



ekey home

en OPERATING INSTRUCTIONS

English

Translation of the original instructions – ID251/564/0/458

Table of contents

About these instructions	3
Note	3
Declaration of conformity	3
Warranty and manufacturer's guarantee	3
Copyright	3
Target group	3
Explanation of symbols, abbreviations, and terminology	4
Safety information	5
Proper use and areas of application	5
Product liability and limitation of liability	5
Classification of notices	6
Notices	6
Introduction to the system	7
System overview	7
Scope of delivery	8
Finger scanner	8
Control panel	12
Technical specifications	13
Installation and activation	14
Activating devices	14
Performing test mode	15
Operating concept	16
Configuration of normal mode and usage of the finger scanner with the app	16
Downloading the app	16
Coupling a mobile device for the first time	17
Changing security codes	18
Storing a finger	19
Disabling Bluetooth	20
Coupling additional mobile devices	20
Managing multiple finger scanners	21
Storing the user coupling code	22
Resetting the app security code	22
Protecting the system in the event that the mobile device is lost	23

Opening a door	24
Configuration of normal mode and usage of the finger scanner with administrator fingers	25
Storing administrator fingers and configuring normal mode.....	26
Storing user fingers	27
Opening a door	29
Deleting user fingers	30
Deleting all user fingers.....	31
Resetting the system to default settings.....	32
Via the app.....	32
Via the finger scanner	33
Via the control panel	34
Via the digital input.....	35
Updating the software	36
Error displays and troubleshooting	36
Control panel	36
Finger scanner	36
Maintenance	37
Disposal	37

About these instructions

Note

Read these instructions carefully before use. These instructions form a component of the product. Ensure that they are stored in a safe place. These instructions contain important information on the product; in particular, its proper use, safety, installation, activation, usage, maintenance, and disposal.

Please contact your dealer for further information about the product.

A large-font version of these instructions is available at <http://www.ekey.net>.

These operating instructions are not subject to updating. We reserve the right to make technical modifications and change the product's appearance; any liability for errors and misprints is excluded.

Declaration of conformity

ekey biometric systems GmbH hereby declares that the product conforms to the relevant European Union regulations.

Warranty and manufacturer's guarantee

The version of our general terms and conditions in force on the date of purchase shall apply. See <http://www.ekey.net>.

Copyright

Copyright © 2017 ekey biometric systems GmbH.

All content, artwork, and any ideas contained in these operating instructions are subject to applicable copyright laws. Any transmission, relinquishment, or transfer of this content or parts thereof to any third party requires the prior written consent of ekey biometric systems GmbH. Translation of the original documentation.

Target group

These instructions are aimed at persons who activate and perform maintenance on the ekey system, create users, and instruct users in how to operate the system.

Explanation of symbols, abbreviations, and terminology

Symbols:

1.	Step-by-step instructions
	References to sections of these instructions
	References to the mounting instructions
	References to the wiring diagram
□	Listing without specified order, 1st level
	Requirements for performing instructions
✓	Outcomes of instructions
<u>Displayed value</u>	Displayed values
<i>ekey home FS AR</i>	Product names
MENU ITEM	Menu items
	Buttons

Abbreviations and terminology

AR	arte
BT	Bluetooth
CP	Control panel
FAR	False acceptance rate: The false acceptance rate describes the likelihood of a biometric security system granting access to someone who does not have access authorization, or the relative frequency with which the system does so.
FRR	False rejection rate: The false rejection rate describes the frequency with which persons are erroneously rejected by a biometric system even though they have access rights or access authorization.
FS	Finger scanner
Matching	Comparison between the stored reference and the identification feature. If the two match, the device signals user recognition.
Normal mode	Default operating status in which the system is operated.

Safety information

Proper use and areas of application

This product is an access control system with a biometric identification feature (finger scan). The system is comprised of a finger scanner and a control panel.

The biometric access control system detects the characteristics (minutiae) of the fingerprint contours, compares them to the biometric information saved from the reference fingerprint image, and opens the door in the event of a match.

The system is primarily designed for opening house doors, apartment doors, and garage doors in homes and businesses.

To ensure proper use, the ekey system must be installed in accordance with the mounting instructions and the wiring diagram. The installation must be performed in full and by a professional. The electrical engineer who installs the equipment must approve the ekey system for use, as well as any accessories that are installed.

The ekey system is suitable for use as outlined in these instructions. Any other kind of use is deemed improper use.

