ekey
YOUR FINGER. YOUR KEY.

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

Réponses aux questions les plus fréquentes

À propos d'ekey

Fondée en 2002, ekey est devenue aujourd'hui le n° 1 en Europe des solutions de contrôle d'accès par lecteur d'empreinte digitale. On peut perdre, oublier ou se faire voler ses clés, ses cartes ou ses codes, mais pas son doigt !

ekey développe depuis 20 ans des solutions de contrôle d'accès pour les particuliers, les entreprises et les organisations. Ce qui était au départ un projet de recherche est devenu aujourd'hui l'un des principaux fabricants de contrôle d'accès biométrique : l'entreprise familiale autrichienne est devenue le leader européen des solutions de contrôle d'accès par lecteur d'empreinte digitale.

Qualité « Made in Austria »

Avant d'être distribué sur le marché, un produit ekey doit être soumis à un test de résistance strict : des simulations intensives allant de la chaleur torride et du froid glacial à une humidité élevée. Chaque lecteur d'empreinte digitale ainsi que l'ensemble de ses composants doivent réussir ces tests un nombre incalculable de fois avant que le produit ne se retrouve enfin entre vos mains.

Designed, developed
and made in Austria.

Le confort associé à la sécurité

Les systèmes de contrôle d'accès par lecteur d'empreinte digitale d'ekey améliorent le quotidien grâce au confort de l'accès sans clé, à la flexibilité et aux fonctionnalités intelligentes. La sécurité est toujours la priorité.

Quel est le niveau de sécurité d'un système de lecteur d'empreinte digitale ekey ? Dans les pages suivantes, vous trouverez les réponses aux questions les plus courantes.

Si vous avez d'autres questions, contactez :

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

Contenu

Les empreintes digitales sont-elles enregistrées ?

Non, ekey n'enregistre aucune empreinte digitale.

Un modèle est créé à partir des caractéristiques biométriques de l'empreinte digitale originale, comme les points, les extrémités de ligne et les bifurcations, ce que l'on appelle le gabarit.

Celui-ci est converti en un code numérique binaire unique par un algorithme logiciel breveté développé en interne, puis enregistré et utilisé pour chaque comparaison.

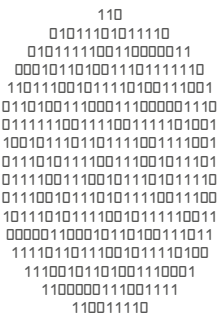
Les gabarits sont chiffrés et stockés dans le nuage ekey bionyx.

La clé de déchiffrage se trouve uniquement sur votre propre terminal (smartphone/tablette), de sorte que les données sont protégées contre tout accès non autorisé. La sécurité peut être comparée à celle d'une application de banque en ligne.

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

Non, le gabarit enregistré (voir « Les empreintes digitales sont-elles enregistrées ? ») ne peut plus être reconverti en empreinte digitale.

Ceci empêche toute reconstitution de l'empreinte digitale originale.

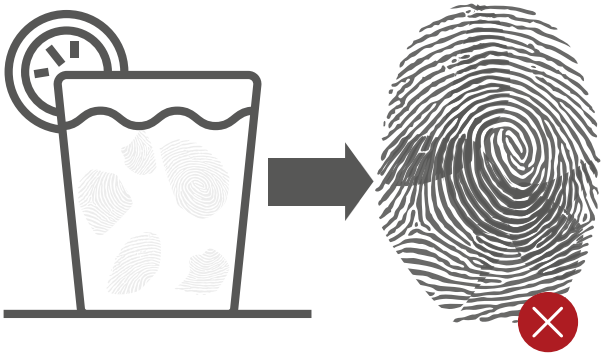


Est-il possible de créer un doigt factice permettant d'ouvrir la porte à partir d'une empreinte digitale trouvée (par ex. sur un verre) ?

ekey s'appuie sur de multiples protections contre la neutralisation frauduleuse par des doigts factices : la vérification que les caractéristiques biométriques proviennent du doigt d'une personne réelle a lieu 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.

En outre, il est quasiment impossible 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.

