YOUR FINGER. YOUR KEY.

Quanto è sicura una soluzione di controllo degli accessi a lettore d'impronta digitale ekey?

Risposte alle domande più frequenti

Chi siamo

ekey ha iniziato la sua attività nel 2002 e oggi è il numero 1 in Europa nelle soluzioni di controllo degli accessi a lettore d'impronta digitale. Chiavi, schede e codici possono essere smarriti, dimenticati o rubati: il tuo dito, invece, è sempre con te!

Da 20 anni, ekey sviluppa soluzioni di controllo degli accessi per privati, aziende e organizzazioni. Quello che era iniziato come progetto di ricerca è oggi uno dei principali produttori di controlli degli accessi biometrici: l'azienda austriaca a conduzione familiare è oggi leader di mercato in Europa per le soluzioni di controllo degli accessi a lettore d'impronta digitale.

Qualità "Made in Austria"

Prima che un prodotto ekey possa essere immesso sul mercato, deve essere sottoposto a un test di resistenza molto rigoroso: simulazioni intense che vanno dal caldo torrido al freddo gelido, fino all'umidità elevata. Ogni lettore d'impronta digitale e i suoi componenti devono superare questi test con successo innumerevoli volte prima che il prodotto possa finalmente pervenire nelle tue mani.

Il comfort incontra la sicurezza

I sistemi di controllo degli accessi a lettore d'impronta digitale di ekey arricchiscono la vita di tutti i giorni con la comodità dell'accesso senza chiave, la flessibilità e le funzioni intelligenti. La sicurezza è sempre al centro.

Quindi, quanto è sicuro un sistema a lettore d'impronta digitale ekey? Nelle pagine seguenti troverai le risposte alle domande più frequenti.

Se hai ulteriori domande, non esitare a rivolgerti a:

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

Contenuto

Le impronte digitali vengono salvate?

No. ekey non salva le impronte digitali,

ma crea un modello, chiamato template, servendosi delle particolarità biometriche dell'impronta digitale originale, quali ad esempio singoli punti, estremità delle linee e biforcazioni.

Con l'ausilio di un algoritmo software appositamente sviluppato e brevettato, questo modello viene successivamente trasformato in un codice numerico binario univoco, salvato e preso come riferimento per ogni confronto.

I template vengono salvati con crittografia nel cloud ekey bionyx.

La relativa chiave si trova solo sul tuo dispositivo finale (smartphone/tablet), quindi i dati sono protetti da accessi non autorizzati. La sicurezza può essere paragonata a quella di una app di netbanking.

Si può ricostruire un'impronta digitale originale partendo dai dati salvati?

No, il template archiviato (vedi "Le impronte digitali vengono salvate?") non può più essere riconvertito in un'impronta digitale.

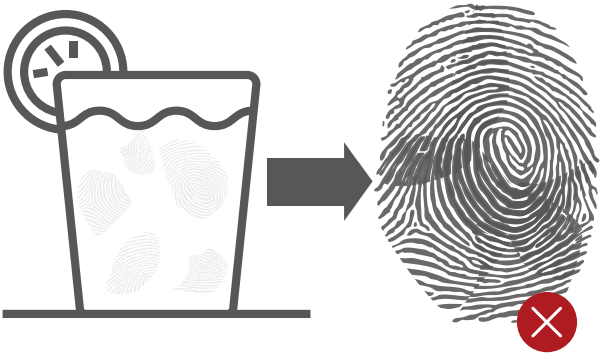
Si esclude così la possibilità di ricostruire l'impronta digitale originale.

Da un'impronta digitale lasciata su una superficie (ad es. su un bicchiere) è possibile realizzare un "fake finger" per aprire una porta?

ekey si basa su molteplici operazioni di sicurezza contro la manipolazione da parte di "fake finger": da un lato, quando si posiziona il dito sul sensore, si verifica la conduttività della pelle viva e, dall'altro, si esegue la valutazione algoritmica dei dati, per verificare se le caratteristiche biometriche provengono dal dito di una persona reale.

Inoltre, è quasi impossibile realizzare un'impronta digitale finta utilizzabile. Le caratteristiche potrebbero essere trasferite su un "fake finger" solo con chiaro intento criminale, ancora più competenza tecnica e condizioni di laboratorio assolutamente perfette.