Product liability and limitation of liability

Safe operation and function of the devices can be impaired in the following situations. Liability due to malfunctioning is transferred to the operator/user in such cases:

- The system devices are not installed, used, maintained, or cleaned in accordance with the instructions
- The system devices are not used within the scope of proper use
- Unauthorized modifications are carried out on the system devices by the operator

Classification of notices



DANGER

Safety notice: Denotes imminent danger which could lead to death or serious injuries.



ATTENTION

Notice: Denotes possible property damage which cannot result in injuries.



NOTICE

Notice: Denotes additional information and useful tips.

Notices



DANGER

Risk of electrocution: All *ekey home* devices are to be operated with Safety Extra Low Voltage (SELV). Only use power supplies rated protection class 2 according to VDE 0140-1.

Failure to do so will create a risk of fatal electrocution.

Only certified electricians are authorized to carry out the electrical installation work.



ATTENTION

Tamper-proofing: Do not mount the control panel outdoors.

If it is mounted outdoors, it could be tampered with.

Mount the control panel in a secure internal area.

Introduction to the system

System overview

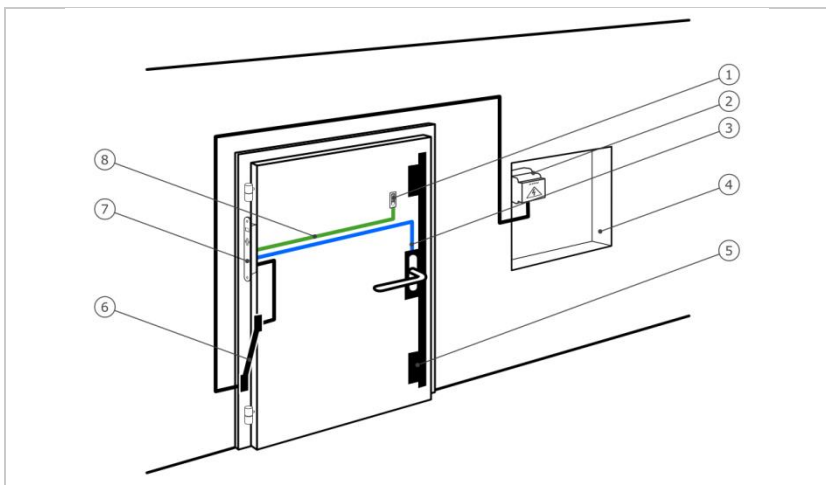


Fig. 1: Overview of the system

- 1 Finger scanner
- 2 Power supply
- 3 Connection from control panel to motorized lock
- 4 Distributor box
- 5 Motorized lock
- 6 Cable transfer
- 7 Control panel
- 8 Connecting cable from finger scanner to control panel

The system is comprised of a finger scanner and a control panel.

The biometric access control system detects the characteristics (minutiae) of the fingerprint contours, compares them to the biometric information saved from the reference fingerprint image, and opens the door in the event of a match.

Scope of delivery

- One finger scanner
 - One control panel
 - Operating instructions, mounting instructions, wiring diagram
 - Optional: matching accessories (cable transfer, power supply, connecting cable, covers, etc.)
-

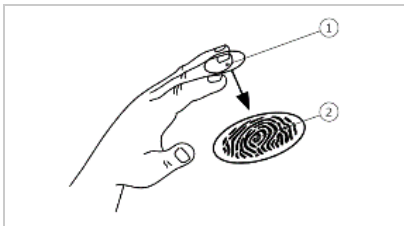
Finger scanner

Product name	ekey FS AR
---------------------	-------------------

Figure	
---------------	---

Table 1: Finger scanner

Function of the finger scanner



- 1 Front phalanx
- 2 Fingerprint

Fig. 2: Fingerprint

The finger scanner detects the fingerprint by means of a line sensor and subsequently processes it. It compares the result with that of the biometric information extracted from the reference fingerprint image and opens the door in the event of a match. The finger scanner only works correctly and reliably with the front phalanx print. Swipe your finger steadily and evenly over the sensor in the correct position.

Control	Function
Finger swipe area	Store fingers by “swiping the finger” evenly downward over the sensor.
Sensor	System programming by “Finger Touch”, a short, rapid touch of the sensor with the finger.

