Designed in Germany
C59501108 | 04| 10.2018 | 20525E

CE

TÜRTECHNIK | DOOR TECHNOLOGY

BKS

B-55600-13-4-6

Vorsprung mit System
Securing technology for you

G-U BKS FERCO

Inhaltsverzeichnis

Originalanleitung

Bitte geben Sie das Dokument an den Benutzer weiter!

1. Sicherheitshinweise

HINWEIS HINWEIS kennzeichnet eine rein informative Aussage.

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

Lesen Sie diese Anleitung aufmerksam vor der Montage und Inbetriebnahme!

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!
- 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!

2. Technische Daten

Spannungsversorgung	10..24 V DC (max. 30 V)
Leistungsaufnahme	< 1 W
Umweltbedingungen	°C +70 °C -20 °C **IP54**
Template-Speicher	99 Fingertemplates
Template- Identifikationsdauer	1..2 s
Falschrückweisungrate (FRR)	1:100
Falschakzeptanzrate (FAR)	1:10.000.000
Lebensdauer	max. 10 Mio. Fingerscans
Zertifizierung	CE Die Zertifikate finden Sie auf www.g-u.com.

3. Manipulationsschutz

Ihr System besteht aus 2 elektronischen Geräten

- Fingerscanner
- SECURE*connect* 200 (Steuereinheit)

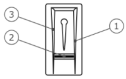
Der Fingerscanner wird in der Regel im Außenbereich (Türaußenseite) montiert. Um einer unbefugten Manipulation vorzubeugen ist Ihr System mit zahlreichen Sicherheitsfunktionen ausgestattet, die einen unbefugten Zutritt verhindern:

- Der Fingerscanner ist über eine Datenleitung mit der Steuereinheit verbunden. Die Datenübertragung ist verschlüsselt.
- Die Aufnahme von Benutzerfingern und die Änderung von Systeminhalten ist nur mittels vorheriger Erkennung eines Adminfingers möglich.
- Fingerscanner und Steuereinheit werden im Rahmen der Erstinbetriebnahme eindeutig miteinander gekoppelt (Pairing).

Um eine Komponente (SECURE*connect* 200R, SECURE*connect* 200F oder Fingerscanner) des Türsystems auszutauschen, muss eine Repairingprozedur durchlaufen werden. 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 Fingerscanner durchlaufen nun einen erneuten Pairingvorgang. Der Fingerscanner wird hierbei auf Werkseinstellung zurückgesetzt.

4. Bedienung des Fingerscanners

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 undgleichmäßig, 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.

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.

5. Inbetriebnahme des Systems

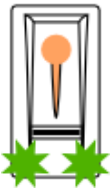
Für die Inbetriebnahme ihres Zutrittssystem gehen Sie schrittweise vor:

- Montieren Sie die Geräte nach beiliegender Montageanleitung.
- Führen Sie die Verkabelung nach beiliegender Montageanleitung aus.
- Nach dem ersten Einschalten führen Fingerscanner und SECURE*connect* eine automatische Koppelung durch. Nach Abschluss der Koppelung blinkt die blaue LED.

Fingerscanner ist nicht mit SC200 gekoppelt

Fingersanner ist mit SC200 gekoppelt. Es ist kein Finger gespeichert

Fingerscanner ist mit Bluetooth-Gerät verbunden



Fingerscanner ist mit SC200 gekoppelt - Adminmenü

5.1 Bedienkonzept

Es stehen zwei unterschiedliche Bedienkonzepte zur Verfügung:

- App – Administration des Bluetooth-Fingerscanners mittels mobilen Gerätes (Punkt 6, ab Seite 10)
- Adminfinger – Administration des Fingerscanners mittels Adminfinger (Punkt 7, ab Seite 19)

5.2 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 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.

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 nicht.

6. 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 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 ekey-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.

6.2 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.

6.3 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.
- 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.**

6.4 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.

6.5 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.

6.6 Mehrere Bluetooth-Fingerscanner verwalten

Die open biometric-App ermöglicht das Verwalten 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 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.

6.7 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.

6.8 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.

6.9 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.

6.10 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 bleibt erhalten!

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

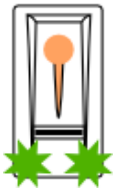
7. Programmierung mit Adminfingern

7.1 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.

Fingersanner ist mit SC200 gekoppelt. Es ist kein Finger gespeichert

3 Finger-Touches innerhalb von 5 s.



Adminmodus aktiv.

Ziehen Sie den ersten Adminfinger über den Sensor.

Der Finger wurde erkannt.

System ist bereit zur Wiederholung.

