YOUR FINGER. YOUR KEY.

Wie sicher ist eine ekey-**Fingerprint-Zutrittslösung?**

Antworten

auf die meistgestellten Fragen

SICHERHEIT von ekey Fingerprint-Zutrittslösungen

ekey garantiert höchsten Standard bei der Sicherheit seiner Produkte gegen missbräuchliche Verwendung und unberechtigten Zugriff auf das Zutrittssystem.

ekey hat bei der Entwicklung, Konstruktion und Fertigung der Produkte folgende Empfehlungen und Richtlinien berücksichtigt:

- Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik www.bsi.bund.de
- Empfehlungen der VdS Schadenverhütung GmbH (Vertrauen durch Sicherheit) zu Zutrittskontrollanlagen www.vds.de

PARTNER & KOOPERATIONEN

KEINBRUCH

interkey

SSG Schweizerische Sicherheitsgruppe

YOUR FINGER. YOUR KEY.

Sie interessieren sich für eine ekey-Fingerprint-Zutrittslösung?

Wir bei ekey entwickeln seit 2002 Fingerprint-Zutrittslösungen für einzigartigen Komfort mit höchster Sicherheit in Unternehmen und Zuhause. Unsere Technologie wird in den verschiedensten Anwendungsbereichen erfolgreich eingesetzt und für neue Einsatzgebiete ständig weiterentwickelt. Dieses jahrelange intensive Engagement macht uns zu Europas Marktführer und verlangt tagtäglich nach höchster Qualität.

Um unseren Qualitätsanspruch auch in puncto Information zu erfüllen, haben wir für Sie diese Broschüre mit den wichtigsten und meistgestellten Fragen sowie den dazugehörigen Antworten zusammengestellt.

Sollten Sie darüber hinaus weitere Fragen zu unseren Qualitätsprodukten haben, erreichen Sie uns unter:

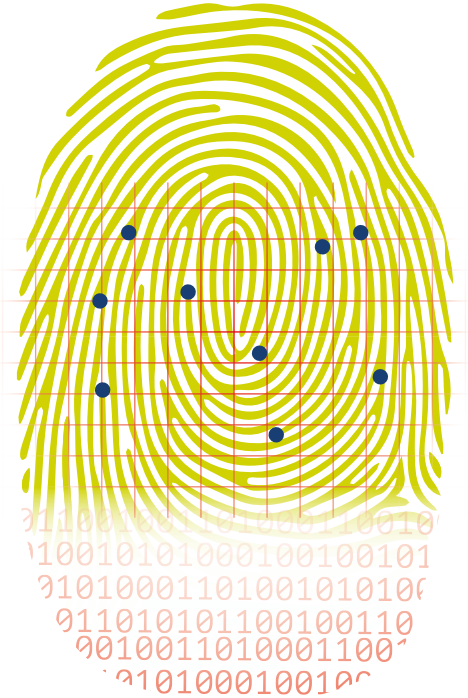
T: +43 732 890 500 - 0
E: office@ekey.net

Apropos Qualität
Wir sind branchenweit der einzige Hersteller und Entwickler, der seine Produkte in Europa/Österreich fertigt. Davon profitieren letztlich Sie: Denn auf alle unsere Erzeugnisse genießen Sie unsere 5 JAHRE QUALITÄTSGARANTIE! Lesen Sie dazu mehr auf Seite 18.

Überzeugen Sie sich selbst – Sie werden begeistert sein!

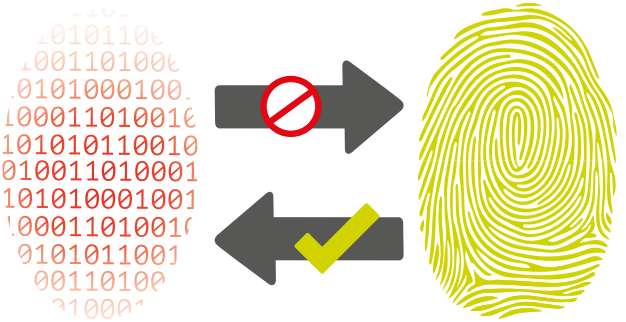
Werden meine Fingerabdrücke im ekey-Fingerprint gespeichert?

