

Si un lecteur d'empreintes digitales ou un clavier à code est raccordé à un SECURE*connect* 200 non appairé, l'unité de saisie est remise à la configuration d'usine et les modèles d'empreintes et les codes PIN sont effacés.

2.3 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. Notre produit a été conçu dans ce but et toute utilisation excédant ce cadre n'est pas autorisée.

Le lecteur d'empreintes digitales et le clavier à code 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 SECURE*connect* 200 en tant qu'unité de commande est nécessaire pour déverrouiller la serrure ou la gâche électrique.

2.4 Utilisation non conforme

Une utilisation autre ou excédant ce cadre n'est pas autorisée et BKS 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 les modifications effectuées en propre sur le produit sont interdites.

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

- L'exploitation du système d'accès à des tensions supérieures à 24 V + 10 % CC n'est pas admissible et peut entraîner une dégradation durable du produit.
- Erreur de polarité des branchements.
- Modifications non autorisées effectuées sur le produit.

2.5 Contenu de la livraison, transport et stockage

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

La livraison est composée des articles suivants :

- Unité de saisie (lecteur d'empreintes digitales ou clavier à code) avec élément décoratif
- Câble d'interconnexion avec l'unité de saisie
- Instructions

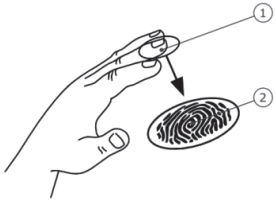
Stockez toujours le produit dans son emballage d'origine et dans les conditions suivantes :

- Stockage uniquement dans des pièces intérieures sèches, propres et modérément ventilées, pas en extérieur
- Stockage sans mouvements et/ou vibrations
- Plage de température de + 15 °C à + 40 °C, sans variations importantes
- Humidité relative de l'air de 30 % à 70 %, sans condensation
- Ne pas soumettre les produits stockés à des milieux agressifs et les protéger des rayons du soleil
- Effectuez régulièrement une inspection de l'état général en cas de stockage prolongé

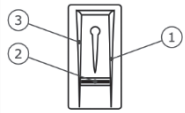
Transportez le produit uniquement dans son emballage d'origine. Prévoyez lors du transport une sécurité contre la chute de même qu'une protection contre l'humidité. Les chocs violents et les vibrations doivent également être évités.

2.6 Fonctionnement

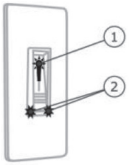
Fonctionnement du lecteur d'empreintes digitales
Le lecteur d'empreintes digitales enregistre l'empreinte grâce à un capteur linéaire et analyse celle-ci. Il compare le résultat avec les informations biométriques enregistrées dans l'empreinte de référence. Si les informations correspondent, la porte s'ouvre.



Le lecteur d'empreintes digitales ne peut fonctionner correctement et avec fiabilité qu'en se basant sur les crêtes papillaires de la première phalange du doigt (1). Déplacez le doigt lentement et régulièrement sur le capteur comme décrit ci-dessous.



Un guidage sur le lecteur d'empreintes digitales permet de positionner correctement le doigt. Il représente en fait l'élément de réglage et se compose du capteur (2), et des arêtes de guidage droite (1) et gauche (3).

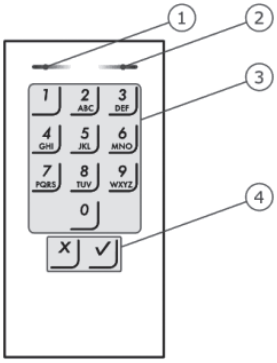


Le lecteur d'empreintes digitales émet deux types de signaux optiques :

1 LED de statut pour l'état de service

2 LED de fonction pour le fonctionnement du système dans son ensemble

Fonctionnement du clavier à code



Deux LED de statut indiquent les états de services (code PIN correct, code PIN erroné, point de menu...).

Un émetteur acoustique signale la pression des touches et l'autorisation d'accès.

1 LED de statut de gauche

2 LED de statut de droite

3 Touches d'entrée

4 Touches de confirmation

Le rétroéclairage de la zone de touches est bleu, à luminosité variable et s'active/se désactive en fonction de la lumière ambiante.

REMARQUE

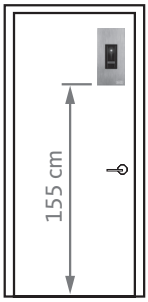
Le clavier à code revient en mode de fonctionnement normal au bout de 10 secondes quand aucune touche n'est actionnée. Les entrées et modifications sont alors rejetées.

3. Montage

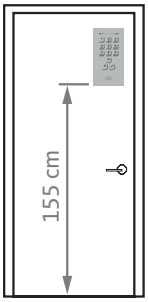
Le lecteur d'empreintes digitales est en général monté à l'extérieur (face extérieure de la porte) (voir la Section 3.6) et est relié à l'unité de commande par un câble de données. Utilisez le câble d'interconnexion BKS pour le branchement.

3.1 Hauteur de montage

B-55600-13-4-6



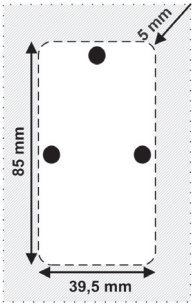
B-55600-10-4-6



- La hauteur de montage prescrite pour le lecteur d'empreintes digitales ou le clavier à code est d'au moins 155 cm ou plus !

REMARQUE **Seul un montage à la bonne hauteur garantit un fonctionnement irréprochable !**

3.2 Cotes de fraisage

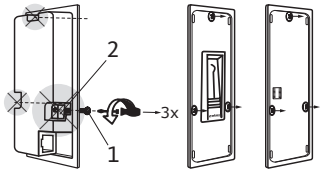


Pratiquez dans le profil de la porte ou dans la porte en bois un fraisage correspondant aux cotes ci-dessous.

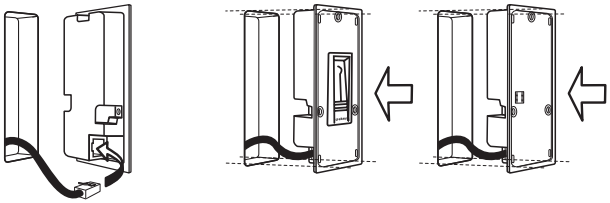
* Cotes de fraisage recommandées (peuvent varier en fonction du matériau), tolérance ± 0,2 mm.

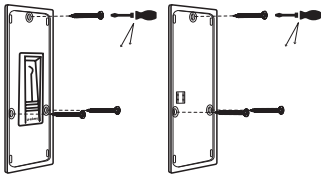
3.3 Variantes de fixation

3.3.1 Fixation dans le vantail de porte en bois

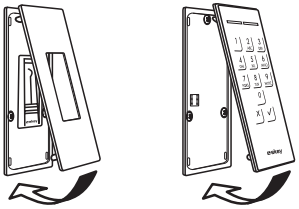


Retirez les trois vis (1) avec les pattes de serrage (2).



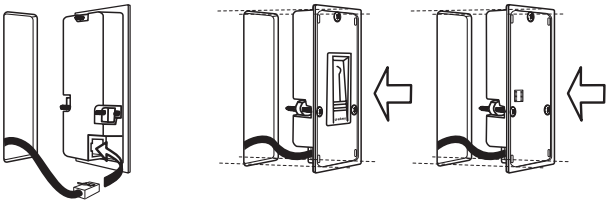


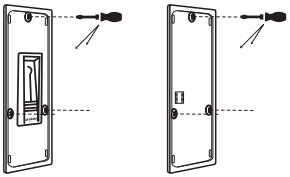
Utilisez les vis fournies pour la fixation en bois.



Pour terminer, faire s'encliqueter la plaque d'habillage
avec joint d'étanchéité pour usage en extérieur.

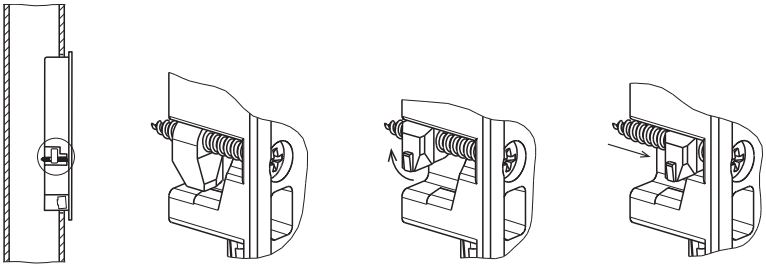
3.3.2 Fixation dans le profil, la plaque frontale, le tableau de commande



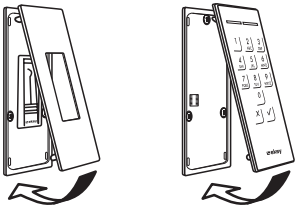


Serrez les vis avec un tournevis jusqu'à ce que le lecteur d'empreintes digitales ou le clavier à code soit bien fixé.

Ne pas serrez trop fort pour ne pas endommager le boîtier.



Le serrage des vis fait sortir les pattes de serrage qui fixent le lecteur d'empreintes digitales ou le clavier à code dans le profil ou dans la plaque frontale.

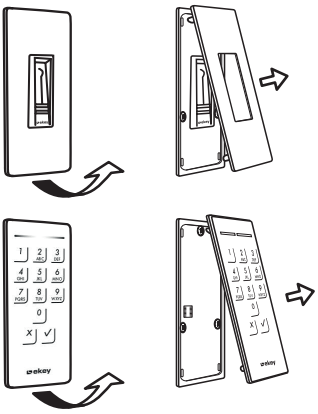


Pour terminer, faites s'encliqueter la plaque d'habillage
avec joint d'étanchéité pour usage en extérieur.

3.4 Démontage de la plaque d'habillage

ATTENTION

Attention : n'endommagez pas la surface de la porte !
Démontez la plaque d'habillage avec précaution.



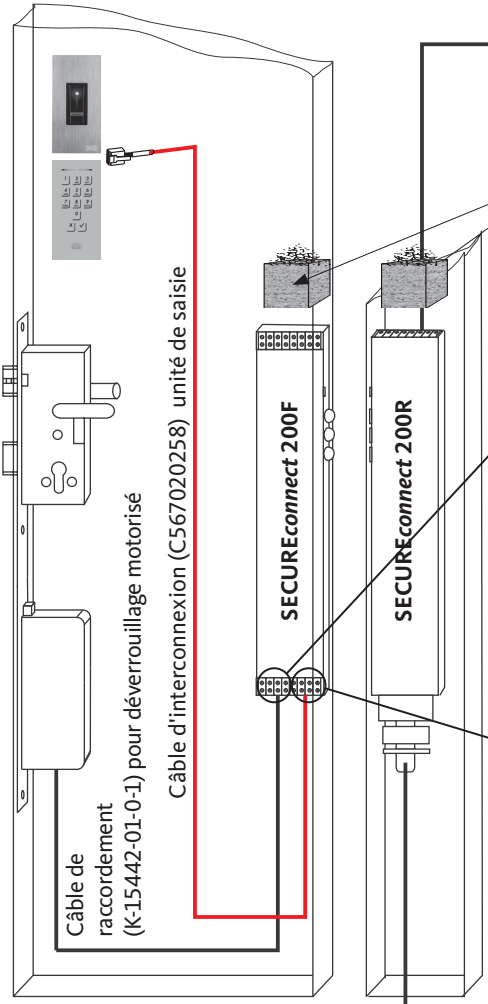
Sur la face inférieure de la plaque d'habillage se trouve une entaille.

Soulevez par là la plaque d'habillage, p. ex. avec un tournevis, jusqu'à ce que les pattes d'arrêt soient dégagées.

Soulevez légèrement vers le haut la plaque d'habillage et retirez-la inclinée vers le haut.

Nettoyez minutieusement le joint et graissez-le si nécessaire avant le montage.

3.5 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.

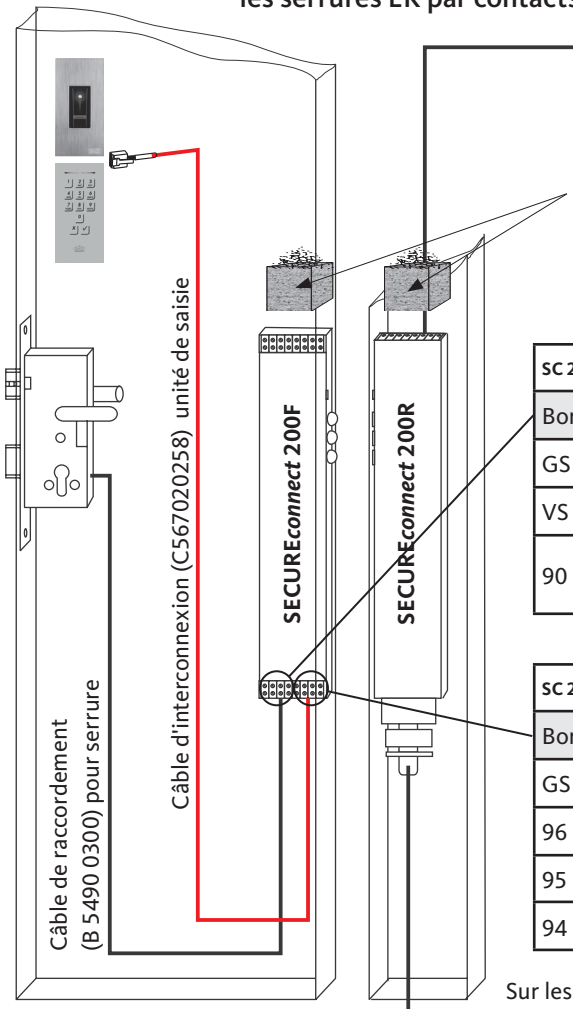
Utilisez les joints fournis comme protection contre les copeaux lors du montage dans des profilés métalliques.