Table 2: Finger scanner controls

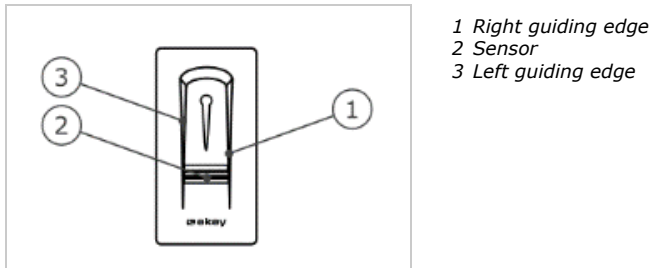


Fig. 3: Finger swipe area and sensor

Correct operation of the finger scanner

Incorrect operation will impair the function of the finger scanner.

"Swiping the finger":

Step	Figure	Description
1st		Hold your finger straight and place it centrally between the guiding edges. Do not twist the finger.
2nd		Place the joint of the front phalanx directly onto the sensor. Place your finger flat onto the finger swipe area.
3rd		Stretch out the neighboring fingers.
4th		Move your finger evenly downward over the sensor. Move the whole hand simultaneously. Swipe the front phalanx fully over the sensor in order to achieve optimal results. The movement takes approx. 1 s.

General hints for achieving a good-quality fingerprint:

- The index, middle, and ring fingers work best. The thumb and small finger supply fingerprints that are difficult to analyze.
- In the case of fingers that are frequently wet, store the images with wet fingers.
- Children's fingerprints work from approx. 5 years of age.

"Finger Touch"

Step	Figure	Description
1st		Briefly touch the sensor with your finger.

Optical signals on the finger scanner

The 3 LEDs on the finger scanner signal the operating status and function of the overall system.



- 1 Status LED
- 2 Function LEDs

Fig. 4: Optical signals on the finger scanner

Control panel

The *ekey home CP micro plus* control panel works with the *ekey home finger scanner arte*. You can only operate 1 finger scanner per control panel.

Product name	<i>ekey home CP micro plus</i>
Figure	
Mounting type	Can be integrated, 1 relay, 1 digital input

Table 3: *Control panel*

Function of the control panel

The control panel is the actuator of the system. The control panel switches a relay and makes a digital input available.

Control and optical signals of the control panel

Control	Function
Button	Reset to default settings: Press and hold for 4 s

Table 4: *Control panel control*

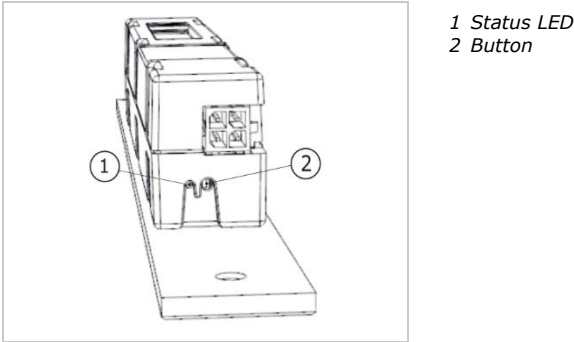


Fig. 5: *Overview of the ekey home CP micro plus*

The status LED indicates whether the control panel is in normal mode and whether the relay switches.

Technical specifications

Name	Unit	Values
Supply voltage	VDC	5
Power	W	Minimal (heating off): 0.5
		Maximal (heating on): 2
Operating temperature	°C	-25 to +70
IP code	IP	54

Table 5: Technical specifications: ekey home finger scanner arte

Name	Unit	Values
Supply voltage	VDC	12-24
Power rating	W	1
Relay	Quantity	1
Relay switching voltage	VDC	42
Relay switching current	A	2
Operating temperature	°C	-25 to +70
IP code	IP	30
Digital inputs	Quantity	1 (potential-free)
Typical matching duration	s	1
Memory	Finger	99
Security	FAR	1:10,000,000
	FRR	1:100

Table 6: Technical specifications: ekey home control panel micro plus

Installation and activation

Activating devices

 ATTENTION

Property damage in the event of incorrect mounting and wiring: The system devices are operated using electricity. They could be destroyed if they are mounted and wired incorrectly. Mount and wire the system devices correctly before connecting the power.



Mount the system in accordance with the supplied mounting instructions.



Wire the system in accordance with the supplied wiring diagram.

You must activate the devices in order to operate your system. The system is operated using the administrator fingers or via the *ekey home app*.
 The system devices must be installed in order for you to activate the system.

Step	Action	Display
1st	Ensure safe installation of the devices. Close the covers.	-
2nd	Connect the power supply to the mains.	 The status LED of the <i>ekey home CP micro plus</i> flashes green: Default setting.
3rd	No action required.	 The finger scanner flashes blue.

