



Quel est le niveau de
sécurité d'une
solution de contrôle d'accès
à empreinte digitale ekey ?



Réponses

aux questions les plus fréquentes

SÉCURITÉ des solutions de contrôle d'accès à empreinte digitale ekey

ekey garantit la sécurité optimale de ses produits contre l'utilisation abusive et l'accès non autorisé au système de contrôle d'accès.

Lors du développement, de la conception et de la fabrication des produits, ekey a tenu compte des recommandations et directives suivantes :

- Recommandations de l'Office fédéral allemand pour la sécurité en matière de technologies de l'information (Bundesamt für Sicherheit und Informationstechnik) www.bsi.bund.de
- Recommandations de la VdS Schadenverhütung GmbH (société renommée allemande s'occupant de la sécurité des entreprises) sur les systèmes de contrôle de l'accès www.vds.de

PARTENARIATS ET COLLABORATIONS



Êtes-vous intéressés par une solution de contrôle d'accès à empreinte digitale ekey ?

Chez ekey, nous développons depuis 2002 des solutions de contrôle d'accès à empreinte digitale qui offrent un maximum de confort et de sécurité aux entreprises et aux particuliers. Notre technologie est employée dans de nombreuses applications et sans cesse perfectionnée pour de nouveaux domaines d'activité. Cet engagement de longue haleine nous a propulsés à la place de leader et exige une qualité irréprochable, chaque jour.

Pour que notre exigence de qualité se reflète également dans nos informations, nous avons élaboré cette brochure contenant les questions les plus fréquentes et leurs réponses.

Pour toute question sur nos produits de qualité, contactez-nous :

T: +43 732 890 500 - 0

E: office@ekey.net

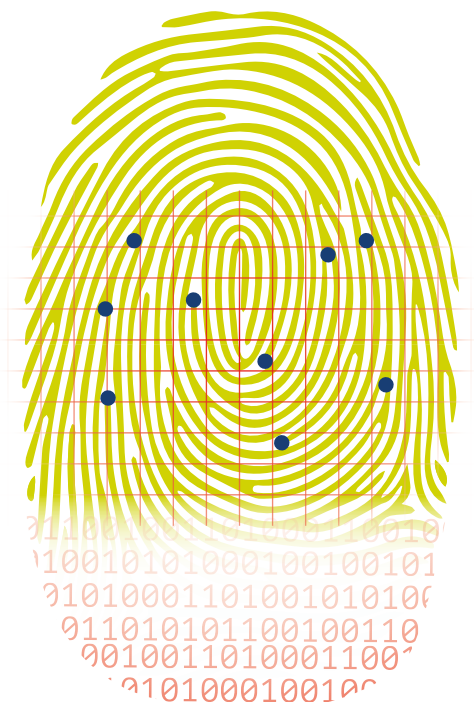
À propos de la qualité

Nous sommes le seul fournisseur du secteur qui fabrique encore ses produits en Europe/Autriche. En fin de compte, c'est vous qui en profitez : tous nos produits sont couverts par notre GARANTIE QUALITÉ DE 5 ANS ! Consultez la page 18 pour en savoir plus.

Découvrez-le par vous-même : vous serez surpris !

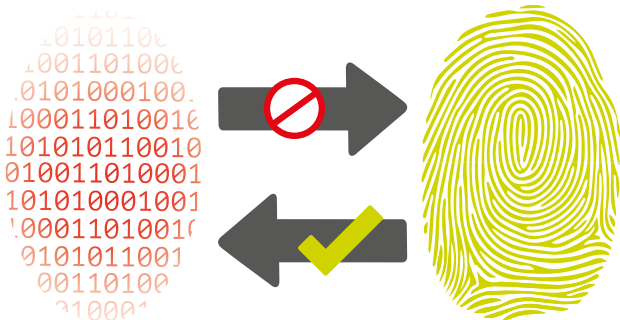
Mes empreintes digitales, sont-elles enregistrées dans le lecteur d'empreinte digitale ekey ?

Non, ekey n'enregistre aucune empreinte digitale. Un modèle (gabarit) est créé à partir des caractéristiques biométriques de l'empreinte digitale originale, comme par ex. les points, les extrémités de ligne et les bifurcations. Ce modèle est converti en un code numérique binaire unique par un algorithme développé en interne, enregistré puis utilisé pour chaque comparaison.



Est-il possible de reconstituer une empreinte digitale originale à partir des données enregistrées ?