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

SC 200F	Câble d'unité de saisie	
Borne	Couleur des fils	Signal
GS	BN | Brun	GND (moins)
96	YE | Jaune	RS485 A
95	GN | Vert	RS485 B
94	WH | Blanc	+ 24 V (plus)

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

3.6 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.

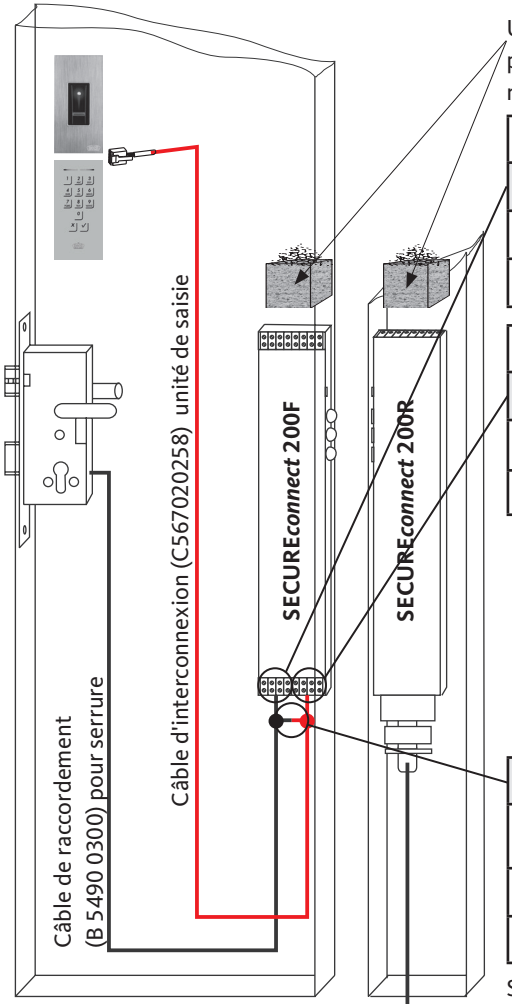
Utilisez les joints fournis comme protection contre les copeaux lors du montage dans des profilés métalliques.

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

SC 200F	Câble de raccordement pour unité de saisie	
Borne	Couleur des fils	Signal
GS	BN | Brun	GND (moins)
96	YE | Jaune	RS485 A
95	GN | Vert	RS485 B
94	WH | Blanc	+ 24 V (plus)

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

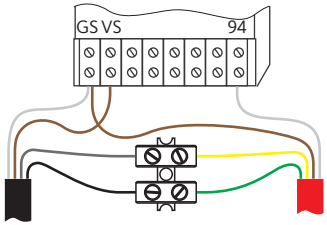
3.7 Schéma de câblage pour les serrures EK par bus RS485



Utilisez les joints fournis comme protection contre les copeaux lors du montage dans des profilés métalliques.

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

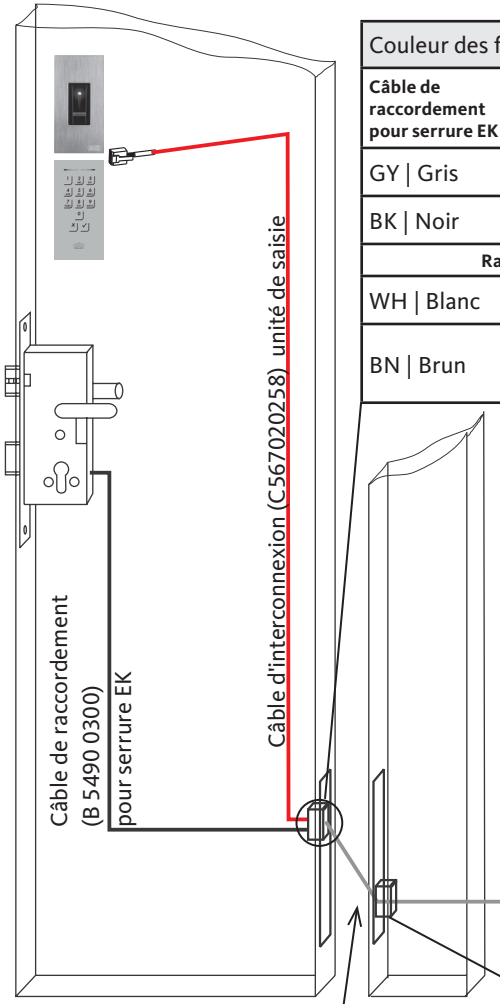
SC 200F	Câble d'interconnexion pour unité de saisie	
Borne	Couleur des fils	Signal
GS	BN | Brun	GND (moins)
94	WH | Blanc	+ 24 V (plus)



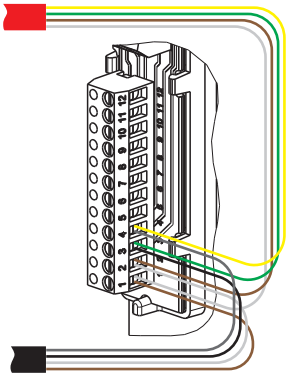
Couleur des fils		Signal
Câble de raccordement pour serrure EK	Câble d'interconnexion pour unité de saisie	
GY | Gris	YE | Jaune	RS485 A
BK | Noir	GN | Vert	RS485 B

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

3.7.1 Raccord à une source de tension externe



Couleur des fils		N°	Signal
Câble de raccordement pour serrure EK	**Câble d'interconnexion pour unité de saisie**	**Passe-câble**	
GY | Gris	YE | Jaune	4	RS485 A
BK | Noir	GN | Vert	3	RS485 B
Raccord à une source de tension externe			
WH | Blanc	BN | Brun	2	GND (moins)
BN | Brun	WH | Blanc	1	+ 12 V – 24 V CC



Bloc d'alimentation B 5570 0402

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

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

L'unité de saisie et l'unité de commande sont automatiquement couplées entre elles de manière univoque lors de la première mise en service (appairage) par l'intermédiaire de la connexion bus RS485.

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 couplage électrique suivant une séquence donnée.

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

- Actionnement continu de la béquille.
- En ouvrant et fermant avec une clé mécanique, passez à 3 reprises sur le capteur du panneton.

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

4. Mise en service

Pour être utilisés, les appareils doivent être mis en service. La mise en service du système appaire l'unité de commande à l'unité de saisie. Pour mettre votre système d'accès en service, procédez par étapes :

- Montez les appareils comme décrit au Chapitre 3.
- Le branchement électrique des composants doit être effectué conformément au schéma de câblage.

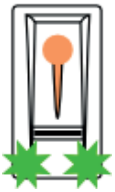
4.1 Mise en service du lecteur d'empreintes digitales

- Raccordez le bloc d'alimentation ou le SECURE*connect* à la tension du réseau.
- Après la première mise en marche, le lecteur d'empreintes digitales et le SECUREconnect ou la serrure EK effectuent un appairage automatique. À la fin de l'appairage, la LED bleue clignote.

Le lecteur d'empreintes digitales n'est pas appairé avec SC 200/ serrure EK

Le lecteur d'empreintes digitales est appairé avec SC 200/serrure EK. Aucun doigt n'est enregistré.

Le lecteur d'empreintes digitales est connecté à l'appareil Bluetooth.



Le lecteur d'empreintes digitales est appairé avec SC 200/serrure EK – menu administrateur.

4.1.1 Concept d'utilisation

Deux concepts d'utilisation sont à disposition :

- Appli – Gestion du lecteur d'empreinte digitales Bluetooth à l'aide de l'appareil mobile (Section 6.1, à partir de la page 186)
- Empreinte maître – Gestion du lecteur d'empreinte digitales à l'aide de l'empreinte maître (Section 6.3, à partir de la page 193)

4.1.2 Mode test

Raccordez la tension réseau et effectuez le test dans les 10 minutes qui suivent. Lorsque les 10 minutes sont écoulées, ce test n'est possible qu'après un reset power on du lecteur d'empreintes digitales.

Le lecteur d'empreintes digitales est appairé avec SECURE*connect* 200. Aucun doigt n'est enregistré.

Posez un doigt sur le capteur pendant 3 à 5 secondes.

Lorsque vous retirez le doigt, le relais (SECURE*connect* ou serrure EK) se déclenche.

REMARQUE

Un test ne fonctionne que lorsqu'aucune empreinte maître n'est encore enregistrée ou lorsqu'aucun appareil mobile n'est couplé.

Posez votre doigt sur le capteur pendant une durée totale de maximum 5 secondes. Lorsque vous laissez le doigt plus longtemps sur le capteur, le relais (SECURE*connect* ou serrure EK) ne se déclenche pas.

4.2 Mise en service du clavier à code

- Après la première mise en marche, le clavier à code et SECURE*connect* ou la serrure EK effectuent un appairage automatique. Les LED de statut du clavier à code clignotent en alternance en jaune. Une fois l'appairage achevé, aucune LED de statut n'est allumée.

Le clavier à code n'est pas appairé avec SC 200/serrure EK.

Le clavier à code est appairé avec SC 200/serrure EK.

ATTENTION

Changez immédiatement le code administrateur d'usine 9999 après la mise en service et le maintenir le secret !
Si le code administrateur n'est pas remplacé, des personnes non autorisées peuvent avoir accès au menu administrateur et donc aux entrées.

4.2.1 Signalisation optique

Affichage	LED de statut de gauche	LED de statut de droite	Signification
	Éteinte	Éteinte	Veille
	Jaune clignotant	Jaune clignotant	Configuration d'usine/pas d'appairage avec l'unité de commande
	Jaune	Éteinte	Prêt pour l'entrée du code administrateur
	Vert	Éteinte	Menu administrateur actif
	Vert	Vert	Entrée positive : code PIN correct, valeur entrée correcte, ...
	Rouge	Rouge	Entrée négative : code PIN erroné, valeur entrée erronée, ...
	Éteinte	Rouge	Blocage du système pendant 1 ou 15 minutes

5. Fonctionnement du lecteur d'empreintes digitales

Passez les doigts

Tenez votre doigt droit, posez-le au centre entre les arêtes de guidage.
Ne le tordez pas.

Placez l'articulation de la première phalange directement sur le capteur.
Posez le doigt à plat sur le lecteur.

Allongez les autres doigts.

Faites glisser le doigt avec régularité vers le bas sur le capteur. Déplacez toute la main. Faites glisser entièrement la première phalange sur le capteur afin d'obtenir un résultat optimal.
Le mouvement dure env. 1 secondes.

Conseils pour obtenir une empreinte de bonne qualité

- L'index, le majeur et l'annulaire conviennent le mieux. Le pouce et le petit doigt produisent des empreintes difficilement analysables.
- Si vos doigts sont souvent humides, enregistrez-les lorsqu'ils sont humides.
- Les doigts d'enfant fonctionnent à partir de 5 ans env.

Effleurement de doigt

Touchez brièvement et rapidement le capteur avec le doigt.

6. Programmation du lecteur d'empreintes digitales

6.1 Programmation avec l'appli open biometric

Le lecteur d'empreintes digitales doit être appairé avec SECURE*connect* pour que la programmation puisse démarrer.

REMARQUE **L'appli open biometric ne peut être utilisée qu'en combinaison avec le lecteur d'empreintes digitales Bluetooth.**

L'appli open biometric sert à programmer le système. De plus, l'appli permet d'ouvrir des portes.

6.1.1 Télécharger l'appli

L'appli est disponible pour les systèmes d'exploitation Apple iOS et Google Android. Téléchargez l'appli open biometric sur l'App Store ou Google Play. Pour ce faire, saisissez le terme de recherche « open biometric ».

Download on the App Store

GET IT ON Google Play

Pour effectuer le premier appairage, vous avez besoin du code de couplage des appareils et du code de sécurité de l'appli. **Les deux codes sont paramétrés sur 9999 en réglage usine.**

- Démarrez l'appli open biometric.
- Effleurez le champ de saisie (Android) ou appuyez sur « Recherche » (iOS). L'appli recherche les appareils Bluetooth disponibles.

- Sélectionnez votre lecteur d'empreintes digitales Bluetooth (les 4 derniers chiffres du numéro de série s'affichent).
- Uniquement pour Android : appuyez sur « Connexion ».
- Saisissez le **code de couplage des appareils 9999.**
- Appuyez sur « Continuer ». L'appareil mobile est appairé avec le lecteur d'empreintes digitales Bluetooth.

- Saisissez un nouveau code de couplage des appareils à 6 chiffres. Pour des raisons de sécurité, vous devez modifier le code de couplage des appareils lors du premier l'appairage du système. Souvenez-vous de ce code car vous en aurez besoin pour appairer d'autres appareils mobiles.

  Le code de couplage des votre appareils :

- Appuyez sur « Modifier » (Android) ou sur « Continuer » (iOS).
- Saisissez le code usine de sécurité 9999.
- Appuyez sur « Continuer ».

L'appairage entre le lecteur d'empreintes digitales Bluetooth et l'appareil mobile a été effectué. Le système se trouve en mode de fonctionnement normal.

Vous pouvez à présent programmer et gérer le système d'accès par lecteur d'empreintes digitales à l'aide de l'appli open biometric.

REMARQUE

Pour gérer votre lecteur d'empreintes digitales Bluetooth, l'appli open biometric intuitive suffit.
Activez les fonctions souhaitées dans l'appli et suivez les instructions sur l'écran.

6.1.2 Modifier le code de sécurité de l'appli

Tous les codes de sécurité peuvent être modifiés à tout moment :

- Code de sécurité de l'appli
- Code de code de couplage administrateur
- Code de couplage utilisateur

REMARQUE

Le code de sécurité de 4 à 6 chiffres de l'appli est nécessaire pour l'interrogation de sécurité de l'appli. Vous pouvez désactiver l'interrogation du code de sécurité de l'appli sous « ADMINISTRATION » si votre appareil dispose de mécanismes de verrouillage sécurisés (empreintes, code, etc.).