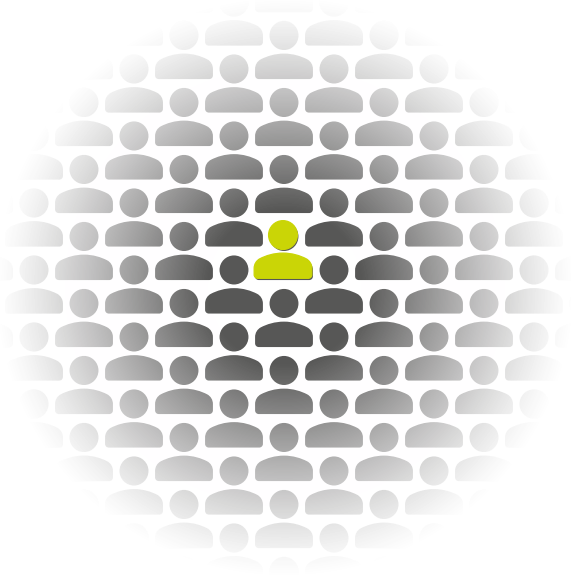
Conclusione: in teoria è possibile, ma in pratica quasi infattibile.



Quanto è alta la probabilità che la porta si apra in presenza di una persona non autorizzata?

Esiste un indicatore speciale per questo: il tasso di false accettazioni (FAR). Con questa espressione si definisce la probabilità che un sistema di sicurezza consenta l'accesso a una persona non autorizzata. Con i lettori d'impronta digitale ekey, il tasso ammonta a 1:10 milioni, purché le impronte siano state registrate correttamente.

Per riassumere: è teoricamente possibile, ma altamente improbabile, che una persona non autorizzata ottenga l'accesso dai lettori d'impronta digitale ekey. Un sistema ekey è 1.000 volte più sicuro del codice a quattro cifre della carta bancomat. E la probabilità di azzeccare una combinazione di sei numeri al lotto (6 su 45) con una sola scommessa è di 1:8.145.000, che è significativamente più elevata rispetto alla probabilità di accesso di una persona non autorizzata.

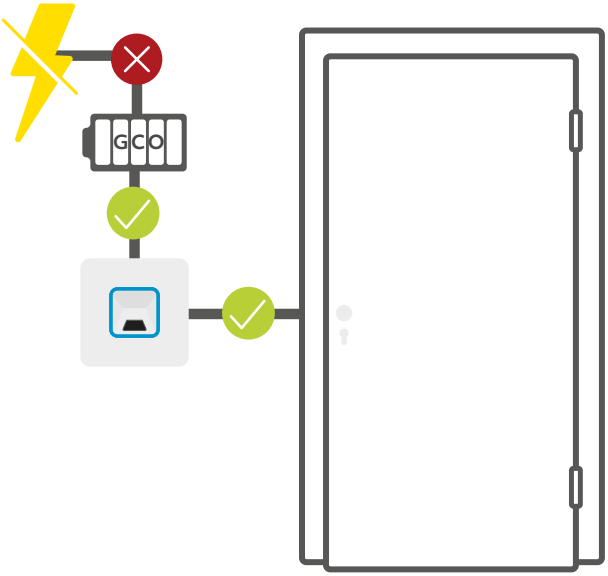


Come si apre la porta in caso di interruzione di corrente?

Se la corrente, Internet o il router saltano, nessuno resta fuori davanti a una porta chiusa. ekey offre un gruppo di continuità (GCO) per i suoi sistemi di controllo degli accessi.

Questo dispositivo mantiene in funzione per qualche ora il lettore d'impronta digitale, la centralina di comando e la serratura motorizzata. In alternativa si può ovviamente utilizzare una chiave in qualsiasi momento.

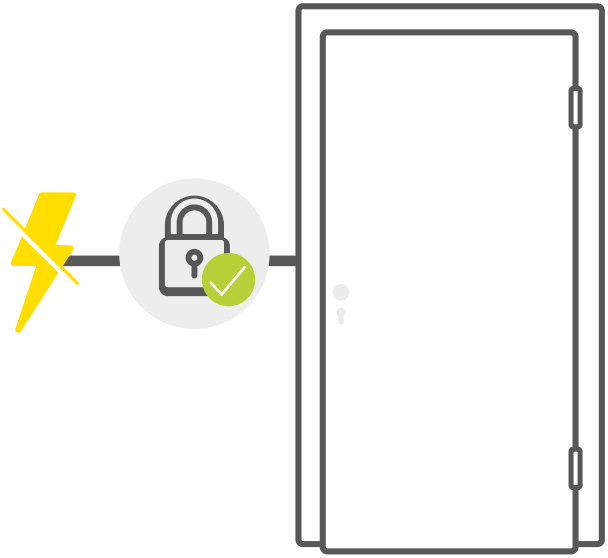
E anche se la connessione a Internet o al router non riesce una volta, la porta può comunque essere aperta.



