ekey
YOUR FINGER. YOUR KEY.

# Wie sicher ist eine ekey Fingerprint-Zutrittslösung?

Antworten auf die meistgestellten Fragen

## Über ekey

ekey startete im Jahr 2002 und ist heute Europas Nr. 1 bei Fingerprint-Zutrittslösungen. Schlüssel, Karten und Codes können verloren, vergessen oder gestohlen werden: Der Finger ist hingegen immer dabei!

Seit 20 Jahren entwickelt ekey Zutrittslösungen für private Haushalte, Unternehmen und Organisationen. Was als Forschungsprojekt begann, ist heute einer der führenden Hersteller von biometrischer Zutrittskontrolle: Das österreichische Familienunternehmen ist mittlerweile europäischer Marktführer bei Fingerprint-Zutrittslösungen.

## Qualität „Made in Austria"

Bevor ein ekey-Produkt auf den Markt darf, muss es sich einem strengen Härtetest unterziehen: intensive Simulationen von glühender Hitze und klirrender Kälte bis hin zu hoher Luftfeuchtigkeit. Diese Tests müssen jeder Fingerprint sowie sämtliche seiner Bauteile unzählige Male erfolgreich abschließen, bevor das Produkt schließlich seinen Weg in Ihre Hände findet.


## Komfort trifft Sicherheit

Fingerprint-Zutrittssysteme von ekey bereichern den Alltag mit dem Komfort von schlüssellosem Zugang sowie Flexibilität und smarten Features. Dabei steht die Sicherheit stets im Zentrum.

Wie sicher ist also ein ekey Fingerprint-System? Auf den nächsten Seiten finden Sie Antworten auf die häufigsten Fragen.

Sollten Sie darüber hinaus weitere Fragen haben, wenden Sie sich gerne an:

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

## Inhalt

## Werden Fingerabdrücke gespeichert?

**Nein.** ekey speichert keine Fingerbilder.

Aus den biometrischen Merkmalen des originalen Fingerabdrucks, wie den einzigartigen Punkten, Linienendungen und Gabelungen, wird ein Muster erstellt – das sogenannte Template.

Dieses wird durch den eigens entwickelten und patentierten Software-Algorithmus in einen eindeutigen binären Zahlencode umgewandelt, abgespeichert und jedes Mal zum Vergleich herangezogen.

Die Templates werden verschlüsselt in der ekey bionyx Cloud abgelegt.

Der Schlüssel dazu befindet sich ausschließlich am jeweils eigenen Endgerät (Smartphone/Tablet), somit sind die Daten vor Fremdzugriff geschützt. Die Sicherheit lässt sich mit jener einer Netbanking-App vergleichen.

## Kann aus den gespeicherten Daten ein originaler Fingerabdruck rekonstruiert werden?

**Nein,** das abgelegte Template (siehe „Werden Fingerabdrücke gespeichert?“) kann nicht mehr zurück in ein Fingerbild umgewandelt werden.

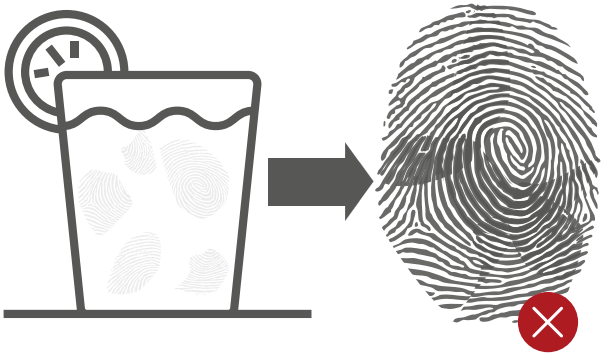
Somit ist eine Rekonstruktion des originalen Fingerabdrucks ausgeschlossen.

