ekey
YOUR FINGER. YOUR KEY.

How secure is an ekey fingerprint access solution?

Answers to the most frequently asked questions

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.

Should you have any further questions, please do not hesitate to contact:

T: +43 732 890 500 – 0
E: office@ekey.net

Contents

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.

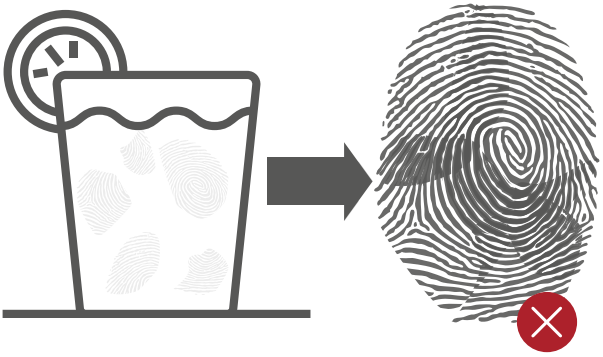
Thus, a reconstruction of the original fingerprint is impossible.

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.

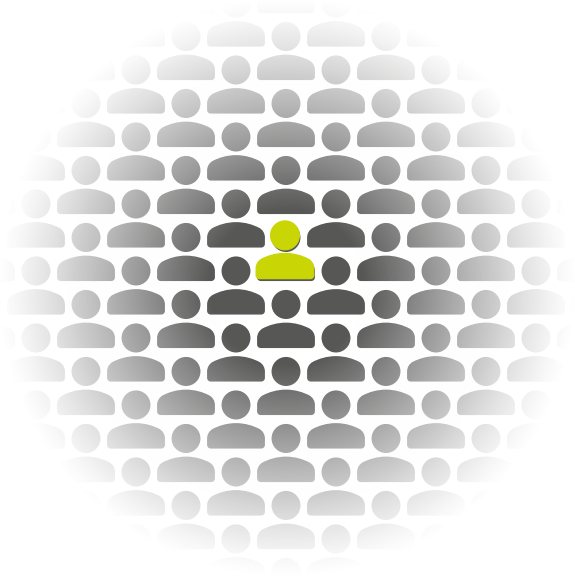
Conclusion: possible in theory, hardly likely in practice.



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 unikely. 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.

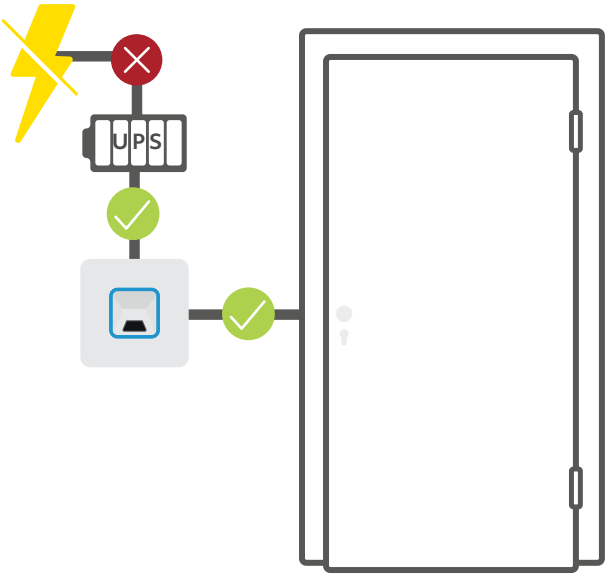


How do you open the door in the event of a power failure?

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.

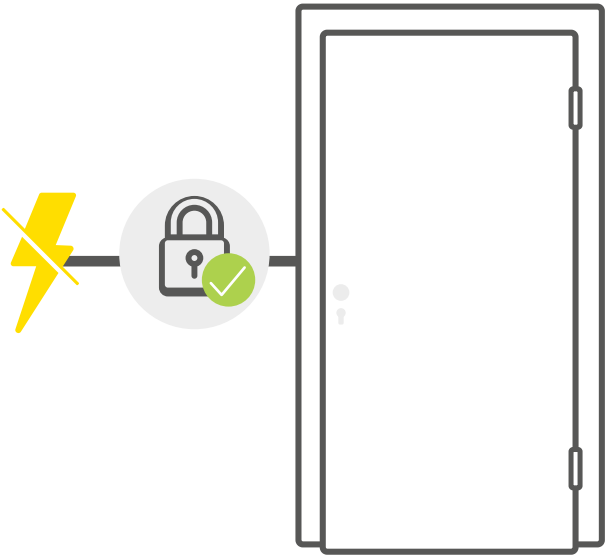
And even if the connection to the Internet or the router fails, the door can still be opened.



