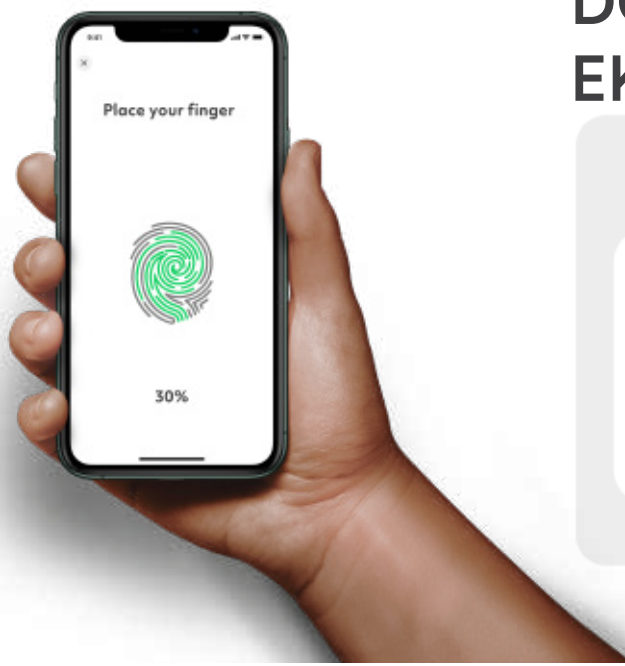


Ekey DLine Fitter & Homeowners Guide



Contents

Comfort Meets Safety	Pg 3
Frequently Asked Questions	Pg 4-15
Homeowner App Information	Pg 16
Information For Fitters	Pg 17
Wiring Diagram For ekey dLine	Pg 18
Contact Us	Pg 19



DOWNLOAD EKEY BIOYNX APP

ekey bionyx App



Apple and the Apple logo are trademarks of Apple Inc., registered in the U.S. and other countries. Google Play and the Google Play logo are trademarks of Google LLC.

Comfort Meets Safety.

About ekey

ekey started in 2002 and is now Europe's No. 1 for fingerprint scanner access solutions. Keys, cards and codes can be lost, forgotten or stolen, whereas your finger is always on hand! ekey has been developing access solutions for private households, companies and organizations for 20 years. What began as a research project is now one of the leading manufacturers of biometric access control: the Austrian family-owned company is now the European market leader for fingerprint scanner access solutions.

Quality "Made in Austria"

Before an ekey product can be launched on the market, it has to undergo a rigorous endurance test: intensive simulations ranging from blazing heat and freezing cold to high humidity. Each fingerprint scanner and all of its components must successfully complete these tests numerous times before the product finally finds its way into your hands.

Comfort Meets Safety.

Fingerprint scanner access systems from ekey enrich everyday life with the convenience of keyless access as well as flexibility and smart features. Security is always at the center of this process.

So how secure is an ekey fingerprint scanner system? On the next pages you will find answers to the most common frequently asked questions.



Frequently Asked Questions

Are fingerprints stored?

No. ekey does not store fingerprints.

The biometric features of the original fingerprint, such as the unique dots, line endings and bifurcations, are used to create a pattern - the so-called template. This is converted into a unique binary number code by the specially developed and patented software algorithm, stored and used for comparison each time. The templates are stored encrypted in the ekey bionyx cloud. The key is located exclusively on the user's own end device (smartphone/tablet), so the data is protected from unauthorized access. The security can be compared to that of a netbanking app.



Can an original fingerprint be reconstructed from the stored data?

No, the stored template (see "Are fingerprints stored?") can no longer be converted back into a fingerprint. Thus, a reconstruction of the original fingerprint is impossible.



Frequently Asked Questions

Is it possible to make a usable fake finger from a fingerprint left behind (e. g. on a glass) to open a door?

ekey relies on multiple safeguards against manipulation by fake fingers: whether the biometric features originate from the finger of a real person is checked on the one hand with the conductivity of the living skin when the finger is placed on the sensor, and on the other hand during the algorithmic evaluation of the data. In addition, it is almost impossible to produce a usable fake fingerprint. With a lot of criminal energy, even more expert knowledge and the best laboratory conditions, the characteristics could be transferred to a fake finger.