**Ist es möglich, von einem hinterlassenen Fingerabdruck (z. B. auf einem Glas) einen brauchbaren Fake-Finger zum Öffnen einer Tür herzustellen?**

ekey setzt auf mehrfache Absicherung gegen Manipulation durch Fake-Finger: Einerseits wird direkt beim Auflegen des Fingers auf den Sensor durch die Leitfähigkeit der lebenden Haut und andererseits bei der algorithmischen Auswertung der Daten geprüft, ob die biometrischen Merkmale von einem Finger eines tatsächlichen Menschen stammen.

Zudem ist es nahezu unmöglich, einen brauchbaren Fake-Fingerabdruck herzustellen. Mit viel krimineller Energie, noch mehr Expertenwissen sowie besten Laborbedingungen könnten die Merkmale auf einen Fake-Finger übertragen werden.

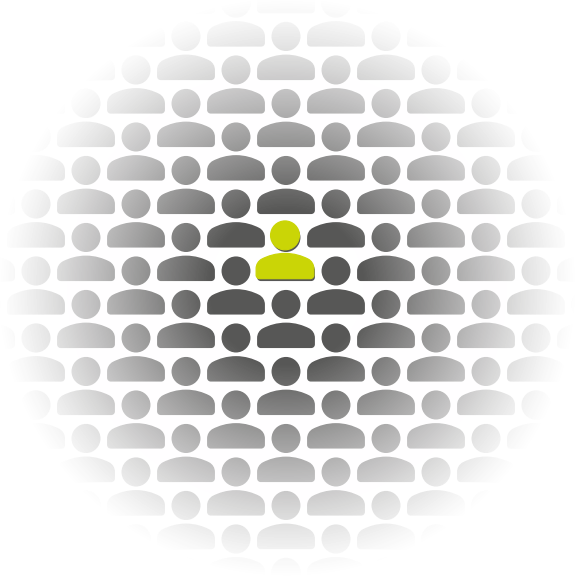
Fazit: In der Theorie möglich, praktisch wohl kaum.



## Wie hoch ist die Wahrscheinlichkeit, dass sich die Tür bei einer nicht berechtigten Person öffnet?

Hierfür gibt es einen speziellen Indikator – die Falschakzeptanzrate (FAR). Diese beschreibt die Wahrscheinlichkeit, mit der eine Person Zutritt bei einem Sicherheitssystem erhält, obwohl sie keine Berechtigung hat. Bei ekey Fingerprints liegt diese bei 1:10 Millionen – vorausgesetzt, die Fingerbilder wurden richtig aufgenommen.

Zusammengefasst: Dass bei ekey Fingerprints eine unberechtigte Person Zutritt erhält, ist theoretisch möglich, aber höchst unwahrscheinlich. Im Vergleich zum vierstelligen Zahlencode einer Bankomatkarte ist ein ekey-System 1.000-mal sicherer. Und auch die Wahrscheinlichkeit, mit einem Tipp einen Lotto-Sechser (6 aus 45) zu landen, liegt mit 1:8.145.000 deutlich höher, als dass eine unberechtigte Person Zutritt erhält.

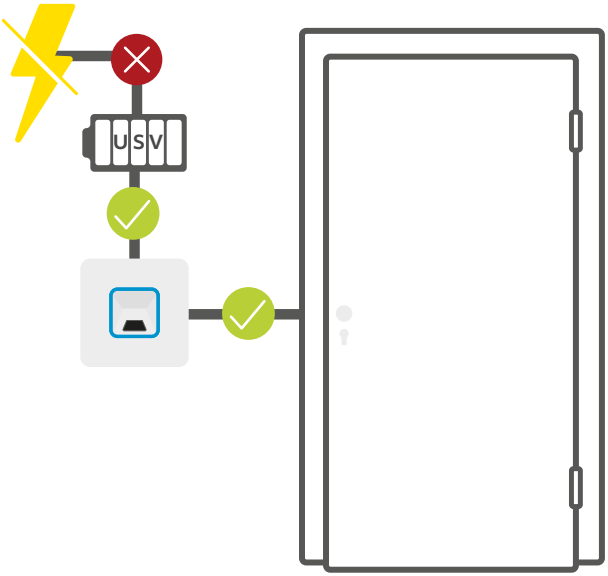


## Wie lässt sich die Tür bei einem Stromausfall öffnen?

Wenn der Strom, das Internet oder der Router ausfallen, steht niemand vor verschlossener Tür. ekey bietet für seine Zutrittssysteme eine Unterbrechungsfreie Stromversorgung (USV) an.

