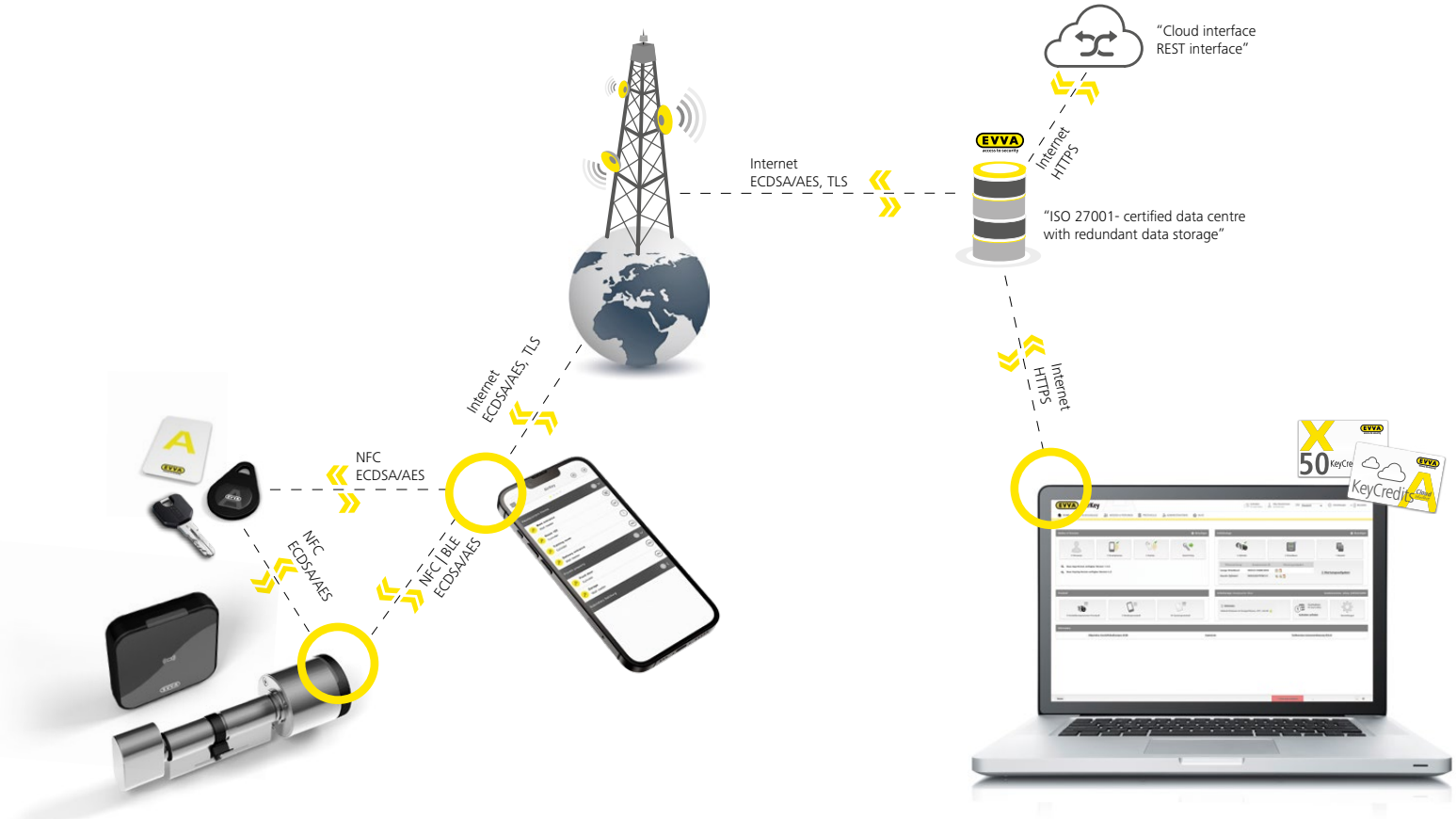
AirKey. Uncompromising security

The AirKey security architecture in detail

EVVA does not compromise on security. And that is the whole idea. How else could we have developed into one of the most successful security companies in the world since the company was founded in 1919! We were equally uncompromising in the implementation of the AirKey security concept. Only top security experts from the areas of mechanical and electronic access systems and software were entrusted with the development of AirKey. Consequently, AirKey is one of the most highly secure electronic access control systems on the market. Discover more about AirKey and be convinced.



Uncompromising mechanical security

Even the standard version of the EVVA AirKey cylinder has the following top security features.

Certifications obtained

- EN15684 (1.6.B.3.A.F.3.2)
- SKG***
- SSF3522 for Scandinavian profiles
- EN1634 fire resistance certification (90 min)
- EN179/1125 anti-panic certification
- ÖNORM B 5351:2011 W_{MZ}6-BZ
- EU-type examination certificate in accordance with Annex III of Directive 2014/53/EU

Protection against environmental impacts

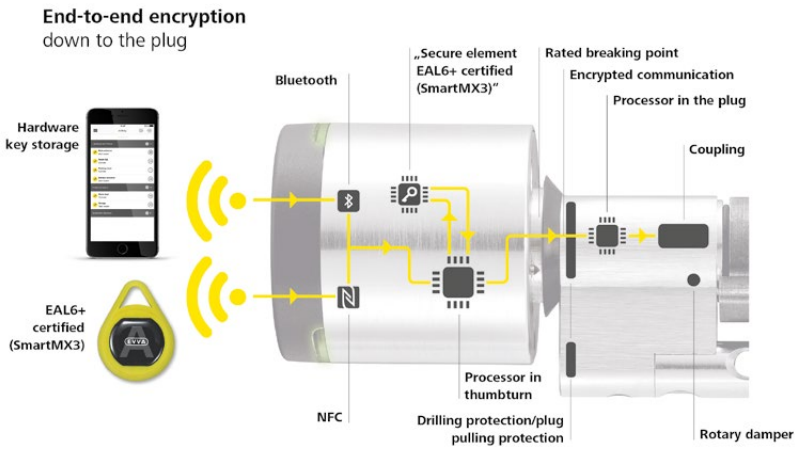
- IP65 protection against ingress of harmful dust and powerful water jets from any direction when installed
- Protective coated electronic components to prevent oxidation due to condensation
- Operating conditions: -20°C - +55°C; 2 lithium CR2 batteries in parallel for greater power supply stability