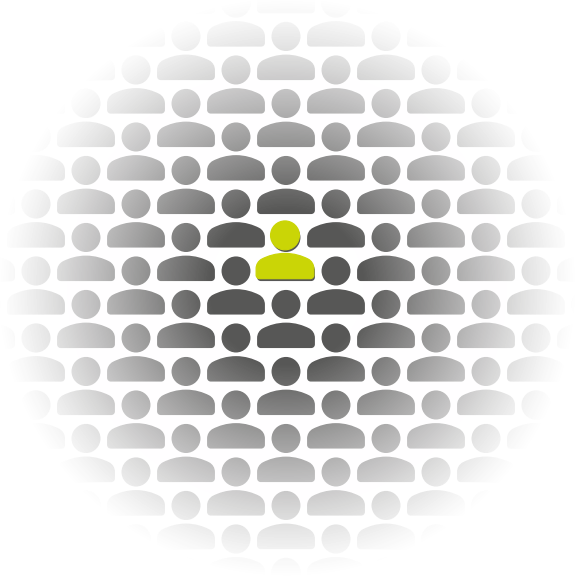
Conclusion : c'est théoriquement possible, mais quasiment impossible en pratique.



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

Il existe un indicateur spécial pour cela : le taux de fausses acceptations (FAR). 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'empreinte digitale ekey, il est de 1 sur 10 millions, à condition que les empreintes digitales aient été correctement enregistrées.

En résumé, il est théoriquement possible qu'une personne non autorisée obtienne l'accès, mais c'est fortement improbable. Un système ekey est 1 000 fois plus sûr que le code à 4 chiffres d'une carte bancaire. Et 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.

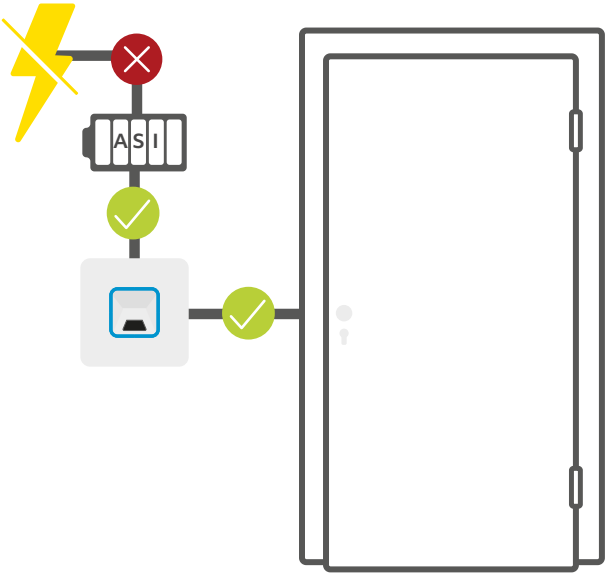


Comment ouvrir la porte en cas de panne de courant ?

En cas de panne de courant, d'Internet ou de routeur, personne ne reste à la porte. ekey propose pour ses systèmes de contrôle d'accès une alimentation sans interruption (ASI).

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 à tout moment.

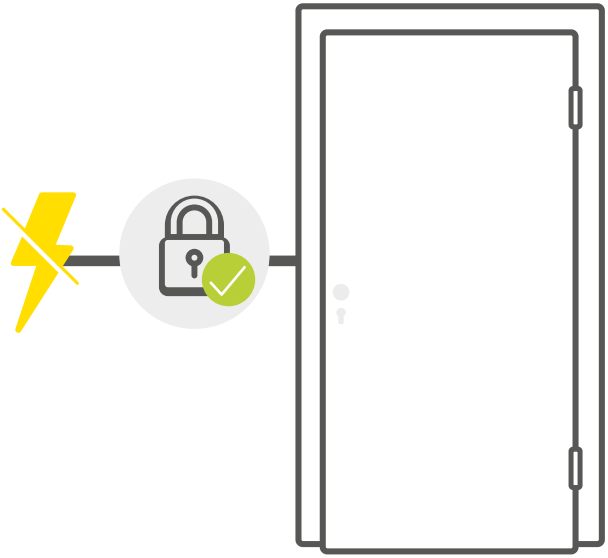
Et même si la connexion à Internet ou au routeur est coupée, la porte peut toujours être ouverte.



