25. Oktober 2023News EVVA Produktnews Produktmanagement, Autor: Martin Bauer

Next Level Verschlüsselung bei AirKey!

Mit dem neuesten AirKey-Update sind wir nicht nur in ein neues Datacenter mit ISO-27001-Zertifiterung gezogen, siehe Produktnews: wwwi.evva.com/aktuell/news/news/datum/2023/10/23/airkey-wird-noch-sicherer/, es wurde ebenso die kryptographische Verschlüsselung auf das nächste Level angehoben. Nur was bedeutet das im Detail?

ECDSA-Schlüssellänge erhöht:

- ECDSA ist ein Verschlüsselungsverfahren.
- Die ECDSA-Schlüssellänge wurde von 224 auf 256 erhöht und die Sicherheit wurde somit erhöht, ohne an Performance einzubüßen

Info: ECSDA wird u.a. von Bitcoin als kryptographischer Verschlüsselungsalgorithmus verwendet und ist somit ein absolut sicheres Verschlüsselungsverfahren!

EAL6+ zertifizierte SE (Secure Elements) und HSM (Hardware-Security-Module am Server)

- EAL ist die Beurteilung des Sicherheitslevels nach gewissen Prüfstandards
- EAL6+ zertifizierteSecure Elements (SE) und Hardware Security Modules (HSMs) sorgen in allen AirKey Komponenten, Identmedien sowie im Backend für höchste Sicherheit in der Erstellung und Speicherung aller Encryption-Keys

Der Branchenstandard ist EAL5+. AirKey ist somit besser als unsere Marktbegleiter!

Hardware-Keystore für Android & iOS

- iOS bereits vorhanden und wurde um den neuen Android-Keystore erweitert
- Das bedeutet, dass die kryptografischen Schlüssel am Smartphone noch besser geschützt werden als bisher.

AirKey bietet somit noch mehr Sicherheit direkt am Smartphone!