YOUR FINGER. YOUR KEY.

Quanto è sicura una **soluzione d'accesso ad impronta digitale ekey?**

Risposte

alle domande più frequenti

SICUREZZA delle soluzioni d'accesso ad impronta digitale ekey

ekey garantisce il più alto standard di sicurezza per la protezione dei suoi prodotti da manomissioni e da richieste illegittime al sistema d'accesso.

Per lo sviluppo, la costruzione e la lavorazione dei suoi prodotti ekey ha tenuto in considerazione le seguenti raccomandazioni e direttive:

- Raccomandazioni dell'Ufficio federale tedesco per la sicurezza e la tecnica informatica www.bsi.bund.de
- Raccomandazioni della VdS Schadenverhütung GmbH (istituzione tedesca per la sicurezza delle imprese) sugli impianti di controllo degli accessi www.vds.de

PARTNER E COLLABORAZIONI

KEINBRUCH

interkey

SSG
Schweizerische Sicherheitsgruppe

Sei interessato a una soluzione d'accesso ad impronta digitale ekey?

Dal 2002 sviluppiamo in ekey soluzioni d'accesso ad impronta digitale per la massima sicurezza di aziende e privati, che offrono un comfort straordinario. La nostra tecnologia viene utilizzata con successo nei più svariati campi di applicazione ed è costantemente perfezionata per nuovi settori d'impiego. L'intenso impegno che dedichiamo da anni alla nostra attività ci ha portato a diventare leader di mercato in Europa, ma esige anche la massima qualità giorno dopo giorno.

Per soddisfare questo requisito di qualità anche a livello informativo, abbiamo preparato per te quest'opuscolo con le domande più importanti e frequenti corredate dalle rispettive risposte.

Se desideri ulteriori chiarimenti sui nostri prodotti di qualità, puoi rivolgerti ai seguenti contatti:

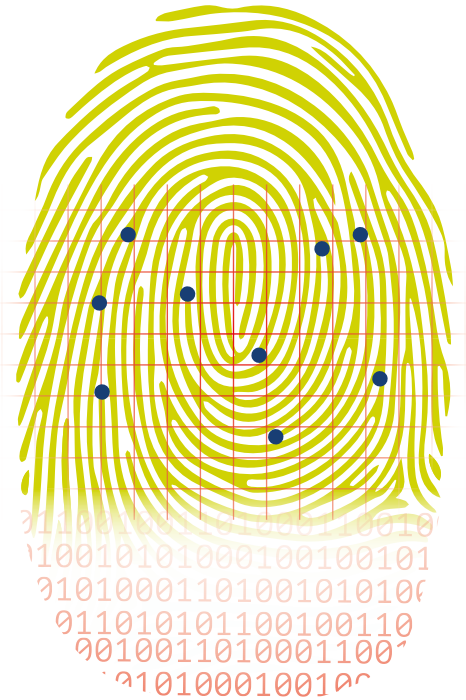
T: +39 0471 922 712
E: italia@ekey.net

A proposito di qualità
Siamo gli unici produttori di tutto il settore a realizzare i nostri dispositivi in Europa/Austria. Alla fine sarai tu a beneficiarne: sull'intera gamma dei nostri prodotti potrai usufruire di 5 ANNI DI GARANZIA! Ulteriori informazioni a pagina 18.

Scopri l'alta qualità dei prodotti ekey, ne sarai entusiasta!

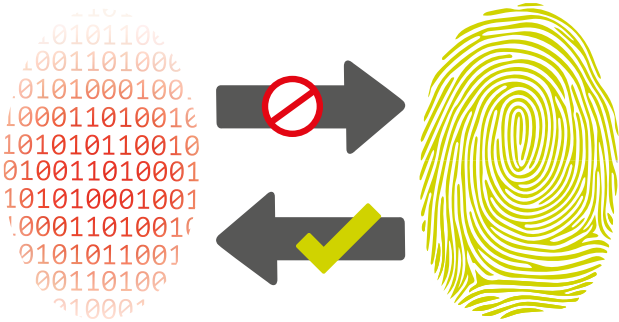
Le mie impronte digitali vengono salvate in un lettore d'impronta digitale ekey?