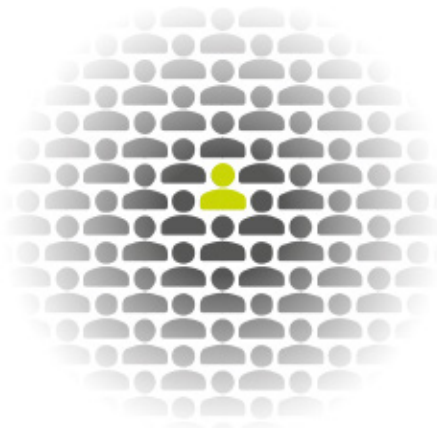
Conclusion: possible in theory, hardly likely in practice.



What is the probability that the door will open for an unauthorized person?

There is a special indicator for this – the false acceptance rate (FAR). This describes the probability of a person gaining access to a security system even though they have no authorization. In the case of ekey fingerprint scanners, this is 1 in 10 million - assuming that the fingerprints were stored correctly. In summary: with ekey fingerprint scanners, it is theoretically possible for an unauthorized person to gain access, but this is highly unlikely.

Compared to the four-digit numeric code of an ATM card, an ekey system is 1,000 times more secure. And at 1:8,145,000, the probability of winning a lottery six (6 out of 45) with a single pick is significantly higher than that of an unauthorized person gaining access.

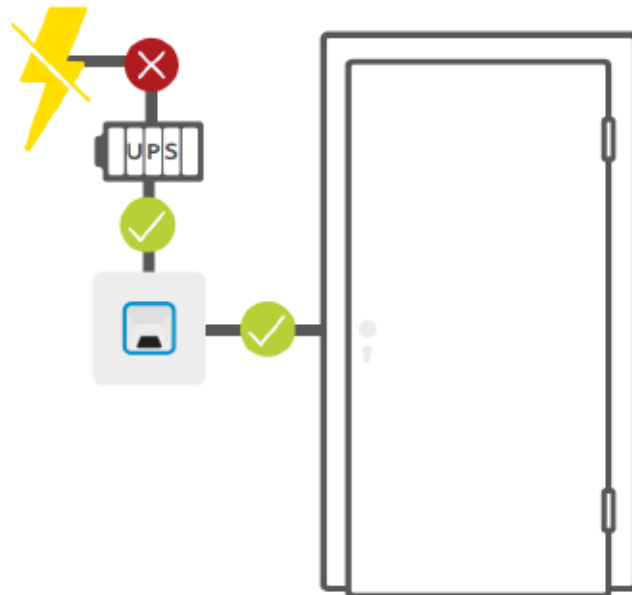


Frequently Asked Questions

How do you open the door in the event of a power failure?

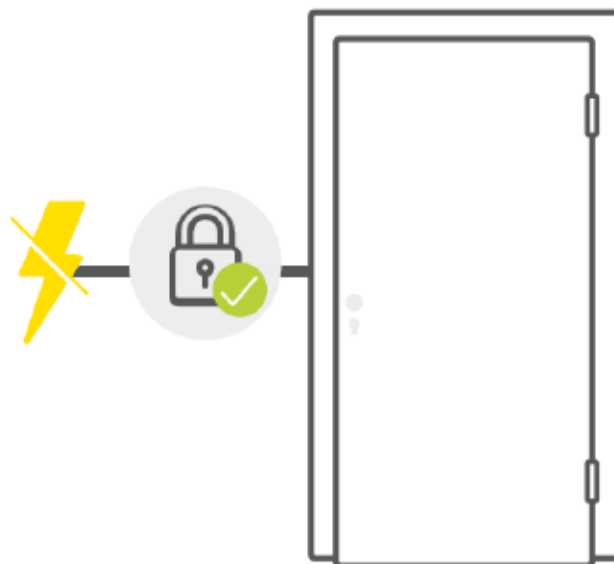
If the power, the Internet or the router fail, no one is left standing in front of a locked door. ekey offers an uninterruptible power supply (UPS) for its access systems. It keeps the fingerprint scanner, the control panel and the motorized lock in operation for several hours.

Alternatively, a key can of course be used at any time. And even if the connection to the Internet or the router fails, the door can still be opened.



Can a door open by itself in the event of a power failure?

No. Power failures cannot trigger an impulse that opens the door in an ekey fingerprint scanner access solution. Only an authorized user can trigger this opening command.



