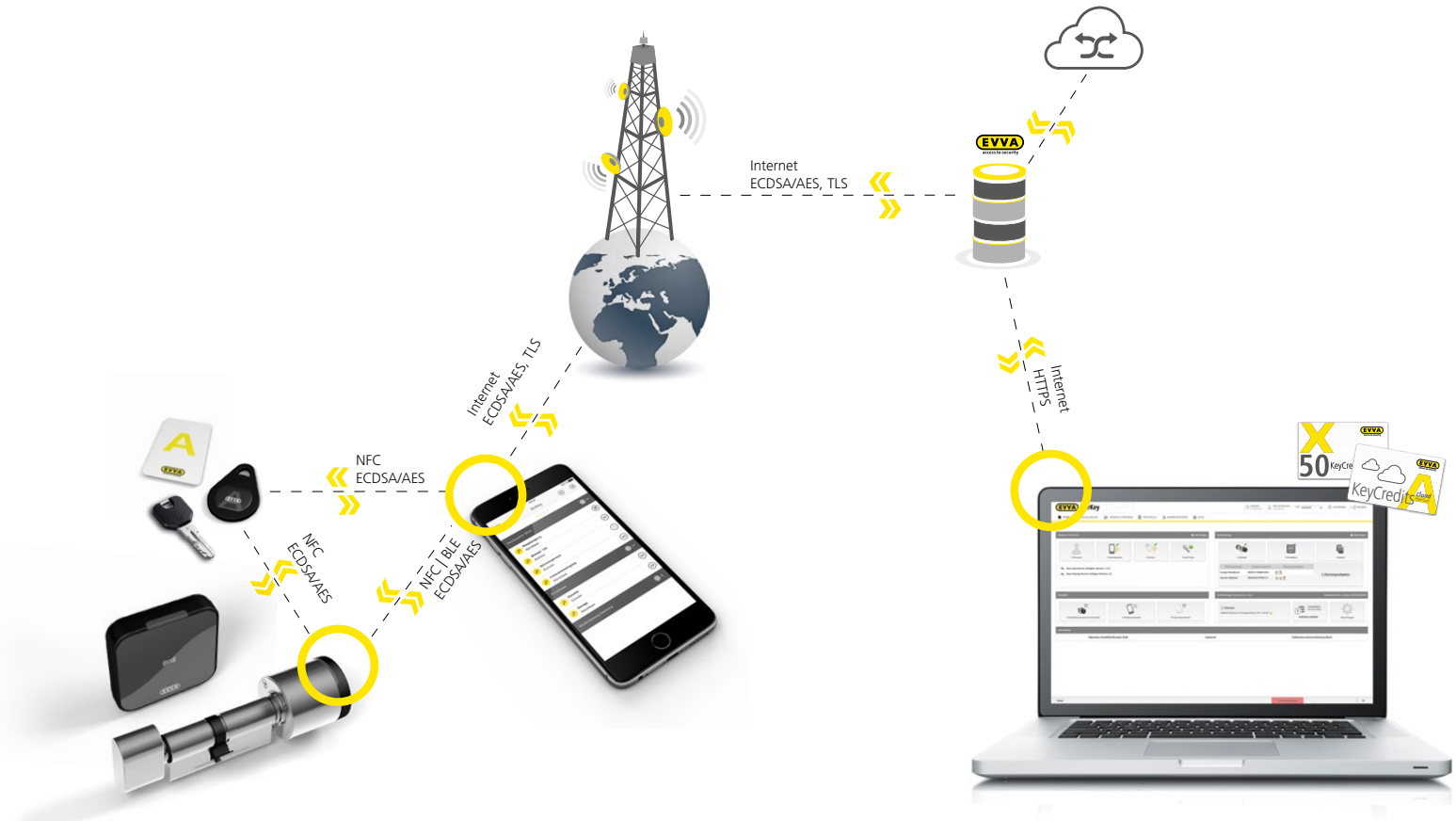
AirKey. Kompromisslös säkerhet helt enkelt

AirKeys säkerhetsarkitektur i detalj

EVVA kompromissar aldrig med säkerheten. Säkert och funktionellt. Annars hade vi inte kunnat utvecklas till ett av världens mest framgångsrika säkerhetsföretag sedan vårt grundande 1919! På samma sätt gör vi inga kompromisser när det gäller utvecklingen av säkerhetskonceptet för AirKey. För utvecklingen av AirKey anlitade vi endast de främsta säkerhetsexperterna inom mekanik, elektronik och programvara. Det har gjort AirKey till ett av de säkraste elektroniska tillträdessystemen på marknaden. Se själv!