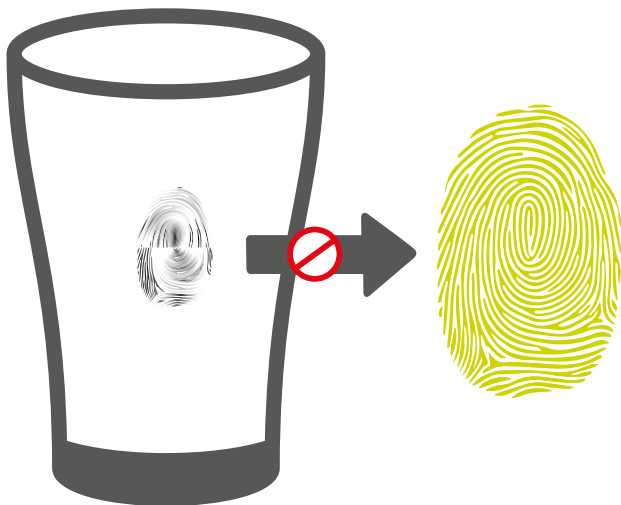
Non. Le code numérique enregistré ne peut pas être reconverti en empreinte digitale. Ceci empêche toute reconstitution de l'empreinte digitale originale.



Est-il possible de créer un doigt factice permettant d'ouvrir la porte à partir d'une empreinte digitale trouvée (par ex. sur un verre) ?

Il est quasiment impossible et extrêmement fastidieux de créer une empreinte digitale exploitable. Les caractéristiques pourraient être transférées sur un doigt factice dans un cadre criminel exigeant des connaissances spécialisées et des conditions de laboratoires optimales.

En résumé : c'est théoriquement possible, mais quasiment impossible en pratique.



Les systèmes ekey utilisent-ils des méthodes de reconnaissance de doigt vivant ?

Oui. Avec la soi-disant « reconnaissance de doigt vivant », il est vérifié si le critère biométrique proposé appartient à une personne vivante. Avec les systèmes ekey, cela se fait deux fois, d'une part directement en posant le doigt, par la conductivité de la peau vivante, et d'autre part lors de l'évaluation algorithmique des données.



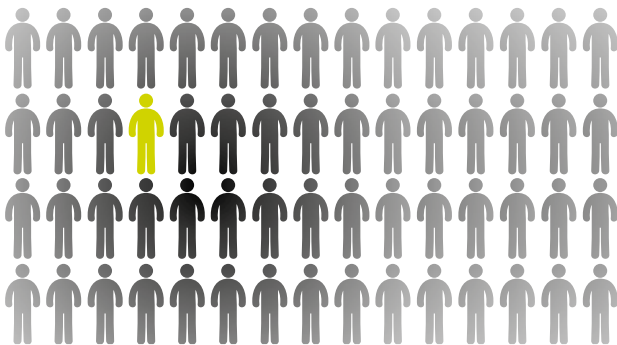
Quelle est la probabilité qu'une porte s'ouvre devant une personne non autorisée ?

Savez-vous ce qu'est le taux de fausses acceptations ? Il correspond à la probabilité qu'une personne obtienne l'accès d'un système de sécurité alors qu'elle n'en a pas l'autorisation. Avec les lecteurs d'empreintes digitales ekey, ce taux est de 1 sur 10 millions, à condition que les traces digitales aient été correctement enregistrées.

Par comparaison : nos lecteurs d'empreintes digitales sont 1.000 fois plus sûrs que le code à quatre chiffres de votre carte de retrait bancaire. Pensez à votre smartphone équipé d'un capteur d'empreintes digitales : il est étonnant que son taux de fausses acceptations est plus élevé. Il est plus de 200 fois plus élevé que celui d'un lecteur d'empreinte digitale ekey.

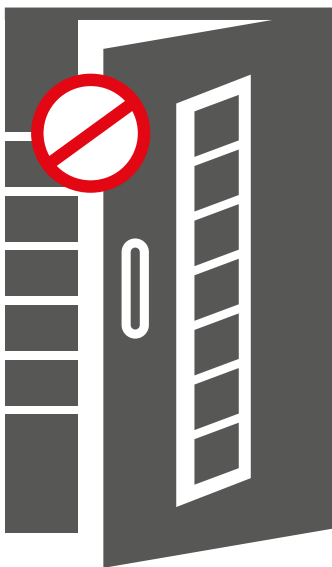
En bref : il est théoriquement possible qu'une personne non autorisée obtienne l'accès, mais c'est fortement improbable.