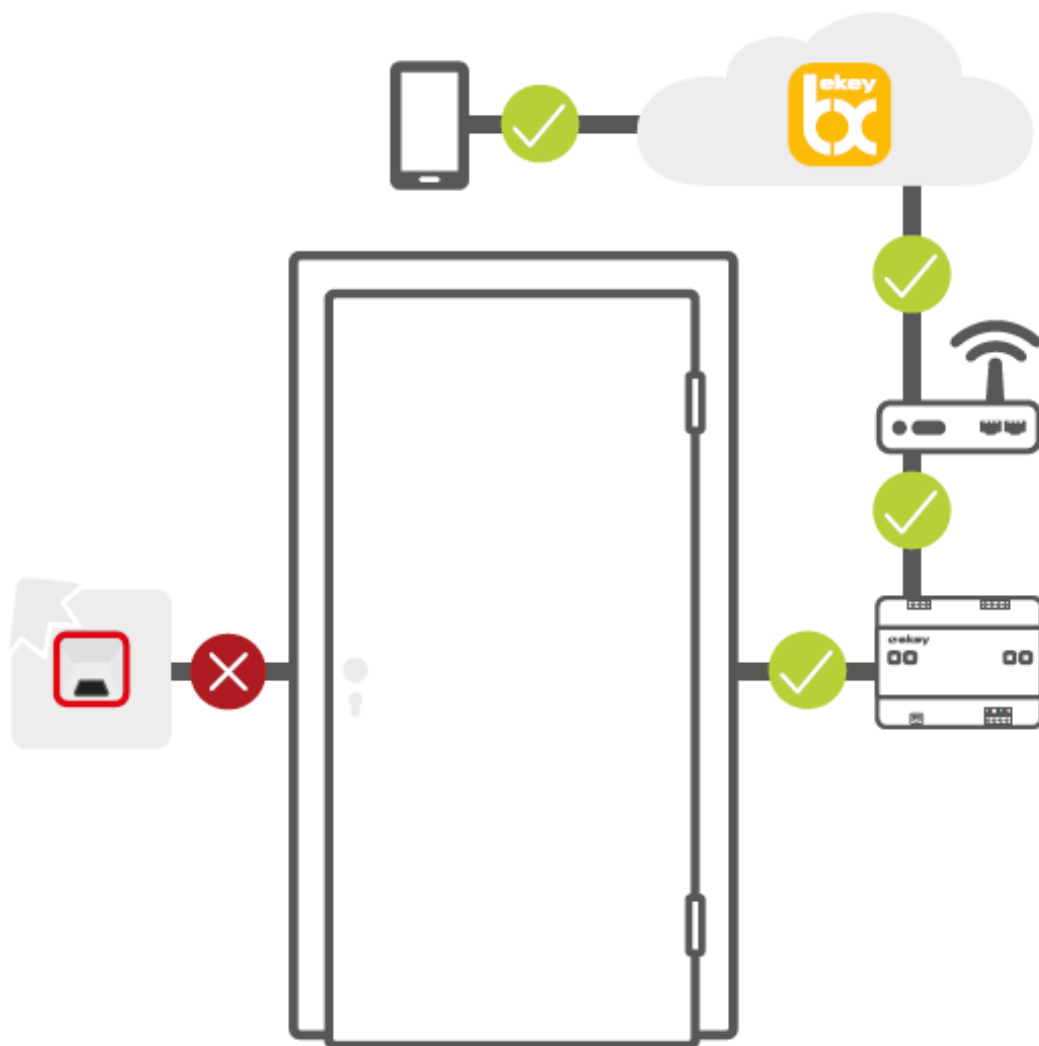
Frequently Asked Questions

Can the ekey fingerprint scanner access solution be manipulated from the outside so that the door opens?

No. The system cannot be manipulated from the outside. Not even through the use of force, because the fingerprint scanner and the control panel are spatially separated. The opening impulse comes from the control panel, which is located in the protected interior area.

The data is also encrypted and secured multiple times at all times.

Data transmission in the ekey bionyx system is end-to-end encrypted. All data is transmitted encrypted across all transmission stations.



