G-U

CE

DOOR TECHNOLOGY

BKS

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

EN

Fingerprint scanner and code keypad
Installation and operating instructions .... PAGE **54**

BKS

Table of contents

BKS

Translation of the original instructions

Please hand over this document to the user!

Your factory code:

1.   Safety instructions
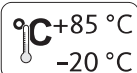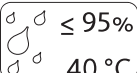
Chapter one to four of this instructions are intended for trained door special-ists with knowledge of installing lock and door hardware components, these instructions provide information on how to install, commission and operate this product.

Please read these instructions carefully before installation and commission-ing.

■ The appropriate local installation specifications, directives and regula-tions 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!

BKS

2. Technical data

Variant	B-55600-23-4-8 B-55600-20-4-8	B-55600-23-1-8 B-55600-20-1-8
Voltage supply	8..24 V DC	8..30 V DC, 8..12 V AC
Power consumption	max. 1 W	max. 3 W
Relay output	via SECURE*connect* 200	24 V AC/DC, 5.0 A
Environmental conditions	+85 °C / −20 °C	≤ 95% / 40 °C IP65 (at the front)
Memory	150 finger templates 150 user codes 1000 events	
Scanning duration template	approx. 1 s	
Template identification duration	approx. 10 ms per comparison	
False rejection rate (FRR)	approx. 0.5%	
False acceptance rate (FAR)	Better than 1 in 1 million (at FRR 0.5%)	
Battery for programming device	CR2032	
Certifications	CE	
Dimensions	44 x 75 x 29 mm	80.5 x 80.5 x 30 mm 55 x 55 x 30 mm (without frame)

3. Version installed in door

3.1 Routing of cable in the door

I/O module for checkback signals

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

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

Use the B-55606-00-4-0 contact grease to protect the contacts against humidity and corrosion.

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

System cable to fingerprint scanner/code keypad

SC200F

SC200R

GY	GND	GS
BN	+24 V	VS
BK	⎍	90

YE	GND	GS
WH	RS-485 A	96
GN	RS-485 B	95
BN	24 V	94

BKS

3.2   Installation in timber and steel doors
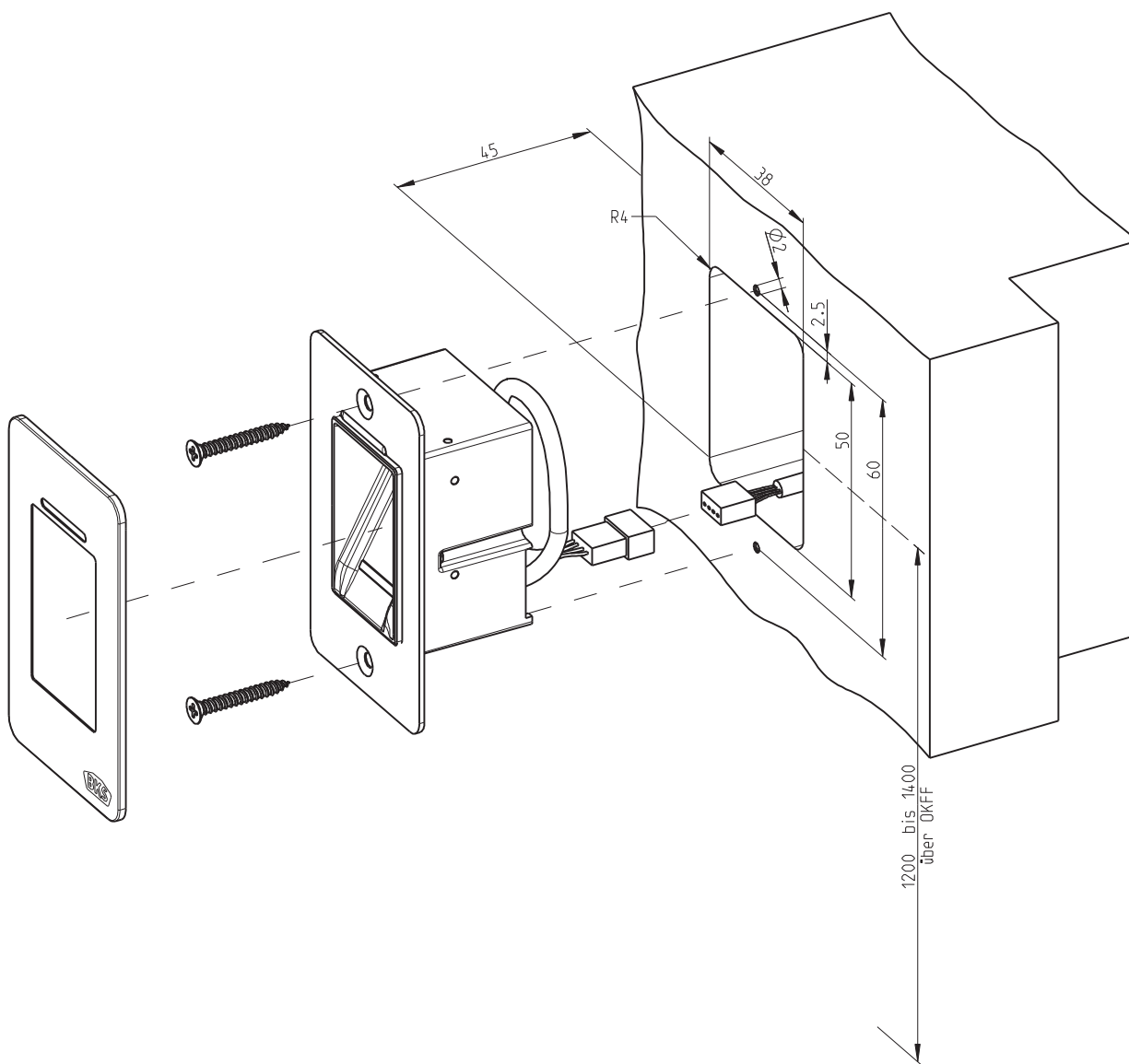
3.3　Installation in aluminium and PVC doors

3.4 Installation with SECURY (A-opener)

3.5   Protection against manipulation

Your system consists of 2 electronic devices:

■ Fingerprint scanner and code keypad

■ SECURE*connect 200* (control unit)

The fingerprint scanner and the code keypad are generally mounted in the external area (on the outside of the door). To prevent unauthorised access, your system is equipped with the following security functions:

■ The fingerprint scanner and code keypad are connected to the control unit using a data cable. Data transmission is encrypted.

