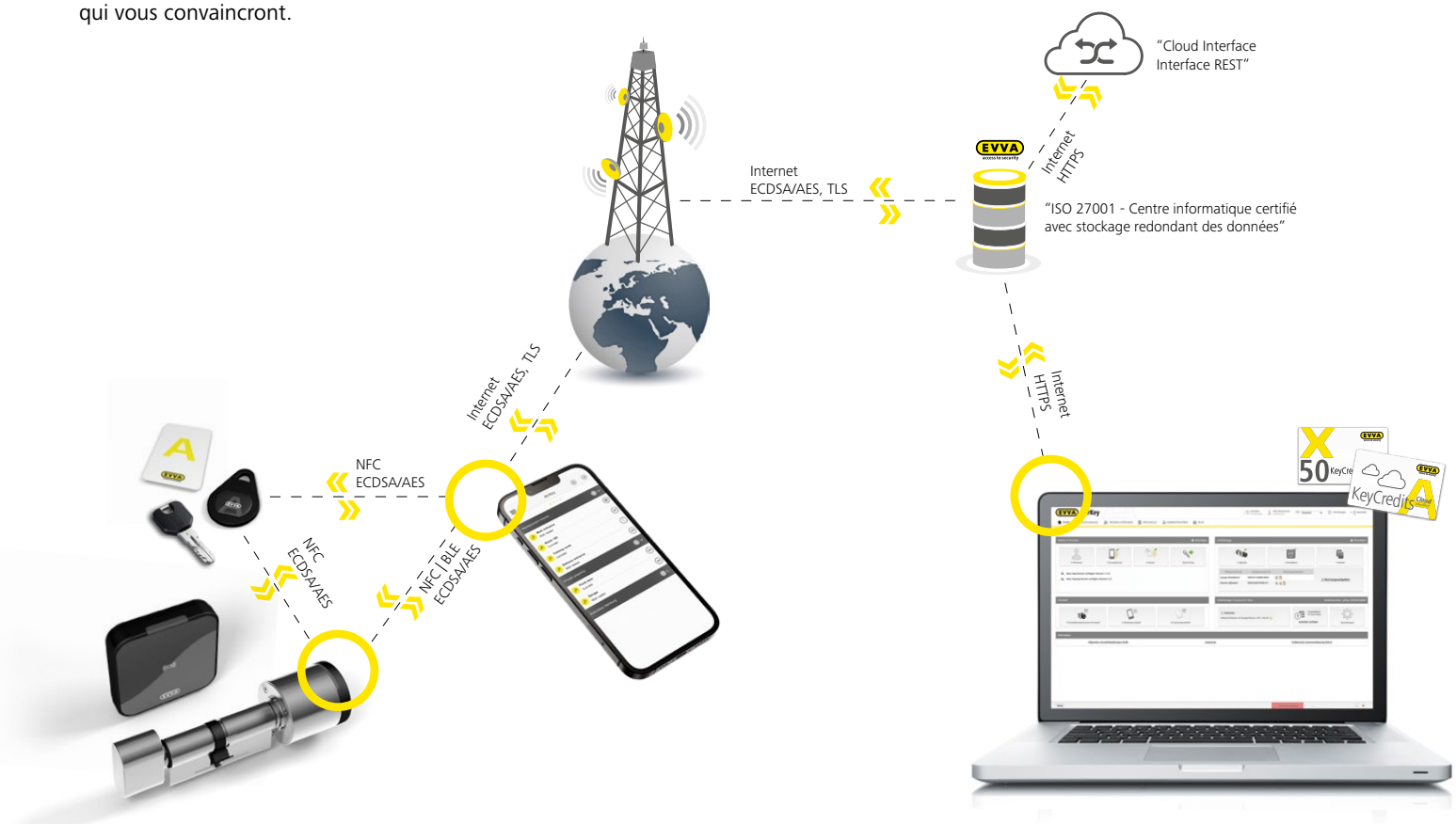
AirKey. La sécurité sans compromis

L'architecture de la sécurité du système AirKey en détail

EVVA ne fait aucun compromis en matière de sécurité. Et c'est bien ainsi car, depuis la création de l'entreprise en 1919, c'est l'un des facteurs essentiels de notre histoire, qui a fait de nous l'une des meilleures entreprises de sécurité au monde ! Notre intransigeance a ainsi été appliquée aussi rigoureusement lors de la mise en œuvre du concept de sécurité d'AirKey. Seuls des experts de haut niveau en matière de sécurité dans les domaines de la mécanique, de l'électronique et des logiciels ont participé au développement d'AirKey. AirKey s'est ainsi hissé au rang des systèmes de contrôle d'accès électroniques les plus sécurisés du marché. Voici quelques explications qui vous convaincront.



Une sécurité mécanique sans compromis

Sur le plan mécanique, le cylindre AirKey d'EVVA présente les caractéristiques maximales de sécurité suivantes dès la version standard.