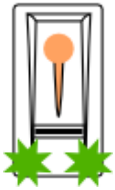
Ziehen Sie den ersten Adminfinger erneut über den Sensor.

Der Finger wurde erkannt.

System ist bereit zur Wiederholung.

Ziehen Sie den ersten Adminfinger erneut über den Sensor.

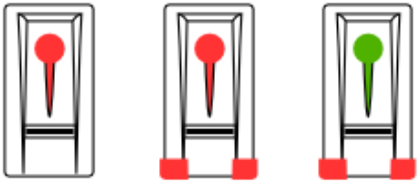
Qualität der drei Scans sehr gut.



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 Admininger vorhanden sind, werden alle bereits gespeicherten Admininger gelöscht.

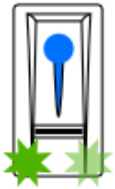
Während des Einspeicherns der Finger dürfen zwischen den einzelnen Fingerscans maximal 10 s vergehen. Das Einspeichern des Fingers wird sonst abgebrochen.

7.2 Benutzerfinger einspeichern

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

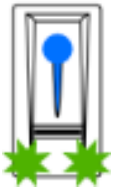
Normalbetrieb.

3 Finger-Touches innerhalb von 5 s.



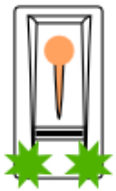
Adminmenü

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.

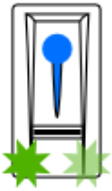
Nach Speichern des Benutzerfingers: Normalbetrieb.

7.3 Benutzerfinger löschen

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

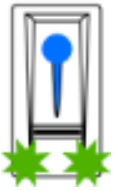
Normal-betrieb

3 Finger-Touches innerhalb von 5 s.



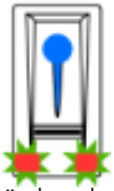
Adminmenü

Ziehen Sie einen beliebiegen Adminfinger über den Sensor.



Adminfinger wurde erkannt. Einspeicher-modus aktiv.

5 s warten!



Löschmodus aktiv

1 Finger-Touch

Verwal-tungsmenü

Ziehen Sie den zu löschenden Finger über den Sensor.

Benutzer-finger gelöscht!

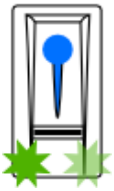
Normal-betrieb

7.4 Alle Benutzerfinger löschen

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

Normalbetrieb

3 Finger-Touches innerhalb von 5 s.

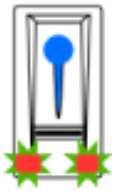


Adminmenü

Ziehen Sie einen beliebiegen Adminfinger über den Sensor.

Adminfinger wurde erkannt. Einspeichermodus aktiv.

5 s warten!

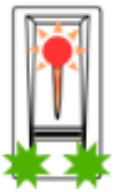


Löschmodus aktiv

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!**

7.5 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 bleibt erhalten!

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

Normal-betrieb

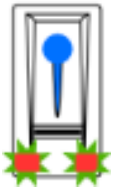
3 Finger-Touches innerhalb von 5 s

Adminmenü

Ziehen Sie einen beliebiegen Adminfinger über den Sensor.

Adminfinger wurde erkannt. Einspeicher-modus aktiv.

5 s warten!



Löschmodus aktiv

1 Finger-Touch

Verwal-tungsmenü

Einen anderen Adminfinger als zuvor scannen.

Alle Benut-zer- und Adminfinger gelöscht!

Fingersanner ist mit SC200 gekoppelt. Es ist kein Finger ge-speichert

8. Öffnen der Tür

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

8.2 Türöffnung mit Fingerscan

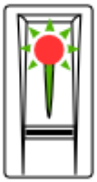
Normalbetrieb

Ziehen Sie einen eingespeicherten Benutzer oder Adminfinger über den Sensor.

Der Finger wurde erfolgreich erkannt.

Nach Türöffnung: Normalbetrieb.

9. Fehleranzeigen und -behebung

Anzeige		Bedeutung	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*.	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.

10. Instandhaltung

Das System ist grundsätzlich wartungsfrei.

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.

11. Entsorgung

HINWEIS

Das Gerät ist als Elektronikschrott an öffentlichen Rücknahmestellen und Wertstoffhöfen zu entsorgen. Die Verpackung ist separat zu entsorgen.

Table of contents

Original instructions

Please hand this document over to the user!

1. Safety instructions

NOTE NOTE denotes a statement which is provided for information only.

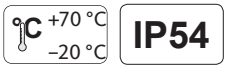
Aimed at trained door specialists with knowledge of installing lock and hardware components, these instructions provide information on how to install, commission and operate this product.

