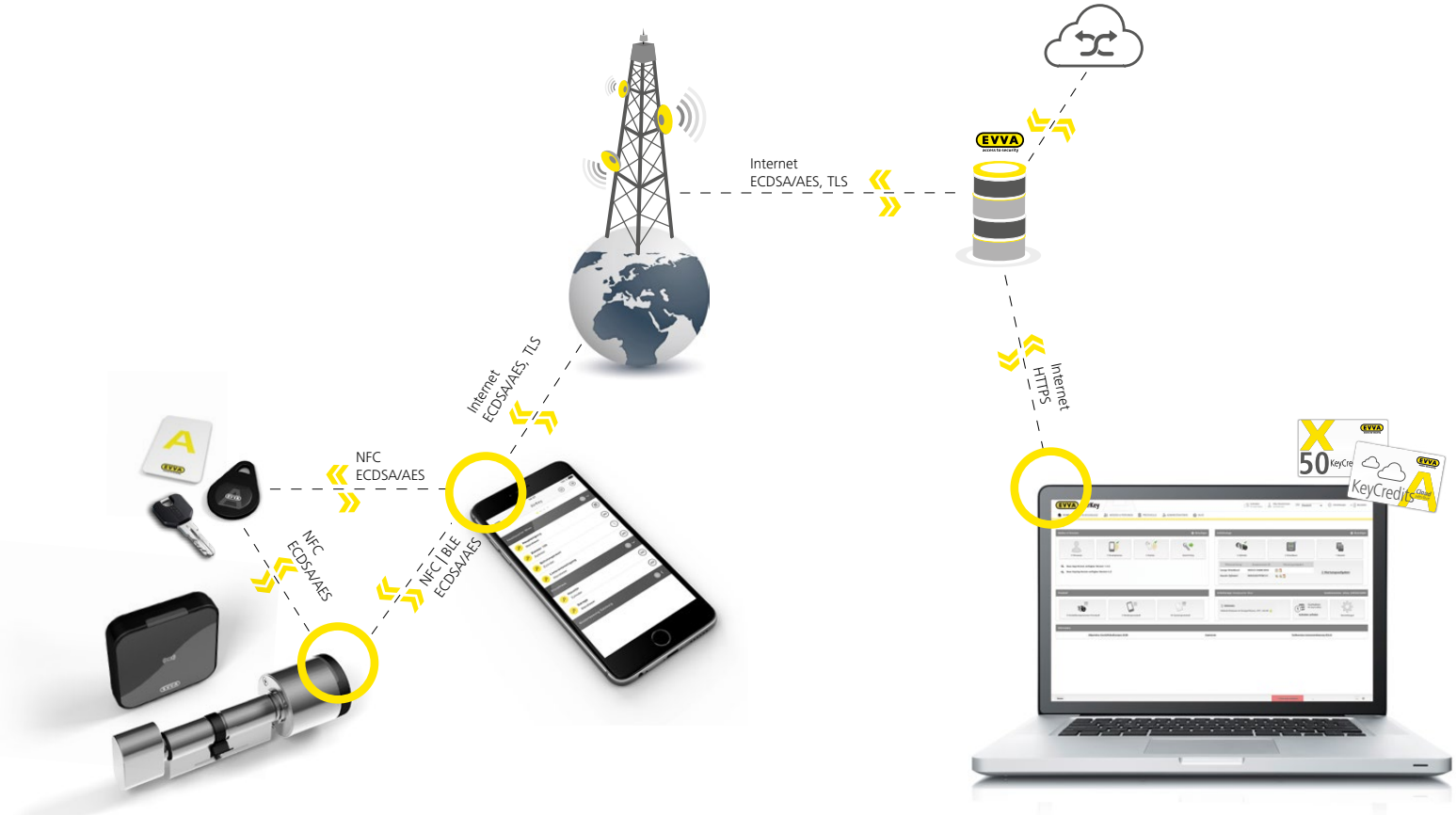
AirKey. Jednoducho nekompromisná bezpečnosť

Detailný prehľad bezpečnostnej architektúry AirKey

Keď ide o bezpečnosť, EVVA nerobí žiadne kompromisy. A tak je to správne. Inak by sa nám nepodarilo vypracovať sa od svojho založenia v roku 1919 na jednu z najúspešnejších spoločností poskytujúcich bezpečnostné systémy na svete. Rovnakú nekompromisnosť sme preukázali aj pri nasadení bezpečnostného konceptu AirKey. Na vývoji AirKey sa podieľali len špičkoví experti v oblasti mechaniky, elektroniky a softvéru. Vďaka tomu je AirKey jeden z najbezpečnejších elektronických prístupových systémov na trhu.
Presvedčiť sa o tom môžete sami.



Nekompromisné mechanické zabezpečenie

Už štandardné vyhotovenie cylindrickej vložky EVVA AirKey poskytuje najvyššie bezpečnostné vlastnosti mechanického systému.

