

disponibili e non è mai stata compromessa.

Il PIN viene visualizzato una volta, dopodiché non può più essere recuperato da nessuno, nemmeno da Salto KS. Se l'utente dimentica il PIN, sarà necessario generarne uno nuovo.

3. CREDENZIALI SMART KEY TAG

Un tag è un dispositivo fisico (portachiavi senza contatto) che funziona in base all'identificazione a radiofrequenza (RFID). La nostra etichetta non contiene batterie e presenta un design robusto e resistente per garantire che non dovrà mai preoccuparsi della loro durata fisica.

Il Tag contiene informazioni memorizzate elettronicamente che sono protette con MIFARE® DESFire EV2, rendendo implausibili la copia o l'hacking dei transponder. Eseguiamo test di sicurezza regolari per garantire che i nostri tag rimangano protetti contro attacchi comuni come la copia delle credenziali.

4. IQ

L'IQ è l'hub centrale, noto anche come il "cervello" del sistema Salto KS. Riceve tutte le modifiche e le impostazioni dall'applicazione Salto KS e garantisce che tutti i blocchi vengano aggiornati in pochi secondi. La distanza massima dall'IQ alla serratura intelligente elettronica è di 10 metri.

Tutti i comandi remoti che influenzano le comunicazioni dirette tra l'IQ e l'hardware sono protetti con un OTP (One Time Password). Questi comandi aderiscono alla stessa crittografia end-to-end della funzione Chiave digitale.

5. COMUNICAZIONI ZIGBEE

ZigBee viene utilizzato principalmente per la comunicazione bidirezionale tra un sensore e un sistema di controllo. ZigBee è una comunicazione a corto raggio e offre connettività fino a 100 metri simile a Bluetooth e Wi-Fi.

Basato su ZigBee, un protocollo di crittografia garantisce che qualsiasi comunicazione tra l'IQ e altro hardware rimanga sicura. Dopo che una nuova serratura si è connessa a un IQ per la prima volta, memorizzerà un parametro crittografato che impedirà le connessioni a qualsiasi altro dispositivo diverso dall'IQ associato.

6. BLOCCHI INTELLIGENTI BLUETOOTH

Bluetooth Low Energy è progettato per ridurre il consumo energetico rispetto al normale Bluetooth. BLE offre diverse funzioni per proteggere la comunicazione tra i dispositivi. Quando l'IQ avvia la connessione con la serratura, inizia un processo di accoppiamento in cui i due dispositivi scambiano le informazioni necessarie per creare la connessione crittografata. Una volta completato il processo di accoppiamento, alla serratura verrà impedito di creare una connessione con qualsiasi altro dispositivo diverso dall'IQ associato.

Ogni dispositivo BLE viene identificato utilizzando un indirizzo del dispositivo. Questi indirizzi sono simili agli indirizzi MAC utilizzati in altri protocolli di comunicazione. Le serrature BLE sono altamente sicure poiché utilizzano chiavi crittografiche per sbloccare.

7. IQ - CLOUD

L'IQ collega le serrature wireless al cloud tramite:

- › Connessione cellulare globale (tramite USB)
- › Wi-Fi
- › Cavo Ethernet (disponibili versioni compatibili PoE)

La comunicazione predefinita tra l'IQ e il KS Core API è protetta e applicata con protocolli di crittografia avanzati. La comunicazione tra l'IQ e il backend KS viene autenticata in base al certificato x509 (uno standard che determina gli accordi per i certificati a chiave pubblica).

Tutti i dati che viaggiano all'interno di questo tunnel TLS sono crittografati. Infatti, non ci sono dati che viaggiano al di fuori di questo tunnel. In assenza di certificazione, non è possibile impersonare l'IQ o il KS Core API. In altre parole, diventa improbabile eseguire attacchi MITM (man-in-the-middle). Durante le nostre verifiche sicurezza esterne, la sicurezza delle comunicazioni viene sempre valutata per garantire di rimanere aggiornati e di utilizzare sempre gli standard del settore

8. CLOUD > WEB, MOBILE, APERTURA REMOTA

L'app mobile e l'interfaccia web di Salto KS Le consentono di gestire l'accesso alle Sue sedi da qualsiasi luogo. Tutto l'hardware viene gestito tramite un'app/un'interfaccia web. Può trattarsi di un'integrazione personalizzata, in cui è possibile utilizzare la propria interfaccia utente, o di una soluzione pronta come Salto KS. Utilizziamo le migliori pratiche del settore per garantire che il processo di accesso alle nostre app sia sicuro, tra cui l'autenticazione a più fattori e le funzionalità di gestione delle sessioni.

Disclaimer:

This is a downloadable version of the website content that we make available to you for informative purposes for an easier consultation and filling. However, SALTO assumes no responsibility for any errors or typos that the downloadable version may contain.

As SALTO reserves the right to modify this content from time to time, please check on the Legal section of our website to find the latest version of the legal documents and their updates.