Una porta può aprirsi da sola in caso di un'interruzione di corrente?

No. In una soluzione di controllo degli accessi a lettore d'impronta digitale ekey le interruzioni dell'alimentazione elettrica non attivano l'impulso di apertura della porta.

Solo un utente autorizzato può emettere questo comando di apertura.



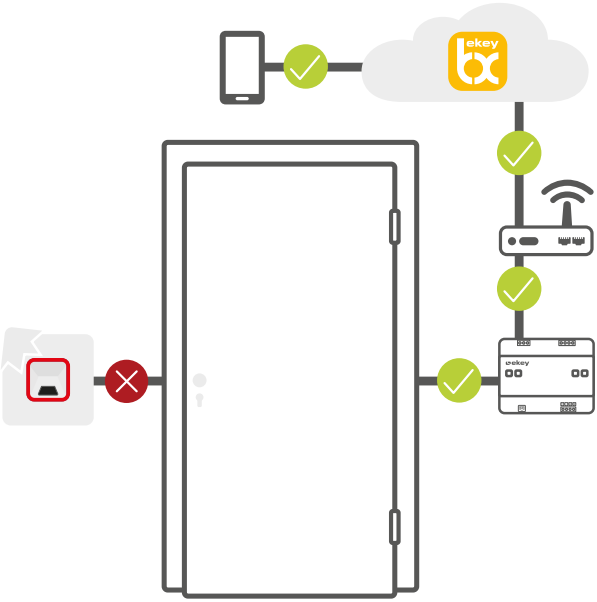
Una soluzione di controllo degli accessi a lettore d'impronta digitale ekey può essere manipolata dall'esterno per aprire la porta?

No. Il sistema non può essere manipolato dall'esterno. Neanche con l'uso della forza, perché il lettore d'impronta digitale è fisicamente separato dalla centralina di comando,

che trasmette l'impulso di apertura da una zona interna protetta.

I dati vengono inoltre crittografati e protetti più volte in ogni momento.

Il trasferimento dei dati nel sistema ekey bionyx avviene tramite crittografia end-to-end. Tutti i dati vengono trasferiti in forma crittografata su tutte le stazioni di trasmissione.



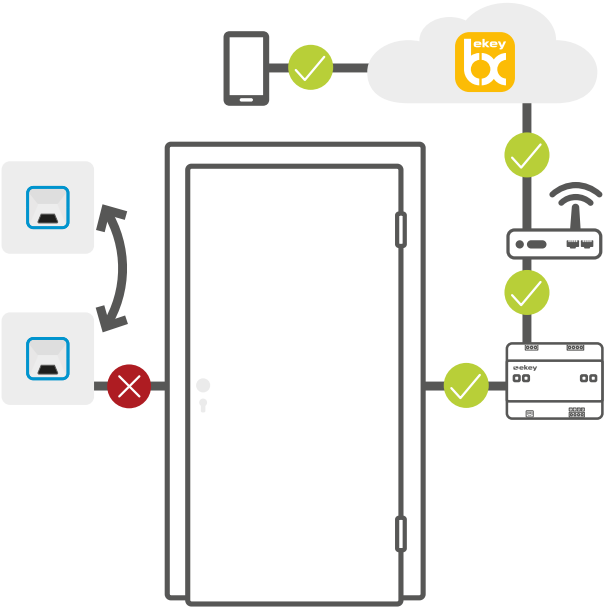
Il sistema può essere manipolato scambiando il lettore d'impronta digitale?

No, il sistema non può essere manipolato scambiando il lettore d'impronta digitale.

Il lettore d'impronta digitale e la centralina di comando vengono accoppiati tra di loro all'atto della messa in servizio e comunicano in forma cifrata. I dati utente vengono salvati assieme al numero di serie del dispositivo. Se viene scambiato il lettore d'impronta digitale o il sistema viene ampliato, questo deve essere verificato da un amministratore nella app ekey bionyx.

Le dita salvate vengono conservate e non devono essere salvate di nuovo.

I dati memorizzati non possono essere trasferiti a un altro dispositivo senza questo processo.



Il sistema è connesso a Internet?

