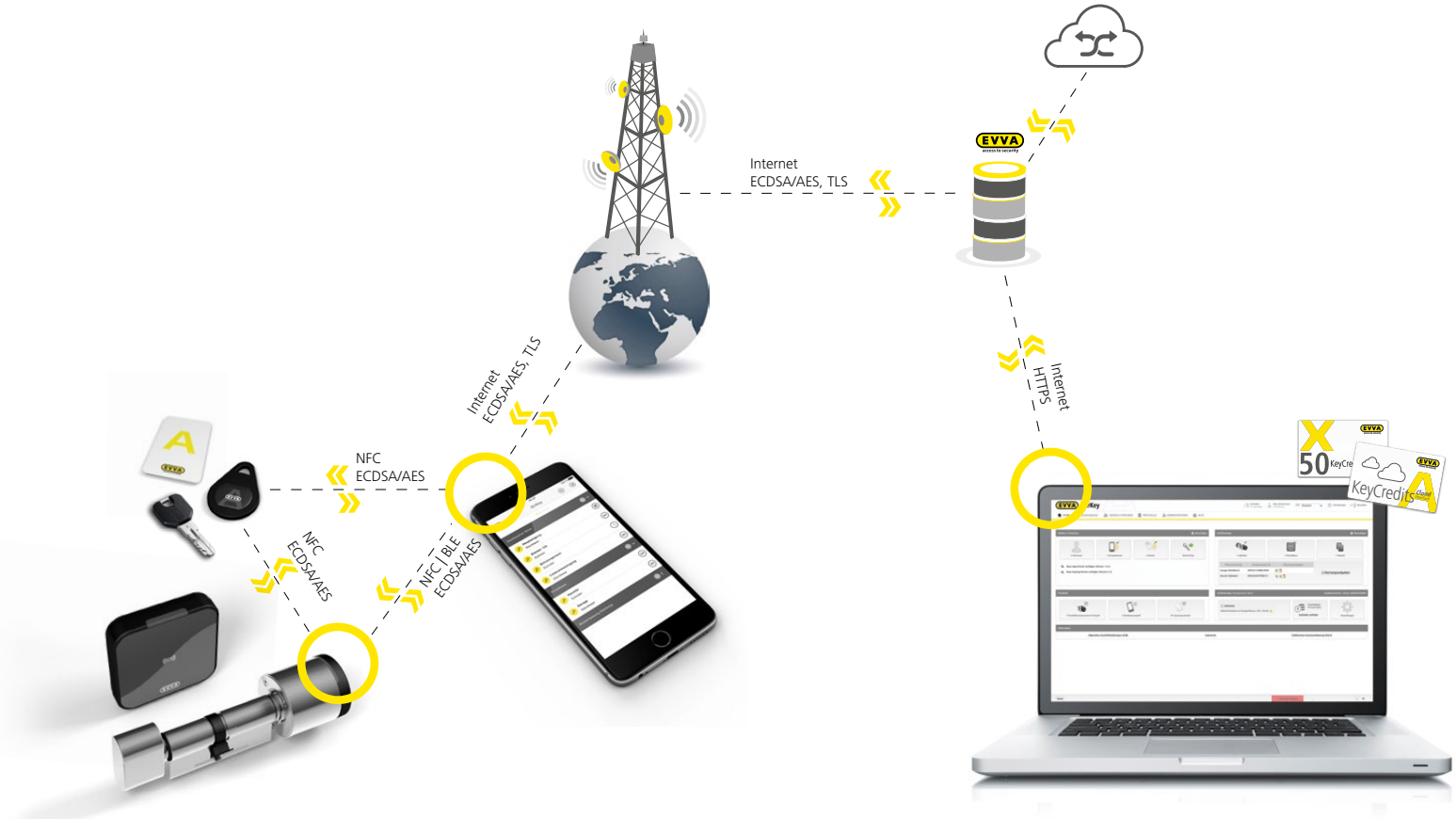
AirKey: prosty, elastyczny, bezpieczny

Poznaj architekturę bezpieczeństwa AirKey

W kwestii bezpieczeństwa firma EVVA nie akceptuje kompromisów. Takie podejście stosujemy konsekwentnie już od chwili założenia firmy w 1919 roku i dlatego obecnie cieszymy się opinią renomowanego przedsiębiorstwa w branży zabezpieczeń! Równie bezkompromisowo przygotowaliśmy koncepcję bezpieczeństwa systemu AirKey. Do prac rozwojowych AirKey angażujemy tylko najlepszych ekspertów ds. bezpieczeństwa z dziedziny mechaniki, elektroniki i oprogramowania. W ten sposób dbamy o to, aby AirKey był jednym z najbezpieczniejszych systemów dostępowych na rynku. Przekonaj się o tym!



Bezkompromisowe bezpieczeństwo mechaniczne

Już w wersji standardowej wkładka EVVA AirKey jest wyposażona w skuteczne, mechaniczne funkcje bezpieczeństwa.