Frequently Asked Questions

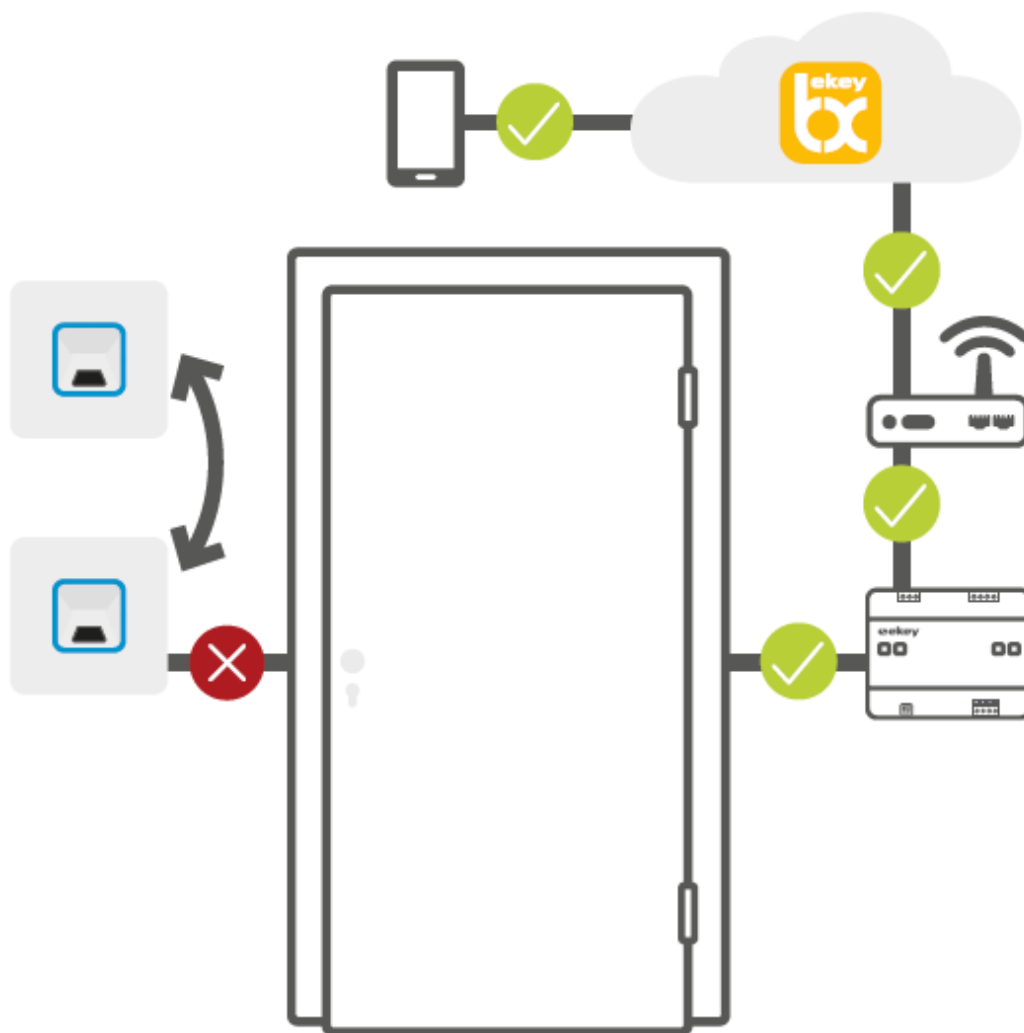
Can the system be manipulated by swapping the fingerprint scanner?

No, the system cannot be manipulated by swapping the fingerprint scanner.

This is because the fingerprint scanner and the control panel are „coupled“ during activation and communicate in encrypted form. The user data created is stored with the serial number of the device. If the fingerprint scanner is swapped or the system is expanded, this must be verified by an administrator in the ekey bionyx app.

In this way, the stored fingers are retained and do not have to be stored again.

Without this process, stored data cannot be transferred to another device.



Frequently Asked Questions

Is the system connected to the Internet?

No. The devices communicate over the Internet exclusively with the ekey bionyx cloud, which is operated via the cloud computing world market leader MS Azure. The data is encrypted at all times and cannot be viewed by either ekey or Microsoft.