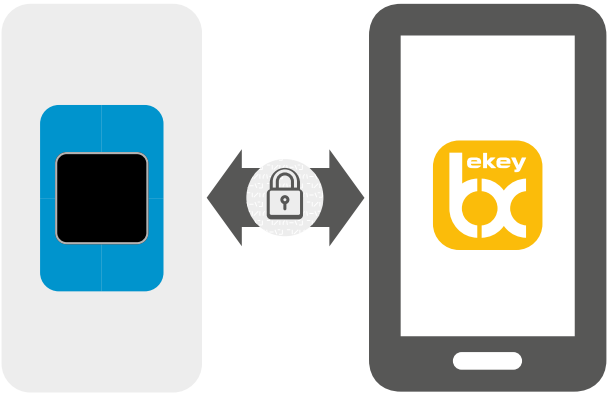
No. I dispositivi comunicano tramite Internet esclusivamente con il cloud ekey bionyx. Ciò è operato dal leader di mercato mondiale del cloud computing MS Azure. I dati sono sempre crittografati e non possono essere visualizzati né da ekey né da Microsoft.

A causa dell'elevato standard di sicurezza, è possibile utilizzare solo reti WLAN crittografate.

Quanto è sicuro il collegamento tra smartphone/ tablet, lettore d'impronta digitale e centralina di comando?

Per la prima creazione del collegamento tra smartphone/ tablet, lettore d'impronta digitale e unità di controllo, viene utilizzato il protocollo sicuro "Transport Layer Security". Con esso, i dati vengono trasferiti tra gli apparecchi esclusivamente in forma cifrata.

Il trasferimento dei dati nella app ekey bionyx avviene tramite crittografia end-to-end. Tutti i dati vengono trasferiti in forma crittografata su tutte le stazioni di trasmissione. I dati inviati non possono essere letti o generati da attacchi esterni o dalla stessa ekey.



Perché ekey si affida a una soluzione cloud?

Oltre all'apparecchio vero e proprio, ovvero l'hardware, un sistema di controllo degli accessi include sempre anche il software corrispondente, dalle capacità di calcolo e di archiviazione al software vero e proprio. Con il cloud ekey bionyx, ekey ha deciso di utilizzare la tecnologia basata su cloud perché offre numerosi vantaggi dal lato software (app ekey bionyx):

1. Protezione dei dati: i principali fornitori di soluzioni basate su cloud si sottopongono a grandi impegni finanziari e personali per proteggere i dati dei propri clienti. Pertanto, tale soluzione è solitamente più professionale in questo senso rispetto a una soluzione interna.

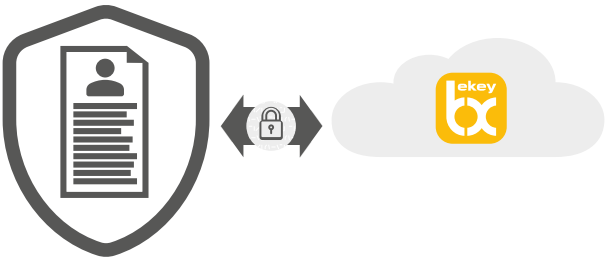
2. Sicurezza: il modello di business dei grandi fornitori di servizi cloud si basa sull'archiviazione sicura dei dati. Pertanto, i data center stessi sono protetti in modo ottimale (ad es. locali, sorveglianza, protezione antincendio, ecc.) e anche la protezione virtuale contro la criminalità informatica è di livello corrispondentemente elevato.

3. Disponibilità: gli accordi sul livello del software possono garantire una disponibilità del software di circa il 99% (l'1% mancante è per lo più tempo di inattività pianificato per gli aggiornamenti). Una disponibilità similmente elevata non è possibile con il proprio server.

4. Aggiornamenti: il software deve essere sempre aggiornato per offrire la massima sicurezza. I sistemi di controllo degli accessi basati su cloud sono sempre aggiornati, dato che gli aggiornamenti sono automatici.

Cosa succede ai dati personali?

La visione di ekey è rendere possibile la biometria per tutti. L'obiettivo associato a ciò è quello di rendere la vita di tutti i giorni il più sicura, flessibile e confortevole possibile e donare benefici pratici. In questo modo ekey vuole migliorare la vita, non invadere la privacy. Il modello aziendale è quindi concepito in modo tale che i prodotti e i servizi non vengano mai scambiati con dati personali e questi non vengano quindi utilizzati da ekey stessa né venduti a terzi.



Cosa succede se perdo il mio smartphone/tablet?