La probabilité de gagner au loto (6 numéros sur 45) est de 1 sur 8.145.000, c'est-à-dire bien plus élevée que la probabilité qu'une personne non autorisée obtienne l'accès.



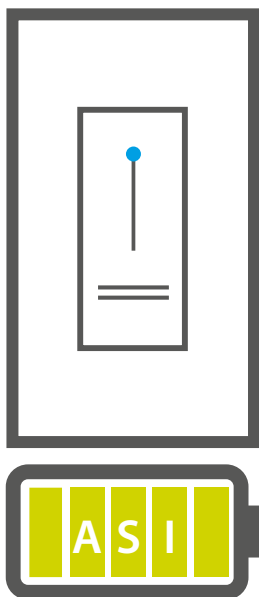
Une porte risque-t-elle de s'ouvrir seule en cas de coupure de courant ?

Non. En cas de panne de courant affectant une solution de contrôle d'accès à empreinte digitale ekey, aucune impulsion n'est envoyée pour ouvrir la porte. Seul un doigt autorisé et vivant peut envoyer cette impulsion d'ouverture.



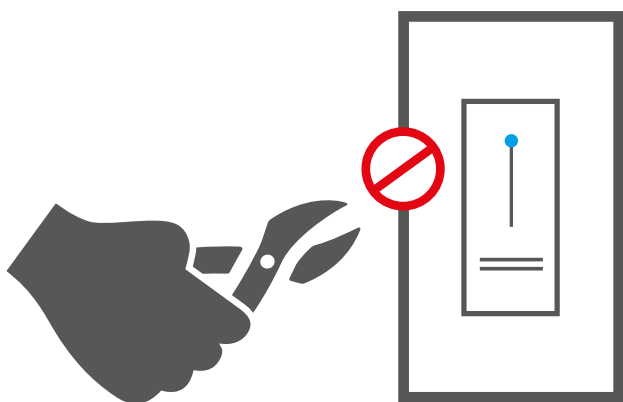
Le courant est coupé. Comment ouvrir ma porte ?

Pour pallier à ces moments obscurs, nos solutions de contrôle d'accès sont équipées d'une ASI (alimentation sans interruption). Celle-ci maintient le fonctionnement du lecteur d'empreinte digitale, du contrôleur et de la serrure motorisée pendant plusieurs heures. Il est également possible d'utiliser une clé.



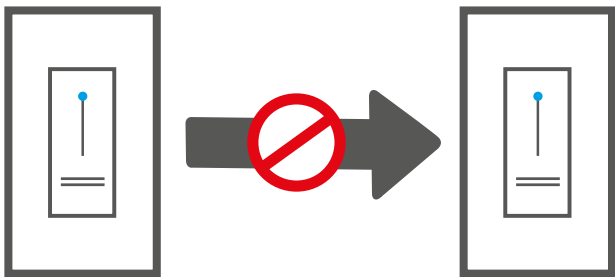
La solution de contrôle d'accès à empreinte digitale ekey, peut-elle être violée depuis l'extérieur pour ouvrir la porte ?

Non. Il est impossible de violer le système depuis l'extérieur. Ni même en forçant, car le lecteur d'empreinte digitale et le contrôleur sont installés dans des zones distinctes. L'impulsion d'ouverture est émise par le contrôleur dans la zone intérieure protégée. Le système ne peut pas non plus être neutralisé par Internet car il n'y est pas connecté.



Est-il possible de violer le système en remplaçant le lecteur d'empreinte digitale ?

Le lecteur d'empreinte digitale et le contrôleur sont couplés lors de la mise en service et communiquent de manière cryptée. Les données utilisateurs créées sont enregistrées avec le numéro de série de l'appareil et ne peuvent pas être copiées vers d'autres appareils. En cas de remplacement des appareils, il est nécessaire de restaurer les réglages par défaut du contrôleur et du lecteur d'empreinte digitale et de les coupler à nouveau. Il est donc nécessaire de pouvoir accéder à la zone intérieure protégée où est installé le contrôleur. Par ailleurs, il sera nécessaire de recréer toutes les données utilisateurs.



La connexion entre le smartphone/la tablette, le lecteur d'empreinte digitale et le contrôleur, est-elle sûre ?