■ The fingerprint scanner and code keypad are paired for initial start-up.
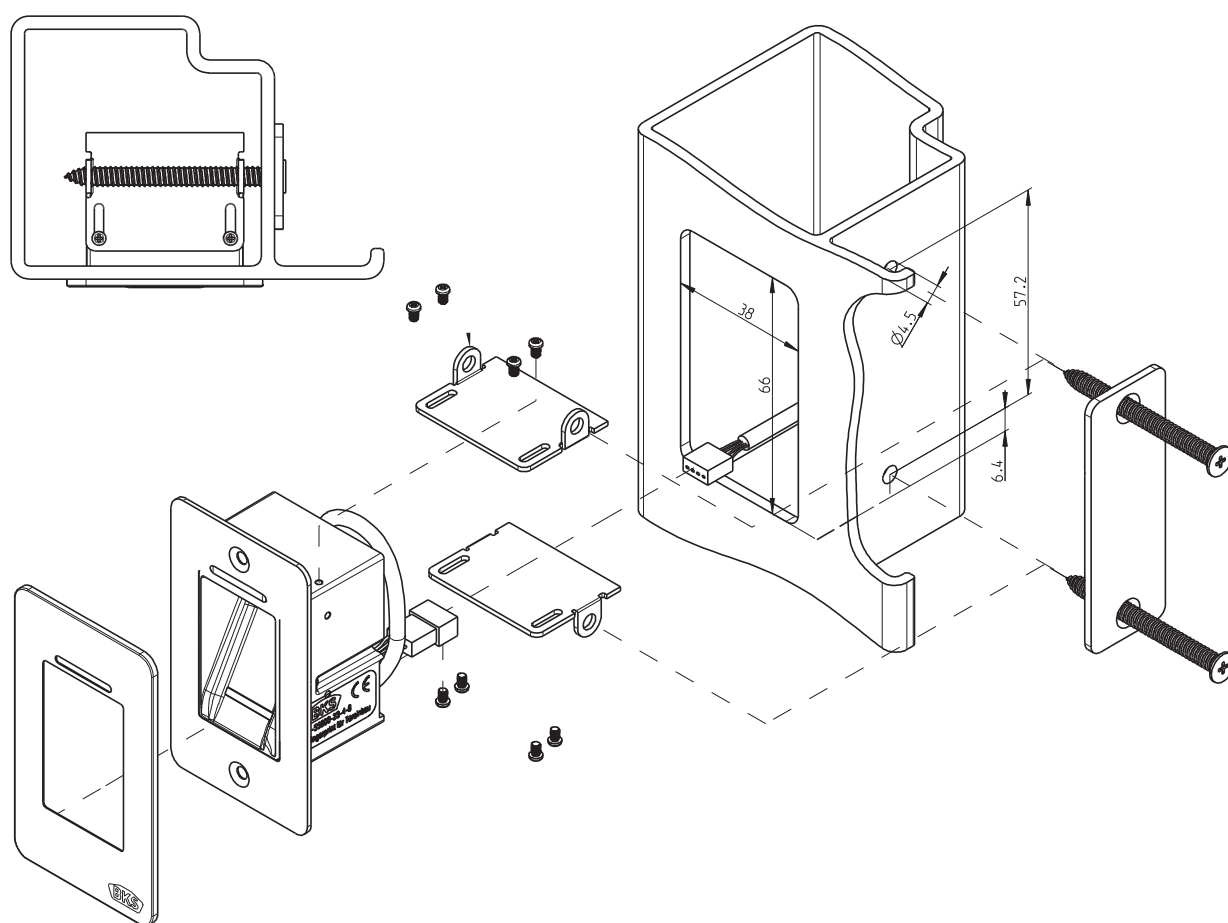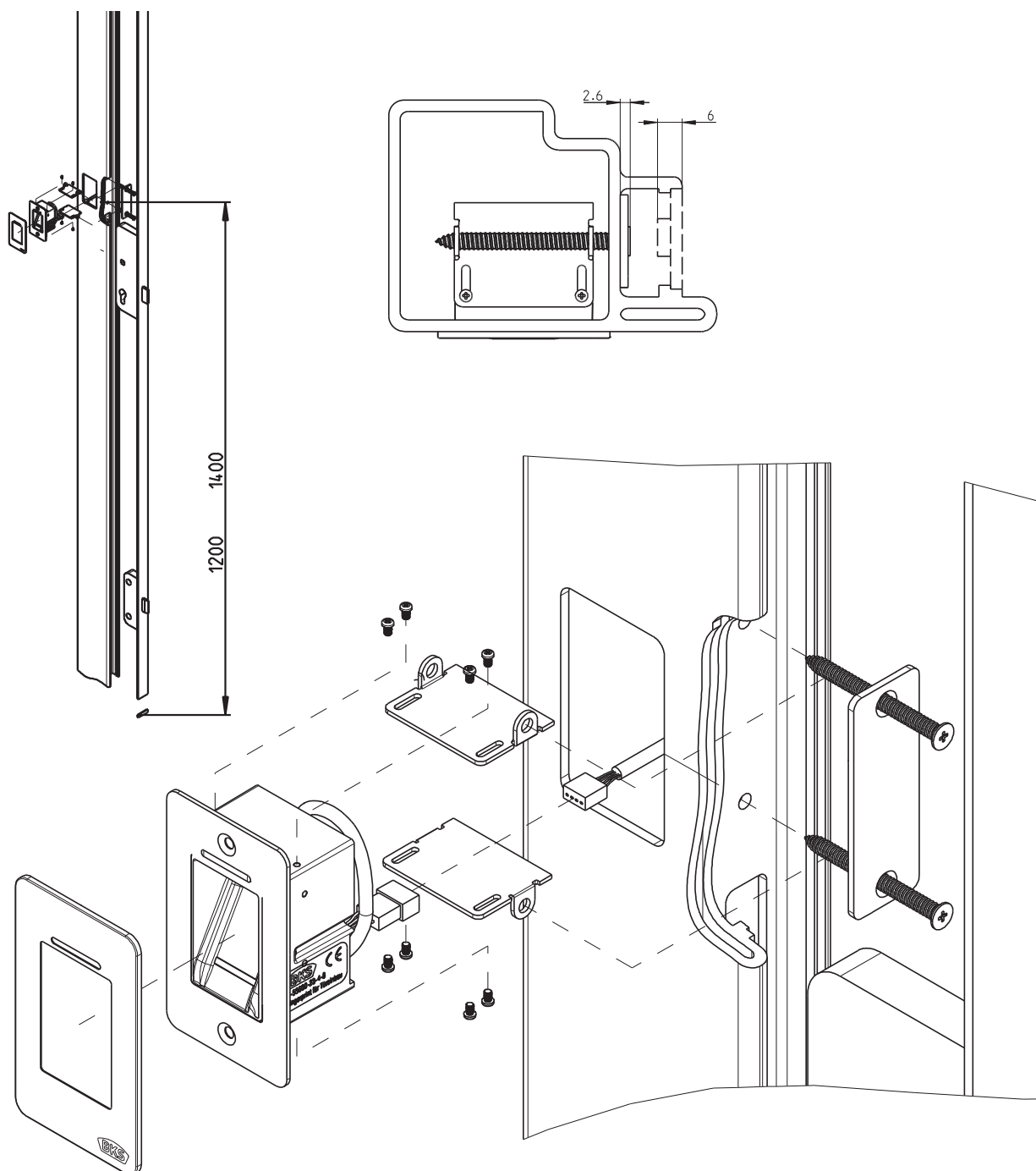
In order to exchange a component of the door system (SECURE*connect 200R*, SECURE*connect 200F* or fingerprint scanner/code keypad), you have to start a re-pairing procedure. To do so, close the reset contact on the board of the SECURE*connect 200F* or SECURE*connect 200R* for a minimum of 3 seconds with the power supply connected. We recommend to use an alligator clip.
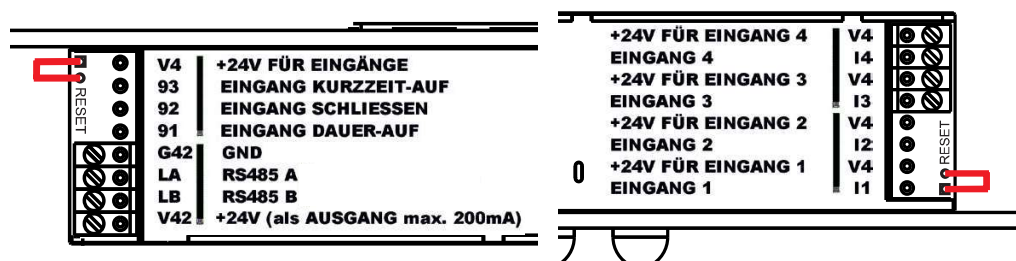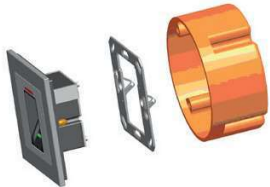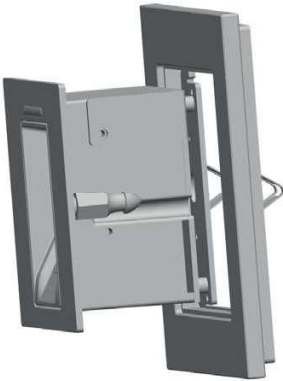
The terminal can be removed. SECURE*connect 200R*, SECURE*connect 200F* and the fingerprint scanner/code keypad start a re-pairing procedure. The fingerprint scanner and the code keypad is reset to the factory setting (all saved finger templates and PIN codes are deleted).