- Sélectionnez « ADMINISTRATION ».
- Sélectionnez « MODIFIER LES CODES DE SÉCURITÉ DE L'APPLI ».
- Modifiez le code souhaité.
- Appuyez sur « Modifier » (Android) ou « Terminé » (iOS).

Le code de sécurité sélectionné a été modifié.

6.1.3 Enregistrer des empreintes digitales

Vous pouvez enregistrer les empreintes maîtres et utilisateurs à l'aide de l'appli open biometric.

- Sélectionnez « ADMINISTRATION ».
- Sélectionnez la « GESTION DES UTILISATEURS ».
- Appuyez sur  (Android) ou « + » (iOS).
- Veuillez entrer le nom d'utilisateur.
- Appuyez sur « Nouvelle autorisation d'administrateur » ou « Nouvelle autorisation d'accès ».
- Sélectionnez le relais devant commuter (pour le SECURE*connect* ou la serrure à couplage électrique connecté).
- Sélectionnez un doigt.
- Appuyez sur « Enregistrer ».
- Lisez la remarque et appuyez sur « Démarrer ».
- Dès que l'enregistrement de votre doigt a réussi, appuyez sur « OK ».
- Appuyez sur « Terminé ».

REMARQUE **Enregistrez au moins une empreinte de chaque main par point d'accès.**

6.1.4 Désactiver le Bluetooth

Vous pouvez désactiver la fonction Bluetooth.
Dans les réglages usine, la fonction Bluetooth est activée.

- Démarrez l'appli open biometric.
- Sélectionnez « ADMINISTRATION ».
- Sélectionnez « ÉTAT DU SYSTÈME ».
- Activez le champ « Désactiver le Bluetooth au bout de 15 minutes » dans « RÉGLAGES BLUETOOTH ».

Ce réglage permet de désactiver le Bluetooth du lecteur d'empreintes digitales au bout de 15 minutes dans un des cas suivants :

- Aucun appareil mobile n'a été connecté.
- Au moins un doigt a été enregistrée.

Pour réactiver le Bluetooth : accédez au menu administrateur et passez n'importe quelle empreinte maître sur le lecteur.

6.1.5 Effectuer l'appairage d'autres appareils mobiles

Vous pouvez effectuer l'appairage d'autres appareils mobiles au lecteur d'empreintes digitales à l'aide du même code de couplage administrateur ou utilisateur à 6 chiffres que vous avez choisi.

- Démarrez l'appli open biometric.
- Couplez l'appareil mobile au lecteur d'empreintes digitales Bluetooth et utilisez le code de couplage administrateur ou utilisateur à 6 chiffres choisi par vos soins.
- L'appairage entre le lecteur d'empreintes digitales Bluetooth et l'appareil mobile s'effectue.

Vous pouvez à présent programmer et gérer le lecteur d'empreintes digitales avec l'appli.

6.1.6 Utiliser plusieurs lecteurs d'empreintes digitales Bluetooth

L'appli open biometric permet d'utiliser plusieurs lecteurs d'empreintes digitales Bluetooth. Pour pouvoir permuter entre deux lecteurs d'empreintes digitales Bluetooth, vous devez réinitialiser l'appairage entre le lecteur d'empreintes digitales Bluetooth et l'appareil mobile.

REMARQUE

Lors de la réinitialisation de l'appairage, les noms de relais (SECURE*connect* ou serrure EK) et les images d'utilisateurs enregistrés sont supprimés. Les noms d'utilisateurs et les autorisations restent enregistrés sur le lecteur d'empreintes digitales Bluetooth.

- Démarrez l'appli open biometric.
- Sélectionnez « ADMINISTRATION ».
- Sélectionnez « RÉINITIALISER LE COUPLAGE ».
- Confirmez la réinitialisation en appuyant sur « Suivant ».

L'appairage entre le lecteur d'empreintes digitales et l'appareil mobile est à présent réinitialisé. Vous pouvez maintenant appairer un autre lecteur d'empreintes digitales.

6.2 Enregistrer le code de couplage utilisateur

Vous pouvez enregistrer un code de couplage utilisateur. Vous pouvez donner ce code à une personne de votre choix. Ce code permet d'exécuter les actions suivantes :

- Ouvrir la porte
- Activer ou désactiver le code de sécurité de l'appli
- Modifier le code de sécurité de l'appli
- Réinitialiser l'appairage entre le lecteur d'empreintes digitales et l'appareil mobile

Pour enregistrer le code de couplage utilisateur, veuillez suivre les étapes suivantes :

- Démarrez l'appli open biometric.
- Sélectionnez « ADMINISTRATION ».
- Sélectionnez « MODIFIER LES CODES DE SÉCURITÉ DE L'APPLI ».
- Saisissez le code de couplage utilisateur souhaité dans le champ correspondant.
- Confirmez les saisies avec « Modifier » (Android) ou « Terminé » (iOS).

Le code de couplage utilisateur est à présent enregistré.

6.2.1 Réinitialiser le code de sécurité de l'appli

- Démarrez l'appli open biometric.
- Saisissez un code de sécurité appli incorrect.
- Confirmez la saisie avec « Suivant ».
- Sélectionnez « RÉINITIALISER LE COUPLAGE ».
- Confirmez la réinitialisation en appuyant sur « Suivant ».

L'appairage entre le lecteur d'empreintes digitales et l'appareil mobile est réinitialisé et le code de sécurité de l'appli est remis à 9999.

Vous pouvez à présent effectuer à nouveau l'appairage du lecteur d'empreintes digitales et attribuer un nouveau code de sécurité appli.

6.2.2 Protéger le système de la perte de l'appareil mobile

Si vous avez perdu votre appareil mobile, vous pouvez modifier le code de couplage administrateur ou utilisateur à l'aide d'un deuxième appareil mobile. Le nouveau code de couplage administrateur ou utilisateur bloque la connexion de l'appareil mobile perdu.

- Démarrez l'appli open biometric sur le deuxième appareil mobile.
- Couplez le deuxième appareil mobile au lecteur d'empreintes digitales Bluetooth.

- Sélectionnez « ADMINISTRATION ».
- Sélectionnez « MODIFIER LES CODES DE SÉCURITÉ DE L'APPLI ».
- Saisissez un nouveau code de couplage administrateur ou utilisateur à 6 chiffres.
- Confirmez la saisie avec « Modifier » (Android) ou « Terminé » (iOS).

Le code de code de couplage administrateur ou utilisateur est modifié dans le système.

L'appareil mobile perdu ne peut désormais plus établir de connexion avec le lecteur d'empreintes digitales Bluetooth. Votre système est protégé des accès non autorisés.

6.2.3 Remettre le système à la configuration d'usine

- Démarrez l'appli open biometric.
- Connectez-vous avec le lecteur d'empreintes digitales Bluetooth.
- Sélectionnez « ADMINISTRATION ».
- Sélectionnez « RÉINITIALISER LE SYSTÈME ».
- Confirmez la réinitialisation en appuyant sur « Suivant ».

Le système est réinitialisé aux réglages usine. Vous pouvez à présent remettre le système en service.

REMARQUE

Toutes les empreintes utilisateurs et les empreintes maîtres sont effacées !
L'appairage entre le lecteur d'empreintes digitales et SECURE*connect* 200 ou la serrure EK est conservé !

Un nouvel appairage du SECURE*connect* 200 permet également de réinitialiser le lecteur d'empreintes digitales aux réglages d'usine.

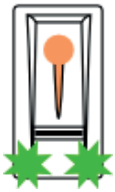
6.3 Programmation avec les empreintes maître

6.3.1 Enregistrer des empreintes maîtres

Les empreintes maîtres servent à programmer le système. Enregistrez dès le début 4 empreintes maître différentes. Chaque empreinte doit être **lue au moins 3 fois.** Nous recommandons d'enregistrer deux doigts de 2 personnes différentes.

Le lecteur d'empreintes digitales est appairé avec SC 200/serrure EK. Aucun doigt n'est enregistré.

Trois effleurements de doigt en 5 secondes.



Mode administrateur actif.

Passez la première empreinte maître sur le capteur.

L'empreinte a été identifiée.

Le système est prêt pour la répétition.

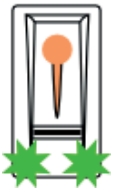
Repassez la première empreinte maître sur le capteur.

L'empreinte a été identifiée.

Le système est prêt pour la répétition.

Repassez la première empreinte maître sur le capteur.

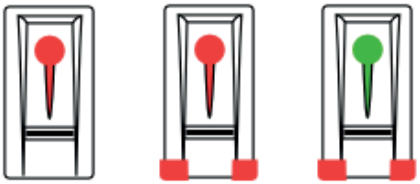
La qualité des trois scans est excellente.



Le lecteur d'empreintes digitales est prêt pour enregistrer les autres empreintes maîtres.

Autres possibilités de messages pendant le processus d'enregistrement :

Qualité des scans suffisante. La qualité peut être améliorée par d'autres scans.



Erreur lors du processus de scan ou qualité insuffisante.
Passez ce doigt encore une fois sur le capteur.

REMARQUE

En cas de redémarrage du lecteur d'empreintes digitales alors que celui-ci est en mode administrateur et qu'il contient moins de 4 empreintes maîtres, toutes les empreintes maîtres déjà enregistrées seront supprimées.

Pendant l'enregistrement des empreintes, les différents scans d'empreintes doivent être espacés de maximum 10 secondes. Dans le cas contraire, l'enregistrement de l'empreinte est interrompu.

6.3.2 Enregistrer les empreintes utilisateurs

Les empreintes utilisateurs permettent d'ouvrir une porte. Toutes les empreintes qui ne sont pas des empreintes maîtres peuvent être utilisées comme empreintes utilisateurs.

Fonctionnement normal

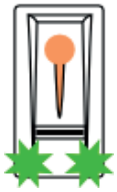
Trois effleurements de doigt en 5 secondes.

Menu administrateur

Passez n'importe quel empreinte maître sur le capteur.

L'empreinte maître a été identifiée. Mode d'enregistrement actif.

Un effleurement de doigt en 5 secondes.



Mode d'enregistrement actif.

Passez le doigt à enregistrer sur le capteur.

L'empreinte a été identifiée.

Le système est prêt pour la répétition.

Passez le doigt à enregistrer sur le capteur.

L'empreinte a été identifiée.

Le système est prêt pour la répétition.

Passez le doigt à enregistrer sur le capteur.

L'empreinte a été identifiée.

L'enregistrement de l'empreinte a réussi.

Après la sauvegarde de l'empreinte de l'utilisateur : fonctionnement normal.

6.3.3 Effacer des empreintes utilisateurs

Des empreintes utilisateurs isolées ne peuvent être effacées que lorsque l'utilisateur concerné est présent.

Fonctionnement normal

Trois effleurements de doigt en 5 secondes.

Menu administrateur

Passez n'importe quel empreinte maître sur le capteur.

L'empreinte maître a été identifiée. Mode d'enregistrement actif.

Attendez 5 secondes !

Mode d'effacement actif

Un effleurement de doigt

Menu administration

Passez l'empreinte à supprimer sur le capteur.

Empreinte utilisateur effacée !

Fonctionnement normal

6.3.4 Effacer toutes les empreintes utilisateurs

Tous les empreintes utilisateurs mémorisées dans le système sont effacées. Les empreintes maîtres sont conservées.

Fonctionnement normal

Trois effleurements de doigt en 5 secondes.

Menu administrateur

Passez n'importe quel empreinte maître sur le capteur.

L'empreinte maître a été identifiée. Mode d'enregistrement actif.

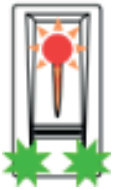
Attendez 5 secondes !

Mode d'effacement actif

Un effleurement de doigt

Menu administration

Scannez à nouveau la même empreinte maître comme mentionné plus haut.



Toutes les empreintes maîtres sont effacées !

Fonctionnement normal

REMARQUE **Contrôlez n'importe quel empreinte utilisateur. Vous ne devez plus obtenir de validation !**

6.3.5 Retour aux paramètres d'usine du lecteur d'empreintes digitales

Vous restaurez ainsi l'état du lecteur d'empreintes digitales à la livraison.

REMARQUE

Toutes les empreintes utilisateurs et les empreintes maîtres sont effacées ! L'appairage entre le lecteur d'empreintes digitales et SECURE*connect* 200 ou la serrure EK est conservé !

Un nouvel appairage du SECURE*connect* 200 ou de la serrure EK permet également de réinitialiser le lecteur d'empreintes digitales aux réglages d'usine.

Fonctionnement normal

Trois effleurements de doigt en 5 secondes.

Menu administrateur

Passez n'importe quel empreinte maître sur le capteur.

L'empreinte maître a été identifiée. Mode d'enregistrement actif.

Attendez 5 secondes !

Mode d'effacement actif

Un effleurement de doigt

Menu administration

Scannez une autre empreinte maître.

Toutes les empreintes utilisateurs et maîtres sont effacées !

Le lecteur d'empreintes digitales est appairé avec SC 200/serrure EK. Aucun doigt n'est enregistré.

7. Programmation du clavier à code

Différents points de menu sont prévus pour la programmation dans le menu administrateur. Ils peuvent être appelés au moyen des touches.

Touche	Point de menu
1	Sauvegarde du code utilisateur
2 ABC	Effacement du code utilisateur
3 DEF	Modification du code administrateur
4 GHI	Remise du système à la configuration d'usine
5 JKL	Réglage du clavier à code

7.1 Modification du code administrateur

Cette fonction permet de modifier le code administrateur existant. Le code administrateur peut avoir de 4 à 8 positions et doit contenir au moins deux chiffres différents. La modification du code administrateur se fait par le menu administrateur. Pour parvenir au menu administrateur, entrez le code administrateur.

