YOUR FINGER. YOUR KEY.

How secure is an ekey **fingerprint access solution?**

Answers

to frequently asked questions

SECURITY of ekey fingerprint access solutions

ekey products guarantee the very highest standard of security against misuse and unauthorized access to the access control system.

During the development, design, and production of its products, ekey has considered the following recommendations and guidelines:

- Recommendations of the German Federal Office for Information Security, www.bsi.bund.de
- Recommendations of the VdS Schadenverhütung GmbH (German-based institution for corporate security) on access control systems, www.vds.de

PARTNERS & COLLABORATIONS

SSG Schweizerische Sicherheitsgruppe

öis.at netzwerk sicherheit

KEINBRUCH

interkey

Are you interested in an ekey fingerprint access solution?

At ekey, we have been developing fingerprint access solutions for unrivaled convenience and maximum security in businesses and homes since 2002. Our technology is used successfully in all kinds of fields and is constantly being developed and adapted for use in new applications. This high level of long-term commitment makes us Europe's market leader and demands top quality day in, day out.

We want this quality standard to be reflected in the information we provide as well, so we have compiled this brochure containing answers to the most important and most frequently asked questions.

If you have any questions about our quality products which are not included in the brochure, please contact us on:

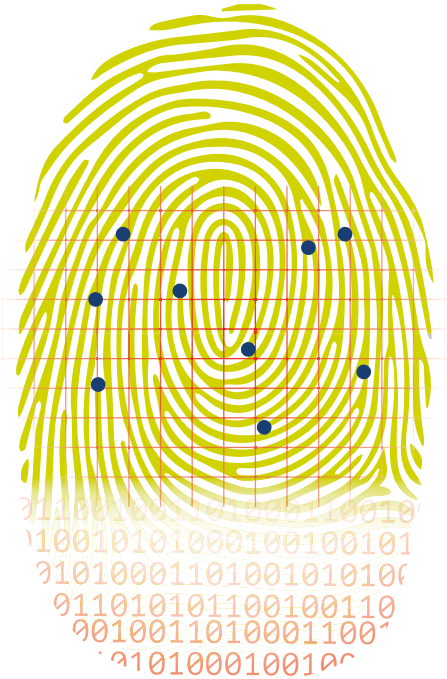
P: +43 732 890 500 - 0
E: office@ekey.net

When it comes to quality
We are the only manufacturer in the industry that produces its products in Europe/Austria. This is ultimately a benefit for you, as we offer a 5-YEAR QUALITY GUARANTEE on all our products! Find out more on page 18.

Take a look for yourself – we guarantee you'll be impressed!

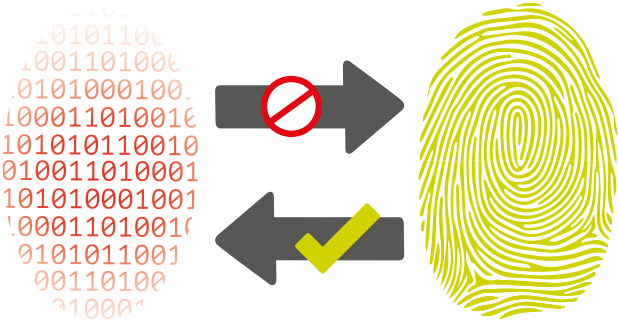
Will my fingerprints be stored in the ekey finger scanner?

No. ekey does not store any fingerprints. The biometric features of the original fingerprint, such as unique points, line ends, forks in the lines, etc. are used to produce a pattern (template). This template is converted into a unique binary number code by means of an algorithm developed in house. It is then stored and used each time for comparison.



Can an original fingerprint be reconstructed from the stored data?

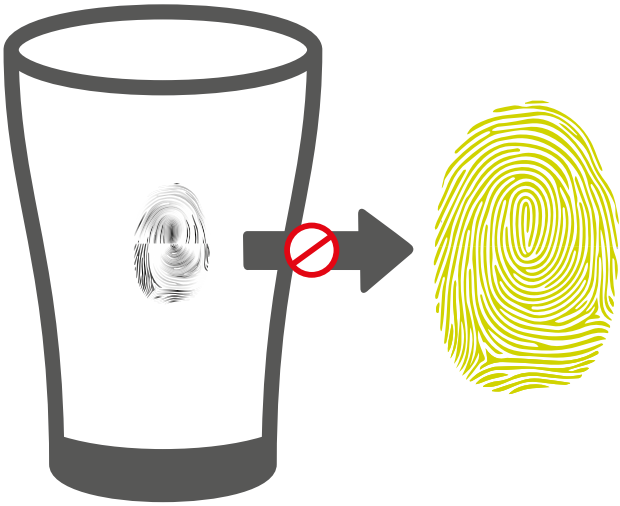
No. The stored number code cannot be converted back into a fingerprint. It is therefore impossible to reconstruct the original fingerprint.