If a fingerprint scanner and a code keypad are connected to an unpaired SECURE*connect 200*, a new system key is generated and the finger templates and the PIN codes are deleted.

BKS
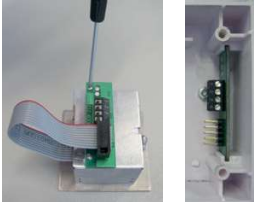
4. In-wall/on-wall installed version
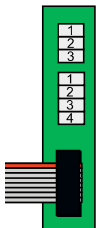
4.1 In-wall installation

	Flush boxes are used for the installation. We recommend an installation height of between 1.2 and 1.4 m above finished floor level.
	■ Fasten the supporting frame to the flush box.
	■ Plug the plastic spacer frame into the supporting frame.
	■ Position the stainless steel outer frame on the spacer frame.
	■ Establish the electrical connection with the module and test the function. ■ Finally, clip the module into the retaining tabs provided. ■ Caution: once the module has been clipped into the supporting frame it is difficult to remove. It may be damaged when it is removed.

4.2   On-wall installation

	Fasten the on-wall housing. We recommend an installation height of between 1.2 and 1.4m above finished floor level. You can use the enclosed screws (3.5 x 25) and plugs for this.
	■ Remove the terminal board by undoing the two screws. ■ Push the terminal board into the groove of the on-wall housing that has been prepared for this.
	■ Connect the supply line to the internal unit accordingly at terminals 1 to 4.
	■ Remove the back of the housing. ■ Note: the module will not fit into the on-wall housing with the back of the housing attached.
	■ Fasten the supporting frame using the 4 enclosed screws (3.5 x 25).

BKS

	■ Attach the plastic spacer frame.
	■ Position the stainless steel outer frame on the spacer frame.
	■ Plug the flat ribbon cable of the outside module onto the terminal board. 　　The red mark on the flat ribbon cable must face in the direction of the terminal clamps.
	■ Once the function test has been successfully performed, clip in the module. ■ Caution: once the module has been clipped into the supporting frame it is difficult to remove. It may be damaged when it is removed.