Please read these instructions carefully before installation and commissioning!

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!
- For safety and product approval (CE) reasons, the product must not be converted or modified.
- 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!

2. Technical data

Supply voltage	10..24 V DC (max. 30 V)
Power consumption	< 1 W
Environmental conditions	
Template memory	99 finger templates
Template identification duration	1–2 s
False rejection rate (FRR)	1/100
False acceptance rate (FAR)	1/10,000,000
Lifetime	max. 10 million finger scans
Certificates	CE The certificates can be found at our website www.g-u.com.

3. Protection against manipulation

Your system consists of 2 electronic devices:

- Fingerprint scanner
- SECURE*connect* 200 (control unit)

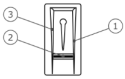
The fingerprint scanner is generally assembled externally (on the outside of the door). To prevent unauthorised access, your system is equipped with numerous security functions:

- The fingerprint scanner is connected to the control unit using a data cable. Data transmission is encrypted.
- Recording of the user finger and the modification of the system content is only possible if master finger has already been recognised by the system.
- The fingerprint scanner and control unit are clearly paired for initial commissioning (pairing).

In order to exchange a component of the door system (SECURE*connect 200R*, SECUREconnect *200F* or fingerprint scanner), you have to start a re-pairing procedure. 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 be removed. The pairing process for the SECURE*connect 200R*, SECURE*connect 200F* and fingerprint scanner now restarts. The fingerprint scanner is reset to the factory setting.

4. Operating 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.

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 s.

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.

5. System commissioning

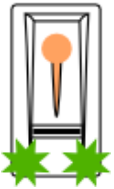
Follow these steps to commission your access system:

- Install the devices in accordance with the accompanying installation instructions.
- Carry out the wiring in accordance with the accompanying installation instructions.
- Once switched on for the first time, the fingerprint scanner and SECURE*connect* carry out automatic pairing. Once pairing is complete the blue LED flashes.

Fingerprint scanner is not paired with SECURE*connect* 200

Fingerprint scanner is paired with SECURE*connect* 200. No fingerprint stored

Fingerprint scanner is connected to Bluetooth device



Fingerprint scanner is paired with SECURE*connect* 200 – admin menu

5.1 Operating concept

Two different operating concepts exist:

- App – administration of the Bluetooth fingerprint scanner using a mobile device (point 6, from page 10)
- Master finger – administration of fingerprint scanner via master finger (point 7, from page 19)

5.2 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 SECURE*connect* 200. No fingerprint stored.

Put a finger on the sensor for 3 - 5 s.

If you take the finger off, the relay 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 s. If you leave your finger on the sensor for longer, the relay will not switch.

6. 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 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 ekey 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 couple 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.

6.2 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.

6.3 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 authorization“ or 'New access authorization'.
- Select the relay to be switched.
- Select a finger.
- Press 'Store'.
- Read the note and press 'Start'.
- Once your fingerprint has been successfully registered, press 'OK'.
- Press 'Done'.

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

6.4 Disabling Bluetooth

You can deactivate 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 fingerprint was stored.

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

6.5 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.

6.6 Administration of several Bluetooth fingerprint scanners

The open biometric app allows several Bluetooth fingerprint scanners to be administered. 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 name 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 COUPLING“.
- 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.

6.7 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.

6.8 Resetting the app security code

- Start the open biometric app.
- Type in an incorrect app security code.
- Confirm your entry with 'Next'.
- Select 'RESET COUPLING“.
- 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.

6.9 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.

6.10 Reset 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 is maintained.

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

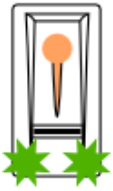
7. Programming with master finger

7.1 Storing the master finger

The master fingers serve exclusively 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 fingerprints from two different people for this purpose.

Fingerprint scanner is paired with SECURE*connect* 200. No fingerprint stored.

3 finger touches within 5 s.



Admin mode is active.

Drag the first master finger over the sensor.

The fingerprint has been recognised.

The system is ready to retry.

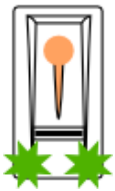
Drag the first master finger across the sensor again.

The fingerprint has been recognised.

The system is ready to retry.

Drag the first master finger across the sensor again.

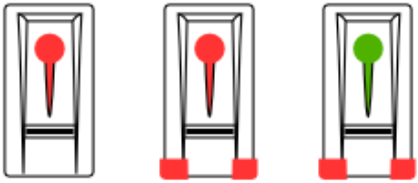
The quality of the three scans is very good.



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

Further possible displays during the saving process:

Quality of the scan 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.

