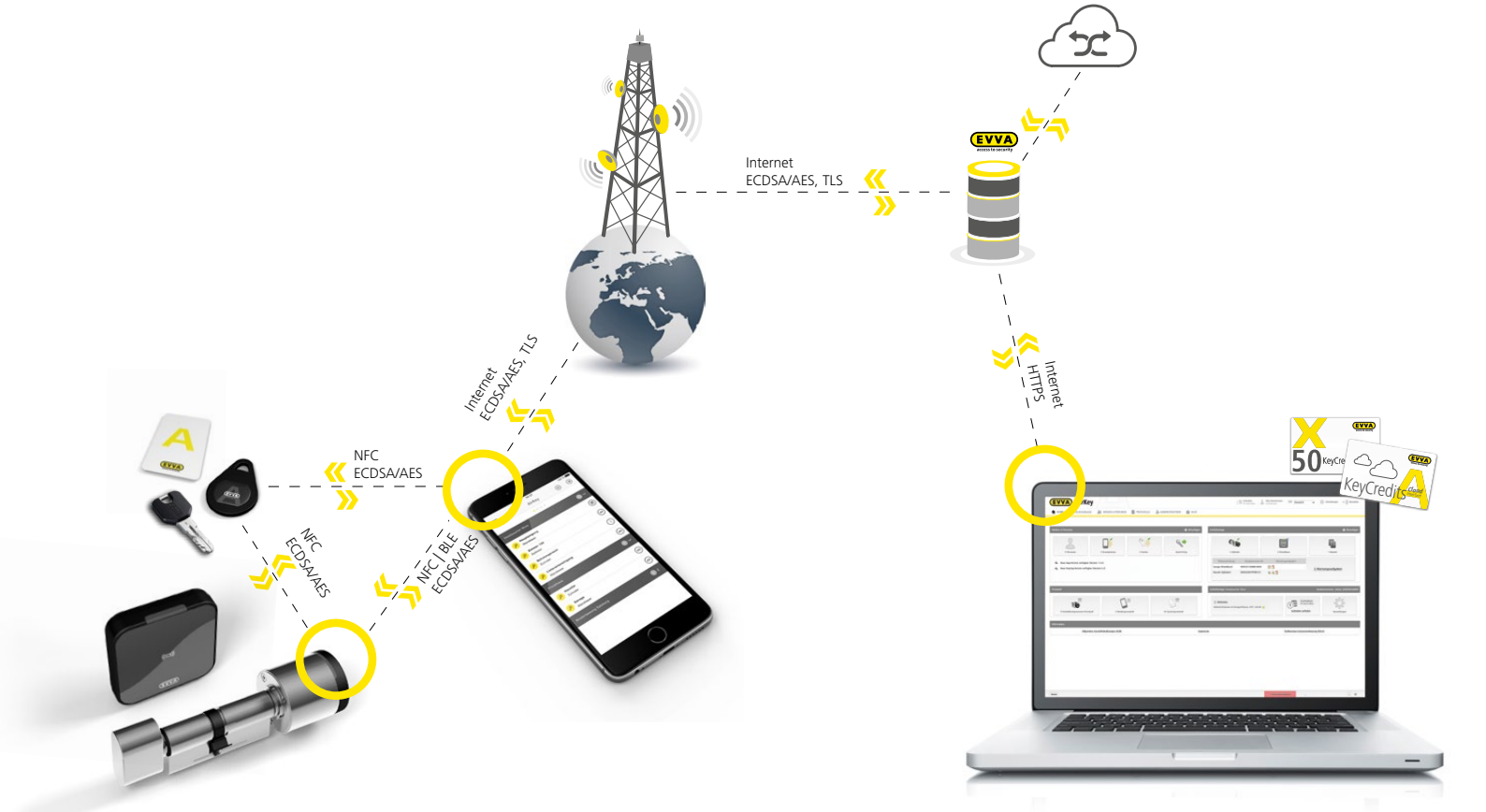
AirKey. Veiligheid zonder compromis

De AirKey-beveiligingsarchitectuur in detail

Als het gaat om veiligheid, sluit EVVA geen compromissen. En dat is een goede zaak. Hoe hadden we anders kunnen uitgroeien tot een van de meest succesvolle beveiligingsbedrijven ter wereld, sinds de oprichting van ons bedrijf in 1919. Zo hebben we ook geen compromissen gesloten bij de realisatie van het beveiligingsconcept van AirKey. Bij de ontwikkeling van AirKey waren alleen de beste beveiligingsdeskundigen op het gebied van mechanica, elektronica en software betrokken. Dit maakt AirKey een van de meest veilige elektronische toegangssystemen op de markt. Ontdek het zelf.