4.3 Electrical connection

The inside and outside units communicate via an encoded bus. For connection of the inside and outside units we recommend using a telecommunication cable, type J-Y(ST)Y 2 x 2 x 0.8. The connection example applies for the GU A-opener.
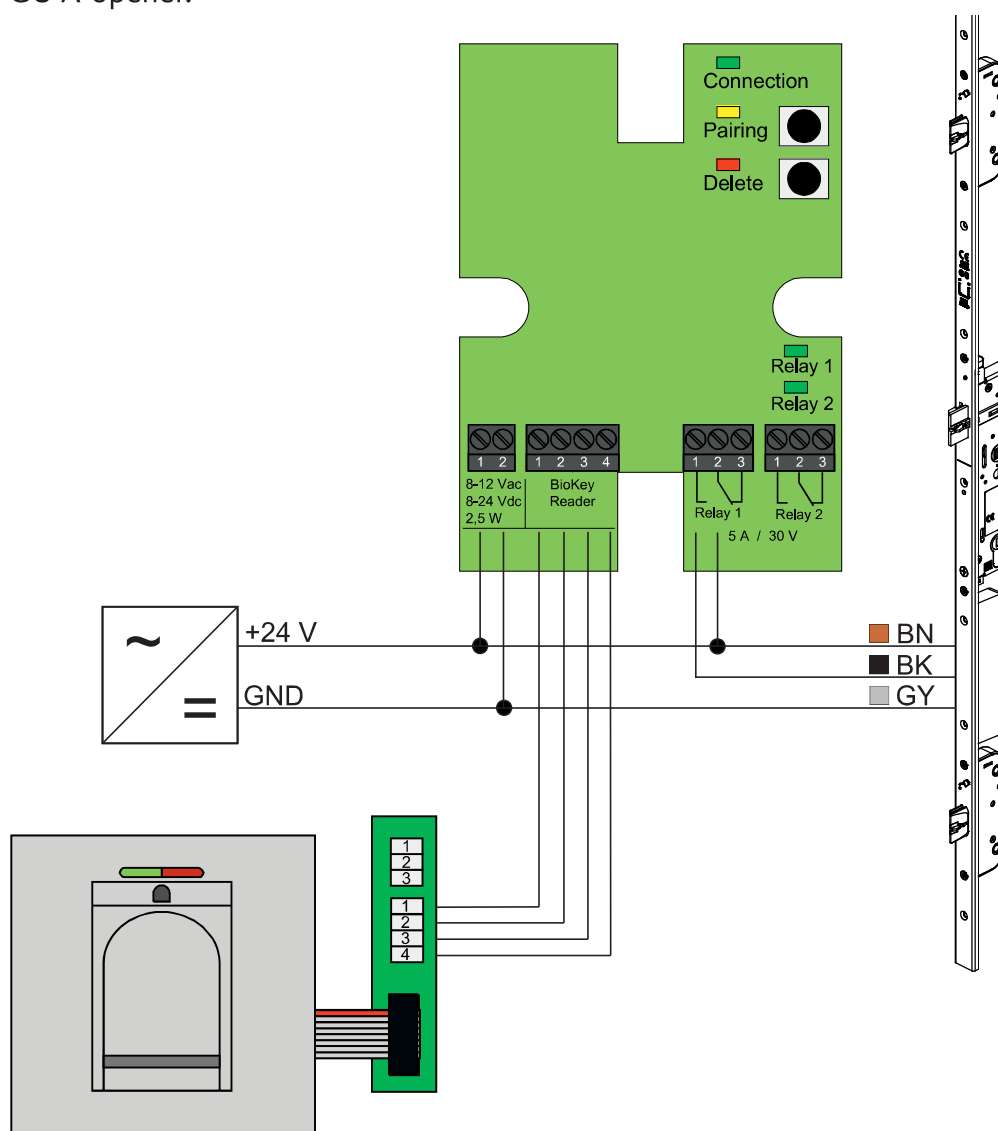
| NOTE | When installing on the wall, the flat ribbon cable must be correctly inserted (red line must be directed to the terminals). |

BKS
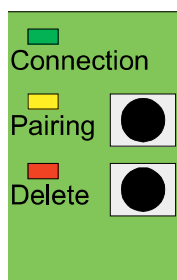
4.4 Protection against manipulation

The inside or outside unit of the in-wall or on-wall version are paired at the factory. If a hardware component is replaced, the pairing must be triggered again by pressing the "Pairing" button on the inside unit. The yellow LED goes out if the pairing is performed successfully.

4.5 Display and operating elements
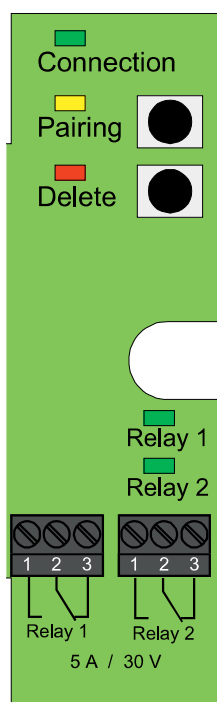
Connection	LED	Lights up continuously, if connection with the outside unit is OK
Pairing	LED	Lights up to indicate its readiness to pair
	Push-button	Starts the pairing procedure
Delete	LED	Lights up during a deletion operation
	Push-button	Deletes all fingerprints (also master finger), the master code remains
Relay 1/2	LED	Lights up when the relevant relay is actuated

4.6 Connection to radio module (I/O)

An outside unit can directly communicate with a radio module I/O (from firmware version 03.00) via an encoded bus. For connection of the radio module I/O and outside unit we recommend using a telecommunication, cable type J-Y(ST)Y 2 x 2 x 0.8.
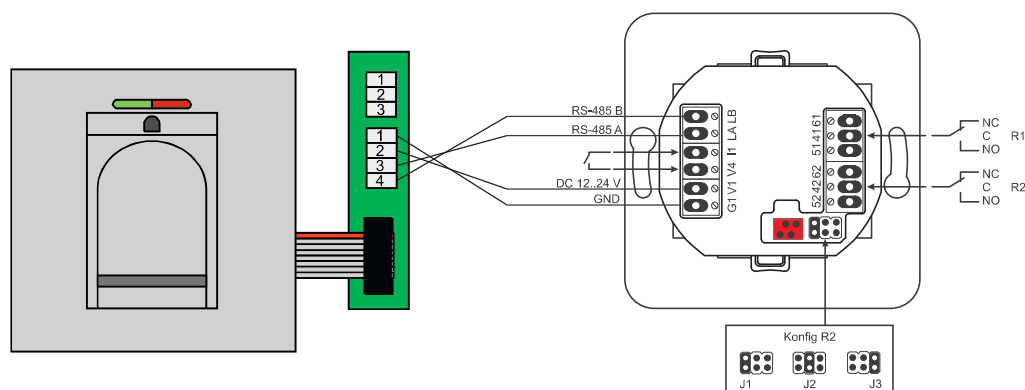
4.6.1 Output functions of radio module I/O

Relay "R2" enables the emission of one of three different electrical signals. It is configured by setting a jumper (see following table). The status is always indicated visually by LED "L2" at the front of the radio module I/O.

Relay "R1" of the radio module I/O is used to display an authorised access, when an access control module is connected via the RS-485. Further configuration of this connection is not possible. The status is indicated visually via LED "L7".