Physical security

- Drilling protection
- Plug pulling protection
- Rotary damper to protect against attacks with a high frequency spindle
- Defined rated breaking point on the thread of the outside thumbturn to protect the plug from mechanical attacks and defend against snapping attacks
- Special mechanical tool for assembly and disassembly of the cylinder thumbturn

Uncompromising electronic security

Electronic security measures in the AirKey system prevent signal and/or cryptographic key material from being misused.



1. Central security architecture

- For all AirKey components there is an extra processor in a secure area, which controls the release.
  E.g.: the cylinder thumbturn of the AirKey cylinder is cryptographically secured by an inbuilt processor in the cylinder plug, which sits behind the drilling protection - swapping the cylinder and the associated unauthorised access is impossible.
- With the use of EAL6+ certified secure elements (highly secure encryption and storage elements) in every AirKey component, EVVA is setting a new security standard for electronic access control systems.
- Only highly secure EAL6+ certified NFC smart cards are used as identification media for AirKey.
  Consequently, unauthorised copying of identification media is impossible.
  Because of this high security standard, this technology **is also used for ePassports** and credit cards.
- **End-to-end encryption via all interfaces**
  - Only tested and certified encryption methods are used
  - AirKey uses a **double** encryption for **all** data transfers:
    - **ECDSA-224** for the authentication
    - **AES-128** for session keys

• The ECDSA algorithm is based on elliptic curves and is used for the authentication between the various AirKey components. Based on the ECDSA authentication, **a random AES session key** is negotiated each time, which is used only **for the current operation** (update, lock, cylinder update, card update, etc). This procedure is used for all communications between AirKey components.

All transfered data is end-to-end encrypted:

- AirKey identification media to AirKey locking components (ECDSA / AES)
- AirKey locking components to AirKey app (ECDSA / AES)
- AirKey app to AirKey identification media (ECDSA / AES)
- AirKey app to AirKey online administration (ECDSA / AES)

2. Backend and online administration

Online administration

- Access via the Internet is secured using **TLS encryption** (https)
- When you create your password, the strength is rated so you can assess the level of security.
- **Two-factor authentication with TAN by email or SMS** can be optionally activated for administrators (6-digit alphanumeric TAN)
- Automatic sending of maintenance tasks and security information (backlists) to administrators by email or for maintenance engineers in the AirKey app.

Backend

- AirKey runs in ISO:27001-certified data centres in Austria. All data is stored on EVVA's own redundant servers in Austria.
- **EAL6+** certified **hardware security modules (HSMs)** ensure the highest level of backend security in creating and storing all encryption keys.

3. AirKey Android & iOS app

For the use of AirKey combined with a smarthphone, EVVA offers a **multi-level security concept** with the AirKey app:

- EVVA recommends that each user of a smartphone activates the **memory encryption** and screen lock with an equally secure **password, PIN or biometric login**.
- Both Android and iOS use the manufacturer-specific hardware security memory modules. (Android: hardware-backed KeyStore; iOS: Apple CryptoKit KeyChain)
- As an added security feature, the AirKey app offers an **additional PIN code** in the app, which must be entered before each locking process.
- The administrator can see whether the PIN code function in the app is activated or deactivated.
- The administrator can also specify whether the handsfree mode can be used even without a screen lock.
- The smartphone can be used **"only" as a key** or also as a **maintenance device**. This can be controlled by the administrator.
- **Automatic security:** After locking with Bluetooth, the blacklist, all identification media event logs and the time are automatically updated. This happens automatically every 6 hours or after each locking process as well when the setting is adjusted in the online administration.

4. Data protection & data security

- **AirKey meets the EU General Data Protection Regulations:** Together with the renowned data protection expert, Dr. Christof Tschohl, AirKey was developed into a data protection compliant access control system. Our own data protection officer will be happy to respond to your requests for more detail. https://www.evva.com/at-de/datenschutzerklaerung/
- The deletion of personal data required by the General Data Protection Regulation is planned in the system. During the deletion of data, all references to a person are irretrievably removed.
- The event logging of access events can be configured for each component (for a limited time as well), and also deactivated, e.g. for a Works Council conference room for which no event logging is allowed.
- The **event logging** in the backend and in the components is **revision-proof.** This means that every locking process can be retraced precisely with a date and time. Consequently, this event logging cannot be manipulated and allows for more transparency than with any mechanical access system.
- Ready for compliance with the European Data Act 2024
- A four-eyes principle for viewing logs can be activated. Access to the event logs must be approved by a second administrator.

Summary

- AirKey is the highly secure and flexible access control system, which both meets the GDPR and ensures the security of EVVA AirKey access control systems with the latest technologies in cryptography, electronic systems, firmware, software and mechanical systems through the use of secure elements, HSMs and NFC smart cards.
- The BSI/NIST **https://www.keylength.com/en/4/** confirms that the encryption procedures used and key lengths are rated as secure until 2030. The key lengths can be increased in the system by EVVA as required in order to keep the security level up-to-date with the latest technology well into the future. This is the great advantage of the JCOP media, apps and secure elements in the AirKey locking components and it also ensures the highest level of investment security thanks to updatability.