✓ The devices have now been activated.

The finger scanner is ready for storing administrator fingers and for creating the coupling between the finger scanner and mobile device.

Performing test mode

Test mode tests the lock after it has been installed in the door. It switches the relay and checks the electrical connections to the motorized lock.



NOTICE

Performing test mode: You can only perform test mode under the following conditions:

- ☐ You have activated the system
- ☐ You have not yet stored an administrator finger
- ☐ You have not yet coupled a mobile device

 Connect the mains supply and perform the test within 10 minutes. If 10 minutes have elapsed, the mains supply will have to be reconnected in order to conduct this test.

Step	Action	Description	Display
1st		Place a finger on the sensor and leave it there for longer than 3 s.	 The finger scanner flashes blue.
2nd		Remove the finger from the sensor within the next 2 s.	 The finger scanner lights up green.

✓ The relay switches.



NOTICE

Keep your finger on the sensor for up to 5 s: You can keep your finger on the sensor for up to 5 s. If the finger is kept on the sensor for longer than this, the relay will not switch.

Operating concept

Different operating concepts are available, depending on the registration unit:

- *ekey home app* – administration of the finger scanner by means of a mobile device
- *ekey administrator finger* – administration of the finger scanner by means of administrator fingers

Go to the operating concept of your choice.

Configuration of normal mode and usage of the finger scanner with the app

The devices must have been activated before you start your system administration.



See “Activating devices”, page 14.

The finger scanner is ready to create the coupling between the finger scanner and mobile device. The *ekey home app* is used for programming the system. Doors can also be opened via the app.

Downloading the app

The app is available for Apple iOS and Google Android. Download the *ekey home app* from the App Store or Google Play. To find it, enter the search term [ekey home app](#).



Coupling a mobile device for the first time

For first-time coupling, you will need the device coupling code and the app security code. Both codes are factory-set as 9999.

Step	Instruction	Display
1st	Start the <i>ekey home app</i> .	
2nd	Touch the input field (Android) or press <u>Search</u> (iOS). The app searches for available Bluetooth devices.	-
3rd	Select your ekey Bluetooth finger scanner.	-
4th	Android only: Press <u>Login</u> .	-
5th	Enter the default device coupling code <u>9999</u> .	 The finger scanner lights up red/blue.
6th	Press <u>Next</u> . The mobile device is coupled with the Bluetooth finger scanner.	
7th	Enter a new 6-digit device coupling code. For security reasons, you must change the default device coupling code the first time you perform the system admin coupling process. Make a note of this code, as you will need it to couple additional mobile devices.	-
8th	Write your new device coupling code here: _____.	
9th	Press <u>Change</u> (Android) or <u>Next</u> (iOS).	
10th	Enter the default app security code <u>9999</u> .	
11th	Press <u>Next</u> .	

✓ The coupling between the finger scanner and the mobile device is established. The system is in normal mode.

You can now start programming and managing the finger scan access control system via the *ekey home app*.



NOTICE

Administration of the finger scanner with the *ekey home App*: The intuitive *ekey home app* is now all you need for the administration of your finger scanner. Tap the required functions in the app and follow the instructions on the display.

Changing security codes

You can change all security codes at any time:

- ☐ the app security code
- ☐ the admin coupling code
- ☐ the user coupling code
- ☐ the control panel security code



NOTICE

App security code: The 4 to 6-digit app security code is required for the app security prompt. You can disable the prompt to enter the app security code under **ADMINISTRATION** if your mobile device supports secure lock mechanisms (fingerprint, code, etc.).

Step	Instruction
1st	Select ADMINISTRATION .
2nd	Select CHANGE SECURITY CODES .
3rd	Change the desired code.
4th	Press (Android) or (iOS).

The selected security code has been changed.

Storing a finger

You can store user fingers with the *ekey home app*.

Step	Instruction
1st	Select ADMINISTRATION .
2nd	Select USER ADMINISTRATION .
3rd	Press  + (Android) or  (iOS).
4th	Enter the user name.
5th	Press  .
6th	Select the relay to be switched.
7th	Select a finger.
8th	Press  .
9th	Read the notice and press  .
10th	Once your finger has been successfully registered, press  .
11th	Press  .



NOTICE

2 fingers per access point: Store a minimum of one finger from each hand per access point.

The user fingers have been stored.

Disabling Bluetooth

The Bluetooth functionality can be disabled: Bluetooth functionality is set to enabled in the default settings.