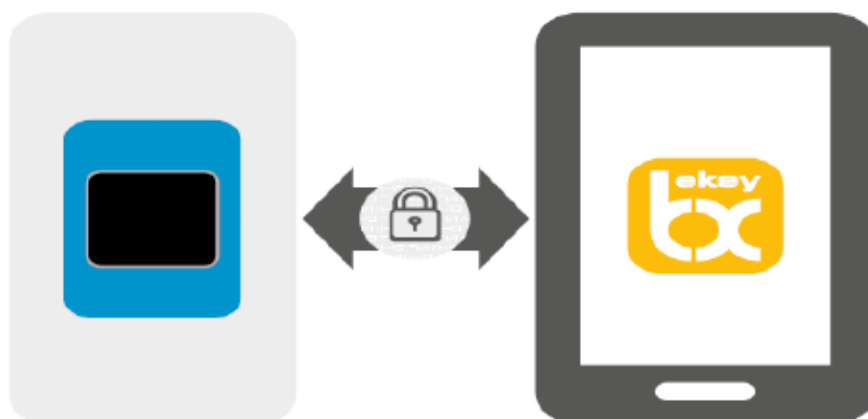
Due to the high security standard, only encrypted WLAN networks can be used.



How secure is the connection between smartphone/tablet, fingerprint scanner and control panel?

The secure “Transport Layer Security” protocol is used for the initial connection between the smartphone/tablet, the fingerprint scanner and the control panel. Data is transmitted between the devices exclusively in encrypted form.

Data transmission in the ekey bionyx app follows end-to-end encryption. All data is transmitted in encrypted form across all transmission stations. The data sent cannot be read or generated either by attackers or by ekey itself.

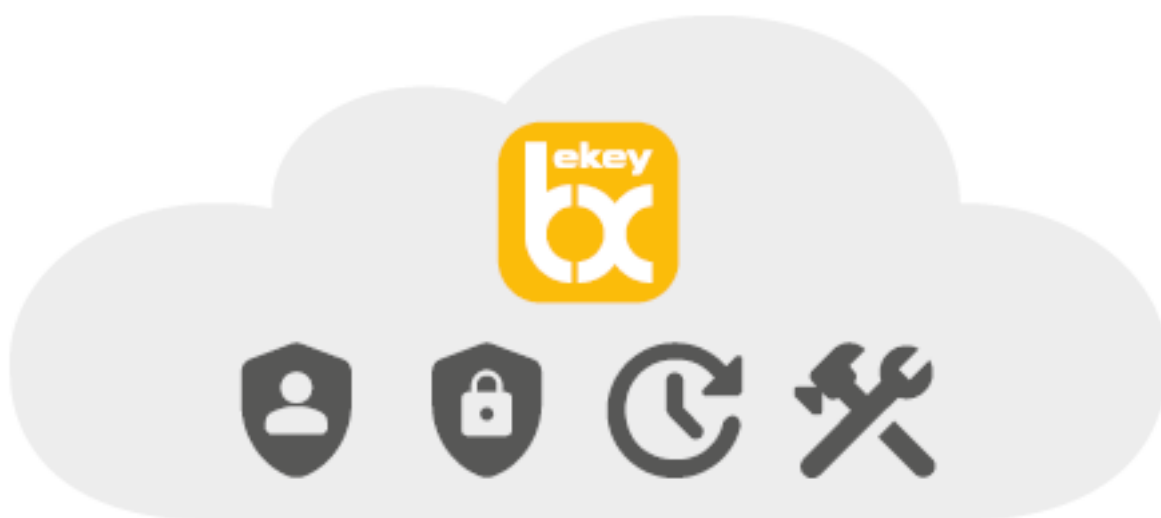


Frequently Asked Questions

Why does ekey rely on a cloud solution?

In addition to the actual device - the hardware - an access system always also includes the corresponding software - from computing and storage capacities to the actual software. With the ekey bionyx cloud, ekey has decided to use cloud-based technology because it offers numerous advantages on the software side (ekey bionyx app):