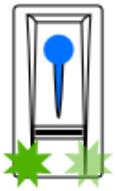
When storing the finger, no more than 10 s can elapse between the individual finger scans. Otherwise the fingerprint storing operation will be aborted.

7.2 Storing the user fingers

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

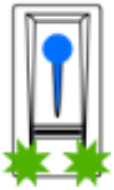
Normal operation.

3 finger touches within 5 s.



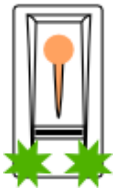
Admin menu

Drag any master finger over the sensor.



Master finger recognised. Saving mode active.

1 finger touch within 5 s.



Recording mode is active.

Drag the finger to be stored over the sensor.

The fingerprint has been recognised.

The system is ready to retry.

Drag the finger to be stored over the sensor.

The fingerprint has been recognised.

The system is ready to retry.

Drag the finger to be stored over the sensor.

The fingerprint has been recognised.

The fingerprint has been stored successfully.

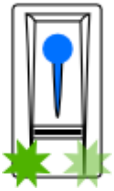
After storing the user finger: normal mode.

7.3 Deleting the user fingers

Some user fingers can only be deleted if the user is present.

Normal operation

3 finger touches within 5 s.

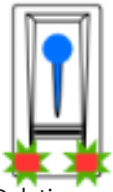


Admin menu

Drag any master finger over the sensor.

Master finger recognised. Saving mode active.

Wait 5 seconds!



Deletion mode active.

1 finger touch

Administration menu

Drag the finger to be deleted over the sensor.

User fingers deleted!

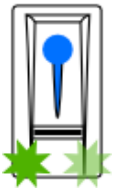
Normal operation

7.4 Deleting all user fingers

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

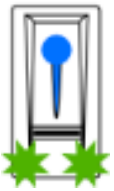
Normal operation

3 finger touches within 5 s.



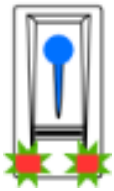
Admin menu

Drag any master finger over the sensor.



Master finger recognised. Saving mode active.

Wait 5 seconds!

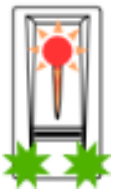


Deletion mode active.

1 finger touch

Administration menu

Rescan the same master finger as shown above.



All user fingers deleted!

Normal operation

NOTE **Check a random user finger. You are no longer able to obtain approval!**

7.5 Reset finger scanner factory settings

Return the finger scanner to its condition at delivery.

NOTE

All user and master fingers are deleted! The pairing between the finger scanner and SECURE*connect* 200 is maintained.

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

Normal operation

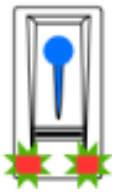
3 finger touches within 5 s.

Admin menu

Drag any master finger over the sensor.

Master finger recognised. 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 SECURE*connect* 200. No fingerprint stored.

8. Opening the door

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

8.1 Opening doors with the 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 motor lock and your door will open.

8.2 Door opening with fingerprint scanner

Normal operation

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

The fingerprint has been recognised successfully.

After door opens: normal operation.

9. Display and elimination of errors

Signalling		Meaning	Remedy
	Status LED lights up red.	The fingerprint has not been recognised.	Drag the finger over the sensor once again.
	All LEDs light up red for 1 minute.	System locked. An unknown fingerprint 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 SECURE*connect*.	Check the wiring or perform a pairing reset.
	Status LED flashed red/ green.	The sensor of the fingerprint scanner is soiled or defective.	Clean or dry off the sensor.

10. Maintenance

The system is basically maintenance-free.

The surface of the fingerprint scanner is more or less self-cleaning because it is repeatedly used (for finger scannng). 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 without cleaning additives. Proceed carefully in the area of the sensor.

11. Disposal

NOTE

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

Table des matières

Notice d'origine

Remettre ce document à l'utilisateur !

1. Consignes de sécurité

REMARQUE REMARQUE indique un renseignement purement informatif.

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.

Lire attentivement cette notice avant le montage et la mise en service !

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 !
- 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 !