Kompromisslös mekanisk säkerhet

AirKey-cylindern från EVVA är konstruerad med följande säkerhetsfunktioner redan i standardutförandet.

Certifieringar

- EN15684 (1.6.B.3.A.F.3.2)
- SKG***
- SSF3522 för skandinaviska profiler
- EN1634 brandskyddscertifiering (90 min)
- EN179/1125 anti-panik-certifiering

Skydd mot miljöpåverkan

- IP65-skydd mot inträngande av skadligt damm och kraftig vattenstråle från alla håll i monterat skick.
- Nano Coated-elektronik för skydd mot oxidation till följd av kondensvatten
- Användningsvillkor: -20 °C till +55 °C; 2 batterier används parallellt för stabilare spänningsförsörjning

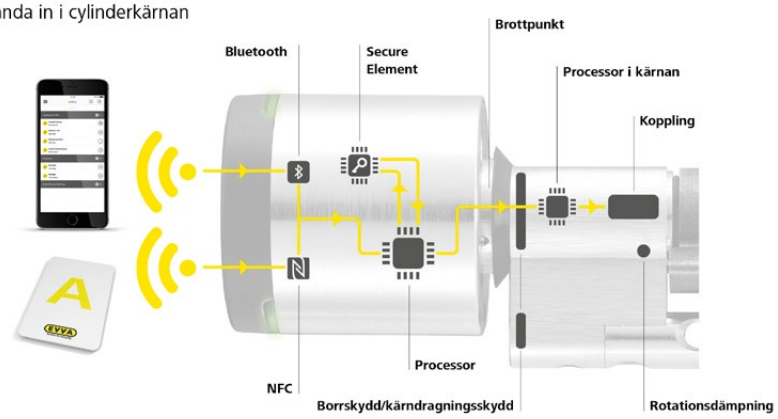
Mekanisk säkerhet

- Borrskydd
- Kärndragningsskydd
- Rotationsdämpning mot angrepp med högfrekvensspindel
- Definierad brottpunkt på yttervredets gänga för att skydda cylinderkärnan mot mekaniska angrepp och förhindra att den demoleras
- Mekaniskt specialverktyg för montering och demontering av cylindervredet

Kompromisslös elektronisk säkerhet

Elektroniska säkerhetsfunktioner i AirKey-systemet förhindrar att signaler och/eller kryptografiskt nyckelmaterial missbrukas.

End-to-End-kryptering
ända in i cylinderkärnan



1. Central säkerhetsarkitektur

- Alla AirKey-komponenter har en extra processor i ett säkert område som reglerar öppettiden.
  Exempel: Cylindervredet i AirKey-cylindern säkras kryptografiskt med en processor som är inbyggd i cylinderkärnan och som sitter **bakom borrskyddet**. Det går därmed inte att byta cylindervredet så att obehöriga får åtkomst.
- Genom användning av **EAL5+-certifierade Secure Elements** (ultrasäkert krypterings- och lagringselement) i varje AirKey-komponent sätter EVVA nya säkerhetsstandarder för elektroniska låssystem.
- I AirKey används uteslutande ultrasäkra EAL5+-certifierade **NFC-smartcards som ID-medier**.
  Det gör det omöjligt att kopiera ID-medier på ett obehörigt sätt.
  Tack vare dessa höga säkerhetsstandarder används denna teknik **för elektroniska pass** och kreditkort.
- End-to-End-kryptering i alla gränssnitt
  - Komunikation sker alltid med kontrollerade och certifierade krypteringsmetoder
  - Vid all dataöverföring **använder AirKey** dubbel **kryptering**:
    - **ECDSA-224** för autentisering
    - **AES-128** för session keys
  - ECDSA-algoritmen bygger på elliptiska kurvor och används för autentisering mellan olika AirKey- komponenter. Baserat på ECDSA-autentiseringen **tas varje gång en tillfällig AES session key** fram**som endast används för den aktuella transaktionen** (uppdateringar, aktiveringar av enheter, , geotaggning, osv.). Denna metod används vid all kommunikation mellan AirKey-komponenter.