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 par lecteur d'empreinte digitale ekey, aucune impulsion n'est envoyée pour ouvrir la porte.

Seul un utilisateur autorisé peut émettre cette commande d'ouverture.



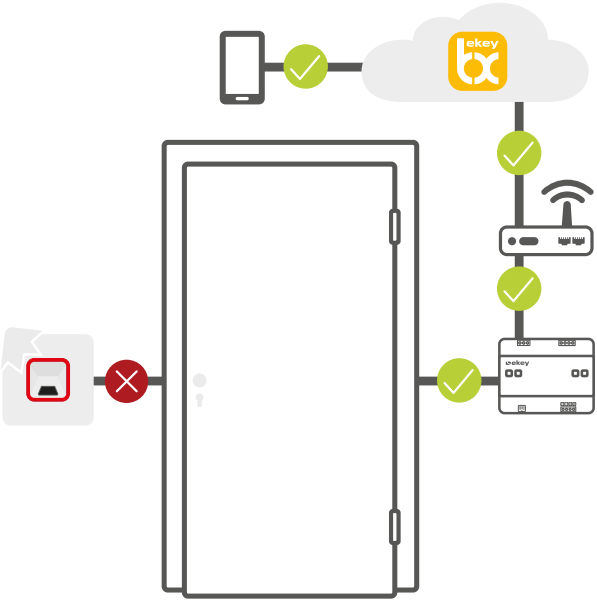
La solution de contrôle d'accès par lecteur d'empreinte digitale ekey peut-elle être neutralisée depuis l'extérieur pour ouvrir la porte ?

Non. Il est impossible de neutraliser 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.

Les données également sont chiffrées plusieurs fois en permanence et sécurisées.

La transmission des données dans le système ekey bionyx est chiffrée de bout en bout. Toutes les données sont transmises sous forme chiffrée sur toutes les stations de transmission.



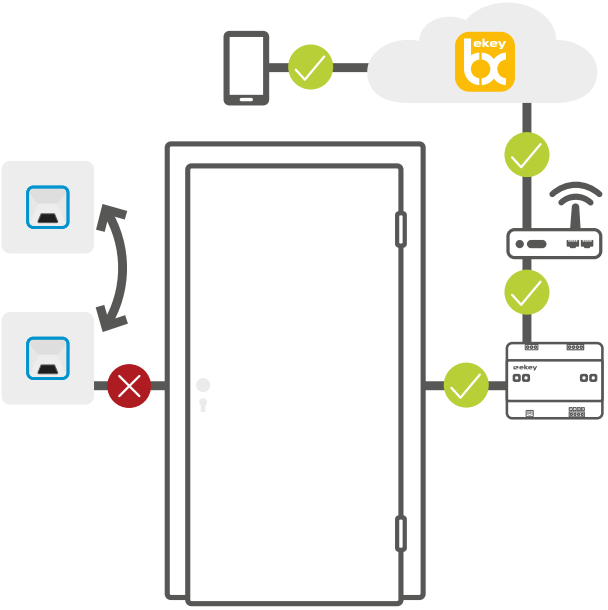
Est-il possible de neutraliser le système en remplaçant le lecteur d'empreinte digitale ?

Non, le système ne peut pas être neutralisé par le remplacement du 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 utilisateur créées sont enregistrées avec le numéro de série de l'appareil. Aussi bien un éventuel remplacement du lecteur d'empreinte digitale qu'une éventuelle extension du système doivent être validés par un administrateur dans l'application ekey bionyx.

Les doigts enregistrés sont conservés et n'ont pas besoin d'être à nouveau enregistrés.

Les données stockées ne peuvent pas être transférées vers un autre appareil sans ce processus.



Le système est-il connecté à Internet ?