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

BKS

4.6.2   Pairing and re-pairing of fingerprint scanner and code keypad

Once an access control module has been connected to the radio module I/O, the so-called 'pairing' occurs. From this point onwards no other module can be operated at the same radio module I/O. If this is necessary, the fingerprint scanner/code keypad pairing can be reset.
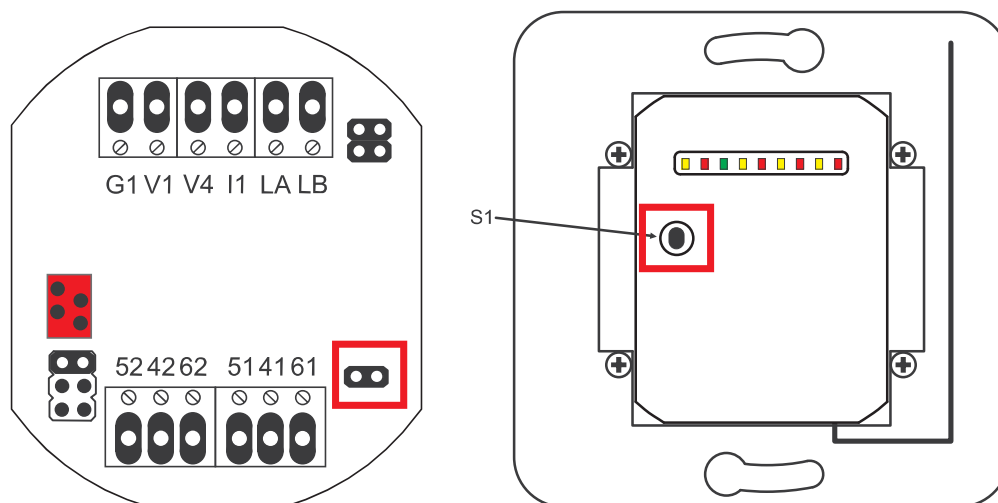
The housing cover must be opened to do this. Disconnect the module from the bus. Insert the jumper next to the terminal "51 41 61". Now press pushbutton "S1" until an acoustic signal is heard. The pairing information has been deleted.

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

5. Operating advices for fingerprint scanner

You can now decide whether you would prefer to scan the user fingers without programming device, whether you would prefer index-based operation of the programming device or whether you would prefer to use a mobile device via Bluetooth. The first 6 fingers to be scanned in the device are master fingers. These are used for administration of the system.

The advantage of the "basic operation" is that you do not require a programming device or mobile phone to scan new user fingers.

The advantage of the "index administration" and "Bluetooth administration" mode is that individual user fingers can be deleted systematically.

You can change the fingerprint scanner module over from Bluetooth operation (default) to another operation mode.

The changeover is only possible in the delivery condition (all LEDs light up). If you have already taught-in fingers, you must perform a factory reset before the changeover. All saved information is lost in this case.

5.1 Changing the operating mode

To change over to operating mode, hold the programming device directly in front of the blue LED of the module.

99 » OK » 51 » OK	Changes a module over to "index administration"
99 » OK » 50 » OK	Changes a module over to "basic operation"
99 » OK » 57 » OK	Changes a module over to "Bluetooth administration"

**NOTE**   **Following a reset, the operating mode retains.**

5.2   Finger guidance

The fingers may be rejected wrongly, if they have not been taught-in correctly. The teach-in process must be carefully performed. The better the finger is taught-in, the better it will be detected during identification later.

If the finger has been taught-in incorrectly, the behaviour can be improved by teaching-in the same finger two to three times.
A large fingerprint area is required in order to effectively identify it. The finger should therefore be as flat as possible when dragged over the sensor.
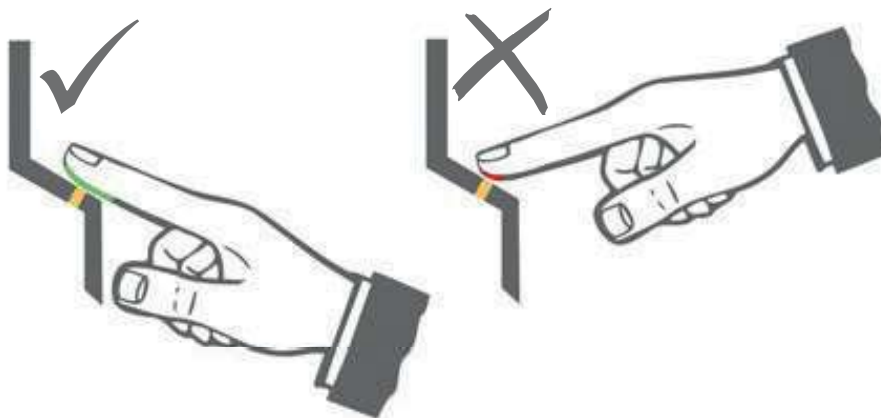
5.3   Door opening behaviour (only door installation)

If the door is opened for longer than 12 s, the fingerprint scanner is shut down. The saved fingerprints for opening the door (templates) are retained in the event of a power failure. After a power failure, the date and time must be set again in order to evaluate events.

6. Operating mode "basic operation"

Key	Meaning	Explanation
DA	Delete All	Delete all, including master finger
OK	OK	Perform function
R1 B	Relay 1 Block	Relay 1 Disable user ID
RT	Relay-Time	Switching time
R2 UB	Relay 2 Unblock	Relay 2 Enable user ID
D	Delete	Delete finger prints
E	Enroll	Record finger prints
Abbreviation	**Meaning**	**Explanation**
MF	Master finger	Administration finger
CODE	PIN-Code	User or master code
ID	Index	User ID
YYYY	Year	Year
MM	Month	Month
DD	Day	Day
HH	Hour	Hour
MM	Minute	Minute
TT	Time	Time (seconds)

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

BKS

Function	Procedure
Test mode (only possible in the delivery condition)	0 » OK
Change the factory code	D » E » old CODE » OK » new CODE » OK » new CODE » OK
Teaching-in master fingers	Teach-in six different master fingers in the delivery condition
Teaching-in user fingers	Scan master finger » Scan user finger » Wait 7 s for timeout
Identification	Scan user fingers
Delete all finger prints (reset)	Scan 3x the master finger Wait 30 s until the delivery condition is reached
Unblock the fingerprint scanner	Scan a taught-in finger (master or user finger)
Teaching-in user code	MF » E » CODE » OK » CODE » OK
Door opening with user code	CODE » OK
Deleting user code	MF » D » 0 » OK
Adding master finger	MF » E » 0 » new master finger
Set the relay switching time	MF » RT » TT » OK *TT = time in s [1...60 s], default = 3 s*
Set date and time	MF » E » RT » YYYY » OK » MM » OK » DD » OK » HH » OK » MM »OK *Example: 2017-07-23, 12:45am* *MF » E » RT » 2017 » OK » 07 » OK » 23 » OK » 12 » OK » 45 »OK*

6.1 Test mode

In the delivery condition (no master fingers has yet been taught-in) a door opening can be performed for test purposes by means of the programming device. To do so, press the buttons 0 » OK.

