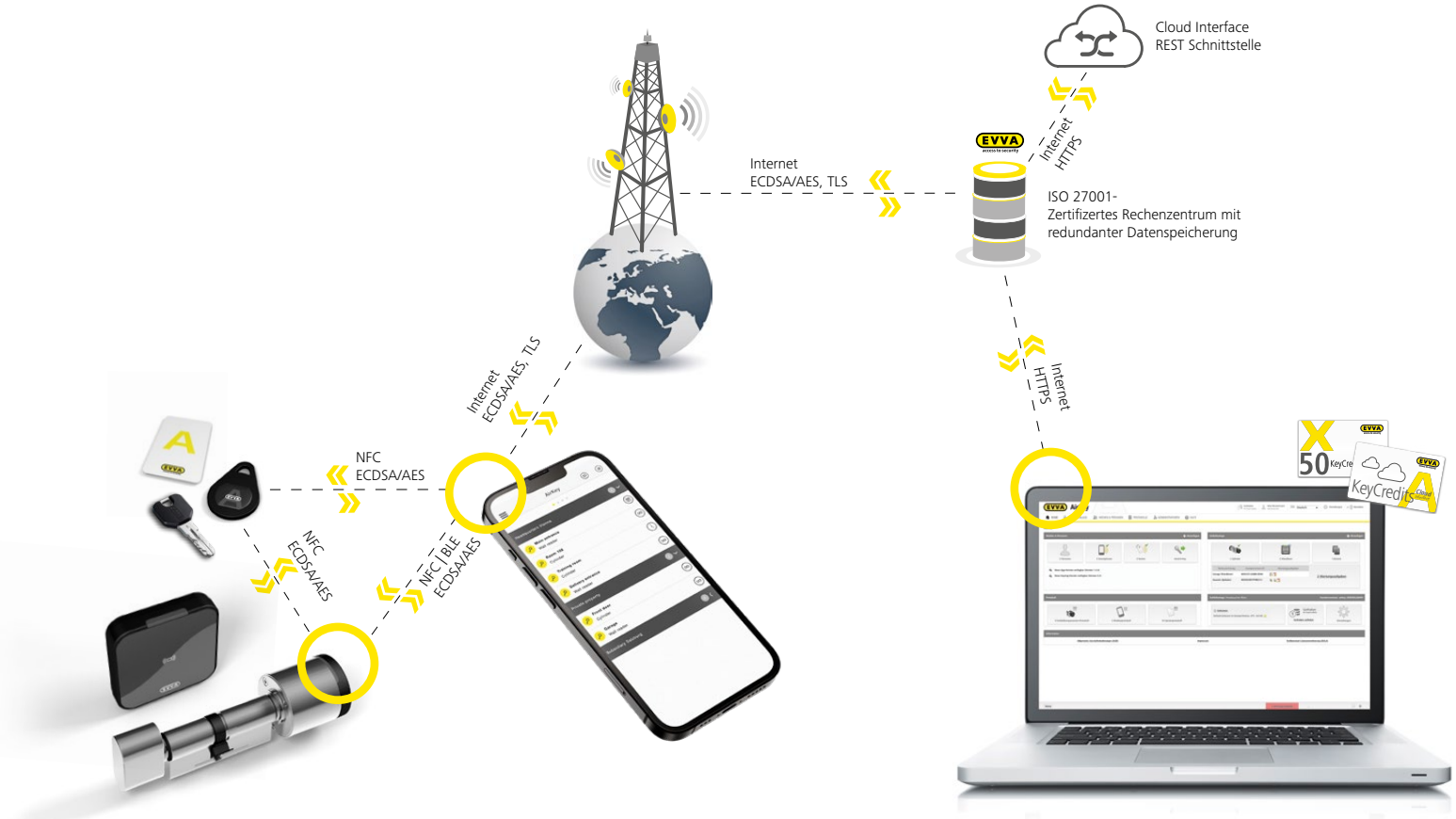
AirKey. Einfach kompromisslos sicher

Die AirKey-Sicherheitsarchitektur im Detail

Bei der Sicherheit macht EVVA keine Kompromisse. Und das ist gut so. Denn wie sonst hätten wir uns seit der Firmengründung 1919 zu einem der erfolgreichsten Sicherheitsunternehmen der Welt entwickeln können! So waren wir auch kompromisslos bei der Umsetzung des Sicherheitskonzeptes von AirKey. Ausschließlich Top-Sicherheitsexperten aus Mechanik, Elektronik und Software wurden mit der Entwicklung von AirKey betraut. Dadurch ist AirKey eines der hochsichersten elektronischen Zutrittsysteme am Markt. Bitte überzeugen Sie sich selbst.



Kompromisslose mechanische Sicherheit

Der EVVA AirKey-Zylinder verfügt mechanisch bereits in der Standardausführung über folgende höchste Sicherheitsmerkmale.