Uzyskane certyfikacje

- EN15684 (1.6.B.3.A.F.3.2)
- SKG***
- SSF3522 dla profilu skandynawskiego
- EN1634, certyfikat ognioodporności (90 min)
- EN179/1125, certyfikat funkcji antypanicznej
- ÖNORM B 5351:2011 W_{MZ}6-BZ

Ochrona przed wpływami atmosferycznymi

- IP65 – ochrona przed wnikaniem szkodliwych pyłów i silnych strumieni wody z dowolnego kierunku w stanie zamontowanym
- Powłoka Nano Coat układów elektronicznych – ochrona przed utlenianiem pod wpływem kondensatu
- Warunki robocze: od -20°C do +55°C; 2 baterie połączone równolegle dla wyższej stabilności napięcia

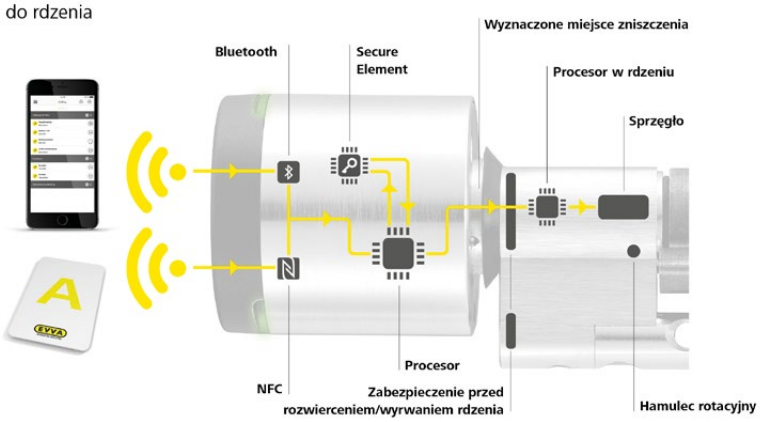
Bezpieczeństwo fizyczne

- Zabezpieczenie przed rozwierceniem
- Zabezpieczenie przed wyciągnięciem rotora
- Hamulec rotacyjny przeciw ingerencjom z użyciem wrzeciona wysokiej częstotliwości
- Wyznaczone miejsce zniszczenia na gwincie gałki zewnętrznej chroni rdzeń przed ingerencją mechaniczną i zniszczeniem zamka (snapping)
- Specjalne narzędzie mechaniczne do montażu i demontażu gałki z wkładką

Bezkompromisowe bezpieczeństwo elektroniczne

Elektroniczne środki bezpieczeństwa w systemie AirKey zapobiegają niepowołanemu użyciu sygnałów i/lub kryptograficznych danych kodujących.

Szyfrowanie End-to-End
aż do rdzenia



1. Centralna architektura bezpieczeństwa

- We wszystkich komponentach AirKey procesor, który steruje procesem odryglowania, znajduje się w bezpiecznej strefie.
  Np.: gałka z wkładką AirKey posiada procesor zamontowany w rdzeniu wkładki, chroniony przez **zabezpieczenie przed rozwierceniem** oraz środki kryptograficzne – zamiana gałki z wkładką i związane z tym ryzyko niepowołanego dostępu nie jest możliwe.
- Dzięki użyciu **chipów Secure Element z certyfikacją EAL5+** (bardzo bezpiecznych układów szyfrujących i zapisujących) w każdym komponencie AirKey firma EVVA wyznacza nowy standard bezpieczeństwa dla elektronicznych systemów dostępowych.
- System AirKey wykorzystuje wyłącznie bardzo bezpieczne **karty Smartcard NFC z certyfikacją EAL5+** jako nośniki identyfikacji.
  Dzięki temu niemożliwe jest niepowołane kopiowanie nośników identyfikacji.
  Ze względu na wysoki poziom bezpieczeństwa tej technologii jest ona stosowana **również w elektronicznych paszportach** i kartach kredytowych.
- Szyfrowanie End-to-End we wszystkich punktach interakcji:
  - Zastosowano wyłącznie przetestowane i certyfikowane metody szyfrowania
  - We **wszystkich** operacjach przesyłania danych AirKey stosuje **podwójne** szyfrowanie:
    - **ECDSA-224** podczas uwierzytelniania
    - **AES-128** dla kluczy sesji
  - Algorytm ECDSA bazuje na krzywych eliptycznych i służy do uwierzytelniania między różnymi komponentami AirKey. Na podstawie autentyfikacji ECDSA generowany jest każdorazowo **losowy klucz sesji AES**, który jest używany tylko **podczas bieżącej operacji** (uaktualnienie, ryglowanie, aktualizacja wkładki, aktualizacja karty itp.). Ten proces zachodzi podczas każdej komunikacji między komponentami AirKey.