Diese hält Fingerprint, Steuereinheit und Motorschloss für mehrere Stunden in Betrieb. Alternativ kann natürlich jederzeit ein Schlüssel verwendet werden.

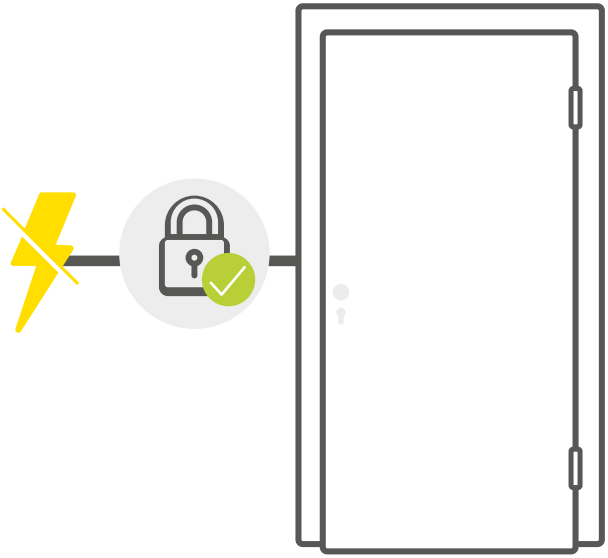
Und auch wenn die Verbindung zum Internet bzw. dem Router einmal ausfällt, ist eine Öffnung der Tür möglich.



## Kann sich eine Tür bei einem Stromausfall selbstständig öffnen?

**Nein.** Spannungsausfälle können bei einer ekey Fingerprint-Zutrittslösung keinen Impuls auslösen, der die Tür öffnet.

Nur ein berechtigter Nutzer kann diesen Öffnungsbefehl geben.



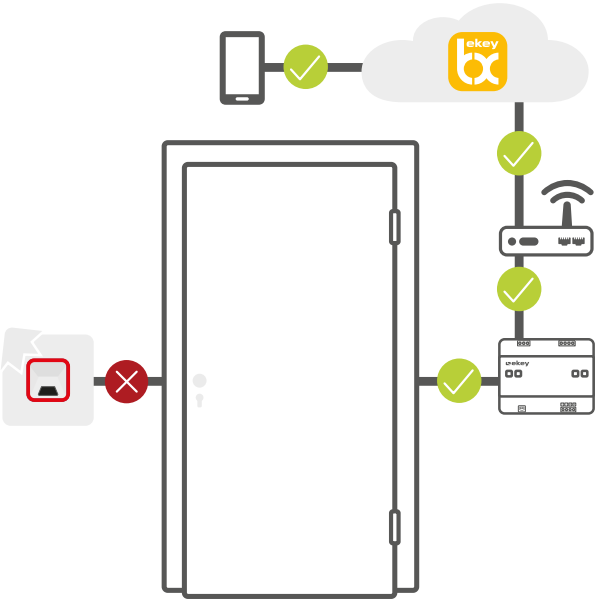
## Kann die ekey Fingerprint-Zutrittslösung von außen manipuliert werden, damit sich die Tür öffnet?

**Nein.** Das System kann nicht von außen manipuliert werden. Auch nicht durch Gewalteinwirkung, denn Fingerprint und Steuereinheit sind räumlich getrennt.

Der Öffnungsimpuls geht von der Steuereinheit im geschützten Innenbereich aus.

Auch die Daten sind zu jeder Zeit mehrfach verschlüsselt und abgesichert.