Mechanische beveiliging zonder compromis

De EVVA AirKey-cilinder heeft in de standaarduitvoering al de volgende maximale mechanische veiligheidskenmerken.

Behaalde certificeringen

- EN 15684 (1.6.B.3.A.F.3.2)
- SKG***
- SSF3522 voor Scandinavische profielen
- EN 1634 brandveiligheidscertificaat (90 min)
- EN179/1125 anti-paniekcertificaat

Bescherming tegen milieu-invloeden

- IP65-bescherming tegen het binnendringen van schadelijk stof en krachtige waterstralen uit elke richting in ingebouwde toestand
- Elektronica met nanocoating tegen oxidatie door condensatie
- Gebruiksvoorwaarden: -20 °C tot +55 °C; 2 parallelle batterijen voor een hogere stabiliteit van de voeding

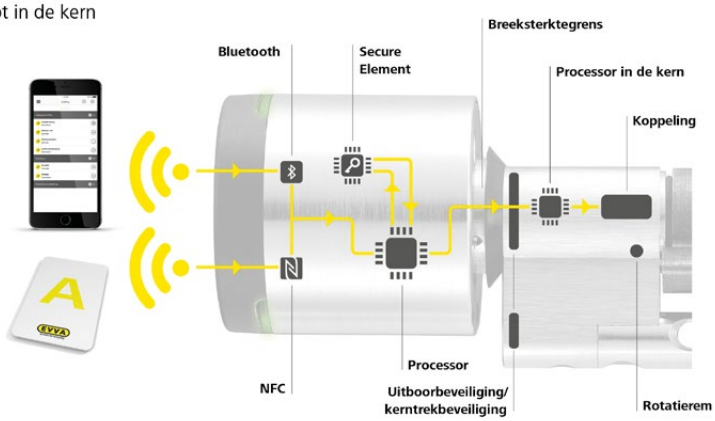
Fysieke beveiliging

- Uitboorbeveiliging
- Kerntrekbeveiliging
- Rotatierem tegen aanvallen met een spil met hoge frequentie
- Gedefinieerde breeksterktegrens op de schroefdraad van de buitenknop om de kern te beschermen tegen mechanische aanvallen en om snapping-aanvallen af te weren
- Speciaal mechanisch gereedschap voor het monteren en demonteren van de cilinderknop

Elektronische beveiliging zonder compromis

Elektronische veiligheidsmaatregelen in het AirKey-systeem voorkomen misbruik van signalen en/of cryptografisch sleutelmateriaal.

End-to-end-codering
tot in de kern



1. Centrale beveiligingsarchitectuur

- Voor alle AirKey-componenten is er één extra processor op een veilige plaats die de vrijgave regelt.
  De cilinderknop van de AirKey-cilinder wordt bijvoorbeeld cryptografisch beveiligd door een in de cilinderkern ingebouwde processor, die zich **achter de uitboorbeveiliging** bevindt. Het vervangen van de cilinderknop en de bijbehorende ongeoorloofde toegang is daarom niet mogelijk.
- Door het gebruik van **EAL5+ gecertificeerde Secure Elements** (zeer veilige coderings- en opslagelementen) in elke AirKey-component, zet EVVA een nieuwe veiligheidsstandaard voor elektronische sluitsystemen.
- Alleen uiterst veilige, EAL5+ gecertificeerde **NFC-smartcards worden gebruikt als identificatiemedia** voor AirKey.
  Het ongeoorloofd kopiëren van identificatiemedia is dus onmogelijk.
  Dankzij deze hoge veiligheidsnormen wordt deze technologie **ook gebruikt voor elektronische paspoorten** en creditcards.
- End-to-end-codering over alle interfaces
  - Alleen geteste en gecertificeerde coderingsmethoden worden gebruikt
  - AirKey gebruikt voor **alle** gegevensoverdrachten een **dubbele** codering:
    - **ECDSA-224** voor de authenticatie
    - **AES-128** voor sessiesleutels
  - Het ECDSA-algoritme is gebaseerd op elliptische krommen en wordt gebruikt voor de authenticatie tussen de verschillende AirKey-componenten. Op basis van de ECDSA-authenticatie wordt telkens **een willekeurige AES-sessiesleutel** bepaald, die alleen wordt gebruikt **voor de huidige transactie** (actualiseren, blokkeren, cilinderupdate, kaartupdate, enz.). Deze procedure wordt gebruikt voor alle communicatie tussen AirKey-componenten.