Wszystkie przesyłane dane są zabezpieczone End-to-End na następujących ścieżkach komunikacji:

- Nośniki identyfikacji AirKey – komponenty zamykające AirKey (metoda ECDSA/AES)
- Komponenty zamykające AirKey – aplikacja AirKey (metoda ECDSA/AES)
- Aplikacja AirKey – nośniki identyfikacji AirKey (metoda ECDSA/AES)
- Aplikacja AirKey – moduł zarządzania online systemu AirKey (metoda ECDSA/AES)

2. Back-end i moduł zarządzania online

Moduł zarządzania online

- Dostęp przez Internet zabezpieczony **szyfrowaniem TLS** (https)
- Skuteczność definiowanego hasła jest analizowana, tak aby zastosować mocno zabezpieczające hasło.
- **Uwierzytelnianie 2-etapowe za pomocą wiadomości SMS z hasłem jednorazowym** jako funkcja opcjonalna dla administratorów (6-znakowe hasło alfanumeryczne TAN)
- Automatyczne przesyłanie zadań konserwacyjnych i informacji bezpieczeństwa (czarna lista) do administratorów przez e-mail lub do technika konserwacyjnego przez aplikację AirKey.

Back-end

- Dane są zapisywane **w należących do EVVA i obsługiwanych przez EVVA redundantnych centrach obliczeniowych** w Austrii.
- **Chipy Hardware Security Module z certyfikacją EAL5+ (moduły HSM)** w obszarze back-end zapewniają najwyższe bezpieczeństwo podczas generowania i zapisywania wszystkich kluczy szyfrujących.

3. Aplikacja AirKey dla systemów Android i iOS

Aby użytkować AirKey przy użyciu smartfona, firma EVVA udostępnia aplikację mobilną AirKey-App opracowaną w oparciu o **wielopoziomową koncepcję bezpieczeństwa**:

- EVVA zaleca użytkownikom smartfonów aktywowanie **szyfrowania pamięci** oraz zabezpieczenie blokady ekranu za pomocą odpowiednio skutecznego **hasła, kodu PIN lub weryfikacji biometrycznej**.
- Jako pozostałą funkcję zabezpieczającą aplikacja AirKey oferuje **dodatkowy kod PIN** w aplikacji, który należy podać przed każdą operacją ryglowania.
- Administrator ma wgląd, czy funkcja kodu PIN w aplikacji jest aktywna lub nieaktywna.
- Administrator może określić, czy można korzystać z trybu „Hands-free" również bez blokady ekranu.
- Smartfon może służyć **„tylko" jako klucz** lub także **jako narzędzie do zadań konserwacyjnych**. To ustawienie kontroluje administrator.
- **Automatyczne bezpieczeństwo:** Po ryglowaniu poprzez Bluetooth następuje automatyczna aktualizacja czarnej listy (blacklist), wpisów do protokołu wszystkich nośników identyfikacji oraz godziny. Odbywa się to automatycznie co 6 godzin lub po każdej operacji ryglowania (po aktywowaniu w module zarządzania online).

4. Ochrona i bezpieczeństwo danych

- **AirKey spełnia wymagania unijnego rozporządzenia w sprawie ochrony danych (RODO)**: Dzięki współpracy z renomowanym ekspertem ds. ochrony danych, dr. Christofem Tschohlem, system AirKey działa jako system zamknięć zgodny z wymogami z zakresu ochrony danych. W razie pytań z tej dziedziny prosimy o kontakt z naszym inspektorem ochrony danych oraz o zapoznanie się z informacjami na stronie https://www.evva.com/at-de/datenschutzerklaerung/
- Również przewidziana w rozporządzeniu RODO możliwość skasowania danych osobowych jest dostępna w systemie. W takim przypadku wszelkie odniesienie osobowe zostaje nieodwołalnie usunięte.
- Protokołowanie zdarzeń dostępowych można skonfigurować indywidualnie dla każdego komponentu (również z ograniczeniem czasowym), a także całkowicie je dezaktywować, np. w sali narad rady zakładowej, gdzie wszelkie protokołowanie jest zabronione.
- **Protokołowanie** w module back-end i w komponentach jest **zabezpieczone przed modyfikacją**. To znaczy, że każdą operację ryglowania można zweryfikować z dokładną datą i godziną. Zmiana tych protokołów nie jest możliwa, co zapewnia wyższy poziom transparentności niż w przypadku systemów mechanicznych.

Podsumowanie

- AirKey to bardzo bezpieczny i elastyczny system dostępowy, spełniający wymogi RODO oraz wykorzystujący najnowsze technologie z zakresu kryptografii, elektroniki, firmware, oprogramowania i mechaniki, a także stosujący chipy zabezpieczające Secure Element, HSM oraz karty NFC Smartcard – co w sumie tworzy kompleksową architekturę bezpieczeństwa systemów zamknięć AirKey.
- Instytut BSI/NIST **https://www.keylength.com/en/4/** potwierdza, że stosowane metody szyfrowania i długości kluczy można uważać za bezpieczne do 2030 roku. Długości kluczy mogą w razie potrzeby zostać zwiększone w systemie przez firmę EVVA, aby dostosować poziom bezpieczeństwa do stanu techniki w przyszłości. Jest to duża zaleta nośników JCOP, aplikacji i chipów Secure Element w komponentach AirKey, która – oprócz bezpieczeństwa – zapewnia długoletnią ochronę inwestycji oraz możliwość aktualizacji.