2. Caractéristiques techniques

Tension d'alimentation	10..24 V DC (max. 30 V)
Puissance absorbée	< 1 W
Conditions environnantes	°C + 70 °C – 20 °C IP 54
Mémoire d'empreintes	99 empreintes digitales
Durée d'identification d'empreintes digitales	1..2 s
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
Certification	CE Vous trouverez les certificats sur notre site web www.g-u.com

3. Protection contre les manipulations

Votre système est composé de deux appareils électroniques :

- lecteur d'empreintes digitales
- SECURE*connect* 200 (unité de commande)

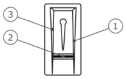
Le lecteur d'empreintes digitales est en général monté à l'extérieur (face extérieure de la porte). Pour éviter toute manipulation non autorisée, votre système est équipé de nombreuses fonctions de sécurité qui empêchent un accès illicite :

- Le lecteur d'empreintes digitales est relié à l'unité de commande par un câble de données. La transmission des données est cryptée.
- L'acceptation des empreintes utilisateurs et la modification des contenus du système ne sont possibles qu'avec identification préalable d'une empreinte maître.
- Le lecteur d'empreintes digitales et l'unité de commande sont couplés entre eux de manière univoque lors de la première mise en service (l'appairage).

Pour remplacer un composant du système de porte (SECURE*connect* 200R, SECURE*connect* 200F ou lecteur d'empreintes digitales), une procédure de reset d'appairage doit être effectuée. 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. Utiliser pour cela p. ex. une pince crocodile. La pince peut ensuite être retirée. Le SECURE*connect* 200R, le SECURE*connect* 200F et le lecteur d'empreintes digitales entament alors une nouvelle procédure d'appairage. Ce faisant, le lecteur d'empreintes digitales est remis à la configuration d'usine.

4. Manipulation 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).

Passage du doigt

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.

Faire 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 s.

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 environ.

Effleurement

Touchez brièvement et rapidement le capteur avec le doigt.

5. Mise en service du système

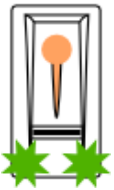
Pour mettre votre système d'accès en service, procédez par étapes :

- montez les appareils conformément à la notice de montage fournie.
- effectuez le câblage conformément à la notice de montage fournie.
- après la première mise en marche, lecteur d'empreintes digitales et SECURE*connect* effectuent un appairage automatique. À la fin de l'appairage, la LED bleue clignote.

Le lecteur d'empreintes digitales n'est pas couplé au SECURE*connect* 200.

Le lecteur d'empreintes digitales est couplé au SECURE*connect* 200. Aucune empreinte n'est enregistrée.

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



Le lecteur d'empreintes digitales est couplé au SECURE*connect* 200 – menu administrateur.

5.1 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 (point 6, à partir de la page 39).
- Empreinte maître – Gestion du lecteur d'empreinte digitales à l'aide de l'empreinte maître (point 7, à partir de la page 47).

5.2 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 couplé au SECURE*connect* 200. Aucune empreinte n'est enregistrée.

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

Lorsque vous retirez le doigt, le relais 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 s. Lorsque vous laissez le doigt plus longtemps sur le capteur, le relais ne se déclenche pas.

6. Programmation avec l'appli open biometric.

Le lecteur d'empreintes digitales doit être couplé au 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 Télécharger l'appli

L'appli est disponible pour les systèmes d'exploitation Apple iOS et Google Android. Télécharger 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 ekey-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 couplé 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 couplage du système. Souvenez-vous de ce code car vous en aurez besoin pour coupler 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.

6.2 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.

6.3 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 à activer.
- Sélectionnez un doigt.
- Appuyez sur " Enregistrer ".
- Lisez la remarque et appuyez sur " Démarrer ".
- Dès que l'enregistrement de votre empreinte a réussi, appuyez sur " OK ".
- Appuyez sur " Terminé ".

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

6.4 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 une empreinte a été enregistrée.

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

6.5 Coupler d'autres appareils mobiles

Vous pouvez coupler 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.

6.6 Administrer plusieurs lecteurs d'empreintes digitales Bluetooth.

L'ppli open biometric permet de gérer 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 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 coupler un autre lecteur d'empreintes digitales.

6.7 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.

6.8 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 coupler à nouveau le lecteur d'empreintes digitales et attribuer un nouveau code de sécurité appli.

6.9 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 d'ouverture biométrique 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.

6.10 Remise du 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 lecteur d'empreintes digitales et SECURE*connect* 200 est conservé !

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

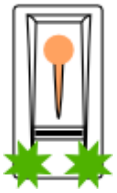
7. Programmation avec des empreintes maîtres

7.1 Enregistrer des empreintes maîtres

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

Le lecteur d'empreintes digitales est couplé au SECURE*connect* 200. Aucune empreinte n'est enregistrée.

3 effleurements de doigt en 5 s.



Mode administrateur actif.

Passer la première empreinte maître sur le capteur.

L'empreinte a été identifiée.

Le système est prêt pour la répétition.

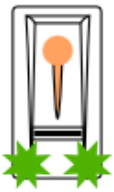
Repasser la première empreinte maître sur le capteur.

L'empreinte a été identifiée.

Le système est prêt pour la répétition.