Nein. ekey speichert keine Fingerbilder. Aus den biometrischen Merkmalen des originalen Fingerabdrucks, wie einzigartige Punkte, Linienendungen, Gabelungen, etc., wird ein Muster (Template) erstellt. Dieses Muster wird durch den eigens entwickelten und patentierten Software-Algorithmus in einen eindeutigen binären Zahlencode umgewandelt, abgespeichert und jedes Mal zum Vergleich herangezogen.



Kann aus den gespeicherten Daten ein originaler Fingerabdruck rekonstruiert werden?

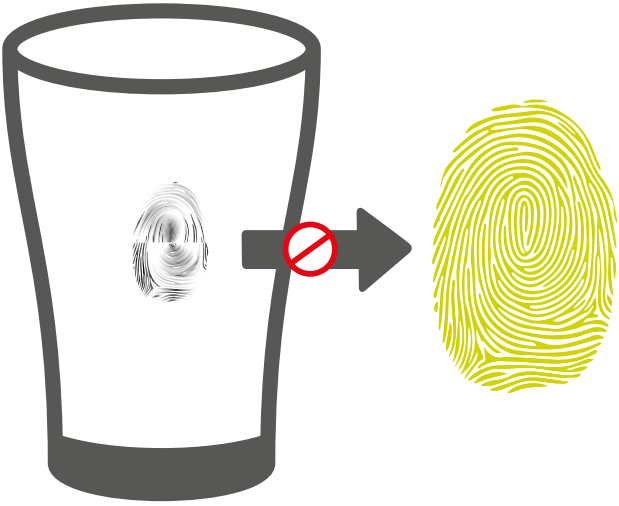
Nein. Der abgelegte Zahlencode kann nicht mehr zurück in ein Fingerbild umgewandelt werden. Somit ist eine Rekonstruktion des originalen Fingerabdrucks ausgeschlossen.



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

Es ist nahezu unmöglich und enorm aufwendig, einen brauchbaren 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.



Nutzen ekey-Systeme Verfahren zur Lebenderkennung?

Ja. Bei der sogenannten „Lebenderkennung“ wird geprüft, ob das angebotene biometrische Merkmal zu einem lebenden Menschen gehört. Bei ekey-Systemen erfolgt dies 2-fach, einerseits direkt beim Auflegen des Fingers durch die Leitfähigkeit der lebenden Haut und andererseits bei der algorithmischen Auswertung der Daten.

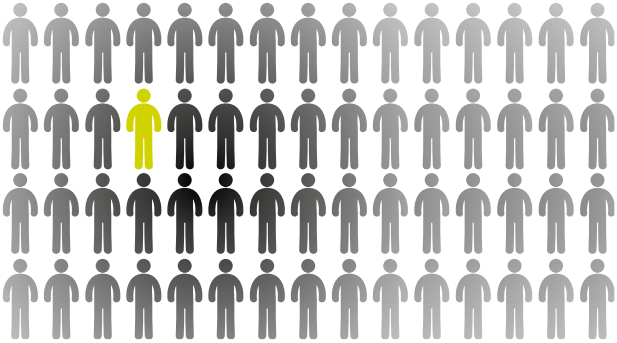
Wie hoch ist die Wahrscheinlichkeit, dass sich die Tür bei einer nicht berechtigten Person öffnet?

Kennen Sie die Falschakzeptanzrate (FAR)? Sie 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.

Zum Vergleich: Unsere Fingerprints sind gegenüber dem 4-stelligen Zahlencode Ihrer Bankomatkarte 1.000 Mal sicherer. Oder denken Sie an Ihr Smartphone mit Fingerprint-Sensor: Hier ist die Falschakzeptanzrate überraschend hoch. Über 200 Mal höher, als bei einem ekey-Fingerprint, um genauer zu sein.

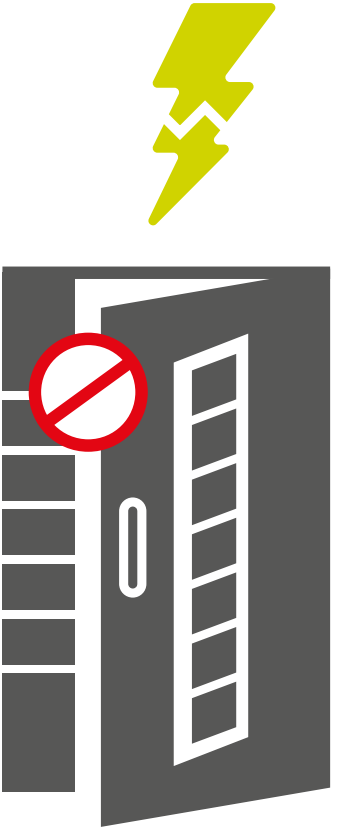
Zusammengefasst: Dass bei ekey-Fingerprints eine unberechtigte Person Zutritt erhält, ist theoretisch möglich, aber höchst unwahrscheinlich.