Certifications

- EN15684 (1.6.B.3.A.F.3.2)
- SKG***
- SSF3522 pour les profils scandinaves
- Certification de protection incendie selon EN1634 (90 min)
- Certification antipanique selon EN179/1125
- ÖNORM B 5351:2011 W_{MZ}6-BZ
- Certificat d'examen de type UE conformément à l'annexe III de la directive 2014/53/UE

Protection contre les conditions environnementales

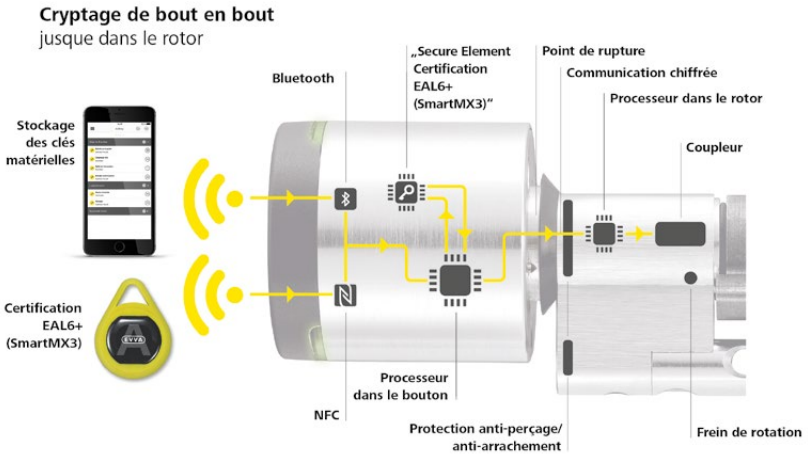
- Protection IP65 contre la pénétration de poussières néfastes et de jets d'eau puissants de toutes directions en état monté
- Module électronique avec vernis de protection contre l'oxydation due à la condensation
- Conditions d'utilisation : -20 °C - +55 °C ; 2 piles lithium CR2 parallèles pour une meilleure stabilité de l'alimentation en tension

Sécurité physique

- Protection anti-perçage
- Protection anti-arrachement
- Frein de rotation contre les attaques à l'aide d'une broche haute fréquence
- Point de rupture défini sur le filetage du bouton extérieur pour protéger le rotor contre les attaques mécaniques et pour parer aux attaques de snapping
- Outil mécanique spécial pour le montage et le démontage du bouton du cylindre

Une sécurité électronique sans compromis

Les mesures de sécurité électroniques du système AirKey empêchent l'utilisation abusive des signaux et/ou des données



1. Architecture centrale de la sécurité

- Tous les composants AirKey sont assujettis à un processeur supplémentaire qui est logé dans une zone sécurisée et qui contrôle la validation.
  Par exemple : le bouton du cylindre AirKey est sécurisé de manière cryptographique par un processeur monté dans le rotor du cylindre, **derrière la protection antiperçage**. Il n'est ainsi pas possible d'échanger le bouton pour procéder à un accès illicite.
- Grâce à l'utilisation de **« Secure Elements » certifiés EAL6+** (éléments de cryptage et de stockage hautement sécurisés) dans chaque composant AirKey, EVVA pose de nouveaux jalons de référence pour les systèmes de fermeture électroniques.
- Les supports d'identification utilisés dans le système AirKey sont exclusivement des **smartcards NFC haute sécurité** certifiées EAL6+.
  La copie illicite de supports d'identification est ainsi impossible.
  En raison de ces normes de sécurité élevées, cette technologie est **également utilisée pour les passeports électroniques** et les cartes de crédit.
- **Cryptage de bout en bout via toutes les interfaces**
  - Seules des procédés de cryptographie homologués et certifiés sont utilisés
  - Dans ce contexte, AirKey utilise un **double** cryptage pour **toutes** les transmissions de données :
    - **ECDSA-224** pour l'authentification
    - **AES-128** pour les clés de session

8 • L'algorithme ECDSA repose sur des courbes elliptiques et est utilisé pour l'authentification entre les différents composants AirKey. Dans le cadre de l'authentification ECDSA, chaque transaction génère la création **d'une clé de session AES aléatoire** utilisée uniquement **pour la transaction en cours** (actualisation, accès, mise à jour du cylindre, mise à jour des cartes, etc.). Ce procédé s'applique à toutes les communications entre les composants AirKey.

Toutes les données transmises sont cryptées de bout en bout :

- Des supports d'identification AirKey vers les composants de fermeture AirKey (ECDSA/AES)
- Des composants de fermeture AirKey vers l'application AirKey (ECDSA/AES)
- De l'application AirKey vers les supports d'identification AirKey (ECDSA/AES)
- De l'application AirKey vers la gestion online AirKey (ECDSA/AES)

2. Back-end et gestion online

Gestion online

- L'accès via le Web est sécurisé par le **cryptage TLS** (HTTPS)
- La force de votre mot de passe est évaluée lors de sa création afin de pouvoir juger du niveau de sécurité.
- **Authentification à double facteur avec code TAN via e-mail ou par SMS** pouvant être activée en option pour les administrateurs (code TAN à 6 caractères alphanumériques)
- Envoi automatique des tâches d'entretien et des informations de sécurité (listes noires) aux administrateurs par e-mail ou aux techniciens de maintenance dans l'application AirKey.

