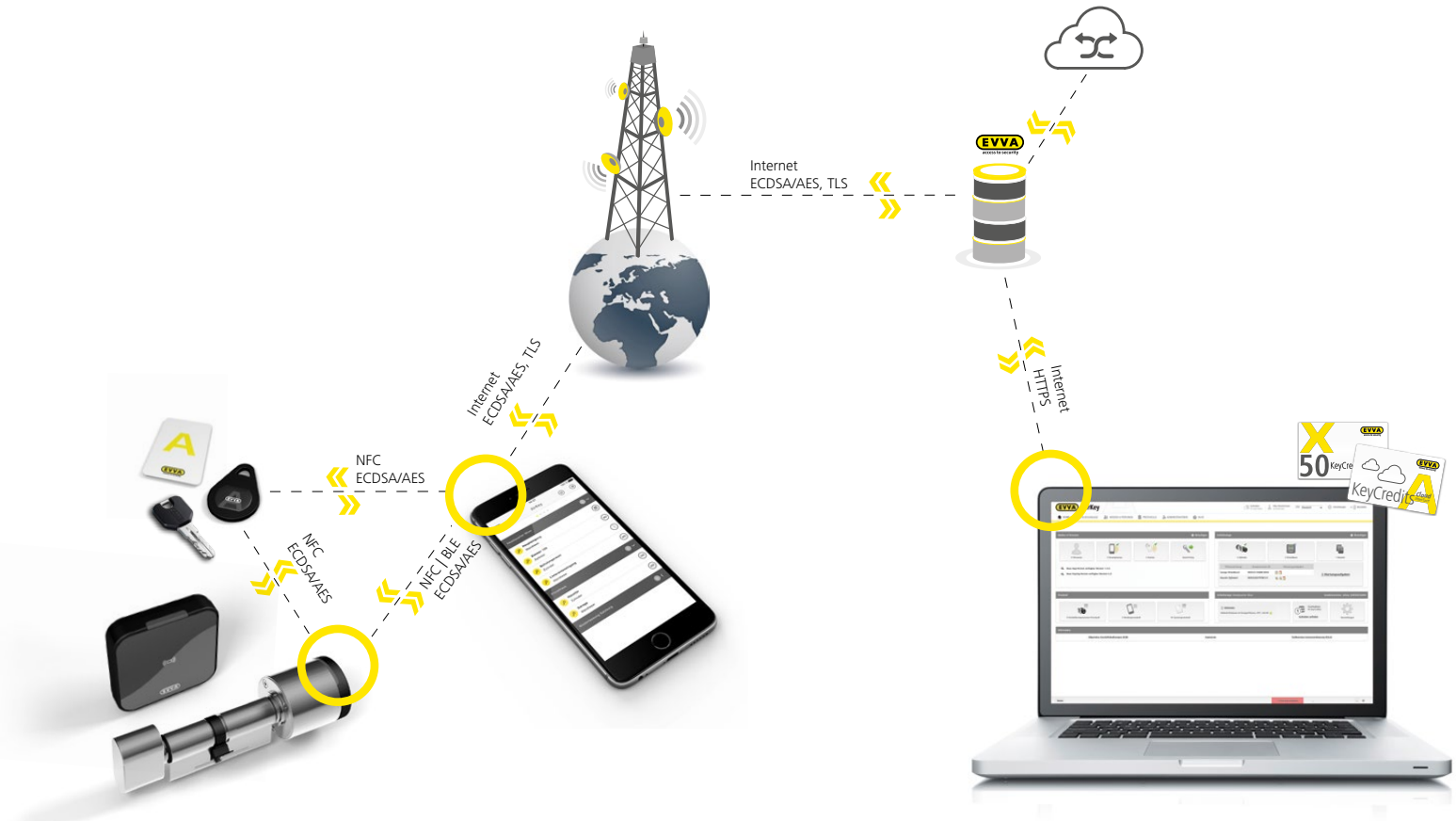
AirKey. Nekompromisní bezpečnost

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 nejúspěšnějších 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_{MZ}6-BZ

Ochrana před vlivy prostředí

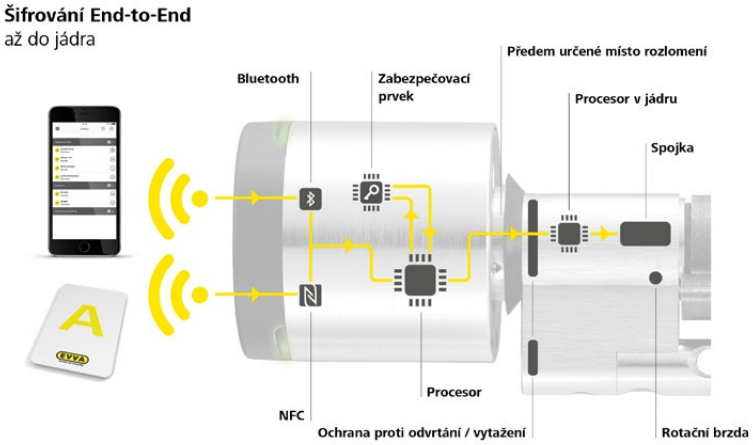
- Ochrana IP65 proti vniknutí škodlivého prachu a silným proudům vody odkudkoliv při instalaci
- Elektronika s nano povrchem proti oxidaci kondenzovanou vodou
- Provozní podmínky: -20°C - +55°C; 2 baterie paralelně pro vyšší stabilitu napájení

Fyzická bezpečnost

- Ochrana proti odvrtání
- a proti vytažení jádra
- Rotační brzda proti napadení vysokofrekvenčním vřetenem
- Definovaný bod zlomu na závitu 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 EAL5+** (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 EAL5+ 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 **dvojího** 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 je posuzována jeho síla, aby bylo zvoleno bezpečné.
- **Pro správce lze volitelně aktivovat** dvoufaktorovou autentizaci pomocí SMS TAN (6místný alfanumerický TAN)
- Automatické odesílání úkonů údržby a bezpečnostních informací (černých listin) správcům e-mailem, nebo pro techniky údržby v aplikaci AirKey.

Backend

- Společnost **EVVA ukládá data do vlastních rezervních zabezpečených datových center** v Rakousku.
- **Hardwarové** bezpečnostní **moduly (HSMs)** s certifikací EAL5 + 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 **vícestupňový bezpečnostní koncept**:

- Společnost EVVA doporučuje, aby každý uživatel smartphonu **aktivoval šifrování úložiště** a zabezpečil zámek obrazovky pomocí bezpečného **hesla, PINem nebo biometrickým přihlášením**.
- 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 černá listina, 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/datenschutzerklaerung/
- 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.

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, aby se v budoucnosti dodržela 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.