Repasser la première empreinte maître sur le capteur.

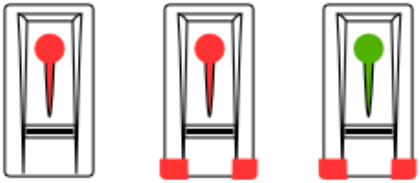
La qualité des trois scans est excellente.



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

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.

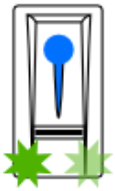
Pendant l'enregistrement des empreintes, les différents scans d'empreintes doivent être espacés de maximum 10 s. Dans le cas contraire, l'enregistrement de l'empreinte est interrompu.

7.2 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.

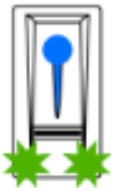
Service normal.

3 effleurements de doigt en 5 s.



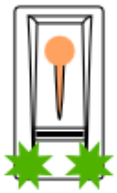
Menu administrateur

Passer n'importe quel empreinte maître sur le capteur.



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

1 effleurement de doigt en 5 s.



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.

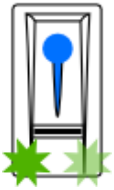
Après la sauvegarde de l'empreinte de l'utilisateur : mode normal.

7.3 Effacer des empreintes utilisateurs

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

Service normal

3 effleurements de doigt en 5 s.

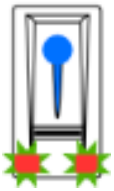


Menu administrateur

Passer n'importe quel empreinte maître sur le capteur.

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

Attendre 5 secondes !



Mode de suppression actif

1 effleurement de doigt

Menu administration

Passez l'empreinte à supprimer sur le capteur.

L'empreinte utilisateur est effacée !

Service normal

7.4 Effacer toutes les empreintes utilisateurs

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

Service normal

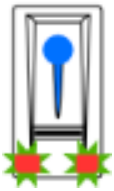
3 effleurements de doigt en 5 s.

Menu administrateur

Passer n'importe quel empreinte maître sur le capteur.

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

Attendre 5 secondes !

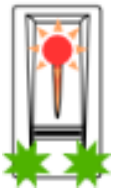


Mode de suppression actif

1 effleurement de doigt

Menu administration

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



Toutes les empreintes maîtres sont effacées !

Service normal

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

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

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

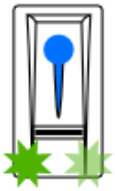
REMARQUE

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

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

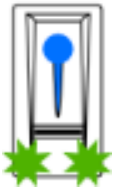
Service normal

3 effleurements de doigt en 5 s.



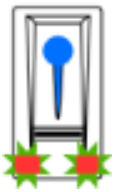
Menu administrateur

Passer n'importe quel empreinte maître sur le capteur.



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

Attendre 5 secondes !



Mode de suppression actif

1 effleurement de doigt

Menu administration

Scanner une autre empreinte maître.

Toutes les empreintes utilisateurs et maîtres sont effacées !

Le lecteur d'empreintes digitales est couplé au SECURE*connect* 200. Aucune empreinte n'est enregistrée.

8. Ouverture de la porte

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

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 l'accès 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.

8.2 Ouverture de la porte avec lecteur d'empreintes digitales

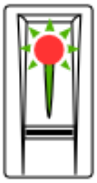
Service normal

Passez une empreinte utilisateur ou maître enregistrée sur le capteur.

L'empreinte a bien été identifiée.

Après l'ouverture de la porte : mode normal.

9. Affichage et élimination des erreurs

Affichage		Signification	Solution
	La LED de statut s'allume en rouge.	L'empreinte n'a pas été identifiée.	Repasser 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 normal.
	La LED d'état clignote en orange.	Connexion Bus vers SECURE*connect* 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.

10. Entretien

Le système ne demande en principe aucune 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 propre sans ajout de produit nettoyant. Procédez avec précaution dans la zone de la surface du capteur.

11. Mise au rebut

REMARQUE

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

Notizen | Notes | Notes | Notas

Tabla de contenido

Instrucciones originales

¡Entregue este documento al usuario!

1. Instrucciones de seguridad

NOTA NOTA indica un enunciado puramente informativo.

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

¡Lea este manual detenidamente antes del montaje y de la puesta en servicio!

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!
- Por motivos de seguridad y de homologación (CE) no se permite transformar ni modificar el producto de manera arbitraria.
- 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!

