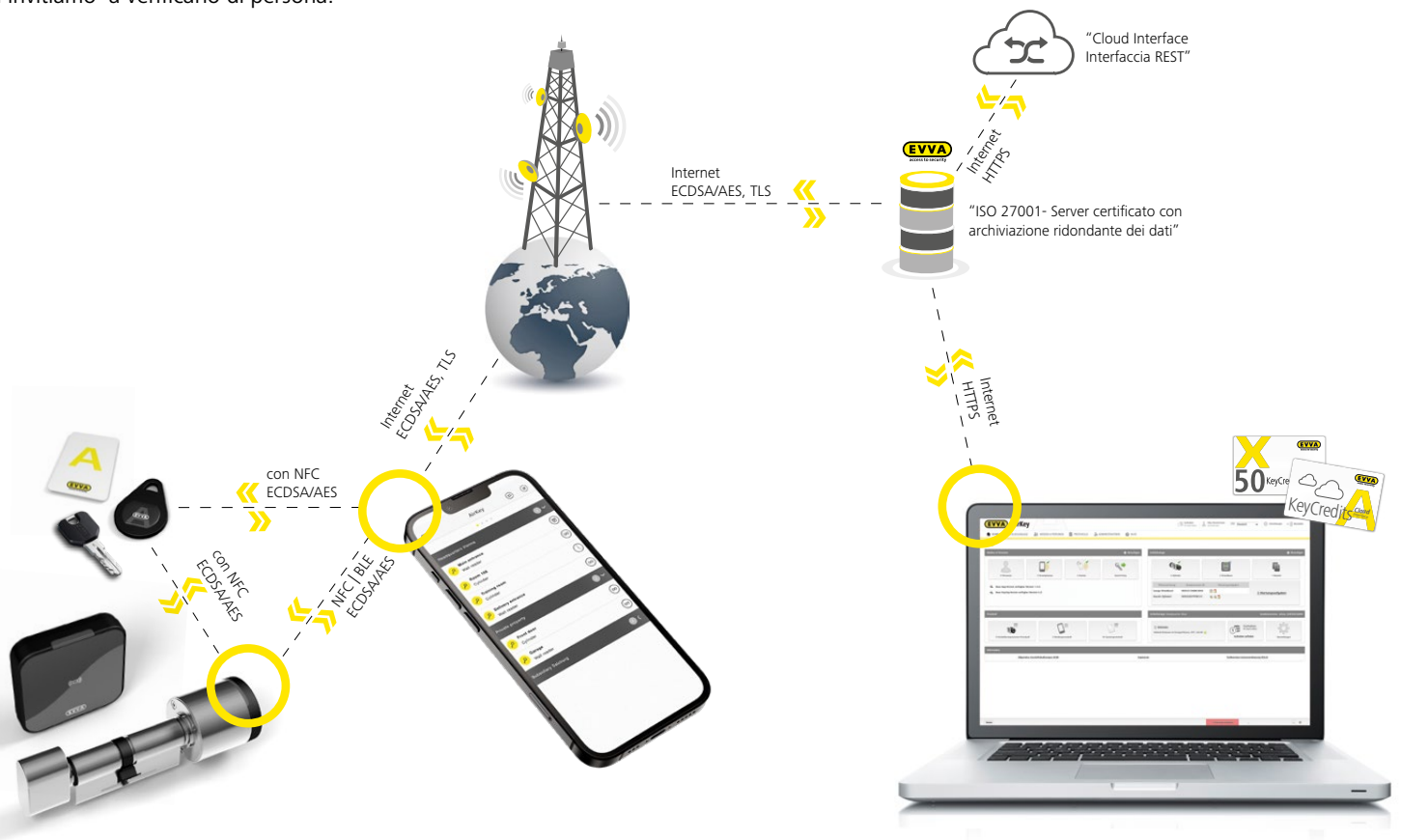




# AirKey. Semplicemente sicuro, senza compromessi

## L'architettura di sicurezza AirKey in dettaglio

L'architettura di AirKey non accetta compromessi quando si tratta di garantire la massima sicurezza. Questo impegno è stato la chiave del nostro successo ed è stato fondamentale per trasformare la nostra azienda, fondata nel 1919, in una delle principali imprese nel settore della sicurezza a livello globale. Non siamo mai scesi a compromessi nemmeno nell'implementazione del concetto di sicurezza di AirKey. Abbiamo affidato lo sviluppo di questo prodotto di punta esclusivamente ai massimi esperti nei settori della meccanica, dell'elettronica e del software, garantendo così che AirKey sia uno dei sistemi di accesso elettronico più sicuri disponibili sul mercato. Vi invitiamo a verificarlo di persona.



# Sicurezza meccanica senza compromessi

Già nella versione standard, il cilindro AirKey vanta le seguenti caratteristiche di massima sicurezza meccanica.