- Alla överförda data är krypterade end-to-end:
  - AirKey-ID-medier till AirKey-enheter (ECDSA/AES)
  - AirKey-enheter till AirKey-app (ECDSA/AES)
  - AirKey-app till AirKey-ID-medier (ECDSA/AES)
  - AirKey-app till AirKey-onlineadministration (ECDSA/AES)

2. Databas och onlineadminstration

Onlineadminstration

- Anslutning via webben säkras med **TLS-kryptering** (https)
- När du skapar ett lösenord utvärderas lösenordets säkerhet så att den är tillräckligt hög.
- **2-faktorsautentisering med SMS TAN** kan aktiveras valfritt för administratörer (6-ställig alfanumeriskt TAN)
- Automatisk information av uppdateringar och säkerhetsinformation (blacklists) till administratörer via e-post eller för auktoriserade tekniker i AirKey-appen.

Databas

- Data lagras i **EVVA:s egna redundant säkrade datorcentraler** i Österrike som EVVA själva driver.
- **EAL5+**-certifierade **Hardware Security Modules (HSMs)** garanterar högsta säkerhet i databasen när encryption keys skapas och sparas.

3. AirKey Android och iOS App

Vid användning av AirKey tillsammans med en smarttelefon har EVVA ett säkerhetskoncept i flera steg **i AirKey-appen**:

- EVVA rekommenderar att alla som använder smarttelefoner aktiverar **minneskrypteringen** och aktiverar skärmlåset med ett säkert **lösenord, en pinkod eller biometrisk inloggning**.
- AirKey-appen har ytterligare en aktiverbar säkerhetsfunktion, vilket innebär att **en extra pinkod** måste anges i appen före varje aktivering av en enhet .
- Administratören kan se om pinkodsfunktionen är aktiverad i appen eller inte.
- Administratören aktiverar i onlineadministrationen om handsfreeläget ska fungera även med skärmlåset aktiverat på smarttelefonen.
- Smarttelefonen kan användas **både som nyckel** och **programering/uppdateringsenhet**. Rättigheten aktiveras i onlineadministrationen av administratören.
- **Automatisk säkerhet:** Vid aktivering av en enhet med Bluetooth uppdateras blacklist, loggposter från alla ID-medier samt klockan i enheten automatiskt. Detta sker automatiskt var sjätte timme vid aktivering eller efter varje aktivering med en smarttelefon.Funktionen aktiveras i onlineadministrationen.

4. Dataskydd och datasäkerhet

- **AirKey uppfyller kraven i EU:s dataskyddsförordning.**: Tillträdessystemet AirKey utvecklades tillsammans med den renommerade dataskyddsexperten Christof Tschohl för att uppfylla alla gällande dataskyddsbestämmelser. Om du har frågor är du välkommen att kontakta vår dataskyddsansvarige. https://www.evva.com/at-de/datenschutzerklaerung/
- I enlighet med kraven i dataskyddsförordningen raderas personuppgifter i systemet. Alla personkopplingar tas då bort permanent.
- Loggning av aktiveringar kan konfigureras individuellt för varje enhet (även tidsbegränsat) eller avaktiveras, t.ex.för konferanslokaler eller styrelserum för företag där ingen loggning tillåts.
- **Loggningen** i databasen och i enheterna är **revisionssäker**. Det innebär att alla aktiveringar kan spåras exakt med datum och klockslag. Denna loggning kan därmed inte manipuleras och möjliggör mer insyn än hos alla typer mekaniska låssystem.

Sammanfattning

- AirKey är ett ultrasäkert och flexibelt tillträdessystem som både uppfyller kraven i GDPR och garanterar säkerheten med den senaste tekniken inom kryptografi, elektronik, mjukvara, hårdvara och mekanik. Med användning av Secure Elements, HSMs och NFC Smartcards.
- BSI/NIST **https://www.keylength.com/en/4/** bekräftar att de använda krypteringsmetoderna och nyckellängderna räknas som säkra fram till 2030. Vid behov kan nyckellängderna ökas av EVVA i systemet, så att säkerhetsnivån ligger på topp även längre fram. Detta är den stora fördelen med JCOP-medier, appar och Secure Elements i AirKey-komponenterna, samtidigt som uppdaterbarhet garanterar högsta investeringssäkerhet.