Die Datenübertragung im ekey bionyx System erfolgt Ende-zu-Ende-verschlüsselt. Sämtliche Daten werden über alle Übertragungsstationen hinweg verschlüsselt übertragen.



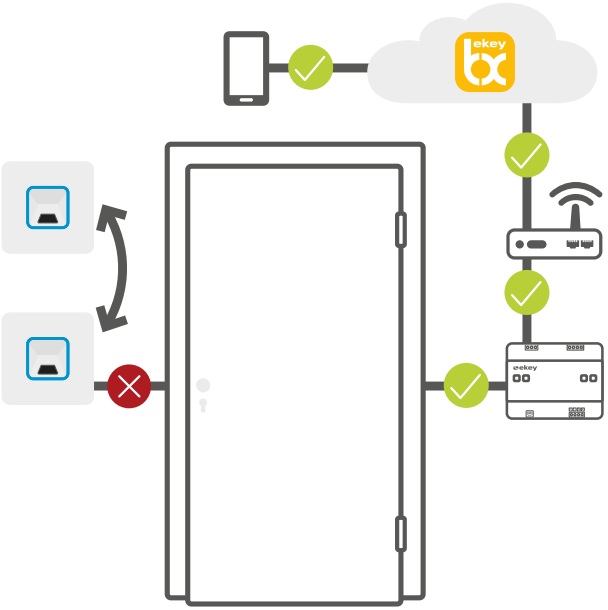
## Kann das System durch den Tausch des Fingerprints manipuliert werden?

**Nein,** mit einem Tausch des Fingerprints kann das System nicht manipuliert werden.

Denn Fingerprint und Steuereinheit werden bei der Inbetriebnahme „verheiratet" und kommunizieren verschlüsselt. Die angelegten Benutzerdaten werden mit der Seriennummer des Geräts abgespeichert. Kommt es zu einem Tausch des Fingerprints oder zu einer Systemerweiterung, muss dies in der ekey bionyx App durch einen Administrator verifiziert werden.

So bleiben die gespeicherten Finger erhalten und müssen nicht erneut eingespeichert werden.

Ohne diesen Prozess lassen sich hinterlegte Daten nicht auf ein anderes Gerät übertragen.



## Hängt das System im Internet?

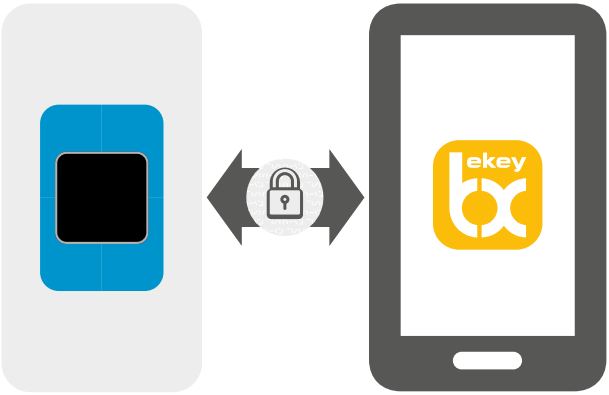
**Nein.** Die Geräte kommunizieren über das Medium Internet ausschließlich mit der ekey bionyx Cloud. Diese wird über den Cloud-Computing-Weltmarktführer MS Azure betrieben. Die Daten sind zu jeder Zeit verschlüsselt und weder von ekey noch von Microsoft einsehbar.

Aufgrund des hohen Sicherheitsstandards können nur verschlüsselte WLAN-Netzwerke verwendet werden.

## Wie sicher ist die Verbindung zwischen Smartphone/Tablet, Fingerprint und Steuereinheit?

Für den initialen Verbindungaufbau zwischen Smartphone/Tablet, Fingerprint und Controller kommt das sichere Protokoll „Transport Layer Security“ zum Einsatz. Dabei werden die Daten zwischen den Geräten ausschließlich verschlüsselt übertragen.