6.2 Changing the factory code

You can replace the factory code (see page 4) by your own master code using the programming device.

D » E » old CODE » OK » new CODE » OK » new CODE » OK

The new master code must contain 6-digits.

NOTE	**We always recommend to replace the factory code by your own master code!**

After a reset, any modified master code is reset to the factory code!

BKS

6.3 Teaching-in master fingers

NOTE	At this time, you must already specify who is going to maintain the system and create new users.
	It is possible to scan in 6 different persons, 6 different fingers as well as the same finger 6 times. A maximum of 6 other master fingers can be added later.

	■ The device is initialised. The red, green and blue LED light up permanently.
	■ Drag the first master finger across the sensor. The blue LED flashes.
	■ Wait approx. 3 s. The red and green LEDs flash. ■ Do not allow more than 60 s to elapse between the individual master finger teach-in operations, otherwise the teach-in operation will need to be repeated.
	■ Drag the second master finger across the sensor. The blue LED flashes.

	■ Wait approx. 3 s. The red and green LEDs flash. ■ Do not allow more than 60 s to elapse between the individual master finger teach-in operations, otherwise the teach-in operation will need to be repeated.
	■ Repeat the teach-in operation for the other master fingers.
	■ If a finger is dragged across the sensor during the teach-in operation and is not accepted as master finger, the red and green LEDs remain lit. The master finger teach-in operation must be repeated. ■ Once all 6 master fingers have been taught-in, the device is operational: only the blue LED lights up. User fingers can now be taught-in.

BKS

6.4 Teaching-in user fingers

	■ The device is operational, only the blue LED lights up. The master fingers must not be taught-in as user fingers!
	■ Drag a master finger across the sensor, the red and green LEDs light up briefly.
	■ Drag a user finger across the sensor. If the teach-in operation has been successful, the green LED lights up. ■ We recommend to teach-in each individual user fingers 3 times in order to optimise the detection rate. When this is done, 3 of the 150 available templates will have been used. With "problematic" fingers, it may be necessary to teach-in the same user fingers up to 6 times or use a different finger.
	■ If the scanning operation is of insufficient quality, the red LED lights up. In this case repeat the user finger teach-in operation.
	■ The teach-in operation is completed by a timeout (wait of approx. 7 s). The operation can be cancelled earlier by reading in a master finger again. The red and green led light up briefly.

6.5 Identification

	■ The device is operational, only the blue LED lights up.
	■ Drag the user finger across the sensor. If the finger is detected, the green LED lights up and the door is opened. ■ With the in-wall/on-wall version, relay 1 is always switched.
	■ If the finger is not detected, the red LED lights up and the door is not opened.

BKS

## 6.6 Deleting all user and master fingers

	■ The device is operational, only the blue LED lights up.
	■ Drag a master finger across the sensor, the red and green LEDs light up briefly.
	■ Once the master finger has been scanned twice, the red and green LEDs flash to indicate that deletion mode is being initialised.
	■ The deletion operation starts after the master finger has been dragged across for the third time. The green LED lights up to signal this.
	■ The device is then in the delivery condition (red, green and blue LEDs light up).

NOTE	Carrying out a re-pairing procedure will also reset the fingerprint scanner.

This also deletes all fingers (including master finger). The master code is reset!

6.6.1 Deleting all user and master fingers (only on-wall/in-wall version)
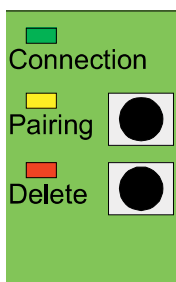
You can restore the factory settings by deleting all finger data at the in-wall or on-wall version of the inside unit. To do this, press the "Delete" button until the red LED lights up. The device is subsequently in the delivery condition (red , green and blue LEDs light up continuously).

NOTE	After a reset, any modified master code is reset to the factory code!

6.6.2 Deleting all user and master fingers (programming device)

Alternatively, the fingerprint module can be reset via the programming device provided. This deletes all finger data that have been saved.

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

Press the button DA » CODE » OK in this sequence to trigger the reset.

For the factory code, refer to page 4 of this manual. The factory code can also be found on an adhesive label on the back of the programming device. If you have assigned a separate master code, then this must be used.

The device is subsequently in the delivery condition (red , green and blue LEDs light up continuously).

NOTE	After a reset, any modified master code is reset to the factory code!

BKS

6.7   Blocking

	■ Blocking: If a finger that has not been taught-in is dragged across the sensor 5 times in succession (red LED lights up), the device enters the blocking mode. This prevents unauthorised persons from gaining unhindered access. If the device is in blocking mode, the red LED flashes to indicate this. The blocking mode initially has a time limit. The blocking time extends up to five times (blocking intervals: 1 minute, 5 minutes, 30 minutes, 1 hour, permanently blocked after that) following each subsequent failed attempt.
	■ Unblocking: Blocking mode can be cancelled earlier by dragging a taught-in finger (master or user fingers) across the sensor. Subsequently, the door can be opened with a user finger.

6.8   Teaching-in user code

It is possible to teach-in a user code using the programming device.

Master finger	E	User code (6-digits)	OK	User code (6-digits)	OK

6.9 Door opening with user code

The user code can be used with the programming device to open the door.

User code	OK

6.10 Deleting user code

Master finger	D	0	OK

6.11 Adding master finger

It is possible to add a maximum of 6 master fingers subsequently to the 6 previously taught-in master fingers.

Master finger	E	0	New master finger	Wait 7 s (red and green LEDs flash 3 times)

BKS

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

The setting applies to both relays. If the relays need to be set separately, see section 7.3.