Die Wahrscheinlichkeit, mit einem Tipp einen Lotto-Sechser (6 aus 45) zu landen, liegt mit 1 : 8.145.000 schon deutlich höher, als dass eine unberechtigte Person Zutritt erhält.



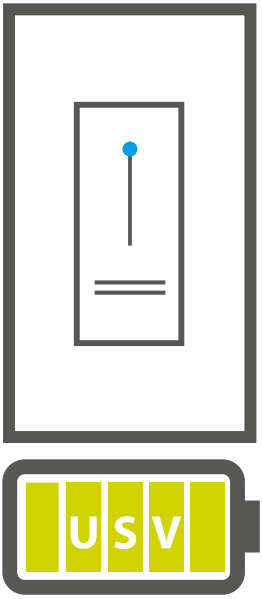
Kann sich eine Tür bei einem Stromausfall selbstständig öffnen?

Nein. Spannungsausfälle können bei einer ekey-Fingerprint-Zutrittslösung keinen Impuls auslösen, der die Tür öffnet. Diesen Öffnungsimpuls kann nur ein berechtigter und – wie wir bereits wissen – lebendiger Finger auslösen.



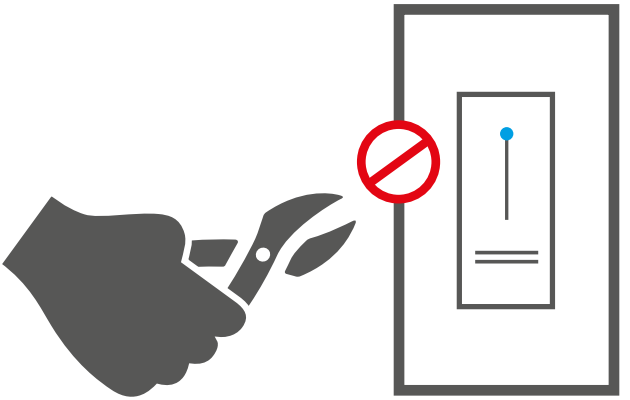
Der Strom ist ausgefallen: Wie kann ich meine Tür öffnen?

Für diesen dunklen Moment bieten wir für unsere Zutrittslösungen eine USV – eine unterbrechungsfreie Stromversorgung – an. Diese hält Fingerprint, Steuereinheit und Motorschloss für mehrere Stunden in Betrieb. Alternativ kann natürlich ein Schlüssel verwendet werden.



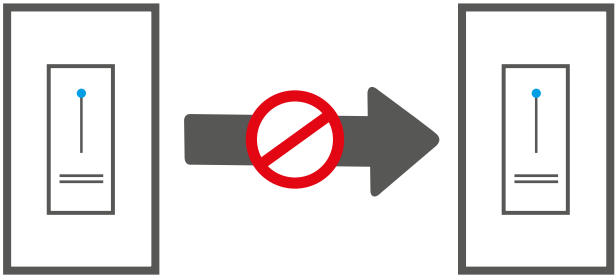
Kann die ekey-Fingerprint-Zutrittslösung von außen manipuliert werden, damit sich die Tür öffnet?

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. Im Übrigen kann das System auch nicht über das Internet manipuliert werden, da es nicht daran angebunden ist.



Kann das System durch den Tausch des Fingerprints manipuliert werden?

Fingerprint und Steuereinheit werden bei der Inbetriebnahme miteinander „verheiratet“ und kommunizieren verschlüsselt. Die angelegten Benutzerdaten werden mit der Seriennummer des Geräts abgespeichert und sind somit auf kein weiteres Gerät übertragbar. Tauscht man die Geräte, müssen Steuereinheit und Fingerprint auf Werkseinstellungen zurückgesetzt und neu „verheiratet“ werden. Dazu braucht man Zugang zum geschützten Innenbereich, wo sich die Steuereinheit befindet. Zudem müssen alle Benutzerdaten neu angelegt werden.