No. ekey non salva le impronte, ma crea un modello (template) servendosi delle particolarità biometriche dell'impronta digitale originale, quali p.es. singoli punti, estremità delle linee, biforcazioni, ecc. Con l'ausilio di un algoritmo appositamente sviluppato, questo modello viene successivamente trasformato in un codice numerico binario univoco, salvato e preso come riferimento per ogni confronto.



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

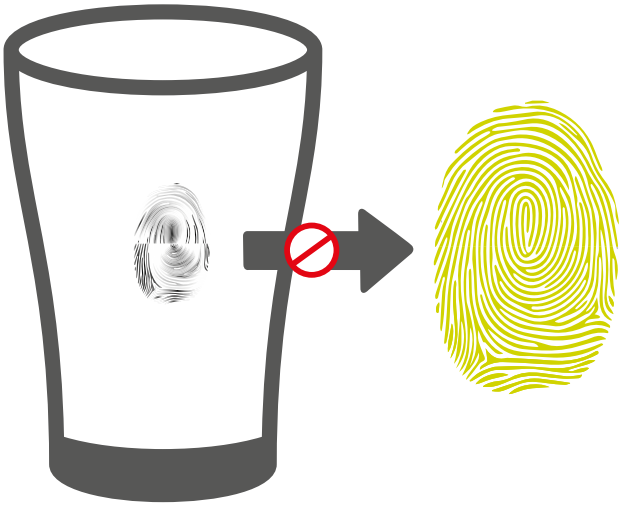
No. Il codice numerico archiviato in memoria non può più essere riconvertito in un'impronta. Si esclude così la possibilità di ricostruire l'impronta digitale originale.



Da un‘impronta digitale lasciata su una superficie (p.es. su un bicchiere) è possibile realizzare un “fake finger“ per aprire una porta?

È quasi impossibile ed estremamente dispendioso realizzare un‘impronta digitale 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.

Per concludere: in teoria è possibile, ma in pratica quasi infattibile.



I sistemi ekey utilizzano metodi per il riconoscimento vivente?

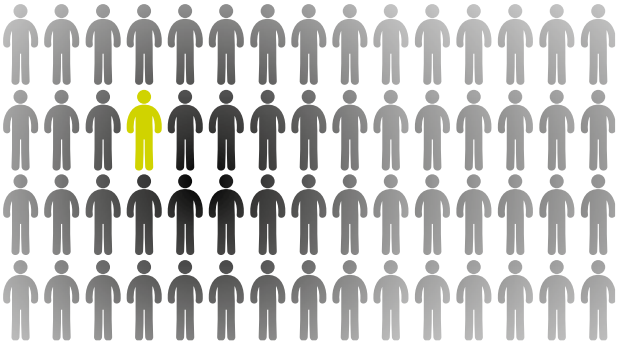
Sì. Con il cosiddetto "riconoscimento vivente" viene verificato se la caratteristica biometrica offerta appartiene a una persona vivente. Con i sistemi ekey, questa verifica avviene due volte: sia direttamente, quando si posiziona il dito attraverso la conduttività della pelle viva, sia attraverso la valutazione algoritmica dei dati.

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

Conosci il tasso di false accettazioni? Con questa espressione si definisce la probabilità che un sistema di sicurezza consenta l'accesso a una persona non autorizzata. Per i lettori d'impronte digitali ekey questo valore si attesta su 1: 10 milioni – purché le impronte siano state registrate correttamente.