Step	Instruction
1st	Start the <i>ekey home app</i> .
2nd	Select ADMINISTRATION .
3rd	Select SYSTEM STATUS .
4th	Under BLUETOOTH SETTINGS , enable the setting Disable Bluetooth after 15 minutes.

✓ This setting disables Bluetooth on the finger scanner after 15 minutes if one of the following situations arises:

- ☐ No mobile device is connected
- ☐ At least one administrator finger has been stored.

You can re-enable Bluetooth by accessing the administrator finger menu.



See "Configuration of normal mode and usage of the finger scanner with administrator fingers", page 25.

Coupling additional mobile devices

You can couple additional mobile devices with the finger scanner using the 6-digit admin/user coupling code you have chosen.

Step	Action	Description	Display
1st		Start the <i>ekey home app</i> .	- -
2nd	Follow the instructions on the display	Couple the mobile device with the finger scanner using the 6-digit admin/user coupling code you have chosen.	 The finger scanner lights up red/blue

✓ The coupling between the finger scanner and the mobile device is established.

You can now start programming and managing the finger scan access control system via the *ekey home app*.

Managing multiple finger scanners

The *ekey home app* allows you to manage multiple finger scanners. To switch between two finger scanners, you must reset the coupling between the finger scanner and the mobile device.



NOTICE

Relay name and user images are deleted: When you reset the coupling, any relay names and user images that have been stored will be deleted. User names and rights will remain stored on the finger scanner.

Step	Instruction
1st	Start the <i>ekey home app</i> .
2nd	Select ADMINISTRATION .
3rd	Select RESET COUPLING .
4th	Confirm that you wish to carry out the reset by selecting Continue .

✓ The coupling between the finger scanner and the mobile device has been reset.
You can now couple another finger scanner



See "Coupling additional mobile devices", page 20.

Storing the user coupling code

The option is available to store a user coupling code. This can be passed on to a person of your choosing, who can then use it to perform the following actions with their mobile device:

- ☐ Open a door
- ☐ Enable/disable the app security code
- ☐ Change the app security code
- ☐ Reset the coupling between the finger scanner and your mobile device

Step	Instruction
1st	Start the <i>ekey home app</i> .
2nd	Select ADMINISTRATION .
3rd	Select CHANGE SECURITY CODES .
4th	Enter the required user coupling code in the corresponding field.
5th	Confirm by selecting Change (Android) or Done (iOS).

✓ The user coupling code was stored.

Resetting the app security code

If you have forgotten the app security code, you can use the app to reset the coupling between the finger scanner and the mobile device. When this reset is performed, the app security code is also reset to the default value of 9999.

Step	Instruction
1st	Start the <i>ekey home app</i> .
2nd	Enter an incorrect app security code.
3rd	Confirm by selecting Next .
4th	Select RESET COUPLING .
5th	Confirm that you wish to carry out the reset by selecting Continue .

✓ The coupling between the finger scanner and the mobile device has been reset and the app security code set to 9999.

You can now recouple the finger scanner.

 See "Coupling additional mobile devices", page 20.

Protecting the system in the event that the mobile device is lost

If you have lost your mobile device, you can use a second mobile device to change the admin/user coupling code. This new admin/user coupling code will stop any connections being established using the lost mobile device.

Step	Instruction
1st	Start the <i>ekey home app</i> on the second mobile device.
2nd	Couple the second mobile device with the finger scanner.
3rd	Select ADMINISTRATION .
4th	Select CHANGE SECURITY CODES .
5th	Enter a new 6-digit admin/user coupling code.
6th	Confirm by selecting Change (Android) or Done (iOS).

✓ The admin/user coupling code in the system has now been changed.

This means that the lost mobile device is no longer able to establish a connection to the finger scanner. Your system is protected against access by unauthorized persons once again.

Opening a door

The primary purpose of the product is to open doors. This can be carried out using the app, the finger scanner, or the digital input.

Using the app

 The system is in normal mode.

Step	Instruction
1st	Start the <i>ekey home app</i> .
2nd	Connect to the finger scanner.
3rd	Select ACCESSES .
4th	Slide the slider of the door to be opened to the right.
5th	The door opens.

✓ The system returns to normal mode.

Using the finger scanner

 The system is in normal mode.

Step	Action	Description	Display
1st		Swipe a stored finger over the sensor.	 The finger scanner lights up green.
			 The finger scanner lights up red.
		The finger was not recognized. Repeat step 1.	- -
2nd	No action required.	The door opens.	 The finger scanner lights up blue.