Bestandene Zertifizierungen

- EN15684:2021-05 1.6.B.3.0.D.3.D
- SKG***
- SSF3522 für skandinavische Profile
- EN1634 Brandschutzzertifizierung (90min)
- EN179/1125 Anti-Panik Zertifizierung
- ÖNORM B 5351:2011 W_{MZ}6-BZ
- EU-Baumusterprüfbescheinigung gemäß Anhang III der Richtlinie 2014/53/EU

Schutz gegen Umwelteinflüsse

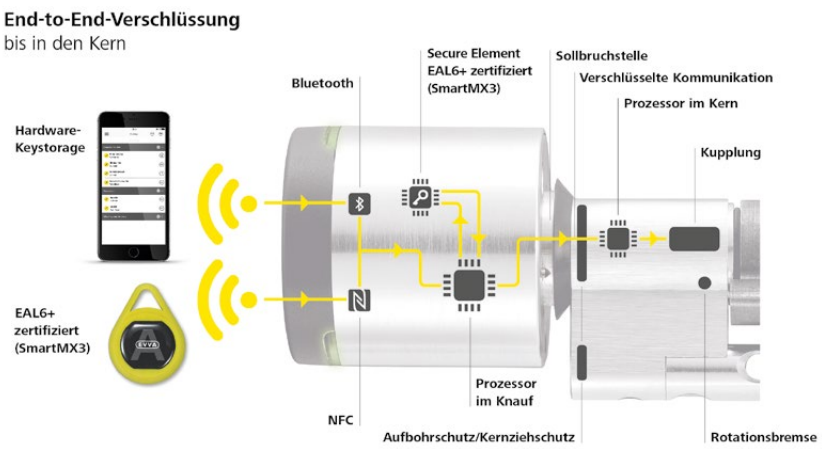
- IP65 Schutz gegen Eindringen von schädlichem Staub und starkem Strahlwasser aus jeder Richtung im eingebauten Zustand
- Schutzlackbeschichtete Elektronik gegen Oxidation durch Kondenswasser
- Einsatzbedingungen: -20°C - +55°C; 2 Lithium CR2 Batterien parallel für höhere Spannungsversorgungsstabilität

Physikalische Sicherheit

- Aufbohrschutz
- Kernziehschutz
- Rotationsbremse gegen Angriffe mit einer Hochfrequenzspindel
- Definierte Sollbruchstelle am Gewinde des Außenknaufs, um den Kern vor mechanischen Angriffen zu schützen und Snapping-Angriffe abzuwehren
- Mechanisches Spezialwerkzeug zur Montage und Demontage des Zylinderknaufs

Kompromisslose elektronische Sicherheit

Elektronische Sicherheitsmaßnahmen im AirKey-System verhindern, dass Signale und/oder kryptographisches Schlüsselmaterial missbraucht werden können.



1. Zentrale Sicherheitsarchitektur

- Bei allen AirKey-Komponenten gibt es jeweils einen weiteren Prozessor in einem sicheren Bereich, der die Freigabe steuert.
  z.B.: Der Zylinderknauf des AirKey-Zylinders ist mit einem im Zylinderkern eingebauten Prozessor, welcher **hinter dem Aufbohrschutz** liegt, kryptographisch abgesichert ein Tausch des Zylinderknaufs und ein damit verbundener unberechtigter Zutritt ist nicht möglich.
- Durch den Einsatz von **EAL6+ zertifizierten Secure Elements** (hochsicheren Verschlüsselungs- und Speicherelementen) in jeder AirKey-Komponente setzt EVVA einen neuen Sicherheitsmaßstab für elektronische Schließsysteme.
- Bei AirKey kommen ausschließlich hochsichere EAL6+ zertifizierte **Smartcards als Identmedien** zum Einsatz.
  Das unberechtigte Kopieren von Identmedien ist dadurch unmöglich.
  Aufgrund dieser hohen Sicherheitsstandards wird diese Technologie **auch für elektronische Reisepässe** und Kreditkarten eingesetzt.
- End-to-End Verschlüsselung über alle Schnittstellen
  - Zum Einsatz kommen ausschließlich geprüfte und zertifizierte Verschlüsselungsverfahren
  - Dabei verwendet AirKey bei **allen** Datenübertragungen eine **doppelte** Verschlüsselung:
    - **ECDSA-256** für die Authentifizierung
    - **AES-128** für Session-Keys
- Der ECDSA Algorithmus basiert auf elliptischen Kurven und wird für die Authentifizierung zwischen den verschiedenen AirKey-Komponenten verwendet. Auf Basis der ECDSA Authentifizierung wird jedes Mal **ein zufälliger AES Session-Key** ausgehandelt, der nur **für die aktuelle Transaktion** verwendet wird (Aktualisieren, Sperren, Zylinder Update, Karten Update, usw). Dieses Verfahren kommt bei allen Kommunikationen zwischen AirKey-Komponenten zum Einsatz.