REMARQUE **Les codes administrateur ne peuvent pas être utilisés comme codes utilisateurs.**

Pressez √ pour lancer l'entrée du code administrateur.

Entrez le code administrateur (par défaut = 9999).

√

3

√

Entrez l'ancien code administrateur.

√

Entrez le nouveau code administrateur.

√

Entrez à nouveau le nouveau code administrateur.

√

7.2 Mémoriser le code utilisateur

Le système permet l'enregistrement d'un maximum de 99 codes utilisateurs. Un code utilisateur est un code PIN par lequel une action est déclenchée sur l'unité de commande, p. ex. l'ouverture d'une porte. Le code utilisateur peut avoir de 4 à 8 positions et doit contenir au moins deux chiffres différents.

REMARQUE

Utilisez des codes utilisateurs longs. Utilisez si possible tous les chiffres. Utilisez différents codes pour les différentes personnes autorisées.

Pressez √ pour lancer l'entrée du code administrateur.

Entrez le code administrateur.

√

1

√

Entrez le code utilisateur.

√

Entrez à nouveau le code utilisateur.

√

7.3 Effacer le code utilisateur

Vous pouvez effacer des codes utilisateurs isolés. Pour cela, vous avez besoin du code à effacer.

L'effacement d'un code utilisateur se fait par le menu administrateur. Pour parvenir au menu administrateur, entrez le code administrateur.

Pressez √ pour lancer l'entrée du code administrateur.

Entrez le code administrateur.

√

2

√

Entrez le code utilisateur à effacer.

√

7.4 Remettre le système à la configuration d'usine

Le clavier à code est remis à la configuration d'usine. Tous les codes utilisateurs sont effacés irrévocablement. Le code administrateur est remis à la valeur d'usine 9999, le seuil de luminosité à 10 %, la valeur de luminosité à 100 %. La signalisation acoustique et optique de la pression de touche et le signal acoustique d'ouverture de porte sont enclenchés.

Une procédure d'appairage (voir la Section 2.2) remet également le clavier à code à la configuration d'usine.

Pressez √ pour lancer l'entrée du code administrateur.

Entrez le code administrateur.

√

4

√

Entrez le code administrateur.

√

7.5 Réglage du rétroéclairage automatique

Vous définissez ici le seuil de luminosité à partir duquel le rétroéclairage est automatiquement activé à la tombée de la nuit.

Le seuil de luminosité peut être réglé en pourcentage. Le réglage d'usine fixe le seuil de luminosité à 10 %. Entrez le pourcentage souhaité :

0 = rétroéclairage automatique désactivé
1 à 100 = seuil de luminosité depuis activation en conditions de grande clarté à activation seulement en conditions de faible clarté

Pressez √ pour lancer l'entrée du code administrateur.

Entrez le code administrateur.

√

51

Valeur du seuil de luminosité souhaité, p. ex. 70.

√

7.6 Réglage de luminosité du rétroéclairage

La luminosité du rétroéclairage peut être réglée au moyen de 4 modes prédéfinis. Le réglage d'usine du rétroéclairage est de 100 %. Entrez le numéro du mode souhaité :

0 = rétroéclairage désactivé
1 = rétroéclairage activé à 33 %
2 = rétroéclairage activé à 66 %
3 = rétroéclairage activé à 100 %

Le réglage de luminosité du rétroéclairage est effectué par le biais du menu administrateur. Pour parvenir au menu administrateur, entrez le code administrateur.

Pressez √ pour lancer l'entrée du code administrateur.

Entrez le code administrateur.

√

52

Numéro du mode souhaité, p. ex. 2.

√

7.7 Réglage de la signalisation de pression des touches

La signalisation acoustique et optique de la pression des touches peut être réglée avec 4 modes prédéfinis. Dans la configuration d'usine, les signaux acoustiques et optiques sont activés pour la pression des touches. Entrez le numéro du mode souhaité :

0 = signaux acoustiques et optiques désactivés
1 = signaux acoustiques activés et signaux optiques désactivés
2 = signaux acoustiques désactivés et signaux optiques activés
3 = signaux acoustiques et optiques activés

Le réglage de la signalisation de la pression des touches est effectué par le biais du menu administrateur. Pour parvenir au menu administrateur, entrez le code administrateur.

Pressez √ pour lancer l'entrée du code administrateur.

Entrez le code administrateur.

√

54

Numéro du mode souhaité, p. ex. 2.

√

7.8 Réglage du signal acoustique à l'ouverture

Le signal acoustique à l'ouverture peut être activé ou désactivé. Dans la configuration d'usine, le signal acoustique est activé. Entrez le numéro du mode souhaité :

0 pour désactiver
1 pour activer

Le réglage du signal acoustique à l'ouverture est effectué par le biais du menu administrateur. Pour parvenir au menu administrateur, entrez le code administrateur.

Pressez √ pour lancer l'entrée du code administrateur.

Entrez le code administrateur.

√

55

Numéro du mode souhaité, p. ex. 0.

√

8. Ouverture de la porte

L'ouverture de la porte peut être effectuée à l'aide de l'appli open biometric, à l'aide du lecteur d'empreintes digitales ou du clavier à code.

8.1 Ouverture de la porte à l'aide de l'appli open biometric

Le système se trouve en mode de fonctionnement normal.

- Démarrez l'appli open biometric. L'appareil mobile se connecte avec le lecteur d'empreintes digitales Bluetooth.
- Sélectionnez « ACCÈS ».
- Poussez le curseur de la porte à ouvrir vers la droite.

Le SECURE*connect* envoie le signal de commande pour le déverrouillage motorisé ou serrure motorisée et votre porte s'ouvre. La serrure EK reçoit directement le signal de commande.

8.2 Ouverture de la porte avec lecteur d'empreintes digitales

Fonctionnement normal

Passez une empreinte utilisateur ou maître enregistrée sur le capteur.

L'empreinte a bien été identifiée.

Après l'ouverture de la porte : fonctionnement normal.

REMARQUE

Si le lecteur d'empreintes digitales est utilisé avec SECURE*connect* 200 et la porte est ouverte pendant plus de 12 s, le lecteur d'empreintes digitales est hors tension. Après la fermeture et le retour de l'alimentation électrique, le lecteur d'empreintes digitales affiche brièvement « Pas de connexion bus » jusqu'à ce que le fonctionnement normal soit restauré automatiquement.

8.3 Ouverture de la porte à l'aide du clavier à code

Entrez un code utilisateur enregistré.

Pressez √ et la porte s'ouvre.

Le code utilisateur n'a pas été identifié.

REMARQUE

Après 3 entrées erronées consécutives a lieu un blocage d'une minute. Après 3 autres entrées erronées consécutives a lieu un blocage de 15 autres minutes. Une nouvelle entrée erronée donne lieu à un blocage de 15 minutes.
L'entrée à deux reprises d'un code utilisateur autorisé permet de mettre fin prématurément au blocage. Il n'y a alors pas de signalisation.

REMARQUE

Si le clavier à code est utilisé avec SECURE*connect* 200 et la porte est ouverte pendant plus de 12 s, le lecteur d'empreintes digitales est hors tension.
Après la fermeture et le retour de l'alimentation électrique, le clavier à code affiche brièvement "Pas de connexion bus" jusqu'à ce que le fonctionnement normal soit restauré automatiquement.

9. Entretien et maintenance

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 est malgré tout encrassé, nettoyez-le à l'aide d'un chiffon humide (non mouillé), non abrasif. Utilisez pour ce faire les cotons-tiges, les chiffons à microfibres et 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 de temps en temps par mesure de précaution avec un chiffon légèrement humide et non abrasif pour éliminer les marques de doigt et les impuretés. Utilisez de l'eau claire sans addition de produit nettoyant.

En cas d'utilisation fréquente, entretenir les contacts du SECURE*connect* 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. Graisser 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 !

10. Défauts et solutions

Affichage et solutions

Lecteur d'empreintes digitales Affichage		Cause	Solution
	La LED de statut s'allume en rouge.	L'empreinte n'a pas été identifiée.	Repassez le doigt sur le capteur.
	Toutes les LEDs s'allument en rouge pendant 1 minute.	Blocage du système. Vous avez tenté de déverrouiller le système avec une empreinte inconnue à 10 reprises.	Patientez 1 minute. Le système passe ensuite en mode de fonctionnement normal.
	La LED d'état clignote en orange.	Connexion bus vers SC 200/serrure EK inexistante.	Vérifiez le câblage ou procédez à un reset de l'appairage.
	La LED de statut clignote rouge/vert.	Le capteur du lecteur d'empreintes digitales est encrassé ou défectueux.	Nettoyez le capteur ou séchez-le.

Clavier à code Affichage		Cause	Solution
	Les deux LED de statut sont rouges.	Le code utilisateur n'a pas été identifié.	Entrez à nouveau le code utilisateur.
		Le code utilisateur souhaité est composé uniquement des mêmes chiffres, p. ex. 1111, 3333.	Utilisez des codes utilisateurs avec différents chiffres.
		Le code utilisateur souhaité est trop court ou trop long, p. ex. 321, 987654321.	Tenez compte de la longueur du code utilisateur : au moins 4 positions, au plus 8 positions.
		Une erreur s'est produite lors de l'entrée de points de menu ou de valeurs.	Répétez l'entrée.
	La LED de statut est rouge à droite	3 fois entrée d'un code utilisateur erroné. Blocage du système pendant 1 ou 15 minutes.	Entrez deux fois un code utilisateur autorisé. La porte peut alors être ouverte avant expiration du blocage avec un code utilisateur autorisé.
	Les LED de statut clignotent en alternance en jaune.	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 d'appairage (voir la Section 2.2).

11. Entretien et pièces de rechange

Le produit ne demande en principe aucune maintenance. 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 intégralement 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 SAV BKS avant une réparation sur place et, si nécessaire et sur concertation, de renvoyer l'appareil.

Démontez le produit hors de son compartiment. 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.

12. 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 lecteur d'empreintes digitales et le clavier à code doivent être remises aux points de collecte publics ou aux déchetteries de tri sélectif. L'emballage doit être éliminé séparément.

Tabla de contenido

¡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 unidad de registro 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 del lector de huella digital o el teclado de código.

Todos los usuarios deben leer y aplicar el manual de instrucciones con el que operan el lector de huella digital o el teclado de código, p. ej., en el caso de:

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

Una vez finalizado el montaje, hay que entregar el manual de instrucciones a los usuarios. Por favor, lea atentamente este manual antes de usar nuestro producto y consérvelo para posteriores usos. Indique a todos los usuarios/responsables 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.

A los constructores y usuarios se les debe recordar que deben cumplir lo indicado en este manual para evitar cualquier montaje defectuoso, así como cualquier maniobra incorrecta. Con este objetivo, se deberá entregar este manual a los constructores y a los usuarios.

- 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 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 equipos.
- Para ello, debe asegurarse de que dispone de los documentos para la colocación, puesta en marcha, manejo, mantenimiento y reparación de los equipos.
- Por motivos de seguridad y de homologación (CE) no se permite transformar ni cambiar 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 unidades de registro 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.

Su sistema de acceso consta de 2 dispositivos electrónicos:

- Unidad de registro: lector de huella digital o teclado de código
- Unidad de control: SECURE*connect* 200

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 y el industrial.

2.1 Datos técnicos

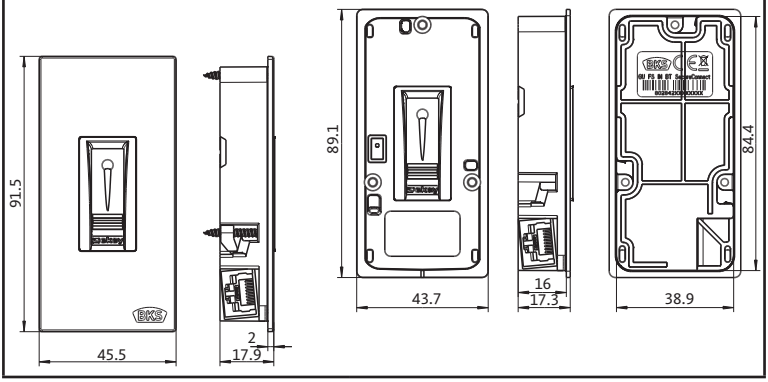
Fuente de alimentación	8–24 V CC (máx. 30 V)
Potencia absorbida	< 1 W
Condiciones ambientales	°C +70 °C / –20 °C **IP54** (parte frontal)
Certificaciones	CE Los certificados se pueden encontrar en nuestra página web www.g-u.com.

Variante	B-55600-13-4-6
Memoria	99 plantillas de dedos
Tiempo de identificación de plantilla	1–2 s
Cuota de denegación errónea (FRR)	1:100

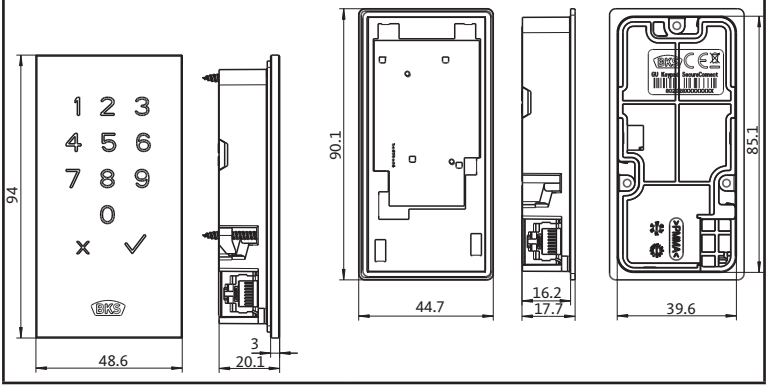
B-55600-13-4-6 | B-55600-10-4-6

Lector de huella digital y teclado de código

Cuota de aceptación errónea (FAR)	1:10.000.000
Vida útil	Máx. 10 millones de escaneados de huella digital
Dimensiones	



Variante	B-55600-10-4-6
Memoria	99 códigos de usuario
Longitud del código PIN	4–8 dígitos
Dimensiones	



2.2 Protección contra manipulaciones

La unidad de registro (lector de huella digital o 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:

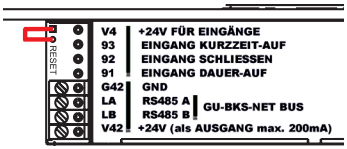
- La unidad de registro está conectada a la unidad de control a través de una línea de datos. La transmisión de datos está codificada.
- La unidad de registro y la unidad de control se acoplan de forma unívoca (emparejamiento) durante la primera puesta en marcha.