Získané certifikácie

- EN15684 (1.6.B.3.A.F.3.2)
- SKG***
- SSF3522 pre škandinávske profily
- EN1634 certifikácia protipožiarnej ochrany (90 minút)
- EN179/1125 certifikácia protipanikovej funkcie
- ÖNORM B 5351:2011 W_{MZ}6-BZ

Ochrana pred poveternostnými vplyvmi

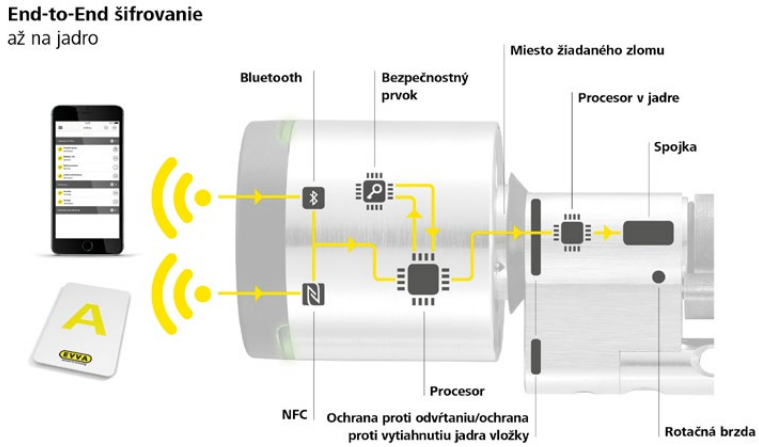
- IP65 ochrana proti vniknutiu škodlivého prachu a silného prúdu vody zo všetkých smerov v zabudovanom stave
- Elektronika s nano povrchovou úpravou proti oxidácii v dôsledku kondenzujúcej vody
- Podmienky použitia: –20 °C až +55 °C; 2 paralelne zapojené batérie na vyššiu stabilitu napájania

Fyzické zabezpečenie

- Ochrana proti odvŕtaniu
- Ochrana proti vytiahnutiu jadra vložky
- Rotačná brzda proti zásahom vysokofrekvenčným vretenom
- Definované miesto žiadaného zlomu na závite vonkajšieho gombíka na ochranu jadra pred mechanickými zásahmi a zabránenie útokom rozlomením
- Mechanické špeciálne náradie na montáž a demontáž cylindrickej vložky

Nekompromisné elektronické zabezpečenie

Elektronické bezpečnostné opatrenia v systéme AirKey zabraňujú tomu, aby bolo možné zneužiť signály alebo kryptografický materiál kľúčov.



1. Centrálna bezpečnostná architektúra

- Všetky komponenty AirKey majú ďalší procesor v zabezpečenej oblasti, ktorý riadi sprístupnenie.
  Napr.: Cylindrická vložka AirKey-je kryptograficky zabezpečená procesorom vstavaným v cylindrickom jadre, ktorý **sa nachádza za ochranou proti odvŕtaniu**. Výmena cylindrickej vložky a s tým spojený neoprávnený prístup teda nie sú možné.
- Vďaka používaniu **bezpečnostných prvkov s certifikáciou EAL5+** (vysoko bezpečné šifrovacie a pamäťové prvky) v každom komponente AirKey stanovuje spoločnosť EVVA nový bezpečnostný štandard pre elektronické uzamykacie systémy.
- V rámci systému AirKey sa ako identifikačné médiá využívajú výlučne vysoko bezpečné **karty NFC-Smartcard** s certifikáciou EAL5+.
  Vďaka tomu nie je možné neoprávnené kopírovanie identifikačných médií.
  Vzhľadom na tento vysoký bezpečnostný štandard sa táto technológia používa **aj v elektronických cestovných pasoch** a kreditných kartách.
- End-to-End šifrovanie vo všetkých rozhraniach
  - Používajú sa výhradne testované a certifikované metódy šifrovania
  - Pritom sa v rámci systému AirKey používa pri **všetkých** prenosoch údajov **dvojité** šifrovanie:
    - **ECDSA-224** na overovanie
    - **AES-128** pre kľúče relácií
  - Algoritmus ECDSA je založený na eliptických krivkách a používa sa overovanie medzi jednotlivými komponentami AirKey. Na základe overenia ECDSA sa vždy vydá **náhodný kľúč relácie AES**, ktorý sa použije len **na aktuálnu transakciu** (aktualizácia, uzamknutie, aktualizácia cylindrickej vložky, aktualizácia kariet a pod.). Táto metóda sa využíva pri každej komunikácii medzi komponentami AirKey.