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.



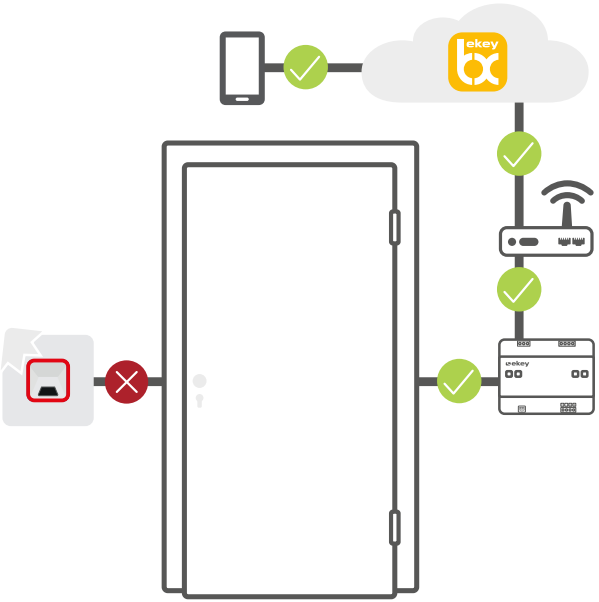
Can the ekey fingerprint scanner access solution be manipulated from the outside so that the door opens?

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.



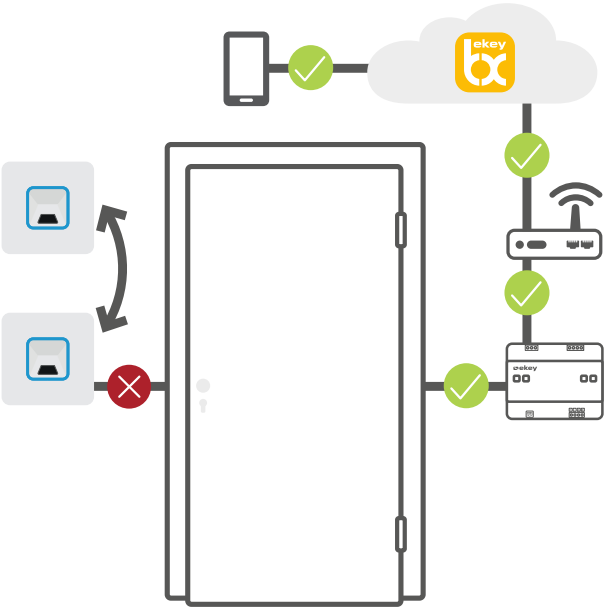
Can the system be manipulated by swapping the fingerprint scanner?

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.



Is the system connected to the Internet?

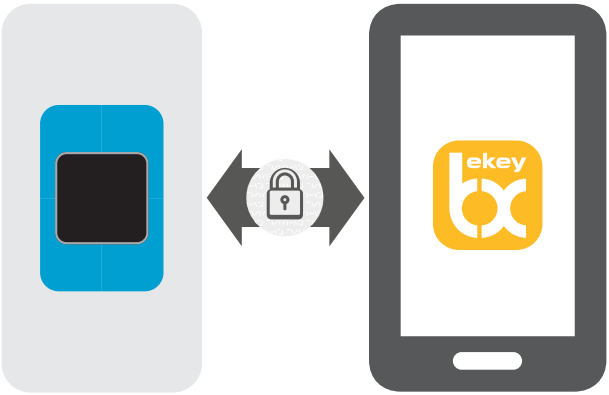
No. The devices communicate over the Internet exclusively with the ekey bionyx cloud, which is operated via the cloud computing world market leader **MS Azure**. The data is encrypted at all times and cannot be viewed by either ekey or Microsoft.