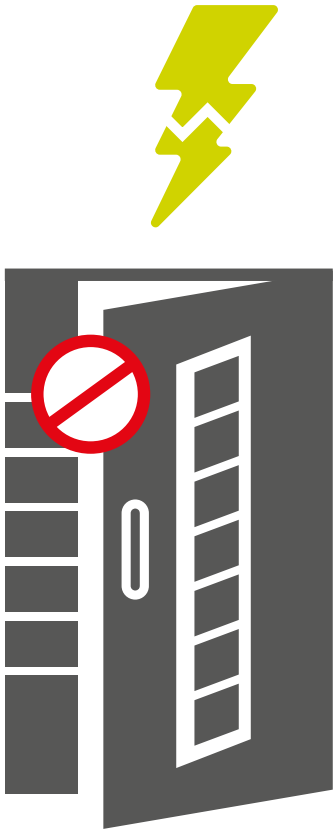
Per fare un confronto: i nostri lettori d'impronte digitali sono 1.000 volte più sicuri del codice a 4 cifre del tuo bancomat. Se invece pensi al tuo smartphone con sensore d'impronta digitale, il tasso di false accettazioni è sorprendentemente elevato. Per essere più precisi, oltre 200 volte più alto del tasso di un lettore d'impronta digitale ekey.
Riassumendo: è teoricamente possibile, ma altamente improbabile, che una persona non autorizzata ottenga l'accesso dai lettori d'impronte digitali ekey.

La probabilità di azzeccare una combinazione di sei numeri al lotto (6 su 45) con una sola scommessa è di 1: 8.145.000, cioè è significativamente più elevata rispetto alla probabilità di accesso di una persona non autorizzata.



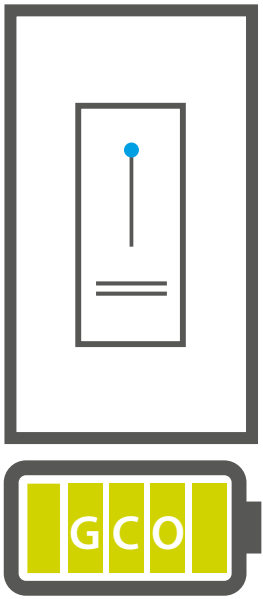
Una porta può aprirsi da sola in caso di un'interruzione di corrente?

No. In una soluzione d'accesso ad impronta digitale ekey le interruzioni dell'alimentazione elettrica non attivano l'impulso di apertura della porta. Come già sappiamo, ciò avviene soltanto tramite un dito vivo e autorizzato.



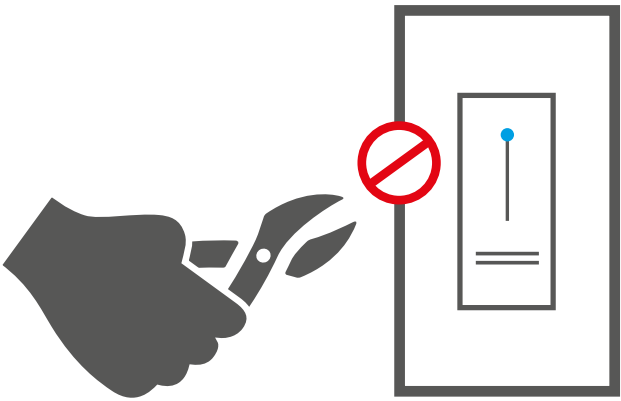
La corrente è saltata: come posso aprire la porta?

Per questi momenti di blackout offriamo un GCO, ossia un gruppo di continuità da collegare alle nostre soluzioni d'accesso. 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.



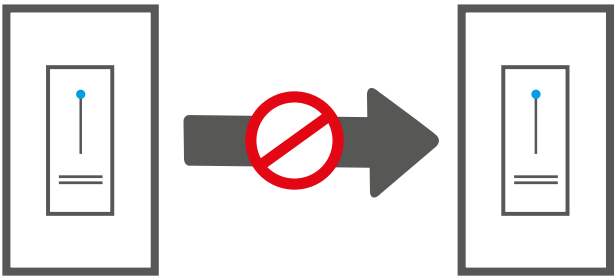
Una soluzione d'accesso ad impronta digitale ekey può essere manipolata dall'esterno per aprire la porta?

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 un'area interna protetta. Per il resto, il sistema non può essere manipolato nemmeno da Internet poiché non vi è connesso.



Il sistema può essere manomesso 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. In seguito vengono creati dei dati utente che, una volta salvati assieme al numero di serie del dispositivo, non possono essere trasferiti ad altri apparecchi. In caso di sostituzione, la centralina di comando e il lettore d'impronta digitale devono essere resettati sulle impostazioni di fabbrica e nuovamente accoppiati. A tale scopo occorre accedere all'area interna protetta dove si trova la centralina di comando. In più si devono ricreare tutti i dati utente.