✓ The system returns to normal mode.

Using the digital input (request-to-exit button)

You can also open the door using the request-to-exit button of the digital input on the control panel. The relay switches for the defined relay switch time. If the digital input is enabled for longer than the defined relay switch time, the relay switches for as long as the digital input is enabled.

Configuration of normal mode and usage of the finger scanner with administrator fingers

The devices must have been activated before you start your system administration.



See "Activating devices", page 14.

The finger scanner is ready to store the administrator fingers. The administrator fingers are used for programming the system. However, they are also able to open doors (like user fingers).

Storing administrator fingers and configuring normal mode

You must store 4 administrator fingers. We recommend storing 2 fingers of 2 different people for this purpose.

 You must activate the system devices in order to store administrator fingers.

Step	Action	Description	Display
1st		Carry out three Finger Touches on the sensor within 5 s. This will take you to the admin menu.	 The left and right LEDs alternate between flashing orange/green. The central LED lights up orange.
2nd		Swipe administrator finger 1 over the sensor to store it. See "Correct operation of the finger scanner", page 10. Repeat this step at least twice. Between each individual finger swipe, the finger scanner lights up orange if the finger storing process is not complete. After the first finger has been swiped once over the sensor, no more than 10 s may pass between each subsequent swipe. Otherwise, the finger storing process will be aborted.	 The central LED lights up green.
			 The finger scanner lights up red.
		The quality of the fingerprint is acceptable. However, it may be possible to improve the quality by swiping the finger again.	- -
		The quality of the fingerprint is poor or the finger was not recognized. Swipe the finger over the sensor again.	- -
3rd	No action required.	-	 The finger scanner lights up green

Step	Action	Description	Display
4th		To store administrator fingers 2, 3, and 4, carry out steps 2 and 3 for administrator fingers 2, 3, and 4.	 The finger scanner lights up blue.

✓ All administrator fingers were successfully stored. The system is in normal mode.



NOTICE

Restarting the finger scanner in admin mode: If, when the finger scanner is restarted, admin mode is active and fewer than 4 administrator fingers are present, all previously stored administrator fingers are deleted.

Storing user fingers

The system enables a maximum of 99 user fingers to be stored.

A user finger is any finger which is used for triggering an action on the control panel, e.g., opening a door. We recommend storing 2 fingers in each case.

 The system is in normal mode.

Step	Action	Description	Display
1st		Carry out three Finger Touches on the sensor within 5 s. This will take you to the admin menu.	 The finger scanner flashes green intermittently on the left and right.
2nd		Swipe any administrator finger over the sensor.	 The finger scanner flashes green.  The finger scanner lights up red.
		The administrator finger was not recognized. Repeat step 1.	-
3rd		Carry out a Finger Touch on the sensor within 5 s.	 The finger scanner lights up orange.

Step	Action	Description	Display	
4th		Swipe the user finger over the sensor to store it. See "Correct operation of the finger scanner", page 10. Repeat this step at least twice. Between each individual finger swipe, the finger scanner lights up orange if the finger storing process is not complete. After the first finger has been swiped once over the sensor, no more than 10 s may pass between each subsequent swipe. Otherwise, the finger storing process will be aborted.		The central LED lights up green.
				The finger scanner lights up red.
			The quality of the fingerprint is acceptable. However, it may be possible to improve the quality by swiping the finger again.	- -
			The user finger was not stored. Repeat the procedure beginning at step 1. After 10 scans, the finger storing process is aborted.	- -
5th	No action required.	-		The finger scanner lights up blue.

✓ The user finger was stored. The system returns to normal mode.

Opening a door

The primary purpose of the product is to open doors. This can be carried out using the app, the finger scanner, or the digital input.

Using the app

 The system is in normal mode.

Step	Instruction
1st	Start the <i>ekey home app</i> .
2nd	Connect to the finger scanner.
3rd	Select ACCESSES .
4th	Slide the slider of the door to be opened to the right.
5th	The door opens.

✓ The system returns to normal mode.

Using the finger scanner

 The system is in normal mode.

Step	Action	Description	Display
1st		Swipe a stored finger over the sensor.	 The finger scanner lights up green.
			 The finger scanner lights up red.
		The finger was not recognized. Repeat step 1.	-
2nd	No action required.	The door opens.	 The finger scanner lights up blue.

✓ The system returns to normal mode.