## Certificazioni ottenute

- › EN 15684 (1.6.B.3.A.F.3.2)
- › SKG\*\*\*
- › SSF3522 per profili scandinavi
- › Certificazione antincendio EN 1634 (90 min)
- › Certificazione antipanico EN 179/1125
- › ÖNORM B 5351:2011 WMZ6-BZ
- › Certificato di conformità UE ai sensi dell'allegato III della direttiva 2014/53/UE

## Protezione dagli agenti ambientali

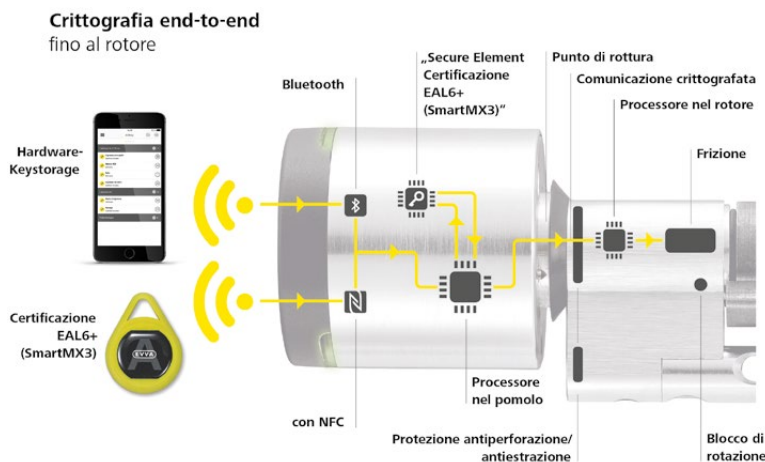
- › Protezione IP65 del prodotto montato contro la penetrazione di polveri dannose e forti getti d'acqua provenienti da qualunque direzione
- › Componenti elettronici rivestiti di vernice protettiva contro l'ossidazione da acqua di condensa
- › Condizioni d'impiego: -20°C - +55°C; 2 batterie al litio CR2 poste in parallelo per una maggiore stabilità di alimentazione

## Sicurezza fisica

- › Protezione antiperforazione
- › antiestrazione
- › Blocco di rotazione antieffrazione con un mandrino ad alta frequenza
- › Punto di rottura definito sul filetto del pomolo esterno per proteggere il rotore da attacchi meccanici e prevenire i tentativi di snapping
- › Speciale utensile meccanico per il montaggio e lo smontaggio del pomolo del cilindro

# Sicurezza elettronica senza compromessi

Le misure di sicurezza elettronica nel sistema AirKey prevengono l'uso improprio dei segnali e/o del materiale crittografato dell'elemento di identificazione.



## 1. Architettura centrale di sicurezza

- › Tutti i componenti AirKey sono provvisti di un ulteriore processore in una zona sicura che gestisce l'apertura. Il pomolo del cilindro AirKey, ad esempio, è protetto a livello crittografico da un processore integrato nel rotore del cilindro **posizionato dietro la protezione anti-trapano**, che non consente la sostituzione del pomolo del cilindro e, quindi, un accesso non autorizzato.
- › Con l'impiego di **Secure Elements certificati EAL6+** (elementi di memorizzazione e crittografia dotati della massima sicurezza) in ogni componente AirKey, EVVA impone un nuovo standard di sicurezza per i sistemi di chiusura elettronici.
- › Come elementi di identificazione, sui prodotti AirKey sono utilizzate esclusivamente **smartcard NFC** dotate della massima sicurezza certificata EAL6+.  
La copia non autorizzata degli elementi di identificazione è quindi impossibile.  
Questo standard di sicurezza elevato fa sì che questa tecnologia sia utilizzata **anche per i passaporti elettronici** e le carte di credito.
- › **Crittografia end-to-end per tutte le interfacce**
  - Sono utilizzati esclusivamente cifrari testati e certificati
  - In **tutte** le trasmissioni dati AirKey utilizza anche una **doppia** crittografia:
    - **ECDSA-224** per l'autenticazione
    - **AES-128** per le chiavi di sessione
- 8• L'algoritmo ECDSA si basa sulle curve ellittiche e viene utilizzato per l'autenticazione tra i diversi componenti AirKey. In base all'autenticazione ECDSA viene assegnata ogni volta **una chiave di sessione AES casuale**, che viene utilizzata solo **per la transazione attuale** (attualizzazione, blocco, update cilindro, update scheda ecc.). Questo metodo viene impiegato in tutte le comunicazioni tra i componenti di AirKey.