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

Per l'instaurazione della connessione tra smartphone/tablet, lettore d'impronta digitale e centralina di comando viene applicato un procedimento di accoppiamento sicuro denominato "Bluetooth Secure Simple Pairing". I dati vengono trasmessi tra gli apparecchi esclusivamente in forma cifrata.

Cosa succede se perdo il mio smartphone/tablet?

Per aprire l'app è necessario un codice di sicurezza composto da 4 fino a 6 caratteri. In questo modo l'app non può essere avviata da persone non autorizzate.

In caso di smarrimento dello smartphone/tablet, la connessione con il lettore d'impronta digitale può essere ripristinata da un altro smartphone o tablet utilizzando l'ekey home app e il codice di accoppiamento amministratore configurato.

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

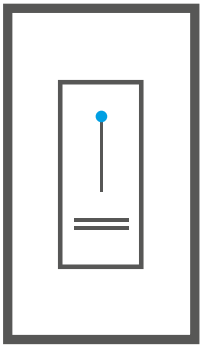
No. Nel suo sistema ekey non ha salvato alcuna possibilità di apertura da parte di un tecnico (tramite codice di fabbrica, ecc.). Il proprietario (e anche amministratore) è l'unica persona che può ripristinare le impostazioni di fabbrica del sistema utilizzando un codice amministratore a 6 caratteri da lui stesso definito.

Esiste una copertura assicurativa nel caso delle soluzioni d'accesso ad impronta digitale?

Ai fini della copertura assicurativa è irrilevante sapere se l'attivazione del blocco è meccanica (con chiave) piuttosto che elettronica (con impronta digitale). In generale, le assicurazioni rispondono solamente quando un accesso è regolarmente bloccato. Se una porta è chiusa solo con lo scrocco, viene considerata come non bloccata.

Tutte le attività sul lettore d'impronta digitale vengono registrate in un log eventi?

Il sistema ekey home – Soluzioni per un singolo accesso non prevede un registro degli accessi. Per le soluzioni ekey multi ed ekey net invece, ekey offre un registro degli accessi consultabile solo dall'amministratore per ogni lettore d'impronta digitale. Vengono registrati anche i tentativi di accesso di persone non autorizzate.



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 ANNI DI GARANZIA

Il prolungamento della garanzia è un'iniziativa volontaria per un'ampliamento prestazionale, perché siamo convinti che i prodotti ekey sono fatti per durare nel tempo. I pregiati componenti e gli approfonditi controlli di produzione, lavorazione e funzionamento sono sinonimo di qualità, funzionalità, durata e sicurezza e forniscono la garanzia di avere acquistato il prodotto migliore sul mercato.

3 + 2 = 5 ANNI DI GARANZIA!

Siamo certi della qualità dei nostri prodotti, per tale ragione offriamo al cliente la possibilità di prolungare ulteriormente di 2 anni la GARANZIA triennale di ekey.

Come usufruire della garanzia?
Per usufruire dell'intera GARANZIA DI 5 ANNI offerta da ekey, è sufficiente registrare il prodotto online entro 4 settimane dalla data di acquisto su
www.ekey.net/it_IT/garanzia/

SPIEGAZIONE DEI TERMINI

Fake finger (in italiano: “dito falsificato“)
Ricostruzione, imitazione o anche falsificazione di un dito.

Porta “chiusa solo con lo scrocco“
Scrocco: parte della serratura che mantiene la porta in posizione di chiusura all’interno della sua cornice.

Template
Modello utilizzato nell‘elaborazione elettronica dei dati.

GCO
Gruppo di continuità: dispositivo che viene utilizzato per continuare ad alimentare corrente in caso di guasti. Il GCO viene inserito nella linea elettrica degli impianti o dei dispositivi da proteggere.

Accoppiare
Collegare due elementi sistematicamente in modo che possano successivamente comunicare tra loro.

YOUR FINGER. YOUR KEY.

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 90696 - 0
E: office@ekey.net

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

Regione Adriatica 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 Copernico 13/A
I-39100 Bolzano
T: +39 0471 922712
E: italia@ekey.net

Made in Austria

www.ekey.net