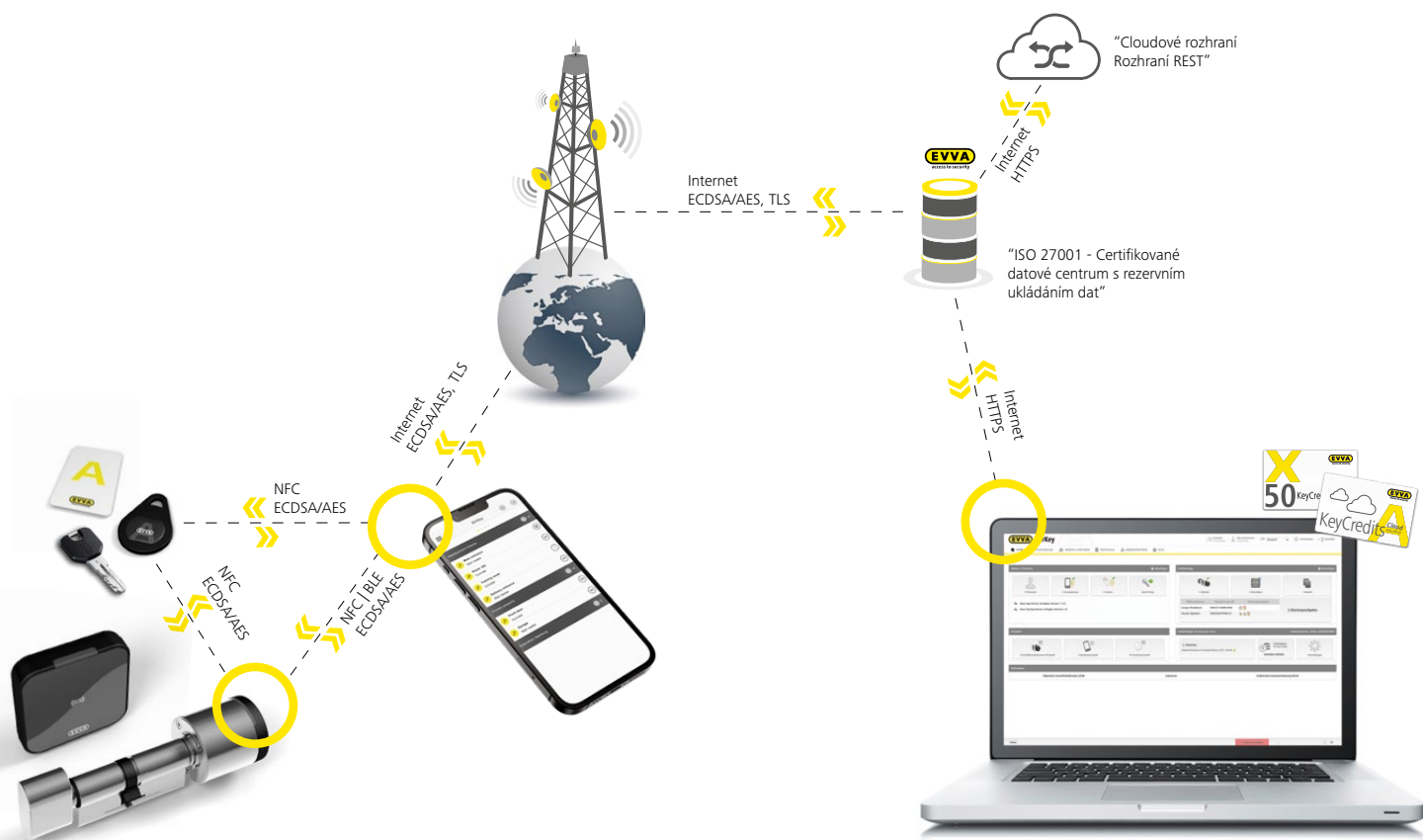




# AirKey. Nekompromisní bezpečnost

## Bezpečnostní architektura AirKey v detailu

Společnost EVVA nedělá žádné kompromisy, pokud jde o bezpečnost. A tak je to správné. Jak jinak bychom se mohli vyvinout v jednu z nejuspěšnějších bezpečnostních firem na světě, od založení společnosti v roce 1919! Při implementaci bezpečnostní koncepce AirKey jsme byli rovněž nekompromisní. Vývojem AirKey byli pověřeni pouze špičkoví bezpečnostní odborníci z oblasti mechaniky, elektroniky a softwaru. Díky tomu je AirKey jedním z nejbezpečnějších elektronických přístupových systémů na trhu. Přesvědčte se sami.



## Nekompromisní mechanické zabezpečení

Již standardní verze cylindrické vložky AirKey má následující nejbezpečnější prvky.