En el lector de huella digital, el registro de dedos de usuarios y la modificación de contenidos del sistema solo es posible con la identificación previa de un dedo administrador.

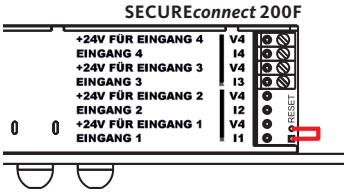
El teclado de código registra el código PIN con el teclado capacitivo. Compara el código introducido con los códigos de referencia guardados. El teclado de código procesa códigos PIN de entre 4 y 8 dígitos. El código PIN debe tener al menos un número diferente. Existen dos tipos de códigos PIN. El código de administrador, para la configuración del sistema, y el código de usuario, para la apertura de la puerta.

Al introducir el código incorrectamente 3 veces, el sistema se bloqueará durante 1 minuto. Al introducir, a continuación, el código incorrectamente 3 veces, el bloqueo durará 15 minutos. Todas las veces en las que se introduzca posteriormente el código de forma incorrecta, el bloqueo será de 15 minutos. El sistema se puede desbloquear antes de que transcurra dicho tiempo introduciendo dos veces seguidas un código de usuario habilitado.

Para cambiar un componente (SECURE*connect* 200R, SECURE*connect* 200F o unidad de registro) del sistema de la puerta, es necesario realizar un procedimiento de reemparejamiento en ambas partes de SECURE*connect*.



SECURE*connect* 200R



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.

Después puede retirarse la pinza. SECURE*connect* 200R, SECURE*connect* 200F y la unidad de registro (escáner de huella dactilar o teclado de código) se someten ahora a un nuevo proceso de emparejamiento. La unidad de registro se restablece con ello a la configuración de fábrica (se borran todas las plantillas de huellas y códigos PIN guardados).

Cuando se conecta un lector de huella digital o un teclado de código a un SECURE*connect* 200 no emparejado, la unidad de registro se restablece con ello a la configuración de fábrica y se borran las plantillas de huellas y códigos PIN.

2.3 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. Nuestro 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 la cerradura o el cerradero eléctrico, es necesario un SECURE*connect* 200 como unidad de control.

2.4 Uso no previsto

No está permitida cualquier otra aplicación, por lo que BKS 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 de nuestro producto en las condiciones descritas a continuación.

- El funcionamiento del sistema de acceso con voltajes que superen los 24 V + 10 % CC no está permitido y puede producir daños permanentes en el producto.
- Fallo en la polaridad de las conexiones.
- En el producto se han realizado modificaciones no autorizadas.

2.5 Alcance del suministro, transporte y almacenamiento

Es necesario comprobar si el suministro está completo y hay desperfectos. En caso de daños, informar al fabricante. Montar y poner en funcionamiento únicamente los productos que se encuentren en perfecto estado.

La entrega se compone de los artículos siguientes:

- Unidad de registro (lector de huella digital o teclado de código) con elemento decorativo
- Cable del sistema para unidad de registro
- Instrucciones

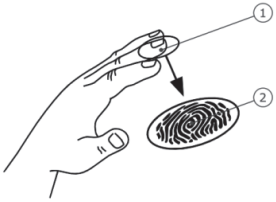
Almacene el producto únicamente en el embalaje original y con las condiciones siguientes:

- Almacenar exclusivamente en un habitáculo seco, limpio y con ventilación suficiente, nunca al aire libre
- Almacenamiento 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
- No almacenar junto con sustancias corrosivas y proteger de la luz solar
- Inspeccionar periódicamente el estado general cuando se den periodos de almacenamiento prolongados

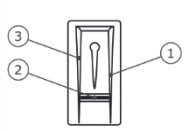
Transporte el producto únicamente en el embalaje original. Para el transporte, proteja el producto ante posibles caídas y use también una protección frente a la humedad. También hay que evitar los golpes fuertes y las vibraciones.

2.6 Funcionamiento

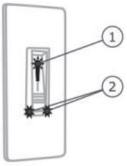
Funcionamiento del escáner de huella digital
El escáner de huella digital captura la imagen del dedo mediante un sensor lineal y la analiza. Compara el resultado con la información biométrica almacenada en la huella dactilar de referencia. En caso de coincidencia abre la puerta. En caso de coincidencia abre la puerta.



Sin embargo, el escáner de huella digital solo funciona de manera correcta y fiable con los surcos interpapilares de la última falange (1).
Deslice el dedo sobre el sensor de manera suave y uniforme, tal como se describe más abajo.



La guía del dedo del escáner de huella digital sirve para la correcta colocación del dedo. Esta guía es el elemento de manejo propiamente dicho, y consta del sensor (2) y de los bordes de referencia derecho (1) e izquierdo (3).

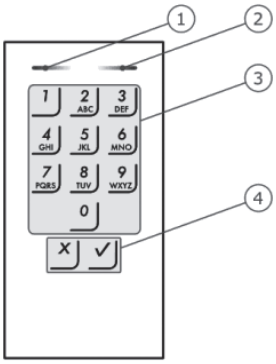


El lector de huella digital dispone de dos tipos de señales ópticas:

1 LED de estado para el estado operativo

2 LED de funcionamiento para el funcionamiento del sistema completo

Funcionamiento del teclado de código



2 LED de estado señalizan los estados de funcionamiento (código PIN correcto, código PIN incorrecto, punto del menú, ...).

Un emisor de señales acústicas señaliza la pulsación de las teclas y la autorización del acceso.

1 LED de estado izquierdo

2 LED de estado derecho

3 Teclas de introducción

4 Teclas de confirmación

La retroiluminación del teclado es azul, de intensidad regulable y se activa o desactiva en función de la luz que haya.

NOTA

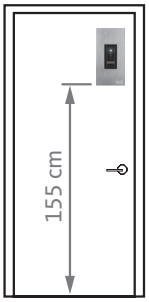
El teclado de código retorna al cabo de 10 segundos al funcionamiento normal si no se pulsa ninguna tecla. En este caso, se desechan las entradas y modificaciones.

3. Montaje

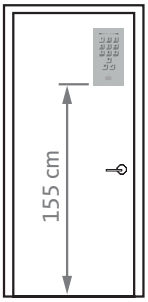
El escáner de huella digital o el teclado de código se montan por lo general en la zona exterior (lado exterior de la puerta) (véase Capítulo 3.6) y conectados a la unidad de control a través de una línea de datos. Utilice el cable del sistema BKS para establecer la conexión.

3.1 Altura de montaje

B-55600-13-4-6



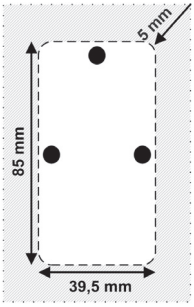
B-55600-10-4-6



- ¡La altura de montaje exigida para el escáner de huella digital es de 155 cm o superior como mínimo!

HINWEIS **Solo con un montaje a la altura correcta queda garantizado un buen funcionamiento.**

3.2 Medidas de fresado

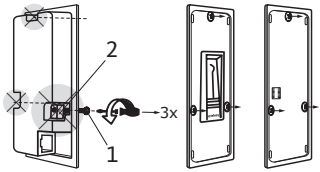


Realice en el perfil de su puerta o en la puerta de madera un fresado con las medidas indicadas a continuación.

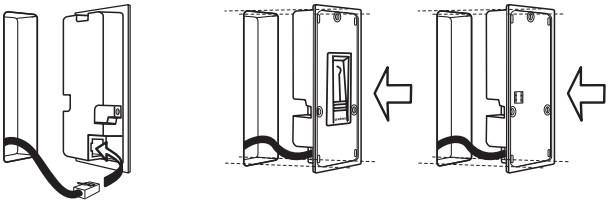
* medidas de fresado recomendadas (pueden variar en función del material), tolerancia ±0,2 mm.

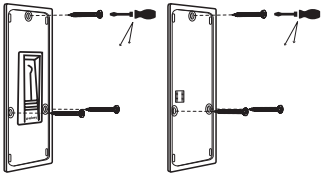
3.3 Variantes de fijación

3.3.1 Fijación en hojas de madera

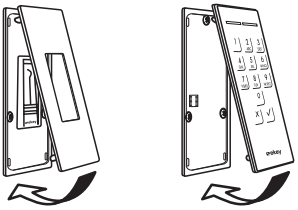


Quite los tres tornillos (1) junto con los salientes (2).



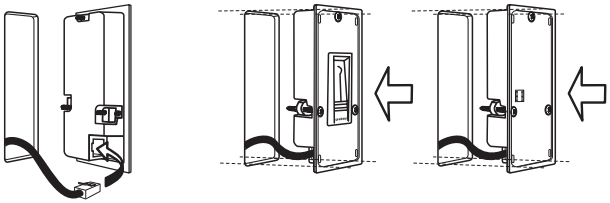


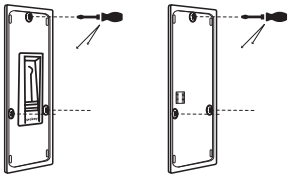
Utilice los tornillos suministrados para la fijación en madera.



Finalmente, fijar a presión
el elemento decorativo, junta incluida,
para el uso exterior.

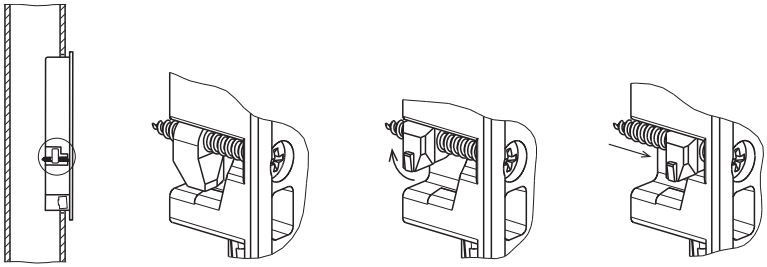
3.3.2 Fijación en el perfil, en la placa frontal, en el cuadro de distribución



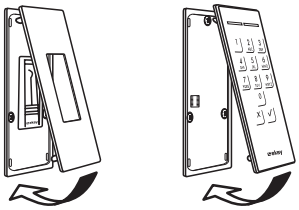


Apretar los tornillos con un destornillador hasta que el escáner de huella digital esté fijo.

No lo fije demasiado, la carcasa podría dañarse.



Apretando los tornillos, los salientes se mueven hacia fuera y aprietan el escáner de huella digital en el perfil o en la placa frontal.

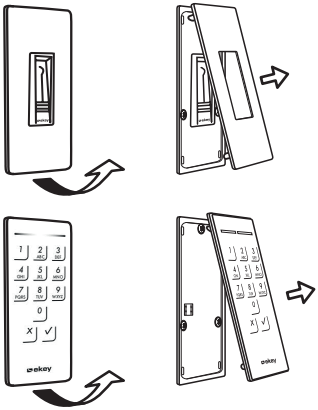


Finalmente, fijar a presión
el elemento decorativo, junta incluida,
para el uso exterior.

3.4 Desmontaje del elemento decorativo

ATENCIÓN

¡Asegúrese de no dañar la superficie de la puerta durante este paso!
Desmotar con cuidado el elemento decorativo.



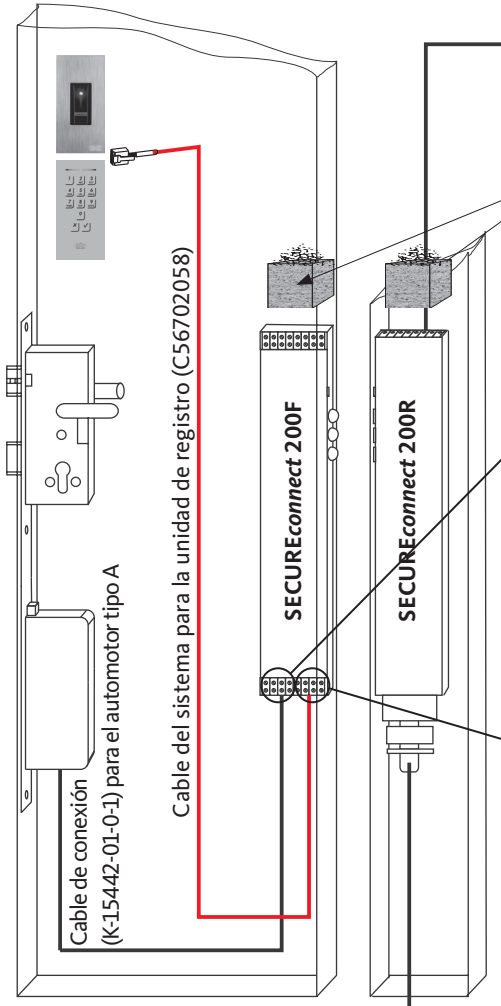
En el lado inferior del elemento decorativo hay una entalladura.

Utilizando, por ejemplo, un destornillador, eleve el elemento decorativo por esta zona hasta desencastrar las lengüetas.