Is it possible to take a fingerprint from a glass, for example, and use it to make a fake finger to open a door?

Creating a usable fingerprint is virtually impossible and would involve an enormous amount of work. With enough criminal efforts, plus expert knowledge and the ideal laboratory conditions, the features could be transferred to a fake finger.

So it is possible in theory, but is extremely unlikely in practice.



What is „live finger detection“?

ekey finger scanners use RF sensor technology (radio waves) to check the nature of the skin in order to differentiate between living and dead tissue. The ekey finger scanner must recognize the tissue as „live“ before a data comparison is carried out. It is therefore not possible to dupe the finger scanner with a photo or a fingerprint left on an object.

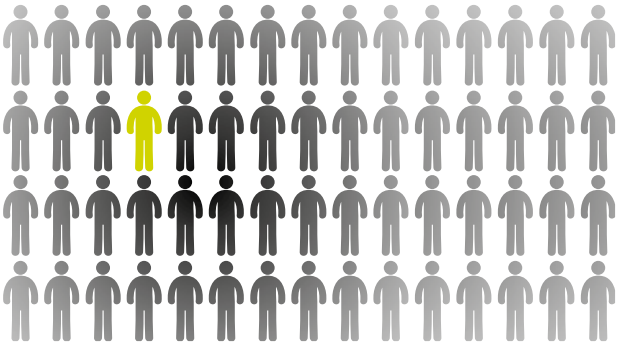
How likely is it that the door will open for an unauthorized person?

Do you know the false acceptance rate? This rate describes the likelihood of a security system granting access to someone who does not have authorization. For ekey finger scanners, this rate is 1 : 10 million – provided that the fingerprints were enrolled correctly.

By way of comparison: our finger scanners are 1,000 times more secure than the 4-digit PIN code for your bank card. If, on the other hand, you take the fingerprint sensor on your smartphone, the false acceptance rate is surprisingly high. To be precise, it is over 200 times higher than that of an ekey finger scanner.

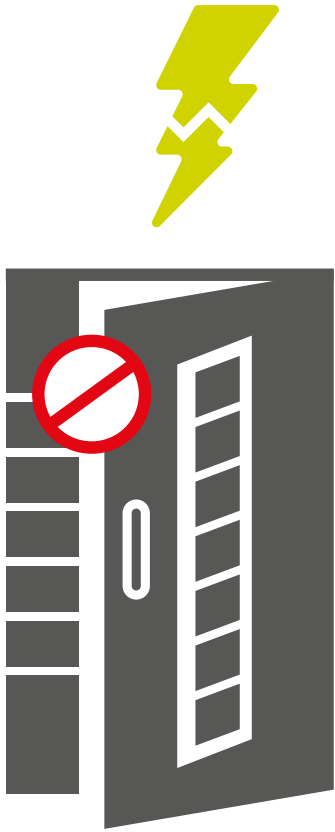
In summary, it is theoretically possible for an unauthorized person to gain access using an ekey finger scanner, but it is extremely unlikely.

The odds of having 6 numbers come up (out of 45) on the lottery are 1 : 8,145,000 – much higher than the chances of an unauthorized person gaining access using the scanner.



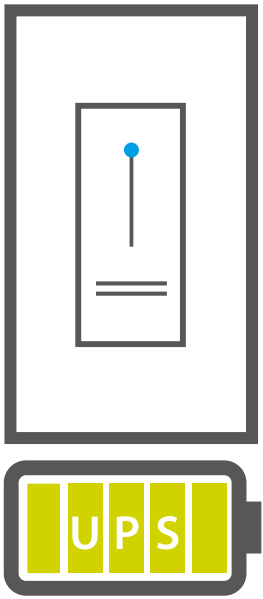
Can a door open itself when there is a power failure?

No. Power failures will not trigger an impulse to open the door on an ekey fingerprint access solution. This opening impulse can only be triggered by an authorized and – as we already know – live finger.



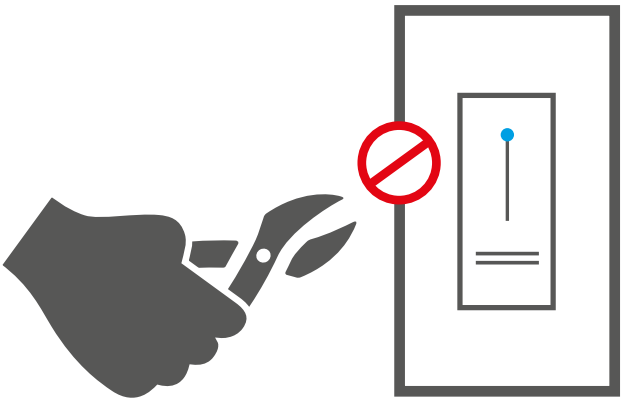
The power is out: how can I open my door?