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

Für den Verbindungsaufbau zwischen Smartphone/Tablet, Fingerprint und Steuereinheit verwenden wir das sichere Koppelungsverfahren „Bluetooth Secure Simple Pairing“. Die Daten zwischen den Geräten werden ausschließlich verschlüsselt übertragen.

Was passiert, wenn ich mein Smartphone/Tablet verliere?

Beim Öffnen der App ist ein 4- bis 6-stelliger App-Sicherheitscode erforderlich. Die App kann somit von keiner unberechtigten Person gestartet werden.

Sollte das Smartphone/Tablet verloren gehen, kann man über ein anderes Smartphone bzw. Tablet mit der ekey home App und dem konfigurierten Admin-Kopplungscode die Verbindung zum Fingerprint wieder herstellen.

Sind versteckte Zutrittsberechtigungen für den Hersteller im System hinterlegt?

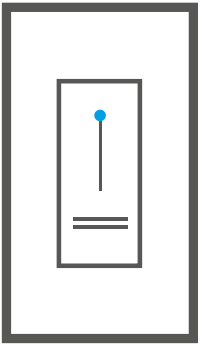
Nein. ekey hat keine Möglichkeit (Werkscode, etc.) für die Öffnung durch einen Techniker im System hinterlegt. Der Eigentümer (gleichzeitig der Administrator) ist die einzige Person, die über einen selbst festgelegten 6-stelligen Administratorcode das System auf Werkseinstellungen zurücksetzen kann.

Besteht Versicherungsschutz mit einer Fingerprint-Zutrittslösung?

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“, gilt das nicht als verriegelt.

Werden alle Aktivitäten am Fingerprint protokolliert?

Beim System ekey home – Einzel-Zutrittslösungen gibt es kein Zutrittsprotokoll. ekey bietet bei den Zutrittslösungen ekey multi und ekey net ein Zutrittsprotokoll über jeden Fingerprint an, das nur der Administrator auslesen kann. Auch Zutrittsversuche unberechtigter Personen werden protokolliert.



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 JAHRE QUALITÄTSGARANTIE

Diese verlängerte Qualitätsgarantie ist eine freiwillige Zusatzleistung, da wir davon überzeugt sind, dass ekey-Produkte für die Zukunft gemacht sind. Unsere hochwertigen Komponenten und umfangreichen Produktions-, Fertigungs- und Funktionskontrollen stehen für Qualität, Funktionalität, Haltbarkeit sowie Sicherheit und geben Ihnen die Garantie, das beste Produkt am Markt erworben zu haben.

3 + 2 = 5 JAHRE QUALITÄTSGARANTIE!

Wir sind von unserer Qualität überzeugt, darum haben Sie die Möglichkeit, diese 3-jährige ekey QUALITÄTSGARANTIE um zusätzlich 2 Jahre zu verlängern.

Was müssen Sie tun?
Registrieren Sie Ihr ekey-Produkt innerhalb von 4 Wochen ab Kaufdatum online unter **www.ekey.net/garantie** und schon genießen Sie die volle ekey 5 JAHRE QUALITÄTSGARANTIE!

BEGRIFFSERKLÄRUNG

Fake-Finger (Deutsch: „gefälschter Finger“)
Eine Rekonstruktion, ein Imitat oder auch eine Fälschung eines Fingers.

Tür „in die Falle/Schlossfalle“ fallen lassen
Die Falle ist jener Teil des Schlosses, der die Tür im Anschlag, im Türrahmen hält.

Template
Eine (Muster-)Vorlage in der elektronischen Datenverarbeitung.

USV
Eine unterbrechungsfreie Stromversorgung wird eingesetzt, um bei Störungen die Stromversorgung sicherzustellen. Sie wird in die Stromzuleitung der zu sichernden Anlagen oder Geräte eingefügt.

„Verheiraten“
Zwei Elemente werden systemtechnisch verbunden/gekoppelt, um in weiterer Folge miteinander zu kommunizieren.

YOUR FINGER. YOUR KEY.

Satz- und Druckfehler vorbehalten.
© ekey biometric systems GmbH - 802700/082020

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 90696 - 0
E: office@ekey.net

Schweiz & Liechtenstein
ekey biometric systems Est.
Landstrasse 79
FL-9490 Vaduz
T: +41 71 560 5480
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.
Via Copernico 13/A
I-39100 Bolzano
T: +39 0471 922712
E: italia@ekey.net

Made in Austria

www.ekey.net

ekey biometric systems