Using the digital input (request-to-exit button)

You can also open the door using the request-to-exit button of the digital input on the control panel. The relay switches for the defined relay switch time. If the digital input is enabled for longer than the defined relay switch time, the relay switches for as long as the digital input is enabled.

Deleting user fingers

You can only delete individual fingers of a user if the person is present.

 The system is in normal mode.

Step	Action	Description	Display
1st		Carry out three Finger Touches on the sensor within 5 s. This will take you to the admin menu.	 The finger scanner flashes green intermittently on the left and right.
2nd		Swipe any administrator finger over the sensor.	 The finger scanner flashes green.
			 The finger scanner lights up red.
		The administrator finger was not recognized. Repeat step 1.	-
3rd		Wait for 5 s.	 The left and right LEDs alternate between flashing red/green.
4th		Carry out a Finger Touch on the sensor within 5 s.	 The left LED lights up red, the right LED lights up green.
5th		Swipe the user finger to be deleted over the sensor.	 The finger scanner flashes red.
6th	No action required.	-	 The finger scanner lights up blue.

✓ The user finger was deleted. The system returns to normal mode.

Deleting all user fingers

All user fingers in the system are deleted. The administrator fingers are retained.

 The system is in normal mode.

Step	Action	Description	Display
1st		Carry out three Finger Touches on the sensor within 5 s. This will take you to the admin menu.	 The finger scanner flashes green intermittently on the left and right.
2nd		Swipe any administrator finger over the sensor.	 The finger scanner flashes green.
			 The finger scanner lights up red.
		The administrator finger was not recognized. Repeat step 1.	-
3rd		Wait for 5 s.	 The left and right LEDs alternate between flashing red/green.
4th		Carry out a Finger Touch on the sensor within 5 s.	 The left LED lights up red, the right LED lights up green.
5th		Swipe the same administrator finger over the sensor as in step 2.	 The finger scanner flashes red.
6th	No action required.	-	 The finger scanner lights up blue.
7th		Swipe any user finger over the sensor in order to verify. No finger should now be able to gain access.	 The finger scanner lights up red.
8th	No action required.	-	 The finger scanner lights up blue.

✓ All user fingers were deleted. The system returns to normal mode.

Resetting the system to default settings

You can reset the system to its default settings either via the app, the finger scanner, the control panel, or the digital input.

Resetting to default settings permanently deletes all rights and resets the system settings to their defaults. Your system is then in the condition in which it was delivered to you once more.

Via the app

The process of resetting to the default settings is initiated via the app. The finger scanner settings are reset to their defaults. All user and administrator fingers will be irrecoverably deleted. The coupling code is reset to the default setting of 9999, the relay switching time to 3 seconds, and the LED brightness of the finger scanner to 2 (LED on). These settings can only be made via the app.

Step	Instruction
1st	Start the <i>ekey home app</i> .
2nd	Connect to the finger scanner.
3rd	Select ADMINISTRATION .
4th	Select RESET SYSTEM .
5th	Confirm that you wish to carry out the reset by selecting <u>Continue</u> .

✓ The finger scanner and the control panel have been reset to the default settings. You can now reactivate the system.



See "Configuration of normal mode and usage of the finger scanner with the app", page 16.

Via the finger scanner

The process of resetting to the default settings is initiated via the finger scanner. The finger scanner settings are reset to their defaults. All user and administrator fingers will be irreversibly deleted. The coupling code for the app is reset to the default setting of 9999.

Step	Action	Description	Display
1st		Carry out three Finger Touches on the sensor within 5 s. This will take you to the admin menu.	 The finger scanner flashes green intermittently on the left and right.
2nd		Swipe any administrator finger over the sensor.	 The finger scanner flashes green.
			 The finger scanner lights up red.
3rd		The administrator finger was not recognized. Repeat step 1.	- -
4th		Wait for 5 s.	 The left and right LEDs alternate between flashing red/green.
5th		Carry out a Finger Touch on the sensor within 5 s.	 The left LED lights up red, the right LED lights up green.
6th		Swipe a different administrator finger over the sensor than was used in step 2.	 The left and right LEDs flash red. The central LED flashes yellow.
7th	No action required.	-	 The finger scanner flashes blue.

✓ The registration unit and the control panel were reset to the default settings. You can now reactivate the system.



See "Configuration of normal mode and usage of the finger scanner with the app", page 16.



See "Configuration of normal mode and usage of the finger scanner with administrator fingers", page 25.

Via the control panel

The process of resetting to the default settings is initiated via the control panel. The finger scanner settings are reset to their defaults. All user and administrator fingers will be irrecoverably deleted. The coupling code for the app is reset to the default setting of 9999.