Mueva un poco hacia arriba el elemento decorativo y tire de este hacia arriba en diagonal.

Limpiar a fondo la junta y engrasar antes del montaje en caso necesario.

3.5 Esquema de conexión del automotor tipo A



Contacto de acceso sin potencial, p. ej., botón pulsador, interfono, control de acceso, interruptor temporizador.

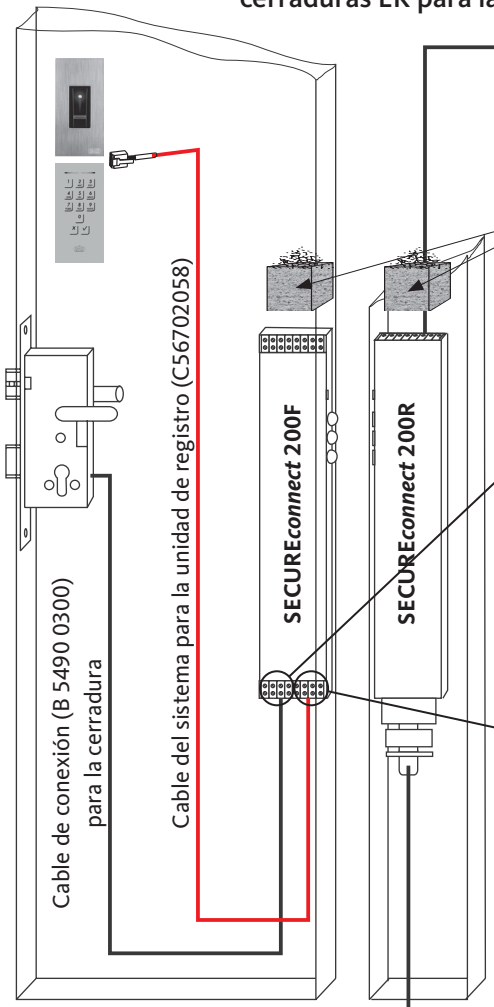
Utilice las esponjas adjuntas como protección contra virutas al realizar el montaje en perfiles metálicos.

SC 200F	Cable de conexión del automotor tipo A	
Borne	Color del cable	Señal
GS	GY | Gris (BU | Azul)	GND (negativo)
VS	BN | Marrón	24 V (positivo)
90	BK | Negro	Conductor de control

SC 200F	Cable del sistema de la unidad de registro	
Borne	Color del cable	Señal
GS	BN | Marrón	GND (negativo)
96	YE | Amarillo	RS485 A
95	GN | Verde	RS485 B
94	WH | Blanco	+24 V (positivo)

En puertas de metal y de PVC, usar la protección de cables incluida para la salida del cable.

3.6 Esquema de conexión de los bloqueos del motor y las cerraduras EK para las conexiones sin potencial



Contacto de acceso sin potencial, p. ej., botón pulsador, interfono, control de acceso, interruptor temporizador.

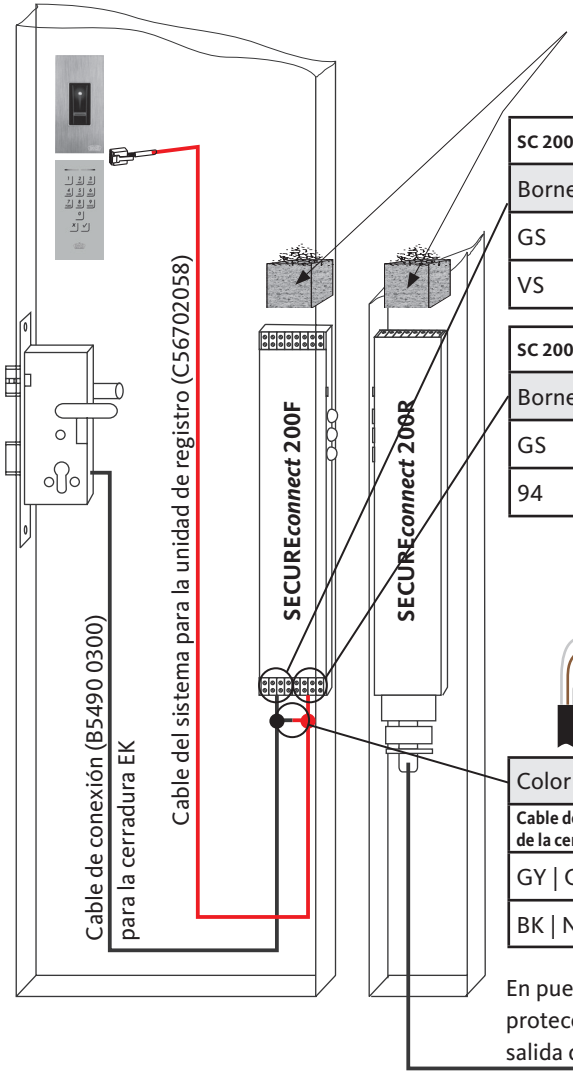
Utilice las esponjas adjuntas como protección contra virutas al realizar el montaje en perfiles metálicos.

SC 200F	Cable de conexión de la cerradura	
Borne	Color del cable	Señal
GS	WH | Blanco	GND (negativo)
VS	BN | Marrón	24 V (positivo)
90	PK | Rosa	Conductor de control

SC 200F	Cable del sistema de la unidad de registro	
Borne	Color del cable	Señal
GS	BN | Marrón	GND (negativo)
96	YE | Amarillo	RS485 A
95	GN | Verde	RS485 B
94	WH | Blanco	24 V (positivo)

En puertas de metal y de PVC, usar la protección de cables incluida para la salida del cable.

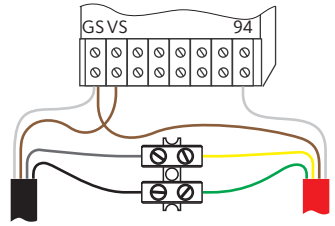
3.7 Esquema de conexión de la cerradura EK para el bus RS485



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 cable	Señal
GS	WH | Blanco	GND (negativo)
VS	BN | Marrón	24 V (positivo)

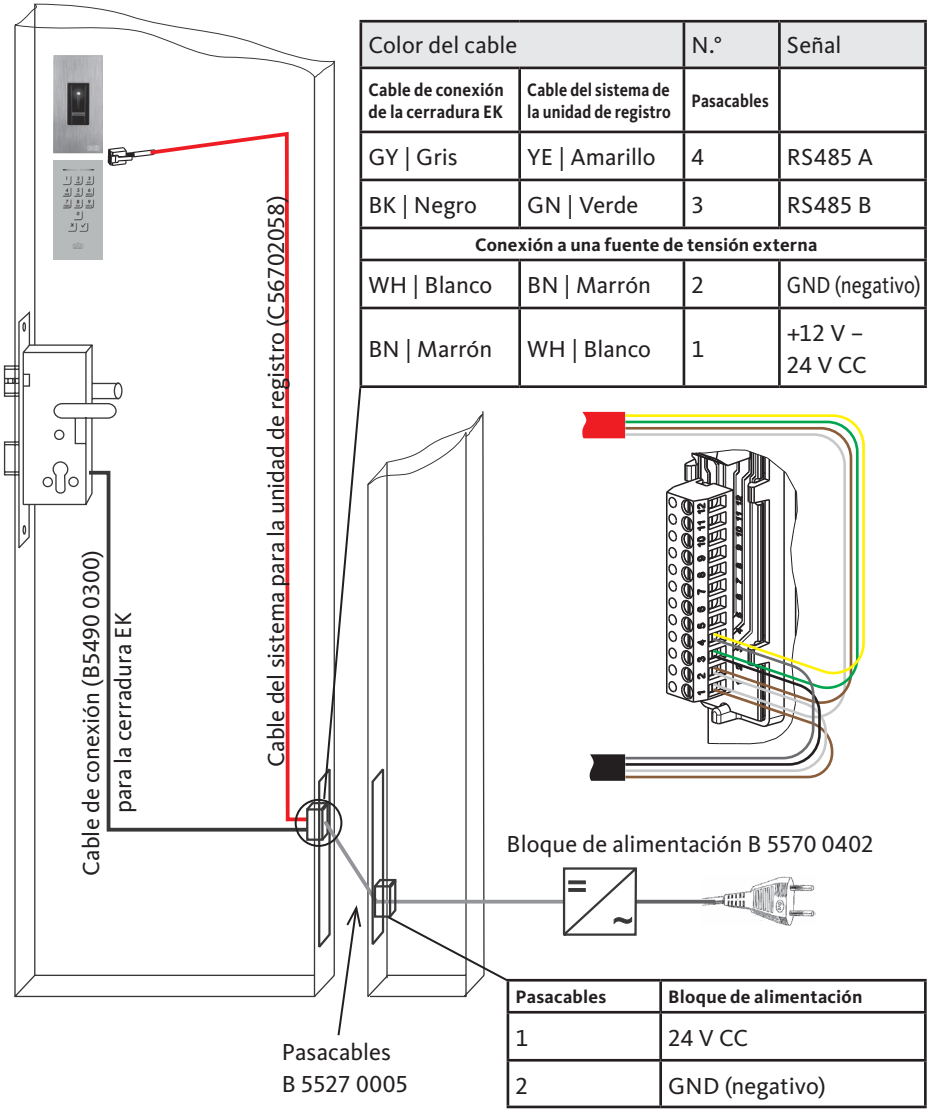
SC 200F	Cable del sistema de la unidad de registro	
Borne	Color del cable	Señal
GS	BN | Marrón	GND (negativo)
94	WH | Blanco	24 V (positivo)



Color del cable		Señal
Cable de conexión de la cerradura EK	Cable del sistema de la unidad de registro	
GY | Gris	YE | Amarillo	RS485 A
BK | Negro	GN | Verde	RS485 B

En puertas de metal y de PVC, usar la protección de cables incluida para la salida del cable.

3.7.1 Conexión a una fuente de tensión externa



Color del cable		N.°	Señal
Cable de conexión de la cerradura EK	**Cable del sistema de la unidad de registro**	**Pasacables**	
GY | Gris	YE | Amarillo	4	RS485 A
BK | Negro	GN | Verde	3	RS485 B
Conexión a una fuente de tensión externa			
WH | Blanco	BN | Marrón	2	GND (negativo)
BN | Marrón	WH | Blanco	1	+12 V – 24 V CC

Pasacables	Bloque de alimentación
1	24 V CC
2	GND (negativo)

3.7.2 Emparejamiento del escáner de huella digital/teclado de código con cerradura EK

La unidad de registro y la unidad de control se acoplan automáticamente de forma unívoca (emparejamiento) durante la primera puesta en servicio mediante la conexión bus RS485.

Para cambiar un componente (lector de huella digital, teclado de código o cerradura) del sistema de la puerta tras el emparejamiento, es necesario realizar el reemparejamiento antes de volver a emparejar 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:

- Accionamiento permanente de la manilla.
- Con la apertura y el cierre utilizando una llave mecánica, pasar 3 veces el sensor del paletón de cierre.

Una vez concluido el reemparejamiento, se eliminan todos los dispositivos emparejados y los componentes pueden volver a «emparejarse» de nuevo.

4. Puesta en marcha

Para manejarlos, es necesario poner en funcionamiento los dispositivos. La puesta en marcha del sistema empareja la unidad de control con la unidad de registro. Para la puesta en marcha de su sistema de acceso, siga los pasos que se indican a continuación:

- Monte los dispositivos tal y como se describe en el Capítulo 3.
- La conexión eléctrica de los componentes debe realizarse conforme al esquema de conexión.

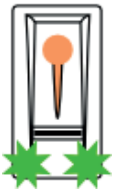
4.1 Puesta en marcha del escáner de huella digital

- Conecte el bloque de alimentación o SECURE*connect* a la red.
- Tras su primera activación, el escáner de huella digital y SECURE*connect* o la cerradura EK realizan un emparejamiento automático. Una vez completado el emparejamiento, el LED azul parpadeará.

El lector de huella digital no está emparejado con SC200/cerradura EK.

El lector de huella digital está emparejado con SC200/cerradura EK. No hay ningún dedo guardado.

Escáner de huella digital acoplado al dispositivo Bluetooth.



El lector de huella digital está emparejado con SC200/cerradura EK - menú de administrador.

4.1.1 Concepto de manejo

Están disponibles dos conceptos de manejo distintos:

- Aplicación: administración del escáner de huella digital Bluetooth mediante un dispositivo móvil (Capítulo 6.1, a partir de la página 186)
- Dedo administrador: administración del escáner de huella digital Bluetooth mediante dedo administrador (Capítulo 6.3, a partir de la página 193)

4.1.2 Modo de prueba

Conecte la tensión de red y realice la prueba antes de que transcurran 10 minutos. Una vez transcurridos los 10 minutos, para realizar la prueba será preciso volver a encender el escáner de huella digital para restablecerlo.

El lector de huella digital está emparejado con SC200/cerradura EK. No hay ningún dedo guardado.

Coloque el dedo sobre el sensor de 3 a 5 segundos.

El relé conmutará cuando retire el dedo (SECURE*connect* o cerradura EK).

NOTA

Solo se podrá realizar una prueba si todavía no hay dedos administradores guardados y si aún no se ha emparejado ningún dispositivo móvil.

Puede colocar su dedo sobre el sensor durante un total de 5 segundos como máximo. Si mantiene el dedo sobre el sensor durante más tiempo, el relé (SECURE*connect* o cerradura EK) no conmutará.

4.2 Puesta en marcha del teclado de código

- Tras la primera conexión, realice un emparejamiento automático del teclado de código y el SECURE*connect*. Los LED de estado del teclado de código parpadean en amarillo de forma alterna. Una vez finalizado el emparejamiento no hay encendido ningún LED de estado.