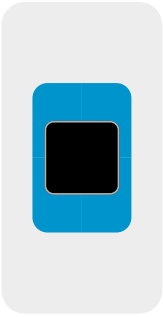
A differenza della chiave, il Finder dello smartphone non ha accesso al sistema.

Smartphone o tablet e app ekey bionyx vengono sbloccati separatamente: il primo tramite l'accesso impostato individualmente tramite dati biometrici (impronta digitale o riconoscimento facciale) oppure con un codice, il secondo tramite dati biometrici o nome utente e password personale. La app, quindi, è protetta da accessi non autorizzati. In caso di smarrimento dello smartphone o del tablet, la connessione al cloud ekey bionyx può essere ripristinata utilizzando un nuovo dispositivo e un codice di backup.

Quindi, anche in caso di smarrimento del dispositivo mobile, è comunque possibile effettuare l'accesso utilizzando un nuovo dispositivo con i dati di accesso.

Le attività sul lettore d'impronta digitale sono registrate?

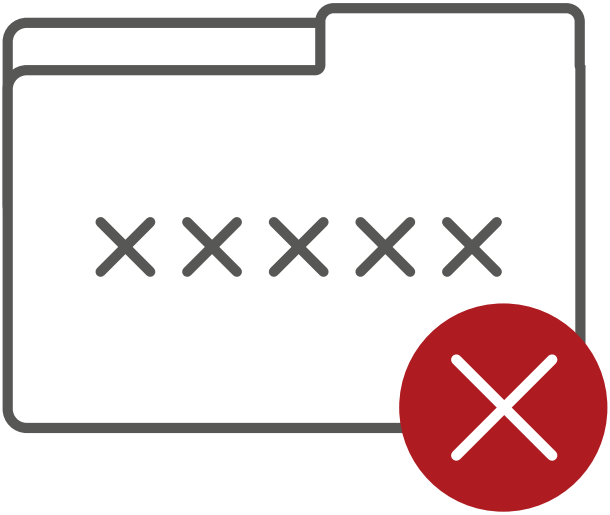
Per impostazione predefinita, le attività vengono archiviate nel log degli accessi per 30 giorni. Il log può essere visualizzato ed eliminato o disattivato dagli amministratori autorizzati.



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

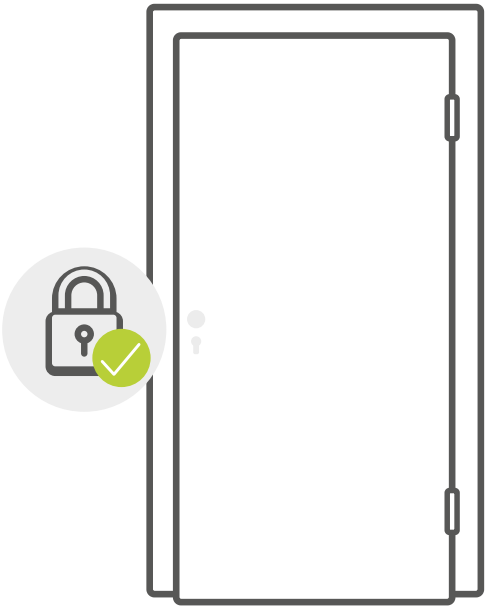
Nel sistema sono salvati diritti di accesso nascosti per il produttore?

No. Nel sistema, ekey non ha salvato alcuna possibilità di apertura da parte di un tecnico (tramite codice di fabbrica, ecc.). Solo un amministratore autorizzato ha la possibilità di apportare modifiche utilizzando il proprio smartphone o tablet in combinazione con i dati di accesso del proprio account (e-mail, password).



Esiste una copertura assicurativa con la soluzione di controllo degli accessi a lettore d'impronta digitale?

Ai fini della copertura assicurativa è irrilevante sapere se l'attivazione del blocco è meccanica (con chiave) piuttosto che elettronica (lettore d'impronta digitale). In generale, le assicurazioni rispondono solo quando un accesso è regolarmente bloccato. Se una porta è chiusa solamente con lo scrocco, quella parte della serratura che mantiene la porta in posizione di chiusura all'interno del suo telaio, viene considerata come non bloccata.



YOUR FINGER. YOUR KEY.

Designed, developed and made in Austria.

Austria (sede centrale)

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

Germania

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

Svizzera e Liechtenstein

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

Regione dell'Adriatico orientale

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

Italia

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

www.ekey.net

852116/270125