Step	Action	Description	Display
1st		Press and hold the button with the unlocking spring for at least 4 s.	 The finger scanner flashes blue.
2nd	No action required	-	 The status LED of the <i>ekey home CP micro plus</i> flashes green.

✓ The registration unit and the control panel were reset to the default settings. You can now reactivate the system.



See "Configuration of normal mode and usage of the finger scanner with the app", page 16.



See "Configuration of normal mode and usage of the finger scanner with administrator fingers", page 25.

Via the digital input

The process of resetting to the default settings is initiated via the digital input. The finger scanner settings are reset to their defaults. All user and administrator fingers will be irrecoverably deleted. The coupling code for the app is reset to the default setting of 9999.

Step	Instruction
1st	Disconnect the <i>ekey home CP micro plus</i> from the mains supply.
2nd	Press and hold the request-to-exit button or short-circuit the pins for the digital input and keep them in this state.
3rd	Connect the <i>ekey home CP micro plus</i> to the mains supply.
4th	Keep the request-to-exit button held down or keep the pins for the digital input short-circuited for at least 5 s.
5th	Release the request-to-exit button or remove the short-circuit. Within 5 s, press and hold the request-to-exit button or short-circuit the pins for the digital input for at least 500 ms.

✓ The finger scanner and the control panel have been reset to the default settings. You can now reactivate the system.



See "Configuration of normal mode and usage of the finger scanner with the app", page 16.



See "Configuration of normal mode and usage of the finger scanner with administrator fingers", page 25.

Updating the software

We are working to improve our products and add new functions all the time. Correspondingly, updates are made available for the finger scanner and control panel software. More information about this can be obtained from your dealer.

Error displays and troubleshooting

Control panel

Display	Meaning	Remedy
	No connection to the control panel.	Check the wiring and the power supply.

If these remedies do not solve the problem, contact your dealer. If the system has to be returned to ekey biometric systems GmbH, ensure that it is correctly packaged. Improper packaging can lead to the warranty being voided.

Finger scanner

Display	Meaning	Remedy
 The finger scanner lights up red.	The finger was not recognized or no fingers have been stored.	Swipe the finger over the sensor again or store a minimum of one finger.
 The finger scanner flashes orange.	No bus connection to the control panel.	Check the wiring or activate the device.
 The finger scanner flashes red/green.	The sensor of the finger scanner is soiled or broken.	Clean the sensor.

If these remedies do not solve the problem, contact your dealer. If the system has to be returned to ekey biometric systems GmbH, ensure that it is correctly packaged. Improper packaging can lead to the warranty being voided.

Maintenance

The system is largely maintenance-free.

The sensor surface of the finger scanner is essentially self-cleaning due to repeated use (swiping of fingers). However, if the finger scanner becomes soiled, clean it gently with a damp (not wet), non-abrasive cloth. Q-tips, microfiber cloths, and glasses-cleaning cloths are suitable for this purpose. Cotton-containing materials, paper towels, tissues, kitchen sponges, damp dish towels, and kitchen roll are not suitable. Use clean water without adding detergent.

Disposal



Pursuant to Directive 2012/19/EU of the European Parliament and of the Council of 4 July 2012 on waste electrical and electronic equipment, electrical and electronic equipment supplied after August 13, 2005 is to be recycled. It must not be disposed of with household waste. As disposal regulations within the EU can differ from country to country, please contact your dealer for further information as necessary.

Austria

ekey biometric systems GmbH
Lunzerstraße 89, A-4030 Linz
Tel.: +43 732 890 500 0
office@ekey.net

Switzerland & Liechtenstein

ekey biometric systems Est.
Landstrasse 79, FL-9490 Vaduz
Tel.: +41 71 560 54 80
office@ekey.ch

Italy

ekey biometric systems Srl.
Via Copernico, 13/A, I-39100 Bolzano
Tel.: +39 0471 922 712
italia@ekey.net

Germany

ekey biometric systems Deutschland GmbH
Industriestraße 10, D-61118 Bad Vilbel
Tel.: +49 6187 906 96 0
office@ekey.net

Eastern Adriatic region

ekey biometric systems d.o.o.
Vodovodna cesta 99, SI-1000 Ljubljana
Tel.: +386 1 530 94 89
info@ekey.si



802675

ID251/564/0/458: Version 2, 2017-03-09;
Media Center ID: 3014

www.ekey.net

Made in Austria