- Alle übermittelten Daten sind End-to-End verschlüsselt:
  - AirKey-Identmedien zu AirKey-Schließkomponenten (ECDSA / AES)
  - AirKey-Schließkomponenten zu AirKey-App (ECDSA / AES)
  - AirKey-App zu AirKey-Identmedien (ECDSA / AES)
  - AirKey-App zu AirKey-Onlineverwaltung (ECDSA / AES)

2. Backend und Onlineverwaltung

Onlineverwaltung

- Der Zugang via Web ist mittels **TLS-Verschlüsselung** gesichert (HTTPS)
- Bei der Erstellung ihres Passwortes wird die Stärke bewertet, um die Sicherheit beurteilen zu können.
- **2-Faktor-Authentifizierung mit TAN via Email oder SMS** für Administratoren optional aktivierbar (6-stelliger alphanumerischer TAN)
- Automatisches Versenden von Wartungsaufgaben und Sicherheitsinformationen (Blacklists) an Administratoren per Mail oder für Wartungstechniker in der AirKey-App.

Backend

- AirKey läuft in ISO:27001 zertifizierten Rechenzentren in Österreich. Alle Daten sind auf EVVA eigenen redundant gesicherten Servern in Österreich gespeichert.
- **EAL6+** zertifizierte **Hardware Security Modules (HSMs)** sorgen im Backend für höchste Sicherheit in der Erstellung und Speicherung aller Encryption-Keys.

3. AirKey Android & iOS App

Für den Einsatz von AirKey in Verbindung mit einem Smartphone bietet EVVA mit der AirKey-App ein **mehrstufiges Sicherheitskonzept**:

- EVVA empfiehlt jedem Benutzer eines Smartphones die **Speicherverschlüsselung** zu aktivieren und die Bildschirmsperre mit einem entsprechend sicheren **Passwort, PIN oder biometrischen Login** zu sichern.
- Sowohl bei Android als auch bei iOS werden die herstellerspezifischen Hardware-Security-Speichermodule verwendet. (Android: Hardware-backed Keystore; iOS: Apple CryptoKit KeyChain)
- Die AirKey-App bietet darüber hinaus als weitere Sicherheitsfunktion einen **zusätzlichen PIN-Code** in der App, welcher vor jedem Sperrvorgang einzugeben ist.
- Der Administrator sieht ob die PIN-Code Funktion in der App aktiviert oder deaktiviert ist.
- Durch den Administrator kann eingestellt werden, ob der Handsfree Modus auch ohne Displaysperre genutzt werden darf.
- Das Smartphone kann **„nur" als Schlüssel** oder auch **als Wartungsgerät** verwendet werden. Dies kann vom Administrator gesteuert werden.
- **Automatische Sicherheit:** Nach dem Sperren mit Bluetooth werden automatisch die Blacklist, Protokolleinträge von allen Identmedien und die Uhrzeit aktualisiert. Dies passiert automatisch alle 6 Stunden oder nach Einstellung in der Onlineverwaltung auch nach jedem Sperrvorgang.

4. Datenschutz & Datensicherheit

- **AirKey erfüllt die EU-Datenschutzgrundverordnung**: Gemeinsam mit dem anerkannten Datenschutz-Experten Dr. Christof Tschohl wurde AirKey zum datenschutzkonformen Zutrittssystem entwickelt. Für Detailfragen stehen wir Ihnen gerne mit unserem eigenen Datenschutzbeauftragtem zur Verfügung. https://www.evva.com/at-de/datenschutzerklaerung/
- Die von der Datenschutzgrundverordnung geforderte Löschung von personenbezogenen Daten ist im System vorgesehen. Dabei wird jeglicher Personenbezug unwiederbringlich entfernt.
- Die Protokollierung von Zutrittsereignissen kann pro Komponente individuell konfiguriert (auch zeitlich begrenzt). sowie auch deaktiviert werden. z.B für ein Betriebsratsbesprechungszimmer bei dem keine Protokollierung erlaubt ist.
- Die **Protokollierung** im Backend und in den Komponenten ist **revisionssicher**. Das heißt, jeder Sperrvorgang kann mit Datum und Uhrzeit exakt nachvollzogen werden. Diese Protokollierung kann damit nicht manipuliert werden und ermöglicht mehr Transparenz als bei jedem mechanischen Schließsystem.
- Vorbereitet zur Erfüllung des European Data Act 2024
- Ein Vier-Augen-Prinzip zur Einsicht von Protokollen kann aktiviert werden. Dabei muss die Einsicht in die Protokolle durch einen zweiten Administrator freigegeben werden.

Resümee

- AirKey ist das hochsichere und flexible Zutrittssystem, das sowohl die DSGVO erfüllt, sowie auch mit neuesten Technologien in der Kryptographie, Elektronik, Firmware, Software und Mechanik durch den Einsatz von Secure Elements, HSMs und NFC Smartcards für die Sicherheit der EVVA AirKey-Schließanlagen sorgt.
- Das BSI/NIST **https://www.keylength.com/en/4/** bestätigt, dass die eingesetzten Verschlüsselungsverfahren und Schlüssellängen bis mindestens 2030 als sicher gelten. Die Schlüssellängen können im System bei Bedarf von EVVA erhöht werden, was 2023 erfolgreich durchgeführt wurde, um auch in weiterer Zukunft das Sicherheitslevel auf dem Stand der Technik zu erhalten. Dies ist der große Vorteil der JCOP Medien, Apps und Secure Elements in den AirKey-Schließkomponenten und sorgt dabei auch für höchste Investitionssicherheit durch Updatebarkeit.