2. Datos técnicos

Fuente de alimentación	10-24 V CC (máx. 30 V)
Potencia absorbida	< 1 W
Condiciones ambientales	°C +70 °C -20 °C IP54
Memoria de plantillas	99 plantillas de dedos
Tiempo de identificación de plantilla	1-2 s
Cuota de denegación errónea (FRR)	1:100
Cuota de aceptación errónea (FAR)	1:10.000.000
Vida útil	máx. 10 millones de escaneados de huella digital
Certificación	CE Los certificados se pueden encontrar en nuestra página web www.g-u.com.

3. Protección contra manipulaciones

Su sistema consta de 2 aparatos electrónicos:

- Escáner de huella digital
- SECURE*connect* 200 (unidad de control)

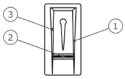
El escáner de huella digital se monta por lo general en la zona exterior (lado exterior de la puerta). Para prevenir una manipulación ilícita, su sistema cuenta con numerosas funciones de seguridad que evitan accesos no autorizados:

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

Para sustituir un componente (SECURE*connect* 200R, SECURE*connect* 200F o escáner de huella dactilar) del sistema de puerta, debe someterse a un proceso de reemparejamiento. Para ello, en la platina 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 el escáner de huella dactilar se someten ahora a un nuevo proceso de emparejamiento. Durante dicho proceso se restablece el escáner de huella digital a los ajustes de fábrica.

4. Manejo 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 imagen del dedo de referencia, y 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).

Arrastrar 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 s.

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 (touch)

Toque el sensor rápida y brevemente con el dedo.

5. Puesta en marcha del sistema

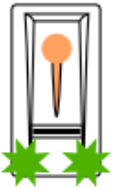
Para la puesta en marcha de su sistema de acceso, siga los pasos que se indican a continuación:

- Monte los aparatos siguiendo las instrucciones de montaje suministradas.
- Instale el cableado siguiendo las instrucciones de montaje suministradas.
- Tras su primera activación, el escáner de huella digital y SECURE*connect* realizan un acoplamiento automático. Una vez completado el acoplamiento, el LED azul parpadeará.

Escáner de huella no acoplado con SECURE*connect* 200

Escáner de huella digital acoplado al SECURE*connect* 200. No hay ningún dedo guardado

Escáner de huella digital acoplado al dispositivo Bluetooth



Escáner de huella digital acoplado al SECURE*connect* 200 - menú de administrador

5.1 Concepto de manejo

Están disponibles dos conceptos de manejo distintos:

- Aplicación: administración del escáner de huella digital Bluetooth mediante un dispositivo móvil (punto 6, a partir de la página 10)
- Dedo administrador: administración del escáner de huella digital Bluetooth mediante dedo administrador (punto 7, a partir de la página 19)

5.2 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.

Escáner de huella digital acoplado al SC200. No hay ningún dedo guardado.

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

El relé conmutará cuando retire el dedo.

NOTA

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

Puede colocar su dedo sobre el sensor durante un total de 5 s como máximo. Si mantiene el dedo sobre el sensor durante más tiempo, el relé no conmutará.

6. Programación con la aplicación open biometric

Para poder iniciar la programación, el escáner de huella digital debe estar acoplado al 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 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 acoplamiento 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 ekey (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 escáner 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 acoplar 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 acoplamiento 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.

6.2 Modificar el código de seguridad de la app

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.

6.3 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 a conmutar.
- 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.**

6.4 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.

6.5 Acoplar otros dispositivos móviles

Puede acoplar 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.
- Acople 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 acoplamiento 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.

6.6 Gestionar varios escáneres de huella digital Bluetooth

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

NOTA

Al restablecer el acoplamiento se borrarán los nombres de relé 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 acoplamiento entre el escáner de huella digital Bluetooth y el dispositivo móvil. Ahora puede acoplar otro escáner de huella digital Bluetooth.

6.7 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
- Modificar el código de seguridad de la app
- Restablecer el acoplamiento 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.

6.8 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 acoplamiento 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 acoplar de nuevo el escáner de huella digital Bluetooth y asignar un nuevo código de seguridad de la aplicación.

6.9 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.
- Acople 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.

6.10 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 acoplamiento entre el escáner de huella digital y SECURE*connect* 200 se mantendrá!

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

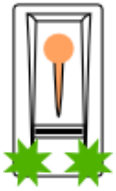
7. Programación con dedos administradores

7.1 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 memorizar 2 dedos de dos personas diferentes.

Escáner de huella digital acoplado al SECURE*connect* 200. No hay ningún dedo guardado.

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



Modo de administración activo.

Deslice el primer dedo administrador sobre el sensor.

Se ha reconocido el dedo.

El sistema está listo para la repetición.

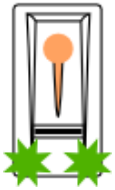
Deslice de nuevo el primer dedo administrador sobre el sensor.