### Úspěšné certifikace

- › EN15684 (1.6.B.3.A.F.3.2)
- › SKG\*\*\*
- › SSF3522 pro skandinávské profily
- › Certifikace požární ochrany EN1634 (90 min)
- › Paniková certifikace EN179/1125
- › ÖNORM B 5351:2011 W<sub>MZ</sub>6-BZ
- › Certifikát EU přezkoušení typu podle přílohy III směrnice 2014/53/EU

### Ochrana před vlivy prostředí

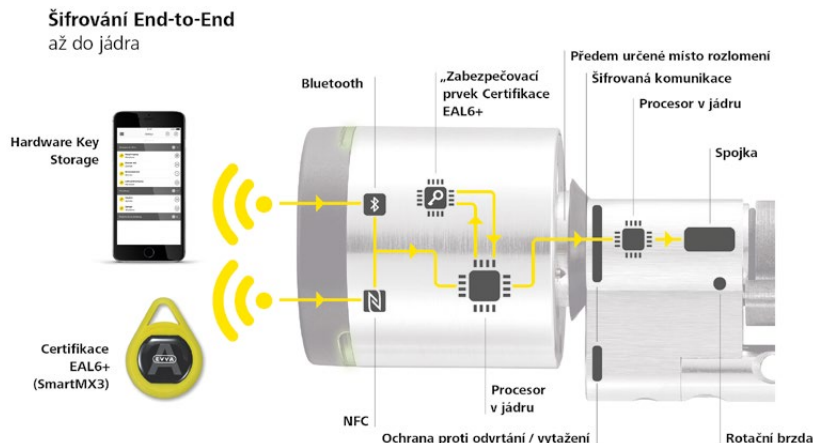
- › Ochrana IP65 proti vniknutí škodlivého prachu a silným proudům vody odkudkoliv při instalaci
- › Elektronika s ochranným lakem proti oxidaci kondenzovanou vodou
- › Provozní podmínky: -20°C - +55°C; 2 lithiové baterie CR2 paralelně pro vyšší stabilitu napájení

### Fyzická bezpečnost

- › Ochrana proti odvrtání
- › Ochrana proti vytažení jádra
- › Rotační brzda proti napadení vysokootáčkovým vřetenem
- › Definovaný bod zlomu na závitě vnějšího knoflíku pro ochranu jádra před mechanickými útoky a pro zabránění napadení
- › Speciální mechanický nástroj pro montáž a demontáž knoflíku cylindrické vložky

## Nekompromisní elektronické zabezpečení

**Elektronická bezpečnostní opatření v systému AirKey** zabraňují zneužití signálů a / nebo materiálu kryptografických klíčů.



### 1. Centrální architektura bezpečnosti

- › Pro všechny komponenty AirKey je v bezpečné vzdálenosti ještě další procesor, který řídí uvolnění, např.: knoflík cylindrické vložky AirKey je kryptograficky zajištěn procesorem zabudovaným do jádra cylindrické vložky, který **je umístěn za ochranou proti odvrtání** - výměna knoflíku cylindrické vložky a s tím spojený neoprávněný přístup není možný.
  - › Použitím **zabezpečených prvků certifikovaných EAL6+** (vysoce zabezpečené prvky šifrování a ukládání) v každé součásti AirKey představuje společnost EVVA nový bezpečnostní standard pro elektronické uzamykací systémy.
  - › AirKey používá jako identifikační médium pouze vysoce bezpečné EAL6+ čipové karty **NFC**. Neautorizované kopírování identifikačních médií není možné. Díky těmto vysokým bezpečnostním standardům se tato technologie **používá také pro elektronické cestovní pasy** a kreditní karty.
  - › **Šifrování End-to-End napříč všemi rozhraními**
    - Používají se pouze testované a certifikované metody šifrování
    - AirKey pro **všechny** datové přenosy používá **dvojitě** šifrování:
      - **ECDSA-224** pro ověření
      - **AES-128** pro klíče relace
    - Algoritmus ECDSA je založen na eliptických křivkách a používá se k autentizaci mezi různými komponenty AirKey.
- Na základě autentizace ECDSA se pokaždé **sjedná náhodný klíč relace AES**, který se použije pouze **pro aktuální transakci** (aktualizace, zámky, aktualizace cylindrické vložky, aktualizace karet atd.). Tento postup se používá pro veškerou komunikaci mezi komponenty AirKey.