El teclado de código no está emparejado con SC200/cerradura EK.

El teclado de código está emparejado con SC200/cerradura EK.

ATENCIÓN

¡Inmediatamente después de la puesta en marcha, cambie el código de administrador de fábrica 9999 y manténgalo en secreto!
Si no se modifica el código de administrador, permitirá que personas no autorizadas accedan a su menú de administración y que, a continuación, entren en su casa.

4.2.1 Señalización óptica

Indicación	LED de estado izquierdo	LED de estado derecho	Significado
	Off	Off	Standby
	Amarillo parpadeante	Amarillo parpadeante	Ajuste de fabrica/ningún emparejamiento con la unidad de control
	Amarillo	Off	Operativo para la introducción del código de administrador
	Verde	Off	Menú de administración activo
	Verde	Verde	Entrada positiva: código PIN correcto, valor de entrada correcto, ...
	Rojo	Rojo	Entrada negativa: código PIN incorrecto, valor de entrada incorrecto, ...
	Off	Rojo	Bloqueo del sistema de 1 minuto o de 15 minutos

5. Manejo del lector de huella digital

Deslice el dedo

Mantenga el dedo recto y colóquelo centrado entre los bordes de referencia. No gire el dedo.

Sitúe la articulación de la última falange directamente sobre el sensor. Apoye el dedo plano sobre la guía del dedo.

Extienda los dedos contiguos.

Mueva de modo uniforme el dedo hacia abajo sobre el sensor. Acompañe el movimiento con toda la mano. Para obtener resultados óptimos, deslice por completo la última falange sobre el sensor.
El movimiento tarda aprox. 1 segundo.

Consejos generales para una buena calidad de la imagen del dedo

- Los mejores resultados se logran con los dedos índice, corazón y anular. Las imágenes proporcionadas por los dedos pulgar y meñique dificultan la evaluación.
- Si suele tener los dedos húmedos, guárdelos en la memoria en estado húmedo.
- Funciona con dedos de niños a partir de unos 5 años.

Toque con el dedo

Toque el sensor rápida y brevemente con el dedo.

6. Programación del escáner de huella digital

6.1 Programación con la aplicación open biometric

Para poder iniciar la programación, el escáner de huella digital debe estar emparejado con SECURE*connect*.

NOTA **La aplicación open biometric solo se puede utilizar en combinación con el escáner de huella digital Bluetooth.**

La aplicación open biometric sirve para la programación del sistema. Además, la aplicación permite abrir puertas.

6.1.1 Descargar aplicación

La aplicación está disponible para Apple iOS y Google Android. Descargue la aplicación open biometric desde la App Store o Google Play. Para ello, introduzca «open biometric» en el campo de búsqueda.

Download on the App Store GET IT ON Google Play

Para el primer emparejamiento necesitará el código de acoplamiento del dispositivos y el código de seguridad de la aplicación. **Ambos códigos son 9999 de fábrica.**

- Inicie la aplicación open biometric.
- Toque el botón de entrada (Android) o pulse «Buscar» (iOS). La aplicación buscará dispositivos Bluetooth disponibles.

- Seleccione su escáner de huella digital Bluetooth (se mostrarán los últimos 4 dígitos del número de serie).
- Solo en Android: pulse «Iniciar sesión».
- Introduzca el **código de acoplamiento del dispositivos de serie 9999**.
- Pulse «Siguiente». El dispositivo móvil se acoplará al lector de huella digital Bluetooth.

- Introduzca un nuevo código de acoplamiento del dispositivos de 6 dígitos. Por motivos de seguridad, durante el primer acoplamiento del sistema deberá cambiar el código de acoplamiento del dispositivos de fábrica. Anote este código, ya que será necesario para emparejar otros dispositivos móviles.

  Su código de acoplamiento del dispositivos:

- Pulse «Cambiar» (Android) o «Siguiente» (iOS).
- Introduzca el código de seguridad de la aplicación de fábrica 9999.
- Pulse «Siguiente».

Se ha realizado el emparejamiento entre el escáner de huella digital Bluetooth y el dispositivo móvil. El sistema se encuentra en funcionamiento normal.

Ahora puede utilizar la aplicación open biometric para programar y gestionar el sistema de acceso mediante escáner de huella digital.

NOTA

Para administrar su escáner de huella digital Bluetooth ya solo necesitará la intuitiva aplicación open biometric.
Pulse las funciones deseadas en la aplicación y siga las instrucciones en la pantalla.

6.1.2 Cambiar código de seguridad

Puede cambiar en cualquier momento todos los códigos de seguridad.

- Código de seguridad de la aplicación
- Código de acoplamiento de administrador
- Código de acoplamiento de usuario

NOTA

El código de seguridad de la aplicación de 4 a 6 dígitos se necesita para la pregunta de seguridad de la aplicación. Puede desactivar la solicitud del código de seguridad de la aplicación en «ADMINISTRACIÓN», en caso de que su dispositivo móvil cuente con mecanismos de bloqueo seguros (huella dactilar, código, etc).

- Seleccione «ADMINISTRACIÓN».
- Seleccione «CAMBIAR CÓDIGOS DE SEGURIDAD».
- Cambie el código deseado.
- Pulse «Cambiar» (Android) o «Listo» (iOS).

Se habrá cambiado el código de seguridad seleccionado.

6.1.3 Guardar dedo

Puede guardar los dedos de administrador y de usuario mediante la aplicación open biometric.

- Seleccione «ADMINISTRACIÓN».
- Seleccione «ADMINISTRACIÓN DE USUARIOS».
- Pulse  (Android) o «+» (iOS).
- Introduzca el nombre de usuario.
- Pulse «Nueva autorización de administración» o «Nueva autorización de acceso».
- Seleccione el relé que hay que conmutar (para el SECURE*connect* o la cerradura EK conectada).
- Seleccione un dedo.
- Seleccione «Guardar».
- Lea el mensaje y pulse «Iniciar».
- En cuanto se haya registrado correctamente su dedo, pulse «OK».
- Pulse «Listo».

NOTA **Guarde como mínimo un dedo de cada mano por punto de acceso.**

6.1.4 Desactivar Bluetooth

Puede desactivar la función de Bluetooth.
La función de Bluetooth está activada en los ajustes de fábrica.

- Inicie la aplicación open biometric.
- Seleccione «ADMINISTRACIÓN».
- Seleccione «ESTADO DEL SISTEMA».
- En «CONFIGURACIÓN DE BLUETOOTH» active «Desactivar Bluetooth al cabo de 15 minutos».

Con este ajuste, el Bluetooth se desactivará en el escáner de huella digital al cabo de 15 minutos si se da uno de los siguientes casos:

- Si no se ha conectado ningún dispositivo móvil.
- Si se ha guardado como mínimo un dedo.

Puede volver a activar Bluetooth: acceda al menú de administrador y deslice cualquier dedo administrador sobre el sensor.

6.1.5 Emparejar otros dispositivos móviles

Puede emparejar otros dispositivos móviles al escáner de huella digital Bluetooth mediante el código de acoplamiento de administrador o de usuario de 6 dígitos que haya escogido.

- Inicie la aplicación open biometric.
- Empareje el dispositivo móvil al escáner de huella digital Bluetooth mediante el código de acoplamiento de administrador o de usuario de 6 dígitos que haya escogido.
- Se realizará el emparejamiento entre el escáner de huella digital Bluetooth y el dispositivo móvil.

Ahora puede utilizar la aplicación para programar y gestionar el escáner de huella digital.

6.1.6 Utilizar varios escáneres de huella digital Bluetooth

La aplicación open biometric permite utilizar varios escáneres de huella digital Bluetooth. Para alternar entre dos escáneres de huella digital Bluetooth, deberá restablecer el emparejamiento entre el escáner de huella digital Bluetooth y el dispositivo móvil.

NOTA

Al restablecer el emparejamiento se borrarán los nombres de relé (SECURE*connect* o cerradura EK) y las fotografías de usuarios guardadas. Los nombres de usuario y las autorizaciones permanecerán guardados en el escáner de huella digital Bluetooth.

- Inicie la aplicación open biometric.
- Seleccione «ADMINISTRACIÓN».
- Seleccione «RESTABLECER ACOPLAMIENTO».
- Confirme el restablecimiento mediante «Continuar».

Se ha restablecido el emparejamiento entre el escáner de huella digital Bluetooth y el dispositivo móvil. Ahora puede emparejar otro escáner de huella digital Bluetooth.

6.2 Guardar código de acoplamiento de usuario

Puede guardar un código de acoplamiento de usuario. Puede facilitar este código a una persona de su elección. Este código permite ejecutar las siguientes acciones:

- Abrir puerta
- Activar o desactivar el código de seguridad de la aplicación
- Cambiar el código de seguridad de la app
- Restablecer el emparejamiento entre el escáner de huella digital y el dispositivo móvil

Para guardar el código de acoplamiento de usuario, ejecute los siguientes pasos:

- Inicie la aplicación open biometric.
- Seleccione «ADMINISTRACIÓN».
- Seleccione «CAMBIAR CÓDIGOS DE SEGURIDAD».
- Introduzca en el campo correspondiente el código de acoplamiento de usuario deseado.
- Confirme las entradas pulsando «Cambiar» (Android) o «Listo» (iOS).

El código de acoplamiento de usuario está ahora guardado.

6.2.1 Restablecer código de seguridad de la aplicación

- Inicie la aplicación open biometric.
- Introduzca un código de seguridad de la aplicación incorrecto.
- Confirme la entrada mediante «Siguiente».
- Seleccione «RESTABLECER ACOPLAMIENTO».
- Confirme el restablecimiento mediante «Continuar».

Se restablecerá el emparejamiento entre el escáner de huella digital Bluetooth y el dispositivo móvil y se establecerá en 9999 el código de seguridad de la aplicación.

Ahora puede emparejar de nuevo el escáner de huella digital Bluetooth y asignar un nuevo código de seguridad de la aplicación.

6.2.2 Proteger el sistema contra pérdida del dispositivo móvil

Si ha perdido su dispositivo móvil, mediante un segundo dispositivo móvil puede cambiar el código de acoplamiento de administrador o de usuario. Mediante el nuevo código de acoplamiento de administrador o de usuario impedirá el establecimiento de conexión del dispositivo móvil extraviado.

- Inicie la aplicación open biometric en el segundo dispositivo móvil.
- Empareje el segundo dispositivo móvil al escáner de huella digital Bluetooth.

- Seleccione «ADMINISTRACIÓN».
- Seleccione «CAMBIAR CÓDIGOS DE SEGURIDAD».
- Introduzca un nuevo código de acoplamiento de administrador o de usuario de 6 dígitos.
- Confirme la entrada pulsando «Cambiar» (Android) o «Listo» (iOS).

Se ha cambiado en el sistema el código de acoplamiento de administrador o de usuario.

El dispositivo móvil extraviado ya no podrá establecer una conexión con el escáner de huella digital Bluetooth. Su sistema estará protegido contra accesos de personas no autorizadas.

6.2.3 Restablecer los ajustes de fábrica en el sistema

- Inicie la aplicación open biometric.
- Conéctese al escáner de huella digital Bluetooth.
- Seleccione «ADMINISTRACIÓN».
- Seleccione «RESTABLECER SISTEMA».
- Confirme el restablecimiento mediante «Continuar».

El sistema se ha restablecido a los ajustes de fábrica. Ahora puede volver a poner el sistema en funcionamiento.

NOTA

¡Se borrarán todos los dedos de usuario y todos los dedos de administrador!
¡El emparejamiento entre el escáner de huella digital y SECURE*connect* 200 o la cerradura EK se mantendrá!

En caso de reemparejamiento del SECURE*connect* 200 también se restablecerá al estado de fábrica el escáner de huella digital.

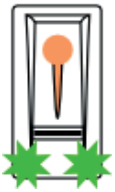
6.3 Programación con dedos administradores

6.3.1 Guardar dedo administrador

Los dedos administradores sirven para la programación del sistema. Guarde inicialmente 4 dedos administradores distintos. Cada dedo deberá **ser escaneado 3 veces como mínimo**. Le recomendamos guardar 2 dedos de dos personas diferentes.

El lector de huella digital está emparejado con SC200/ cerradura EK. No hay ningún dedo guardado.

Tres toques con el dedo en un lapso de 5 segundos.



Modo de administración activo.

Deslice el primer dedo administrador sobre el sensor.

Se ha detectado el dedo.

El sistema está listo para la repetición.

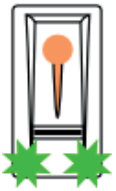
Deslice de nuevo el primer dedo administrador sobre el sensor.

Se ha detectado el dedo.

El sistema está listo para la repetición.

Deslice de nuevo el primer dedo administrador sobre el sensor.

La calidad de los tres escaneos es excelente.



El escáner de huella digital está listo para escanear los demás dedos administradores.

Otras indicaciones posibles durante el proceso de memorización:

La calidad del escaneo es suficiente. Se puede mejorar la calidad mediante escaneos adicionales.

Error durante el proceso de escaneo, o la calidad es insuficiente.
Deslice de nuevo este dedo sobre el sensor.

NOTA

Al reiniciar el escáner de huella digital, si este se encuentra en modo de administración y están guardados menos de 4 dedos administradores, se borrarán todos los dedos administradores ya guardados.

Durante el proceso de memorización de los dedos no deben transcurrir más de 10 segundos entre los escaneos de dedos. De lo contrario se cancelará la memorización del dedo.

6.3.2 Guardar dedo de usuario

Mediante los dedos de usuario puede ejecutar una apertura de puerta. Se pueden utilizar como dedos de usuario todos los dedos que no sean dedos administradores.

Funcionamiento normal

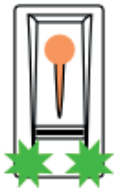
Tres toques con el dedo en un lapso de 5 segundos.