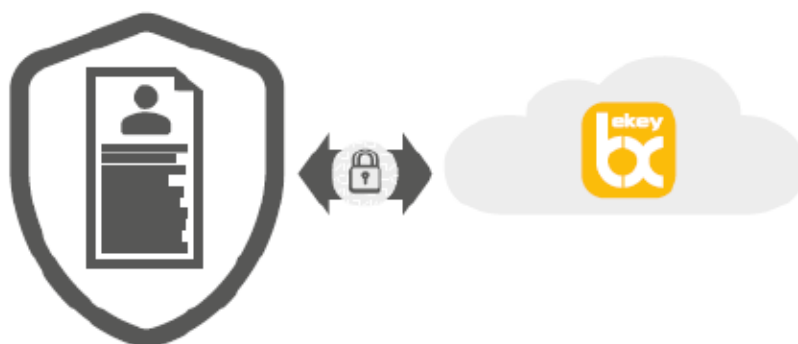
1. **Data protection:** Leading providers of cloud-based solutions invest a great deal of financial and human resources in protecting their customer's data. For this reason, such a solution is usually more professional in this respect than an in-house solution.
2. **Security:** The business model of large cloud providers is based on keeping data safe. Therefore, both the data centers themselves are extremely well protected (e. g. premises, surveillance, fire protection, etc.) and the virtual protection against cybercrime is at a correspondingly high level.
3. **Availability:** Software level agreements ensure software availability of around 99% (the missing 1% are usually planned downtimes for updates). A comparably high availability is not possible with a server of your own.
4. **Updates:** Software must always be kept up to date in order to offer maximum security. Cloud-based access systems are always up to date, and updates are automatic.



Frequently Asked Questions

What happens to the personal data?

ekey's vision is to make biometrics possible for everyone. The associated goal is to make everyday life as secure, flexible and convenient as possible, and to create practical benefits. ekey thus wants to improve life, not invade privacy. The business model is therefore designed in such a way that the products and services are never exchanged for personal data and these are therefore neither used by ekey itself nor sold to third parties.



What happens if I lose my smartphone/tablet?

Unlike a key, the finder of the smartphone does not have access to the system: the smartphone or tablet and the ekey bionyx app are unlocked separately – the former through the individually set access via biometrics (fingerprint or facial recognition) or code, the latter via biometrics or the user name with a personal password. The app is thus protected against unauthorized access. If the smartphone or tablet is lost, the connection to the ekey bionyx cloud can be restored via a new device and a backup code.

So, even if the mobile device is lost, it is still possible to log in using a new device with the access data.



Frequently Asked Questions

Are fingerprint scanner activities logged?

By default, activities are stored in the access log for 30 days. The access log can be viewed and deleted or deactivated by authorized administrators.



06:13	Entrance	User 002
07:27	Warehouse	User 002
08:15	Garage	User 003
09:13	Office 2	User 001
09:23	Office 2	User 003
09:45	Entrance	User 001
10:23	Warehouse	User 002
11:50	Entrance	User 003
11:59	Garage	User 001
12:05	Entrance	User 002
13:13	Entrance	User 003
13:17	Warehouse	User 002
13:34	Warehouse	User 001
15:07	Garage	User 001
15:26	Entrance	User 002
16:16	Entrance	User 003
17:46	Garage	User 002
17:47	Office 2	User 003
17:58	Entrance	User 002
18:11	Office 3	User 003
18:27	Warehouse	User 004
19:22	Entrance	User 003
19:38	Entrance	User 001
19:45	Garage	User 001
20:18	Entrance	User 003

Frequently Asked Questions

Are hidden access authorizations for the manufacturer stored in the system?

No. ekey has no option in the system for opening by a technician (factory code, etc.). Only an authorized administrator can make changes using their smartphone or tablet in combination with their account access data (email, password).



Does insurance coverage exist with a fingerprint scanner access solution?

It is irrelevant for insurance coverage whether locking is triggered with a key or electronically with a fingerprint scanner. In principle, insurance coverage only exists if the access is properly locked. If a door only “falls into the latch” - that part of the lock that holds the door in the door frame when it stops – it is not considered to be locked.



Frequently Asked Questions

Are hidden access authorizations for the manufacturer stored in the system?

No. ekey has no option in the system for opening by a technician (factory code, etc.). Only an authorized administrator can make changes using their smartphone or tablet in combination with their account access data (email, password).