Back-end

- Le système AirKey est géré par des centres informatiques certifiés ISO:27001situés en Autriche. Toutes les données sont sauvegardées sur les propres serveurs redondants d'EVVA en Autriche.
- **Des modules HSM (Hardware Security Module)** certifiés **EAL6+** assurent une sécurité maximale dans le back-end pour la création et le stockage de toutes les clés de chiffrement.

3. Application AirKey Android et iOS

Pour l'utilisation d'AirKey en combinaison avec un smartphone, EVVA offre un **concept de sécurité à plusieurs niveaux** avec l'application AirKey :

- EVVA recommande à chaque utilisateur d'un smartphone d'activer le **cryptage de la mémoire** et de sécuriser le déverrouillage de l'écran avec un **mot de passe, un code PIN ou un identifiant biométrique** correctement sécurisé.
- Les appareils Android et iOS utilisent les modules de mémoire de sécurité matérielle spécifiques aux fabricants. (Android : Hardware-backed Keystore ; iOS : Apple CryptoKit KeyChain)
- L'application AirKey offre en outre une fonction de sécurité supplémentaire qui exige l'entrée d'un **code PIN supplémentaire** dans l'application avant chaque opération d'accès.
- L'administrateur voit si la fonction de code PIN est activée ou désactivée dans l'application.
- L'administrateur peut définir si le mode mains libres peut également être utilisé sans déverrouillage de l'écran.
- Le smartphone peut être utilisé **« uniquement » comme clé** ou aussi comme appareil d'entretien. Cela peut être défini par l'administrateur.
- **Sécurité automatique :** Après un accès par Bluetooth, la liste noire, les entrées de journalisation de tous les supports d'identification ainsi que l'heure sont automatiquement mis à jour. Cette procédure se déroule automatiquement toutes les 6 heures ou après chaque opération d'accès en fonction du paramétrage correspondant dans la gestion online.

4. Protection et sécurité des données

- **AirKey répond aux exigences du règlement général européen sur la protection des données :** AirKey a été développé en coopération avec Dr. Christof Tschol, l'expert reconnu de la protection des données, pour constituer un système de contrôle d'accès conforme aux impératifs de la protection des données. Notre propre délégué à la protection des données se tient volontiers à votre disposition pour vous fournir de plus amples informations. https://www.evva.com/at-de/datenschutzerklaerung/
- La suppression des données à caractère personnel exigée par le règlement général européen de la protection des données est prévue dans le système. Dans ce contexte, tout lien à une personne est supprimé de manière irréversible.
- La journalisation des événements d'accès peut être configurée individuellement pour chaque composant (aussi avec une durée limitée) ou être désactivée, ce qui est nécessaire, par exemple, pour une salle de réunion du comité d'entreprise où la journalisation est interdite.
- La **journalisation** dans le back-end et dans les composants est **sécurisée**, c.-à-d. non modifiable. En d'autres termes, chaque opération d'accès est retraçable exactement avec la date et l'heure. Cette journalisation ne peut ainsi pas être manipulée et offre une meilleure transparence que pour un système de fermeture mécanique.
- Préparé pour se conformer au règlement européen sur les données 2024
- Il est possible d'activer un principe des quatre yeux pour la consultation des journalisations. Pour cela, la consultation des journalisations doit être autorisée par un deuxième administrateur.

Résumé

- AirKey est le système de contrôle d'accès hautement sécurisé et flexible qui répond aux exigences du RGPD tout en assurant la sécurité des installations de fermeture AirKey EVVA avec des technologies ultramodernes de cryptographie, d'électronique, de firmware, de logiciel et de mécanique grâce à l'utilisation de Secure Elements, de modules HSM et de smardcards NFC.
- L'Office fédéral allemand de la sécurité des technologies de l'information (BSI) et l'Institut national des normes et de la technologie des États-Unis (NIST) **https://www.keylength.com/en/4/** confirment que les procédés de cryptage et les longueurs des clés utilisés sont considérés comme sûrs jusqu'en 2030. Les longueurs des clés peuvent être augmentées dans le système par EVVA si nécessaire, ce qui a été réalisé avec succès en 2023, afin de maintenir le niveau de sécurité à l'état de la technique dans un avenir plus lointain. Cela repose sur le grand avantage des supports JCOP, des applications et des Secure Elements dans les composants de fermeture AirKey, ce qui assure également une sécurité d'investissement maximale grâce aux possibilités de mise à jour/niveau.