Pour établir la connexion entre un smartphone/tablette, le lecteur d'empreinte digitale et le contrôleur, nous utilisons le procédé de couplage « Bluetooth Secure Simple Pairing ». Le transfert des données entre les appareils est systématiquement crypté.



Que se passe-t-il si je perds mon smartphone/ma tablette ?

Un code de sécurité de 4 à 6 caractères doit être saisi à l'ouverture de l'application. Ainsi, les personnes non autorisées ne pourront pas démarrer l'appli.

En cas de perte du smartphone/tablette, il est possible de rétablir la connexion avec le lecteur d'empreinte digitale à l'aide d'un(e) autre smartphone/tablette avec l'key home appli et le code de couplage administrateur configuré.



Le fabricant a-t-il dissimulé des autorisations d'accès dans le système ?

Non. ekey n'a dissimulé aucune option d'ouverture (code d'usine, etc.) par un technicien dans le système. Le propriétaire (également administrateur) est la seule personne capable de restaurer les réglages par défaut du système à l'aide d'un code administrateur à 6 caractères qu'il a défini lui-même.



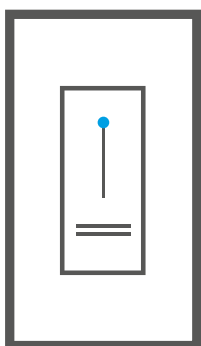
La solution de contrôle d'accès à empreinte digitale est-elle couverte par les assurances ?

Les compagnies d'assurance ne font aucune différence entre le verrouillage mécanique par clé ou électronique par empreinte digitale. Seul le verrouillage correct de l'accès permet de bénéficier d'une couverture d'assurance. Si la porte ne fait que se refermer avec le pêne, elle n'est pas considérée comme verrouillée.



Toutes les activités, sont-elles enregistrées dans le lecteur d'empreinte digitale ?

Le système ekey home solutions de contrôle d'accès simple ne tient pas un journal des accès. Avec les solutions de contrôle d'accès ekey multi et ekey net, ekey propose un journal des accès avec chaque lecteur d'empreinte digitale que seul peut lire l'administrateur. Les tentatives d'accès des personnes non autorisées sont également consignées.



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 ANS DE GARANTIE DE QUALITÉ

Cette garantie de qualité étendue est une prestation supplémentaire facultative, car nous sommes persuadés que les produits ekey sont faits pour durer. Nos composants de qualité supérieure et nos contrôles approfondis de la production, de la finition et du fonctionnement sont les garants de la qualité, de la fonctionnalité, de la résistance et de la sécurité. Vous êtes donc assuré d'avoir choisi la meilleure solution du marché.

3 + 2 = 5 ANS DE GARANTIE DE QUALITÉ !

Nous sommes sûrs de la qualité de nos produits, c'est pourquoi vous pouvez prolonger de 2 ans la GARANTIE DE QUALITÉ ekey de 3 ans.

Comment faire ?

Il vous suffit d'enregistrer votre produit dans les 4 semaines suivant la date de votre achat à l'adresse www.ekey.net/fr_FR/garantie/ pour bénéficier aussitôt de la GARANTIE DE QUALITÉ ekey de 5 ANS.



LEXIQUE

Doigt factice

Une reconstruction, une imitation ou une falsification du doigt.

Laisser la porte se refermer avec le pêne

Le pêne est la pièce de la serrure qui maintient la porte en butée dans l'encadrement de porte.

Gabarit

Il s'agit d'un modèle utilisé pour le traitement électronique des données.

ASI

L'alimentation sans interruption est utilisée pour prendre le relais de l'alimentation secteur en cas de panne de courant. Elle est intégrée dans l'alimentation électrique des installations ou appareils à protéger.

Couplage

Deux éléments sont couplés techniquement pour pouvoir communiquer ensemble.



YOUR FINGER. YOUR KEY.



Sous réserve d'erreurs d'impression ou de rédaction.
© ekey biometric systems GmbH - 08.2020

Autriche (siège)

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

Allemagne

ekey biometric systems Deutschland GmbH
Industriestraße 10
D-61118 Bad Vilbel
T: +49 6187 90696 - 0
E: office@ekey.net

Suisse et Liechtenstein

ekey biometric systems Est.
Landstrasse 79
FL-9490 Vaduz
T: +41 71 560 5480
E: office@ekey.ch

Adriatique orientale

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

Italie

ekey biometric systems Srl.
Via Copernico 13/A
I-39100 Bolzano
T: +39 0471 922712
E: italia@ekey.net



www.ekey.net