Die Datenübertragung in der ekey bionyx App erfolgt nach Ende-zu-Ende-Verschlüsselung. Sämtliche Daten werden über alle Übertragungsstationen hinweg verschlüsselt übertragen. Die gesendeten Daten können weder von Angreifern noch von ekey selbst gelesen oder erzeugt werden.



## Warum setzt ekey auf eine Cloud-Lösung?

Ein Zutrittssystem umfasst neben dem tatsächlichen Gerät – der Hardware – immer auch die entsprechende Software – von Rechen- und Speicherkapazitäten bis zur eigentlichen Software. ekey hat sich mit der ekey bionyx Cloud dazu entschieden, cloudbasierte Technologie einzusetzen, weil damit softwareseitig (ekey bionyx App) zahlreiche Vorteile verbunden sind:

**1. Datenschutz:** Führende Anbieter von cloudbasierten Lösungen betreiben großen finanziellen und personellen Aufwand, um die Daten ihrer Kunden zu schützen. Deshalb ist eine solche Lösung in dieser Hinsicht meist professioneller aufgestellt als eine hauseigene Lösung.

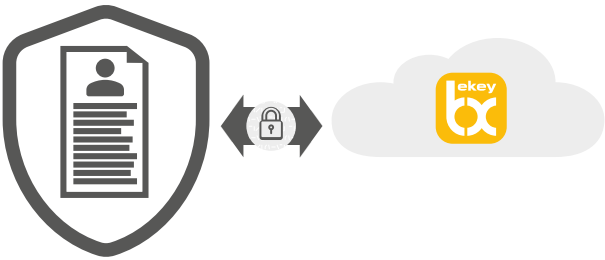
**2. Sicherheit:** Das Geschäftsmodell großer Cloud-Anbieter basiert darauf, dass Daten sicher verwahrt werden. Daher sind sowohl die Rechenzentren an sich bestens geschützt (z. B. Gelände, Überwachung, Brandschutz usw.) als auch der virtuelle Schutz vor Cyberkriminalität auf entsprechend hohem Niveau.

**3. Erreichbarkeit:** Durch Software-Level-Agreements kann eine Software-Verfügbarkeit von rund 99 % gewährleistet werden (fehlendes 1 % sind meist geplante Ausfallzeiten für Updates). Mit einem eigenen Server ist eine vergleichbar hohe Verfügbarkeit nicht möglich.

**4. Updates:** Eine Software muss stets aktuell gehalten werden, um höchste Sicherheit zu bieten. Cloudbasierte Zutrittssysteme sind immer aktuell, Updates erfolgen automatisch.

## Was passiert mit den persönlichen Daten?

Die Vision von ekey ist es, Biometrie für alle zu ermöglichen. Das damit verbundene Ziel ist, den Alltag so sicher, flexibel und komfortabel wie möglich zu gestalten sowie praktischen Nutzen zu stiften. ekey will so das Leben verbessern, nicht in die Privatsphäre eindringen. Daher ist das Geschäftsmodell so gestaltet, dass die Produkte und Services niemals im Austausch für personenbezogene Daten stehen und diese daher weder von ekey selbst genutzt noch an Dritte verkauft werden.



## Was passiert, wenn ich mein Smartphone/ Tablet verliere?

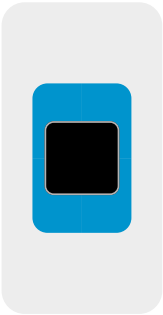
Im Gegensatz zu einem Schlüssel hat der Finder des Smartphones keinen Zugriff auf das System:

Smartphone oder Tablet sowie die ekey bionyx App werden separat entsperrt – ersteres durch den individuell eingestellten Zugang über Biometrie (Fingerabdruck oder Gesichtserkennung) oder Code, zweiteres über Biometrie oder den Benutzernamen mit persönlichem Passwort. Die App ist damit vor unberechtigten Zugriffen geschützt. Im Falle des Verlusts von Smartphone oder Tablet kann über ein neues Gerät sowie einen Backup-Code die Verbindung zur ekey bionyx Cloud wiederhergestellt werden.