For dark moments like this, we offer a UPS – uninterruptible power supply – for our access solutions. This will supply power to the finger scanner, control panel, and motorized lock for several hours. Alternatively, of course, you can also use a key.



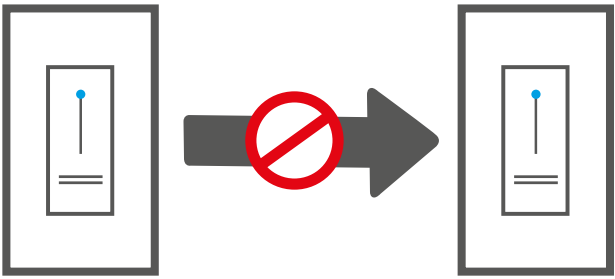
Can the ekey fingerprint access solution be tampered with from outside in order to open the door?

No. The system cannot be tampered with from outside. Nor can it be influenced by force, because the finger scanner and control panel are physically separate. The opening impulse is emitted from the control panel in the protected interior area. Incidentally, the system cannot be tampered with via the Internet either, because it does not have an Internet connection.



Can the system be tampered with by replacing the finger scanner?

The finger scanner and control panel are „coupled“ together during the commissioning process and their communication is encrypted. The user data that is entered is stored with the serial number of the device and therefore cannot be transferred to another device. If the devices are replaced, the control panel and finger scanner must be reset to the default settings and „re-coupled“. This requires access to the protected interior area where the control panel is located. In addition, all of the user data must be re-entered.



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

To establish the connection between the smartphone/tablet, finger scanner and control panel, we use the „Bluetooth Secure Simple Pairing“ process. All data is encrypted before being transferred between the devices.

What happens if I lose my smartphone/tablet?

When the app is opened, a security code of between 4 and 6 digits must be entered. This means that the app cannot be started by an unauthorized person.

If you lose your smartphone/tablet, you can use a different smartphone/tablet to restore the connection to the finger scanner using the *ekey home app* and the configured admin coupling code.

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

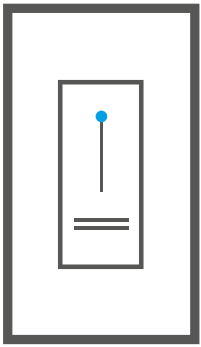
No. There is no option (factory code, etc.) for the door to be opened by an engineer stored in the system. The owner (who is also the administrator) is the only person who can reset the system to the default settings using the 6-digit administrator code that he himself has set.

Is a fingerprint access solution covered by insurance?

For the insurance coverage, it does not matter whether the locking mechanism is actuated mechanically using a key or electronically via a fingerprint. The insurance coverage is only in place if the access point is locked correctly. If a door is merely „on the latch“, it does not count as locked.

Are all activities logged on the finger scanner?

The *ekey home single-point access solution* system does not have an access log. For the *ekey multi* and *ekey net* access solutions, ekey offers an access log for each finger scanner which only the administrator can read. Access attempts made by unauthorized persons are also logged.



06:13	Entance	User 003
07:23	Warehouse	User 002
08:20	Garage	User 005
09:05	Office 2	User 005
09:13	Office 3	User 006
09:30	Garage	User 003
09:35	Office 5	User 003
10:13	Warehouse	User 003
10:25	Garage	User 001
12:28	Entance	User 002
15:53	Garage	User 002
16:09	Garage	User 003

5-YEAR QUALITY GUARANTEE

This extended quality guarantee is an additional service provided voluntarily, as we are confident that ekey products are fit for the future. Our high-quality components and extensive production, manufacturing, and functional testing stand for quality, functionality, durability, and security, and guarantee that you have purchased the best product on the market.

3 + 2 = 5-YEAR QUALITY GUARANTEE!

We are confident of our quality, which is why you have the option of extending this 3-year ekey QUALITY GUARANTEE by an additional 2 years.

What do you need to do?
Register your ekey product online at **www.ekey.net/en/guarantee** within 4 weeks of purchase and then take advantage of the full ekey 5-YEAR QUALITY GUARANTEE!

EXPLANATION OF TERMS

Fake finger
A reconstruction, imitation, or falsification of a finger.

Leaving the door „on the latch“
The latch is the part of the lock which holds the door in the door frame.

Template
A sample (reference data) in electronic data processing.

UPS
An uninterruptible power supply is used to ensure the supply can continue in the event of power failures. It is integrated into the power supply line of the systems or devices to be protected.

„Coupling“
Two elements are connected/coupled by the system so they can communicate with each other.

802732 / 1706

Austria (headquarters)
ekey biometric systems GmbH
Lunzerstraße 89
A-4030 Linz
P: +43 732 890 500 - 0
E: office@ekey.net

Made in Austria

www.ekey.net