Se ha reconocido el dedo.

El sistema está listo para la repetición.

Deslice de nuevo el primer dedo administrador sobre el sensor.

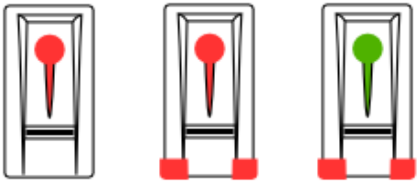
La calidad de los tres escaneos es excelente.



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.

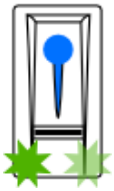
Durante el proceso de memorización de los dedos no deben transcurrir más de 10 s entre los escaneos de dedos. De lo contrario se cancelará la memorización del dedo.

7.2 Guardar dedos 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.

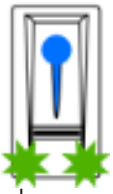
Funcionamiento normal.

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



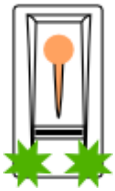
Menú de administración

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 s.



El modo de registro está activado.

Deslice sobre el sensor el dedo que desee memorizar.

Se ha reconocido el dedo.

El sistema está listo para la repetición.

Deslice sobre el sensor el dedo que desee memorizar.

Se ha reconocido el dedo.

El sistema está listo para la repetición.

Deslice sobre el sensor el dedo que desee memorizar.

Se ha reconocido el dedo.

Se ha guardado correctamente el dedo.

Después de guardar el dedo de usuario: funcionamiento normal.

7.3 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 s.

Menú de administración

Deslice un dedo administrador cualquiera sobre el sensor.

¡Espere 5 segundos!

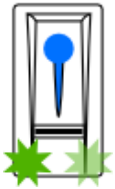
Dedo administrador detectado. Modo de memorización activo.

7.4 Borrar todos los dedos de usuario

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

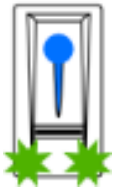
Funcionamiento normal

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



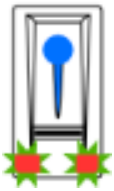
Menú de administración

Deslice un dedo administrador cualquiera sobre el sensor.



Dedo administrador detectado. Modo de memorización activo.

¡Espere 5 segundos!

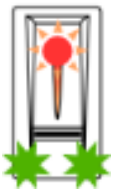


Modo de borrado activo

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!

7.5 Reseteo de fábrica del escáner de huella digital

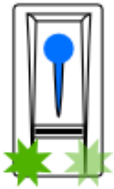
Con esta acción restablecerá el estado de suministro del escáner de huella digital.

NOTA

¡Se borrarán todos los dedos de usuario y todos los dedos de administrador! ¡El acoplamiento entre el escáner de huella digital y SECURE*connect* 200 se mantendrá!
En caso de reparación del SECURE*connect* 200 también se restablecerá al estado de fábrica el escáner de huella digital.

Funcionamiento normal

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

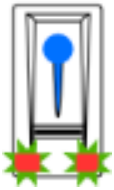


Menú de administración

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!

Escáner de huella digital acoplado al SC200. No hay ningún dedo guardado.

8. Apertura de puerta

La apertura de puerta puede tener lugar con la aplicación open biometric o con el escáner de huella digital.

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 mando al automotor tipo A y a la cerradura motorizada y su puerta se abrirá.

8.2 Apertura de puerta con escáner de huella digital

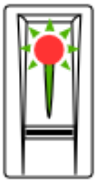
Funcionamiento normal

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

Se ha reconocido correctamente el dedo.

Tras la apertura de puerta: funcionamiento normal.

9. Indicaciones de error y su solución

Indicación		Significado	Solución
	El LED de estado se ilumina en rojo.	No se ha reconocido 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 SECURE*connect*.	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.

10. Mantenimiento

El sistema no requiere mantenimiento.

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 detergente. Limpie con cuidado la superficie del sensor.

11. Eliminación

NOTA

El dispositivo se debe desechar como basura electrónica en los puntos de recogida públicos y en los puntos de selección de residuos reciclables. El embalaje se debe eliminar por separado.

Notizen | Notes | Notes | Notas

Notizen | Notes | Notes | Notas

10.2018 | 20525E | Designed in Germany

Notizen | Notes | Notes | Notas

Herausgeber | Editor:
BKS GmbH
Heidestr. 71
D-42549 Velbert
Tel. + 49 (0) 20 51 2 01-0
Fax + 49 (0) 20 51 2 01-97 33

www.g-u.com

Vorsprung mit System
Securing technology for you