Also, auch wenn das mobile Endgerät verloren geht, ist eine Anmeldung über ein neues Gerät mit den Zugangsdaten möglich.

## Werden Aktivitäten am Fingerprint protokolliert?

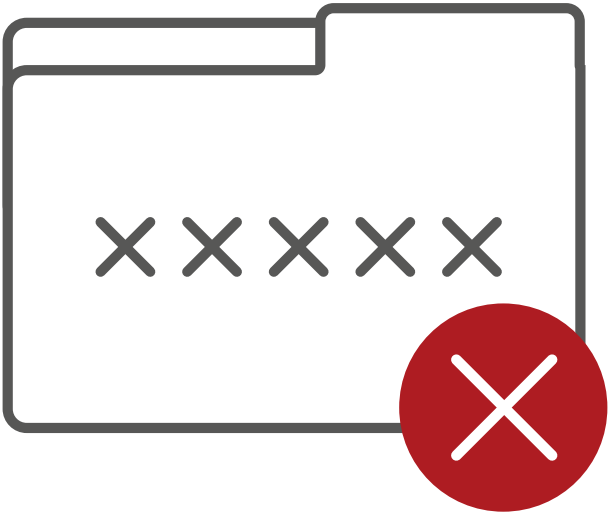
Im Standard werden Aktivitäten im Zutrittsprotokoll für sieben Tage gespeichert. Es kann durch berechtigte Administratoren angesehen und gelöscht bzw. deaktiviert werden.



| | | |
|---|---|---|
| 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 |

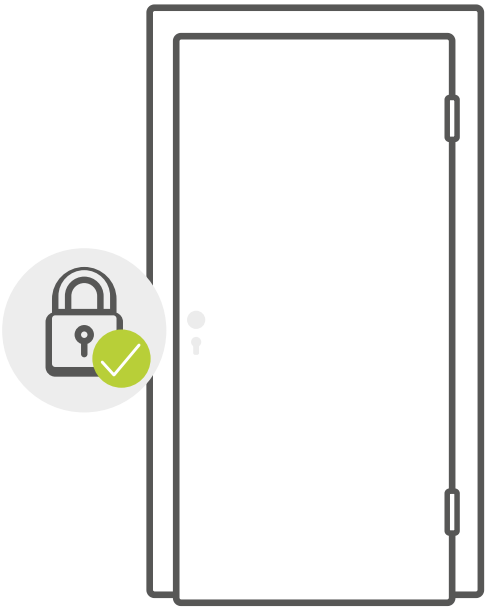
## Sind versteckte Zutrittsberechtigungen für den Hersteller im System hinterlegt?

**Nein.** ekey hat keine Möglichkeit (Werkscode etc.) für die Öffnung durch einen Techniker im System hinterlegt. Nur ein berechtigter Administrator hat die Möglichkeit, mit seinem Smartphone oder Tablet in Kombination mit seinen Kontozugangsdaten (E-Mail, Passwort) Änderungen vorzunehmen.



## Besteht mit einer Fingerprint-Zutrittslösung Versicherungsschutz?

Für den Versicherungsschutz ist es nicht relevant, ob die Verriegelung mechanisch per Schlüssel oder elektronisch per Fingerprint ausgelöst wird. Grundsätzlich besteht nur dann Versicherungsschutz, wenn der Zugang ordnungsgemäß verriegelt ist. Fällt eine Tür nur „in die Falle" – jenen Teil des Schlosses, der die Tür im Anschlag im Türrahmen hält –, gilt sie nicht als verriegelt.



YOUR FINGER. YOUR KEY.

Designed, developed
and made in Austria.


**Österreich (Zentrale)**

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

**Deutschland**

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

**Schweiz & Liechtenstein**

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

**Region Adria Ost**

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

**Italien**

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


**www.ekey.net**



802700/070922