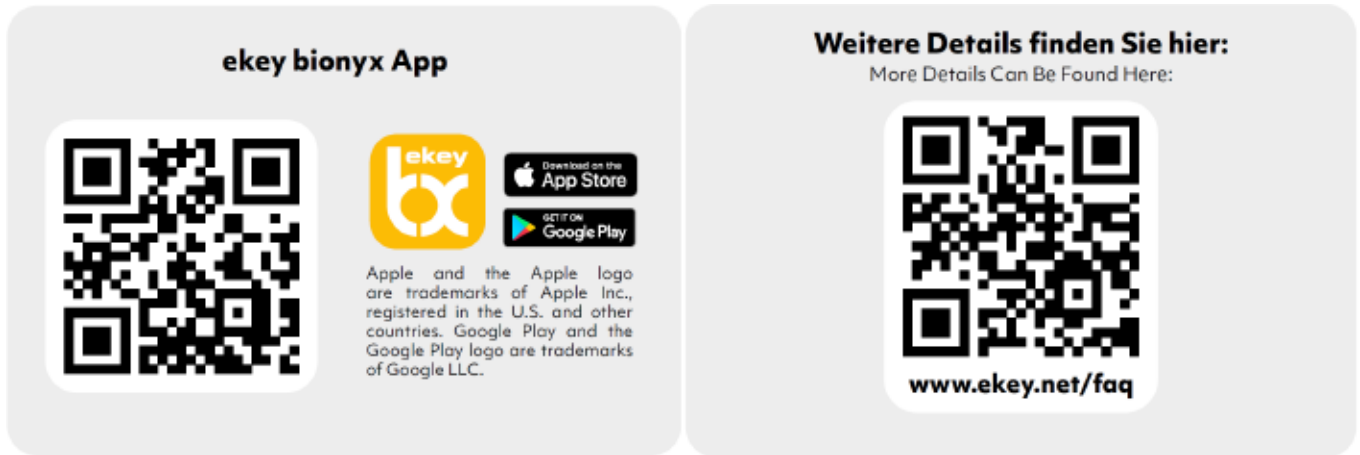


Does insurance coverage exist with a fingerprint scanner access solution?

It is irrelevant for insurance coverage whether locking is triggered with a key or electronically with a fingerprint scanner. In principle, insurance coverage only exists if the access is properly locked. If a door only “falls into the latch” - that part of the lock that holds the door in the door frame when it stops – it is not considered to be locked.



Homeowner App Information



ekey fingerprint scanner activation

The ekey bionyx app is required to activate the system. It guides you intuitively through the entire process. In order to use all the functions of the ekey bionyx system, a stable, password-protected 2.4 GHz WLAN network with at least WPA2-PSK encryption is required in the wireless range of the fingerprint scanner. If no WLAN network is available, a smartphone hotspot can be used for a short time.

Functional test before the system is activated

To test the successful installation of the fingerprint scanner before activation, any finger can be placed on the sensor of the device. If the door opens, the wiring is fine. This test mode is active for 10 minutes after the power is applied. After this period of time has elapsed or after the activation has been completed, this function is automatically deactivated.

You need help? Our support is there for you!

Austria & Germany
E: support@ekey.net

Switzerland & Liechtenstein
E: supportschweiz@ekey.net

Adriatic East region
E: info@ekey.si

International
E: support@ekey.net

Information For Fitters



Test mode

Fitters or electricians have a test mode for the basic function: the door is opened by placing any finger on the fingerprint scanner. Test mode is only available within the first 10 minutes after power is applied. After this period of time has elapsed or after the system has been activated, this function is deactivated.

Activating an ekey fingerprint scanner

Your customer needs the 'ekey bionyx app' to activate the system. This guides him intuitively through the entire activation process.

Prerequisite for activation

A stable, password-protected 2.4 GHz WLAN network with WPA-PSK2 encryption is essential in the wireless range of the front door.

You can also set up activation via a hotspot on your mobile device. The procedure for setting up the hotspot can be found in the operating instructions for your mobile device.

Do you need support? Our technical support department is here for you!