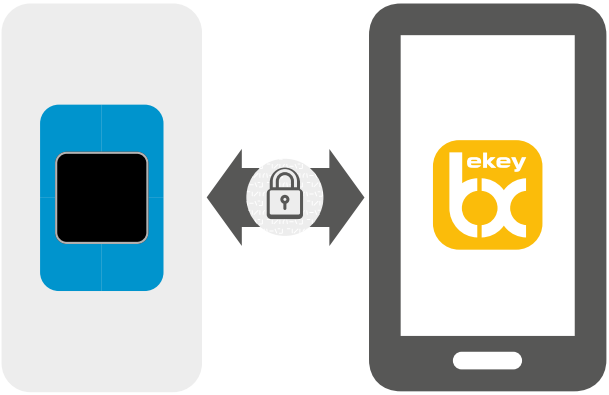
Non. Les appareils communiquent via Internet exclusivement avec le nuage ekey bionyx. Celui-ci est exploité par le leader mondial du cloud computing MS Azure. Les données sont chiffrées en permanence et ne peuvent être consultées ni par ekey ni par Microsoft.

Du fait des normes de sécurité élevées, seuls des réseaux sans fil chiffrés peuvent être utilisés.

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

Le protocole sécurisé « Transport Layer Security » est utilisé pour l'établissement de la connexion initiale entre le smartphone/la tablette, le lecteur d'empreinte digitale et l'unité de commande. Le transfert des données entre les appareils est ainsi systématiquement crypté.

La transmission des données dans l'application ekey bionyx s'effectue grâce à un chiffrement de bout en bout. Toutes les données sont transmises sous forme chiffrée sur toutes les stations de transmission. Les données envoyées ne peuvent être lues ou générées ni par des attaquants ni par ekey elle-même.



Pourquoi ekey s'appuie-t-elle sur une solution en nuage ?

En plus de l'appareil physique (le matériel), un système de contrôle d'accès comprend toujours également le logiciel correspondant (des capacités de calcul et de stockage jusqu'au logiciel proprement dit). Avec le nuage ekey bionyx, ekey a décidé d'utiliser la technologie de l'informatique en nuage, car elle offre de nombreux avantages côté logiciel (application ekey bionyx) :

1. Protection des données : les principaux fournisseurs de solutions d'informatique en nuage déploient d'importants efforts financiers et humains pour protéger les données de leurs clients. Par conséquent, une telle solution est généralement plus performante à cet égard qu'une solution interne.

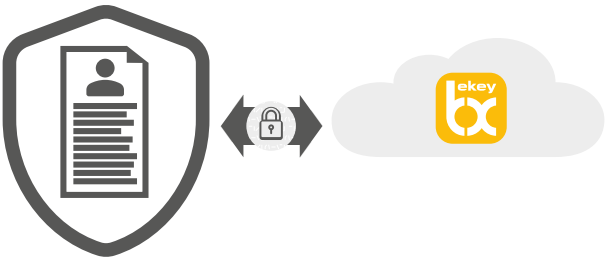
2. Sécurité : le modèle commercial des grands fournisseurs de cloud repose sur le stockage sécurisé des données. Par conséquent, les centres de données eux-mêmes sont protégés de manière optimale (par ex. locaux, surveillance, protection contre les incendies, etc.) et la protection virtuelle contre la cybercriminalité est à un niveau élevé.

3. Disponibilité : les accords de niveau logiciel peuvent garantir une disponibilité logicielle d'environ 99 % (le 1 % manquant correspond principalement à des temps d'arrêt planifiés pour les mises à jour). Une disponibilité comparable n'est pas possible avec votre propre serveur.

4. Mises à jour : les logiciels doivent toujours être tenus à jour afin d'offrir une sécurité maximale. Les systèmes de contrôle d'accès utilisant la technologie de l'informatique en nuage sont toujours à jour, les mises à jour sont automatiques.

Que deviennent les données personnelles ?

La vision d'ekey est de rendre la biométrie accessible à tous. L'objectif associé est de rendre la vie quotidienne aussi sûre, flexible et confortable que possible et de créer des solutions pratiques. ekey veut ainsi améliorer la vie, et non empiéter sur la vie privée. Le modèle commercial est donc conçu de manière à ce que les produits et services ne soient jamais échangés contre des données personnelles et que celles-ci ne soient donc ni utilisées par ekey elle-même ni vendues à des tiers.