Všetky prenášané údaje majú šifrovanie end-to-end:

- Identifikačné médiá AirKey voči uzamykacím komponentom AirKey (ECDSA/AES)
- Uzamykacie komponenty AirKey voči aplikácii AirKey (ECDSA/AES)
- Aplikácia AirKey voči identifikačným médiám AirKey (ECDSA/AES)
- Aplikácia AirKey voči online správe AirKey (ECDSA/AES)

2. Backend a online správa

Online správa

- Prístup cez web je zabezpečený pomocou **šifrovania TLS** (https)
- Pri vytváraní hesla sa vyhodnocuje jeho sila, ktorá udáva mieru jeho bezpečnosti.
- **Dvojfaktorové overovanie pomocou SMS TAN** je možné voliteľne aktivovať pre správcov (6-miestny alfanumerický kód TAN)
- Automatické odosielanie údržbových úloh a bezpečnostných informácií (čierne listiny) správcom cez e-mail alebo technikom údržby v aplikácii AirKey.

Backend

- Údaje sú uložené **vo vlastných počítačových centrách EVVA v Rakúsku, ktoré prevádzkuje a zabezpečuje spoločnosť EVVA**.
- **EAL5+** certifikované **hardvérové bezpečnostné moduly (HSM)** zabezpečujú v Backende najvyššiu mieru bezpečnosti pri vytváraní a ukladaní všetkých kľúčov šifrovania.

3. Aplikácia AirKey pre Android a iOS

Na použitie systému AirKey so smartfónom poskytuje EVVA v rámci aplikácie AirKey **viacstupňový koncept zabezpečenia**:

- EVVA odporúča každému používateľovi smartfónu aktivovať si **šifrovanie pamäti** a vybaviť zablokovanie obrazovky dostatočne silným **heslom, kódom PIN alebo prihlásením pomocou biometrických údajov**.
- Aplikácia AirKey poskytuje ako ďalšiu funkciu zabezpečenia **doplňujúci kód PIN** v aplikácii, ktorý je nutné zadať pred každým procesom odomknutia.
- Správca vidí, či je funkcia PIN kódu v aplikácii aktivovaná alebo dezaktivovaná.
- Správca môže nastaviť, či sa smie používať režim Handsfree aj bez zablokovania obrazovky.
- Smartfón sa dá použiť **„len" ako kľúč** alebo aj **ako údržbový prístroj**. Správca môže ovládať toto nastavenie.
- **Automatické zabezpečenie:** Po uzamknutí s Bluetooth sa automaticky aktualizujú čierna listina, protokolové záznamy všetkých identifikačných médií a čas. Uskutoční sa to každých 6 hodín, prípadne po príslušnom nastavení v online správe aj po každom procese odomknutia.

4. Ochrana a zabezpečenie údajov

- **AirKey spĺňa požiadavky všeobecného nariadenia EÚ o ochrane údajov.**: Spoločne s uznávaným expertom na ochranu údajov Dr. Christofom Tschohlom bol prístupový systém AirKey vyvinutý tak, aby vyhovoval predpisom týkajúcim sa ochrany údajov. Ak máte doplňujúce otázky, ochotne vám ich zodpovie osoba poverená ochranou údajov. https://www.evva.com/at-de/datenschutzerklaerung/
- Systém umožňuje odstránenie osobných údajov v súlade so všeobecným nariadením EÚ o ochrane údajov. Pritom dochádza k nenávratnému odstráneniu akéhokoľvek spojenia s konkrétnou osobou.
- Protokolovanie prístupových udalostí je možné individuálne nakonfigurovať pre každý komponent (k dispozícii je aj možnosť časového obmedzenia), ako aj dezaktivovať, napr. v prípade zasadačky závodnej rady, pre ktorú nie je protokolovanie povolené.
- **Protokolovanie** v Backende a komponentoch je **zabezpečené voči nedovolenej manipulácii**. Znamená to, že každý proces odomknutia je možné presne vysledovať podľa dátumu a času. S takýmto protokolovaním preto nie je možné manipulovať, v dôsledku čoho umožňuje väčšiu transparentnosť ako akýkoľvek mechanický uzamykací systém.

Zhrnutie

- AirKey je vysoko bezpečný a flexibilný prístupový systém, ktorý spĺňa požiadavky GDPR a vďaka najnovším technológiám z oblasti kryptografie, elektroniky, firmvéru, softvéru a mechaniky a využívaniu bezpečnostných prvkov, modulov HSM a kariet NFC Smartcard dosahuje zabezpečenie uzamykacích systémov EVVA AirKey.
- BSI/NIST **https://www.keylength.com/en/4/** potvrdzuje, že použité metódy šifrovania a dĺžky kľúčov sa považujú za bezpečné do roku 2030. Dĺžky kľúčov v systéme môže EVVA podľa potreby zvýšiť, aby bola zachovaná miera zabezpečenia v súlade s aktuálnym stavom techniky aj v budúcnosti. Ide o najväčšiu výhodu médií JCOP, aplikácií a bezpečnostných prvkov v uzamykacích komponentoch AirKey, ktorá zabezpečuje aj najvyššiu bezpečnosť investícií vďaka možnosti aktualizácie.