Austria & international

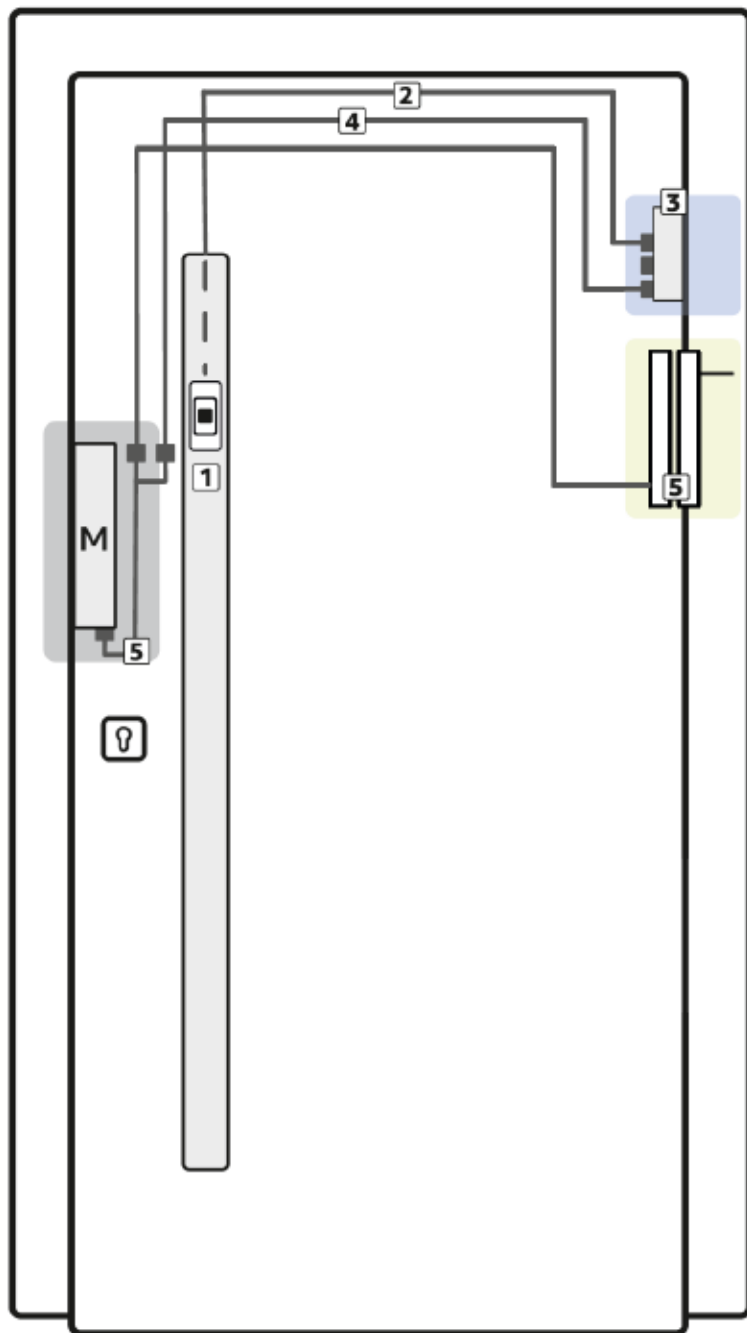
Mon–Thu: 8:00 AM–5:00 PM

Fri: 8:00 AM–1:00 PM

T: +43 732 890 500 – 0

E: support@ekey.net

Wiring Diagram For ekey dLine



Connection to the motorized lock

Pin	Color	Description
1	white	VDC (+)
2	brown	GND (-)
3	green	Switching impulse (+)

Connection to the control unit

Pin	Color	Description
4	yellow	Opening signal
3	green	Opening signal
2	brown	GND (-)
1	white	VDC (+)

⚠ Jumper must be removed! ⚠

Connection to the electrical installation

Color	Description
white	VDC (+) (12)
brown	GND (-)
green	External opening signal
yellow	Signal swing door opener
gray	Signal swing door opener
pink	Not used
green/white = input for external potential-free contact (e.g. unlocking via intercom)	
yellow/gray = output signal swing door opener (optional), only with „swing door“ motor housing	

⚠ Each unused core must be insulated separately! ⚠

1 ekey dLine fingerprint 450007

2 ekey dLine cable FP

3 ekey dLine controller 450008

4 ekey dLine cable MT 3,5 m Winkhaus blueMatic EAV 201360

5 Winkhaus set Cable transition with Y-cable Winkhaus part no. 5040508

⚠ DANGER ⚠

Risk of electrocution: All ekey devices are to be operated with Safety Extra Low Voltage (SELV). Only use power supplies rated protection class 2 with safety approval according to EN 62368-1. Failure to do so will create a risk of fatal electrocution. Only certified electricians are authorized to carry out electrical installation work on mains systems.

⚠ 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.

📢 NOTICE

This wiring diagram is 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.

Contact Us

Tel: 0115 982 7744

Email: enquiries@entrancecds.com

Website: www.entranceway.co.uk