- Alle verzonden gegevens zijn end-to-end gecodeerd:
  - AirKey-identificatiemedia naar AirKey-sluitcomponenten (ECDSA/AES)
  - AirKey-sluitcomponenten naar AirKey-app (ECDSA/AES)
  - AirKey-app naar AirKey-identificatiemedia (ECDSA/AES)
  - AirKey-app naar AirKey-online-systeem (ECDSA/AES)

2. Backend en online-systeem

Online-systeem

- Webtoegang is beveiligd met **TLS-codering** (https)
- Wanneer u een wachtwoord aanmaakt, wordt de sterkte geëvalueerd om een veilig wachtwoord te kiezen.
- **2-factor-authenticatie met SMS TAN** kan optioneel worden geactiveerd voor beheerders (6-cijferige alfanumerieke TAN)
- Automatisch versturen van onderhoudstaken en beveiligingsinformatie (blacklists) naar beheerders via mail of naar onderhoudsmonteurs in de AirKey-app.

Backend

- De gegevens worden opgeslagen in de **redundant beveiligde datacenters van EVVA in Oostenrijk, die door EVVA zelf worden geëxploiteerd**.
- **EAL5+** gecertificeerde **Hardware Security Modules (HSM's)** bieden de hoogste veiligheid in de backend voor het maken en opslaan van alle encryptiesleutels.

3. AirKey-app voor Android en iOS

Met de AirKey-app biedt EVVA een **meervoudig beveiligingsconcept** voor het gebruik van AirKey in combinatie met een smartphone:

- EVVA raadt elke smartphonegebruiker aan om de **geheugencodering** te activeren en de schermvergrendeling te beveiligen met een veilig **wachtwoord, pincode of biometrische login**.
- De AirKey-app biedt in de app ook een **extra pincode** als extra beveiligingsfunctie, die vóór elk vergrendelingsproces moet worden ingevoerd.
- De beheerder kan zien of de pincodefunctie in de app is in- of uitgeschakeld.
- De beheerder kan instellen of de handsfree-modus gebruikt mag worden zonder het scherm te vergrendelen.
- De smartphone kan **"alleen" als sleutel** of als **onderhoudsapparaat** worden gebruikt. Dit kan door de beheerder worden bepaald.
- **Automatische beveiliging:** Na sluiten door middel van Bluetooth worden voortaan de blacklist, de protocolnotities van alle identificatiemedia en de tijd automatisch geactualiseerd. Dit gebeurt automatisch om de 6 uur of na elk vergrendelingsproces, afhankelijk van de instelling in het online-systeem.

4. Gegevensbescherming

- **AirKey voldoet aan de EU-verordening inzake gegevensbescherming.**: Samen met de gerenommeerde export op het gebied van gegevensbescherming, Dr. Christof Tschohl, werd AirKey ontwikkeld tot een toegangssysteem dat voldoet aan de voorschriften voor gegevensbescherming. Voor uitgebreide informatie kunt u contact opnemen met onze eigen gegevensbeschermingsfunctionaris. https://www.evva.com/be-nl/privacyverklaring/-https://www.evva.com/nl-nl/privacyverklaring/
- Het systeem voorziet in de verwijdering van persoonsgegevens, zoals vereist door de basisverordening inzake gegevensbescherming. Elke persoonlijke verwijzing wordt daarbij onherroepelijk verwijderd.
- De protocollering van toegangsgebeurtenissen kan voor elke component afzonderlijk worden geconfigureerd (ook voor een beperkte periode) en gedeactiveerd, bijvoorbeeld voor een vergaderzaal van de ondernemingsraad waar protocollering niet is toegestaan.
- De **protocollering** in de backend en in de componenten is **tegen revisie beveiligd**. Dit betekent dat elk vergrendelingsproces precies met datum en tijd kan worden gevolgd. Deze protocollering kan niet worden gemanipuleerd en biedt meer transparantie dan bij een mechanisch sluitsysteem.

Samenvatting

- AirKey is het uiterst veilige en flexibele toegangssysteem dat voldoet aan de AVG en dat ook de veiligheid van EVVA AirKey-sluitsystemen garandeert met behulp van de nieuwste technologieën op het gebied van cryptografie, elektronica, firmware, software en mechanica door het gebruik van Secure Elements, HSM's en NFC-smartcards.
- Het BSI/NIST **https://www.keylength.com/en/4/** bevestigt dat de gebruikte coderingsmethoden en sleutellengtes tot 2030 als veilig worden beschouwd. Indien nodig kan EVVA de sleutellengtes in het systeem verhogen om het beveiligingsniveau in de toekomst op het hoogste niveau te houden. Dit is het grote voordeel van de JCOP-media, apps en Secure Elements in de AirKey-sluitcomponenten en zorgt ook voor maximale investeringszekerheid door de updatebaarheid.