Menú de administración

Deslice un dedo administrador cualquiera sobre el sensor.

Dedo administrador detectado. Modo de memorización activo.

Un toque con el dedo en un lapso de 5 segundos.



El modo de registro está activado.

Deslice sobre el sensor el dedo que desee guardar.

Se ha detectado el dedo.

El sistema está listo para la repetición.

Deslice sobre el sensor el dedo que desee guardar.

Se ha detectado el dedo.

El sistema está listo para la repetición.

Deslice sobre el sensor el dedo que desee guardar.

Se ha detectado el dedo.

Se ha guardado correctamente el dedo.

Después de guardar el dedo de usuario: funcionamiento normal.

6.3.3 Borrar dedo de usuario

Los dedos de usuario solo se pueden borrar si está presente el respectivo usuario.

Funcionamiento normal

Tres toques con el dedo en un lapso de 5 segundos.

Menú de administración

Deslice un dedo administrador cualquiera sobre el sensor.

Dedo administrador detectado. Modo de memorización activo.

¡Espere 5 segundos!

Modo de borrado activo.

Un toque con el dedo.

Menú de gestión

Deslice sobre el sensor el dedo que desee borrar.

¡Dedo de usuario borrado!

Funcionamiento normal

6.3.4 Borrar todos los dedos de usuario

Se borrarán todos los dedos de usuario guardados en el sistema. Los dedos de administrador no se eliminarán.

Funcionamiento normal

Tres toques con el dedo en un lapso de 5 segundos.

Menú de administración

Deslice un dedo administrador cualquiera sobre el sensor.

Dedo administrador detectado. Modo de memorización activo.

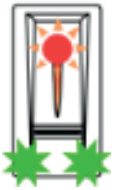
¡Espere 5 segundos!

Modo de borrado activo.

Un toque con el dedo.

Menú de gestión

Escanee de nuevo el mismo dedo administrador como arriba.



¡Se han borrado todos los dedos de usuario!

Funcionamiento normal

NOTA **Compruebe un dedo de usuario cualquiera. ¡Ya no deberá obtener autorización!**

6.3.5 Reseteo de fábrica del escáner de huella digital

Con esta acción restablecerá el estado de suministro del escáner de huella digital.

NOTA

¡¡Se borrarán todos los dedos de usuario y todos los dedos de administrador! ¡El emparejamiento entre el escáner de huella digital y SECURE*connect* 200 o la cerradura EK se mantendrá!

En caso de reemparejamiento del SECURE*connect* 200 o la cerradura EK también se restablecerá al estado de fábrica el escáner de huella digital.

Funcionamiento normal

Tres toques con el dedo en un lapso de 5 segundos.

Menú de administración

Deslice un dedo administrador cualquiera sobre el sensor.

Dedo administrador detectado. Modo de memorización activo.

¡Espere 5 segundos!

Modo de borrado activo.

Un toque con el dedo.

Menú de gestión

Escanee un dedo administrador distinto al escaneado anteriormente.

¡Se han borrado todos los dedos de usuario y de administrador!

El lector de huella digital está emparejado con SC200/ cerradura EK. No hay ningún dedo guardado.

7. Programación del teclado de código

Para la programación hay disponibles una serie de puntos en el menú de administración. Para acceder a los mismos pueden utilizarse las teclas.

Tecla	Punto del menú
1	Guardar el código de usuario
2 ABC	Borrar el código de usuario
3 DEF	Cambiar el código de administrador
4 GHI	Restablecer los ajustes de fábrica en el sistema
5 JKL	Ajustar el teclado para la introducción de código

7.1 Cambiar el código de administrador

Esta función permite cambiar el código de administrador existente. El código de administrador puede tener entre 4 y 8 dígitos y tiene que contener al menos un número diferente. La modificación del código de administrador se realiza mediante el menú de administrador. Para acceder a este menú, introduzca el código de administrador.

NOTA **Los códigos de administrador no se pueden utilizar como códigos de usuario.**

Pulse √ para iniciar la entrada del código de administrador.

Introduzca el código de administrador (por defecto = 9999).

√

3

√

Introduzca el antiguo código de administrador.

√

Introduzca el nuevo código de administrador.

√

Vuelva a introducir el nuevo código de administrador.

√

7.2 Guardar el código de usuario

El sistema permite guardar un máximo de 99 códigos de usuario. Un código de usuario es un código PIN con el que se activa una acción en la unidad de control como, por ejemplo, la apertura de una puerta. El código de usuario puede tener entre 4 y 8 dígitos y tiene que contener al menos un número diferente.

NOTA

Utilice un código de usuario largo. De ser posible, utilice todos los numéros. Utilice diferentes códigos para cada usuario autorizado.

Pulse √ para iniciar la entrada del código de administrador.

Introduzca el código de administrador.

√

1

√

Introduzca el código de usuario.

√

Vuelva a introducir el código de usuario.

√

7.3 Borrar el código de usuario

Ud. puede borrar los códigos de usuario. Para ello, necesita el código del usuario que desea borrar.

Un código de usuario se borra mediante el menú de administrador. Para acceder a este menú, introduzca el código de administrador.

Pulse √ para iniciar la entrada del código de administrador.

Introduzca el código de administrador.

√

2

√

Introduzca el código de usuario que desea borra.

√

7.4 Restablecer los ajustes de fábrica en el sistema

Se restablecen los ajustes de fábrica en el teclado para la introducción de código. Se borran todos los códigos de usuario de forma irreversible. Se restablece el código de administrador de fábrica 9999, se restablece el umbral de brillo al 10 % y el valor del brillo al 100 %. Se vuelve a activar la señalización acústica y óptica para la pulsación de las teclas y la señal acústica para la apertura de la puerta.

Los ajustes de fábrica también se restablecen en el teclado para la introducción de código mediante un proceso de reemparejamiento (véase Capítulo 2.2).

Pulse √ para iniciar la entrada del código de administrador.

Introduzca el código de administrador.

√

4

√

Introduzca el código de administrador.

√

7.5 Ajustar la retroiluminación automática

Aquí puede establecer el umbral de brillo con el que se activará automáticamente la retroiluminación azul durante las horas crepusculares.

El umbral de brillo se puede ajustar con porcentajes. El umbral de brillo de fábrica es del 10 %. Introduzca el porcentaje deseado:

0 = retroiluminación automática
De 1 a 100 = umbral de brillo desde la activación en un entorno con mucha claridad hasta la activación en un entorno muy oscuro

Pulse √ para iniciar la entrada del código de administrador.

Introduzca el código de administrador.

√

51

Valor del umbral de brillo deseado, p. ej. 70.

√

7.6 Ajustar el brillo de la retroiluminación

El brillo de la retroiluminación se puede ajustar mediante 4 modos predefinidos. De fábrica, la retroiluminación establecida es del 100 %. Indique el número del modo deseado:

0 = retroalimentación desactivada
1 = retroalimentación activada al 33 %
2 = retroalimentación activada al 66 %
3 = retroalimentación activada al 100 %

El ajuste del brillo de la retroiluminación se realiza mediante el menú de administración. Para acceder a este menú, introduzca el código de administrador.

Pulse √ para iniciar la entrada del código de administrador.

Introduzca el código de administrador.

√

52

Número del modo deseado, p. ej., 2.

√

7.7 Ajustar la señalización de la pulsación de las teclas

La señalización acústica y óptica de la pulsación de las teclas se puede ajustar mediante 4 modos predefinidos. Las señales acústicas y ópticas para la pulsación de las teclas viene activada de fábrica. Indique el número del modo deseado:

0 = señales ópticas y acústicas desactivadas
1 = señales acústicas activadas y señales ópticas desactivadas
2 = señales acústicas desactivadas y señales ópticas activadas
3 = señales acústicas y ópticas activadas

El ajuste de la señalización de la pulsación de las teclas se realiza mediante el menú de administración. Para acceder a este menú, introduzca el código de administrador.

Pulse √ para iniciar la entrada del código de administrador.

Introduzca el código de administrador.

√

54

Número del modo deseado, p. ej., 2.

√

7.8 Ajustar la señal acústica de la apertura

La señal acústica de la apertura se puede desactivar y activar. La señal acústica viene activada de fábrica. Indique el número del modo deseado:

0 para desconectar
1 para conectar

El ajuste de la señal acústica de la apertura se realiza mediante el menú de administración. Para acceder a este menú, introduzca el código de administrador.

Pulse √ para iniciar la entrada del código de administrador.

Introduzca el código de administrador.

√

55

Número del modo deseado, p. ej., 0.

√

8. Apertura de puerta

La apertura de puerta puede tener lugar con la aplicación open biometric o con el teclado de código.

8.1 Apertura de puerta con la aplicación open biometric

El sistema se encuentra en funcionamiento normal.

- Inicie la aplicación open biometric. El dispositivo móvil se conectará al escáner de huella digital Bluetooth.
- Seleccione «ACCESOS».
- Deslice hacia la derecha el control deslizante del acceso que desee abrir.

SECURE*connect* enviará entonces la señal de control al automotor tipo A y a la cerradura motorizada y su puerta se abrirá. La cerradura EK recibe directamente la señal de control.

8.2 Apertura de puerta con escáner de huella digital

Funcionamiento normal

Deslice sobre el sensor un dedo de usuario o administrador guardado.

Se ha detectado correctamente el dedo.

Tras apertura de puerta: funcionamiento normal.

NOTA

Al utilizar el lector de huella digital con un SC200, si deja la puerta abierta durante más de 12 segundos, el lector de huella digital se desconecta de la red. Una vez se haya cerrado y se haya restablecido la fuente de alimentación, el escáner de huella digital mostrará durante poco tiempo «No hay ninguna conexión de bus» hasta que el funcionamiento normal se haya restablecido automáticamente.

8.3 Apertura de puerta con teclado de código

Introduzca un código de usuario guardado.

Pulse √ y la puerta se abrirá.

No se ha detectado el código de usuario.

NOTA

Al introducir el código incorrectamente 3 veces, el sistema se bloqueará durante 1 minuto. Al introducir, a continuación, el código incorrectamente 3 veces, el sistema se bloqueará otros 15 minutos. Al volver a introducir el código incorrectamente, el sistema se bloqueará otros 15 minutos.
El sistema se puede desbloquear antes de que transcurra dicho tiempo introduciendo dos veces seguidas un código de usuario habilitado. En este caso, el usuario no recibirá ninguna señalización.

NOTA

Al utilizar el teclado de código con un SC200, si deja la puerta abierta durante más de 12 segundos, el teclado de código se desconecta de la red.
Una vez se haya cerrado y se haya restablecido la fuente de alimentación, el teclado de código mostrará durante poco tiempo «No hay ninguna conexión de bus» hasta que el funcionamiento normal se haya restablecido automáticamente.

9. Mantenimiento y cuidado

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 escáner de huella digital se ensucie de todos modos, límpielo con un paño suave húmedo (no empapado). Son adecuados los bastoncillos de algodón y los paños de microfibra y para 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 de vez en cuando 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.

En caso de uso frecuente, trate los contactos del SECURE*connect* con la grasa de contacto B-55606-00-4-0.

La disponibilidad del dispositivo de salida 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!

10. Búsqueda de fallos

Indicador y soluciónes

Indicador del lector de huella digital		**Causa**	**Solución**
	El LED de estado se ilumina en rojo.	No se ha detectado el dedo.	Deslice de nuevo el dedo sobre el sensor.
	Todos los LED se iluminan en rojo durante 1 minuto.	Bloqueo del sistema. Se ha detectado un dedo desconocido diez veces consecutivas.	Espere un minuto: el sistema volverá entonces al funcionamiento normal.
	El LED de estado parpadea en naranja.	No hay conexión de bus con SC200/ cerradura EK.	Compruebe el cableado o realice un nuevo restablecimiento de emparejamiento.
	El LED de estado parpadea en rojo/verde.	El sensor del escáner de huella digital está sucio o averiado.	Limpie o seque el sensor.

Indicador del teclado de código		Causa	Solución
	Los dos LED de estado se encienden en rojo.	No se ha detectado el código de usuario.	Vuelva a introducir el código de usuario.
		El código de usuario deseado está compuesto únicamente de números iguales, p. ej., 1111. 3333	Utilice códigos de usuario con números diferentes.
		El código de usuario deseado es demasiado corto o demasiado largo, p. ej., 321, 987654321.	Tenga en cuenta la longitud del código de usuario: mín. 4 dígitos, máx. 8 dígitos.
		Se ha producido un error al introducir puntos del menú o valores.	Repita la introducción.
	El LED de estado derecho se ilumina en rojo	3 intentos no válidos de introducción del código de usuario. Bloqueo del sistema durante 1 minuto o durante 15 minutos.	Introduzca dos veces seguidas un código de usuario autorizado. A continuación, se podrá abrir la puerta antes de que haya transcurrido el tiempo de bloqueo utilizando un código de usuario autorizado.
	Los LED de estado parpadean en amarillo de forma alterna.	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 reset de emparejamiento (véase Capítulo 2.2).

11. Mantenimiento y piezas de recambio

El producto no requiere mantenimiento. 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 de corriente y descargue la energía residual almacenada.

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 de BKS antes de realizar la reparación in situ y, en caso necesario, acordar el envío del dispositivo.

Desmonte el producto del espacio correspondiente. 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. Con respecto al uso de piezas de otros fabricantes, no existe ningún tipo de reclamación de responsabilidad, garantía o prestación de servicio.

12. 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 lector de huella digital y el teclado de código se deben desechar como basura electrónica en los puntos públicos de recogida y en los puntos de selección de residuos reciclables. El embalaje se debe eliminar por separado.

Notizen | Notes | Notes | Notas

03.2021 | 24413E | Designed 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