- › **Tutti i dati trasmessi sono crittografati end-to-end:**
  - Dagli elementi di identificazione AirKey ai componenti di chiusura AirKey (ECDSA / AES)
  - Dai componenti di chiusura AirKey all'app AirKey (ECDSA / AES)
  - Dall'app AirKey agli elementi di identificazione AirKey (ECDSA / AES)
  - Dall'app AirKey al sistema di gestione online (ECDSA / AES)

## 2. Backend e sistema di gestione online

### Sistema di gestione online

- › L'accesso via Web è protetto mediante **crittografia TLS** (HTTPS)
- › Nel creare la propria password, viene verificata la sua robustezza per poterne determinare il livello di sicurezza.
- › **Autenticazione a 2 fattori con TAN tramite e-mail o SMS**, per amministratori attivabile opzionalmente (TAN alfanumerico a 6 cifre)
- › Invio automatico di attività di manutenzione e informazioni di sicurezza (blacklist) agli amministratori via e-mail o all'app AirKey per i tecnici manutentori.

### Backend

- › In Austria AirKey si avvale di centri di dati certificati ISO 27001. Tutti i dati sono salvati sui server sicuri e ridondanti di EVVA Austria.
- › **I moduli HMS** (Hardware Security Modules) certificati **EAL6+** assicurano nel backend la massima sicurezza nella creazione e il salvataggio di tutte le chiavi crittografiche.

## 3. App Android e iOS per AirKey

Per utilizzare AirKey con lo smartphone, con l'app AirKey EVVA propone un **concetto di sicurezza multilivello**:

- › EVVA consiglia agli utenti di uno smartphone di attivare la **crittografia della memoria** e di proteggere il blocco dello schermo con una **password, un PIN o un login biometrico** adeguatamente sicuri.
- › Sia Android che iOS utilizzano moduli di memoria di sicurezza hardware specifici del produttore. (Android: Keystore supportato da hardware; iOS: Apple CryptoKit KeyChain)
- › L'app AirKey offre inoltre un'ulteriore funzione di sicurezza, ovvero un **codice PIN supplementare** nell'app da inserire prima di ogni procedura di apertura.
- › L'amministratore vede se la funzione PIN-Code nell'app è attivata o disattivata.
- › L'amministratore può impostare se la modalità vivavoce possa essere utilizzata anche senza blocco del display.
- › Lo smartphone può essere utilizzato **"solo" come chiave** oppure anche **come dispositivo di manutenzione**. Questa funzione può essere gestita dall'amministratore.
- › **Sicurezza automatica:** Dopo l'apertura con Bluetooth vengono aggiornate automaticamente la blacklist, le voci di registro di tutti gli elementi di identificazione e l'ora. L'archiviazione viene eseguita automaticamente ogni sei ore oppure, a seconda delle impostazioni nel sistema di gestione online, anche dopo ogni procedura di apertura.

## 4. Protezione e sicurezza dei dati

- › **AirKey è conforme al Regolamento generale sulla protezione dei dati dell'UE:** insieme al rinomato esperto in materia di protezione dei dati, il Dr. Christof Tschol, AirKey è stato trasformato in un sistema di accesso conforme alle norme. Il nostro responsabile interno della protezione dei dati è a disposizione per eventuali domande specifiche. <https://www.evva.com/at-de/datenschutzerklaerung/>
- › La cancellazione dei dati personali richiesta dal Regolamento generale sulla protezione dei dati è prevista nel sistema. Ogni riferimento personale viene rimosso e non può più essere recuperato.
- › La registrazione degli eventi di accesso può essere configurata e anche disattivata in modo specifico per ogni componente (anche a tempo determinato), ad es. per una sala riunioni del consiglio di fabbrica in cui non è consentita alcuna registrazione.
- › La **registrazione** nel backend e nei componenti è **a prova di revisione**. Ciò significa che è possibile tracciare esattamente ogni processo di apertura con la data e l'ora. Questa registrazione non può dunque essere manomessa e consente una maggiore trasparenza rispetto a qualsiasi sistema di chiusura meccanico.
- › Predisposto per essere conforme alla legge europea sui dati ("Data Act 2024")
- › È possibile attivare la funzione di doppio controllo per la visualizzazione dei registri. In questo modo la visione dei registri deve essere autorizzata da un secondo amministratore.

## Riassunto

- › AirKey è il sistema di accesso flessibile e ultrasicuro che soddisfa l'RGPD e che, con tecnologie all'avanguardia in termini di crittografia, elettronica, firmware, software e meccanica, assicura la sicurezza dei sistemi di chiusura AirKey di EVVA attraverso l'impiego di Secure Elements, HSM e smartcard NFC.
- › Il BSI/NIST <https://www.keylength.com/en/4/> conferma che i sistemi di crittografia impiegati e le lunghezze delle chiavi sono considerati sicuri fino al 2030. Come già avvenuto nel 2023, EVVA potrà aumentare, se necessario, le lunghezze delle chiavi all'interno del sistema in modo tale di mantenere anche nel futuro il livello di sicurezza aggiornato allo stato dell'arte. È questo il grande vantaggio dei media JCOP, delle app e dei Secure Elements nei componenti di chiusura AirKey che, essendo aggiornabili, assicurano anche la massima sicurezza dell'investimento.