Master finger	RT	Switching time [1...60 s]	OK

6.13 Initialising the date and time

The fingerprint scanner can save the last accesses. The audit set (B-55606-00-3-0) can be used to read out the list of last accesses (see chapter 9).
In order to assign a time stamp to each access, the time needs to be set once.

	■ Drag a master finger across the sensor, the red and green LEDs light up briefly.
	■ E » RT » YYYY » OK » MM » OK » DD » OK » HH » OK » MM »OK ■ Example: 2017-07-23, 12:45 a.m. E » RT » 2017 » OK » 07 » OK » 23 » OK »12 » OK » 45 »OK **NOTE** After a power failure, the date and time must be set again.

7. Operating mode "Bluetooth administration"

7.1 Download the "BKS BioKey" app

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

NOTE	The app can only be used once 6 master fingers have been taught in (see section 6.3 "Teaching in master fingers").

- ■ Start the "BKS BioKey" app.

- ■ Click the "Select device" button. The app searches for available devices.

- ■ Select the Bluetooth finger scanner from the list.

- ■ Scan master finger at the Bluetooth fingerprint scanner to identify yourself.

- ■ The mobile device is now connected for this session and the scanner can be configured via the app.

- ■ If the app is not used for one minute, you will need to repeat the identification via the master finger.

BKS

7.2   Adding user

■ Start the "BKS BioKey" app.

■ Scan master finger at the Bluetooth fingerprint scanner to identify yourself.

■ Select "Users".

■ Press "+" in the upper right corner.

■ Enter a user name.

■ To add a new Master: activate "Master user".

■ Select "Add fingers".

■ Enter a description for the new finger.

You can assign several fingers with different rights to one user. It may therefore make sense to name the individual fingers.

■ Assign the rights for the corresponding finger under "Authorisations".

■ Select "Teach new finger".

The sensor must now successfully record the finger eight times. The green LED lights up to signal successful detection. The app also displays a counter that shows how many attempts have already been made.

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

■ Select "<" (iOS) or "<- back"(Android). The new finger is now displayed on the user side.

7.3   Editing and deleting users

■ Start the "BKS BioKey" app.

■ Scan master finger at the Bluetooth fingerprint scanner to identify yourself.

■ Select "Users".

■ Select the user you want to edit from the list.

You can change the name, add a new finger
(see section 7.2 "Adding user") and delete the user in this view.

7.4   Displaying the access protocol

■ Start the "BKS BioKey" app.

■ Scan master finger at the Bluetooth fingerprint scanner to identify yourself.

■ Select "Access protocol".

You can display the log of the Bluetooth fingerprint scanner in this view. Successful and unsuccessful identifications at the scanner are displayed in the list, together with the date, time and, for fingers that have been identified, the corresponding user and enabled outputs. The list also shows when a new finger was taught.

7.5   Setting the relay module switching time

■ Start the "BKS BioKey" app.

■ Scan master finger at the Bluetooth fingerprint scanner to identify yourself.

■ Select "Relay time".

A name can be assigned to every output and is displayed in the access log and when rights are assigned. A switching time of between 0 and 6.5 seconds can be selected.

BKS

7.6 Displaying the memory usage

■ Start the "BKS BioKey" app.

■ Scan master finger at the Bluetooth fingerprint scanner to identify yourself.

■ Select "Settings".

The information acquired by the Bluetooth fingerprint scanner can be displayed in this menu. In addition to the installed Firmware version, the memory space required for the taught-in fingerprint and the available memory are also displayed.

8.   Operating mode – "index administration"

The "index administration" operating mode provides you with further functions that will be described in detail below.

8.1   Overview of functions

Function	Procedure
Teach-in user fingers	MF » E » ID » OK » Scan user finger » wait until timeout
Set the relay switching time of relay 1 (only on-wall/in-wall version)	MF » RT » R1 » TT » OK *TT = time in s [1...60 s], default = 3 s*
Set the relay switching time of relay 2 (only on-wall/in-wall version)	MF » RT » R2 » TT » OK *TT = time in s [1...60 s], default = 3 s*
Teach-in user finger for relay 1	MF » E » ID » R1 » OK » Scan user finger» wait for timeout
Teach-in user finger for relay 2	MF » E » ID » R2 » OK » Scan user finger » wait until timeout
Delete a fingerprint	MF » D » ID » OK » MF
Delete all finger prints (reset)	DA » master code » OK
Disable IDs	MF » B » ID » OK
Enable IDs	MF » UB » ID » OK
Check ID	OK » ID » OK

BKS

8.2 Teaching-in user fingers

	■ The device is operational, only the blue LED lights up. The master fingers must not be taught-in as user fingers!
	■ Drag a master finger across the sensor, the red and green LEDs light up briefly.
	■ Press the "E" (Enroll) button on the programming device. ■ Enter an ID of between 1 and 150 via the programming device. ■ Press "OK" to confirm.
	■ Drag a user finger across the sensor. If the teach-in operation has been successful, the green LED lights up. ■ We recommend to teach-in each individual user fingers 3 times in order to optimise the detection rate. When this is done, 3 of the 150 available templates will have been used. With "problematic" fingers, it may be necessary to teach-in the same user fingers up to 6 times or use a different finger.

	■ If the scanning operation is of insufficient quality, the red LED lights up. In this case repeat the user finger teach-in operation.
	■ The teach-in operation is completed by a time-out (wait of approx. 7 s). The operation can be cancelled earlier by reading in a master finger again. The red and green LEDs light up briefly.

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

In the "index administration" operating mode, you can specify the switching duration per relay separately.

Master finger	RT	R1 for relay 1 or R2 for relay 2	Switching time [1...60 s]	OK

BKS

8.4 Teaching-in user finger for relay 1 or 2 (only on-wall/in-wall version)

With the in-wall/on-wall version, the two relays can be switched separately from each other when in the "index administration" operating mode.

	■ Drag a master finger across the sensor, the red and green LEDs light up briefly.
	■ Press the "E" (Enroll) button on the programming device. ■ Enter an ID of between 1 and 150 via the programming device. ■ Select the relay via "R1" or "R2" buttons. ■ Press "OK" to confirm.
	■ Drag a user finger across the sensor. If the teach-in operation has been successful, the green LED lights up. ■ The teach-in operation is completed by a timeout.