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.



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.

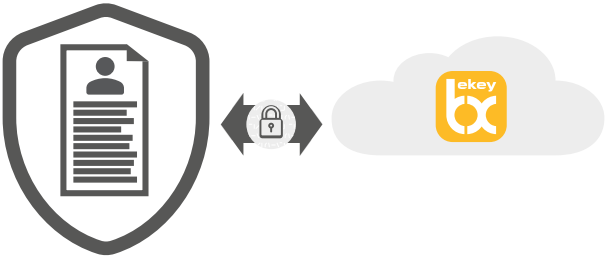
2. Security: The business model of large cloud providers is based on keeping data safe. Therefore, both the data centers themselves are extremely well protected (e. g. premises, surveillance, fire protection, etc.) and the virtual protection against cybercrime is at a correspondingly high level.

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.

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.



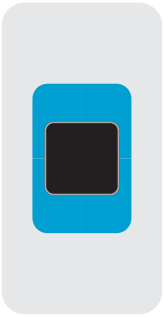
What happens if I lose my smartphone/tablet?

Unlike a key, the finder of the smartphone does not have access to the system: the smartphone oder 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.

Are fingerprint scanner activities logged?

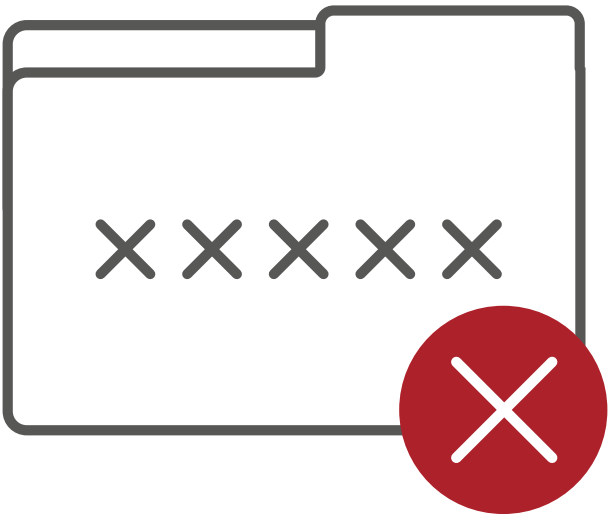
By default, activities are stored in the access log for seven days. The access log can be viewed and deleted or deactivated by authorized administrators.



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

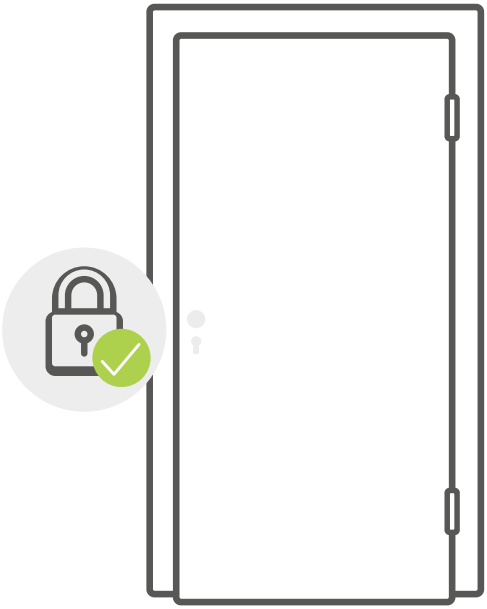
Are hidden access authorizations for the manufacturer stored in the system?

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.



YOUR FINGER. YOUR KEY.

Designed, developed and made in Austria.

Austria (headquarters)

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

Germany

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

Switzerland & Liechtenstein

ekey biometric systems Schweiz AG
Schaanerstrasse 13
FL-9490 Vaduz
T: +41 71 560 54 80
E: office@ekey.ch

Adriatic East region

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

Italy

ekey biometric systems Srl.
Via Perathoner 31
I-39100 Bolzano
T: +39 0471 922 712
E: italia@ekey.net

www.ekey.net

850689/050923