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

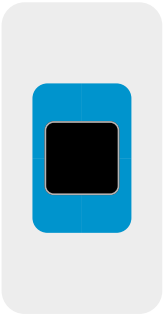
Contrairement à une clé, la personne qui trouve le smartphone n'a pas accès au système :

le smartphone ou la tablette ainsi que l'application ekey bionyx sont déverrouillés séparément : les premiers via l'accès défini individuellement et utilisant la biométrie (empreinte digitale ou reconnaissance faciale) ou le code, le second via la biométrie ou le nom d'utilisateur avec un mot de passe personnel. L'application est ainsi protégée contre les accès non autorisés. Si vous perdez votre smartphone ou votre tablette, la connexion au nuage ekey bionyx peut être restaurée à l'aide d'un nouvel appareil et d'un code de sauvegarde.

Ainsi, même si l'appareil mobile est perdu, il est toujours possible de se connecter sur un nouvel appareil avec les données d'accès.

Les activités sur le lecteur d'empreinte digitale sont-elles enregistrées ?

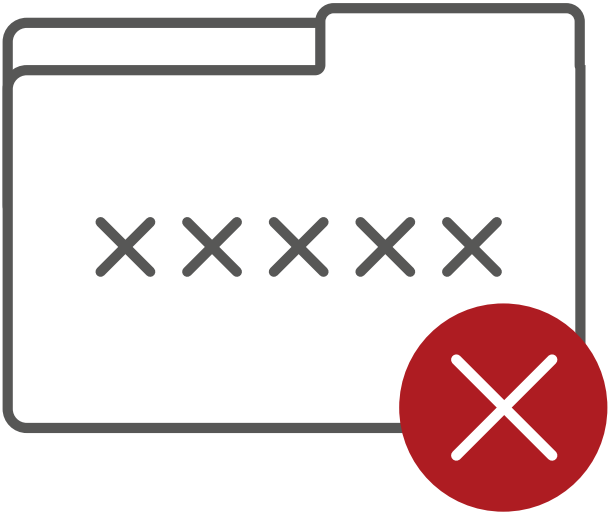
Par défaut, les activités sont stockées dans le journal des accès pendant 30 jours. Celui-ci peut être consulté et supprimé ou désactivé par les administrateurs autorisés.



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

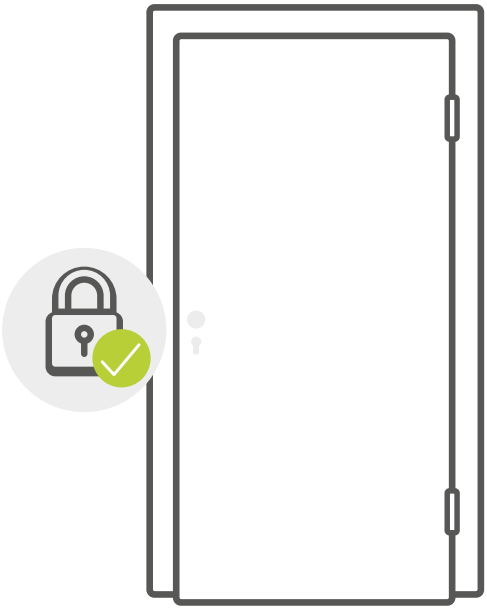
Le fabricant a-t-il dissimulé des autorisations d'accès dans le système ?

Non. ekey n'a dissimulé aucune option d'ouverture (code d'usine, etc.) par un technicien dans le système. Seul un administrateur autorisé a la possibilité d'apporter des modifications en utilisant son smartphone ou sa tablette et les données d'accès à son compte (e-mail, mot de passe).



L'utilisation d'une solution de contrôle d'accès par lecteur d'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 lecteur d'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 (la partie de la serrure qui maintient la porte dans le dormant), elle n'est pas considérée comme verrouillée.



ekey
YOUR FINGER. YOUR KEY.

Designed, developed and made in Austria.

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 906 96 - 0
E : office@ekey.net

Suisse & Liechtenstein
ekey biometric systems
Schweiz AG
Schaanerstrasse 13
FL-9490 Vaduz
T : +41 71 560 54 80
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 Perathoner 31
I-39100 Bolzano
T : +39 0471 922 712
E : italia@ekey.net

www.ekey.net