8.5 Deleting individual user fingers

	■ Drag a master finger across the sensor, the red and green LEDs light up briefly.
	■ Press the"D" (Delete) button on the program-ming device, the green LED lights up. ■ Enter the ID of the user finger to be deleted. ■ Confirm with "OK", the green LED lights up.
	■ Scan the master finger again to conclude the deletion. The red and green LEDs light up briefly.

BKS

8.6   Deleting all user and master fingers

	■ Press the "DA" (Delete all) button on the programming device, the green LED lights up.
	■ Enter the master code.
	■ Press "OK" to conclude the deletion operation.

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

8.7   Disabling IDs

	■ Drag a master finger across the sensor, the red and green LEDs light up briefly.
	■ Press „R1 (B)" button ■ Enter ID ■ Confirm with "OK" ■ All fingerprints saved under the ID that has been entered are now disabled and will subsequently be rejected. ■ Individual IDs can be disabled provisionally without the taught-in fingerprints being discarded. These can subsequently be enabled without the relevant person having to be present in order to teach-in your finger again.

BKS

8.8 Enabling IDs

	■ Drag a master finger across the sensor, the red and green LEDs light up briefly.
	■ Press "R2 (UB)" button ■ Enter ID ■ Confirm with "OK" ■ All fingerprints with this ID are enabled once again.

8.9 Checking ID

|	
	■ Press "OK" ■ Enter the ID to be checked ■ Press "OK" button again ■ If the ID is already assigned, both LEDs (red and green) light up ■ If the ID is not yet assigned, only the red LED lights up

8.10   Assignment of ID and person

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

BKS

9.   Reading of events (audit set)

The fingerprint scanner saves the last 1000 events. This includes access operations, access attempts and system messages. The chronological order of the accesses can be ascertained.
With the B-55606-00-3-0 audit set you have the possibility to export access data from the fingerprint scanner.

■ Install the BKS audit software on your PC.

■ Connect the USB cable to a free USB port on the PC.
   An appropriate USB driver is automatically installed.

■ Remove the fingerprint scanner.

■ Disconnect the cable coupling between the fingerprint scanner and the control unit.

■ Connect the audit set to the fingerprint scanner.

■ Connect the power supply unit of the audit set to the power supply.

■ Start the audit software.

■ Press the "Receive access log" button.
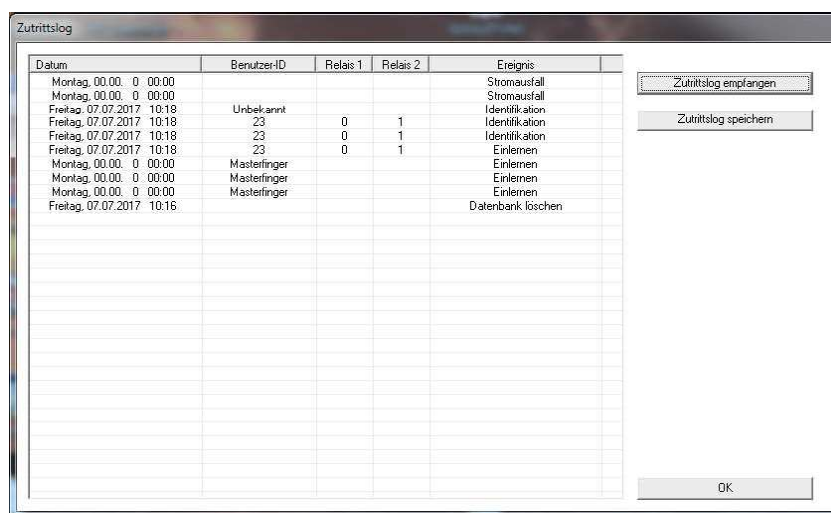
■ Press the "Save access log" button or exit the software using "OK".

10. Operation of code keypad

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

In the delivery condition all 3 LEDs (red/green/blue) light up continuously. A programming device is not included in the scope of delivery as all entries can be made at the code keypad itself.

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

Certain master code or user code combinations are excluded for security reasons. These are regular combinations of numbers such as 8888, 123456 or 4321, etc. The master code or user code can contain a combination of 4–6 digits.
For the initial master code (factory code) refer to page 4 of this manual.

NOTE	**We always recommend to replace the factory code by your own master code!**

If an incorrect user code is entered 5 times in succession, the device switches to the blocking mode. This prevents unauthorised persons from gaining access. If the device is in blocking mode, the red LED flashes to indicate this. The blocking mode initially has a time limit. The blocking time extends up to five times (blocking intervals: 1 minute, 5 minutes, 30 minutes, 1 hour, permanently blocked after that) following each subsequent failed attempt. If a valid user code is entered two times in succession, the blocking mode is cancelled.

BKS

10.1 Test mode

In the delivery condition a door opening can been performed for test purposes. To do so, press the buttons 0 » 🔑

10.2 Changing the master code

*	Master code	*	1	*

New master code	*	New master code	*

10.3 Setting/changing user code

*	Master code	*	2	*

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

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

10.4   Deleting user code

*	Master code	*	3	*

User ID	*

Alternative:

*	Master code	*	3	*

0	*	User code	*

BKS

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

*	Master code	*	4	*

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

10.6 Deleting all user and master codes

*	Master code	*	0	*

Master code	*

| NOTE | Carrying out a re-pairing procedure will also reset the code keypad. This deletes all user codes.

After deleting any modified master code, it is reset to the factory code. |

10.7 Opening the door

User code	

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

11. Troubleshooting

Error description	Cause	Help
Red LED flashes permanently several times per second (approx. 2 Hz).	No bus connection with the control unit.	Check the wiring or commission the device.
	No pairing or faulty pairing.	Reset the pairing.
Red LED flashes permanently every two seconds (approx. 0.5 Hz).	Blocking mode: system is blocked after several invalid identifications.	Scan the authorised finger.
Green LED lights up when an access attempt is made, but the door does not open.	Connection problem between SC200F and SC200R.	Clean the contacts of the SECURE*connect 200*. Check the installation position of the SECURE*connect 200*.

BKS

12.   Maintenance and care

However, as a precautionary measure clean the fingerprint scanner from time to time using a soft, damp (not wet) cloth. Use clean water with no cleaning additives.

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

The serviceability of the locking system must be verified at regular intervals. To do so, check all fastening points and retighten screws, if required. The mechanical properties of the lock (key or lever handle operation/latchbolt) must not be impaired by dirt and shall be maintained and lubricated regularly (e.g. BKS high-performance maintenance spray).

13.   Disposal

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