- › **Všechna přenášená data jsou šifrována od začátku do konce:**
  - Identifikační média AirKey pro uzamykací komponenty AirKey (ECDSA / AES)
  - Uzamykací komponenty AirKey pro aplikaci AirKey (ECDSA / AES)
  - Aplikace AirKey pro identifikační média AirKey (ECDSA / AES)
  - Aplikace AirKey pro online správu AirKey (ECDSA / AES)

## 2. Backend a online správa

### Online správa

- › Online přístup je zabezpečen pomocí **šifrování TLS** (HTTPS)
- › Při vytváření hesla se hodnotí jeho síla, aby bylo možné posoudit bezpečnost.
- › Volitelně lze aktivovat 2faktorové ověřování pomocí TAN prostřednictvím e-mailu nebo SMS pro správce (6místný alfanumerický TAN)
- › Automatické odesílání úkonů údržby a bezpečnostních informací (černých listin) správcům e-mailem, nebo pro techniky údržby v aplikaci AirKey.

### Backend

- › Systém AirKey běží v datových centrech certifikovaných podle ISO:27001 v Rakousku. Všechna data jsou uložena na vlastních rezervně zabezpečených serverech společnosti EVVA v Rakousku.
- › **Hardwarové bezpečnostní moduly (HSMs)** s certifikací EAL6 + zajišťují nejvyšší bezpečnost při vytváření a ukládání všech šifrovacích klíčů v backendu.

## 3. AirKey aplikace pro Android a iOS

Pro použití AirKey ve spojení se smartfonem nabízí EVVA s aplikací AirKey **vícetupňový bezpečnostní koncept:**

- › Společnost EVVA doporučuje, aby každý uživatel smartphonu **aktivoval šifrování úložiště** a zabezpečil zámek obrazovky pomocí bezpečného **hesla, PINem nebo biometrickým přihlášením**.
- › Android i iOS používají hardwarové bezpečnostní paměťové moduly specifické pro výrobce. (Android: Hardware-backed Keystore; iOS: Apple CryptoKit KeyChain)
- › Jako další bezpečnostní funkce nabízí aplikace AirKey také **další PIN kód** v aplikaci, který musí být zadán před každým uzamykáním.
- › Správce může zjistit, zda je funkce PIN kódu v aplikaci aktivována nebo deaktivována.
- › Správce může nastavit, zda lze režim handsfree použít i bez zámku obrazovky.
- › Smartphone lze **použít „pouze“ jako klíč** nebo také **jako zařízení pro údržbu**. To může řídit správce.
- › **Automatické zajištění bezpečnosti:** Po uzamčení přes Bluetooth se automaticky aktualizuje seznam zakázaných položek, protokolové záznamy ze všech identifikačních médií a čas. To se děje automaticky každých 6 hodin nebo po nastavení v online správě také po každém uzamykání.

## 4. Ochrana a bezpečnost dat

- › **AirKey splňuje nařízení EU o ochraně osobních údajů.:** Ve spolupráci s uznávaným odborníkem na ochranu osobních údajů Dr. Christofem Tschohlem byl systém AirKey vyvinut, aby odpovídal nejpřísnějším nárokům na zabezpečení údajů. V případě dotazů na podrobnosti je vám k dispozici náš pracovník na ochranu údajů. <https://www.evva.com/at-de/datenschutz/erklaerung/>
- › V systému se předpokládá smazání osobních údajů požadované základním nařízením o ochraně údajů. Všechny osobní údaje jsou nenávratně odstraněny.
- › Protokolování přístupů lze individuálně konfigurovat pro každou komponentu (také po omezenou dobu), stejně jako deaktivovat. např. pro zasedací místnost zaměstnanců, kde není povoleno protokolování.
- › **Protokolování** v backendu a v komponentách je **revizně bezpečnostní**. To znamená, že každé blokování lze sledovat s přesným datem a časem. S tímto protokolováním nelze manipulovat a umožňuje větší transparentnost než u jakéhokoli mechanického uzamykacího systému.
- › Připraveno tak, aby vyhovovalo evropskému datovému zákonu v roce 2024
- › Lze aktivovat princip čtyř očí pro prohlížení protokolů. Přístup k protokolům musí schválit druhý správce.

## Shrnutí

- › AirKey je vysoce bezpečný a flexibilní přístupový systém, který splňuje jak GDPR, tak i nejnovější technologie v kryptografii, elektronice, firmwaru, softwaru a mechanice, a to pomocí zabezpečovacích prvků, HSMs a NFC smart cards k zajištění bezpečnosti uzamykacích systémů EVVA AirKey.
- › BSI/NIST <https://www.keylength.com/en/4/> potvrzuje, že použité metody šifrování a délky klíčů jsou považovány za bezpečné do roku 2030. Délky klíčů v systému lze v případě potřeby u společnosti EVVA prodloužit, což bylo úspěšně provedeno v roce 2023, aby byla do budoucna zachována nejmodernější úroveň zabezpečení. To je velká výhoda médií JCOP, aplikací a zabezpečovacích prvků JCOP v uzamykacích komponentách AirKey a díky možnosti aktualizace také zajišťuje maximální bezpečnost investic.