EVIDEN

CardOS V8 PQC

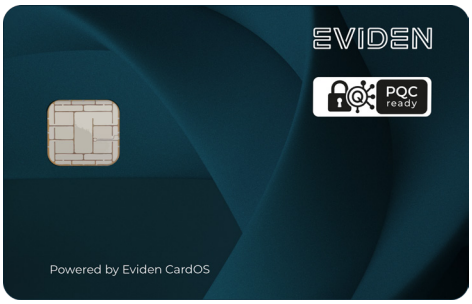
Post-Quantum Cryptography with CardOS

CardOS V8 PQC brings post-quantum security to the trusted CardOS platform, enabling the use of ML-KEM and ML-DSA—today's most important post-quantum cryptographic algorithms.

CardOS is a high-security, native smart card operating system that provides all essential functions to support a wide range of applications via both contact-based and contactless interfaces. It powers solutions such as eID and ePassport systems, citizen and health cards, employee badges, signature and loyalty cards—all of which can be easily expanded with customized packages.

The cryptographic foundation of CardOS is built on state-of-the-art algorithms including AES, SHA-2, and elliptic curves. Certified according to Common Criteria EAL4+ and listed as an eIDAS-compliant QSCD and QSealCD in the official eIDAS member states notification list, CardOS stands for proven trust and compliance.

With the release of CardOS V8 PQC, CardOS enters the post-quantum era. The new version supports ML-KEM (CRYSTALS-Kyber) and ML-DSA (CRYSTALS-Dilithium)—today's most important post-quantum cryptographic algorithms—ensuring long-term protection against quantum computing threats.



Product highlights

CardOS V8 PQC ...

- enhances the smart card operating system CardOS with additional features,
- is based on Infineon 28nm technology TEGRION™, a highly innovative hardware platform,
- supports PQC-based signature applications—as one of the first commercial PQC smart cards,
- supports version 2 of Extended Access Control (EACv2),
- is currently being EAL5+ certified according to the latest CC version,
- provides certified patch management,
- is optimized for efficient initialization and personalization,
- uses flash memory efficiently, which provides more user memory,
- executes inspection procedures especially fast, which includes the reading of large biometric data (photo, fingerprint),
- offers excellent integration support for partners with respect to tools and know-how.

EVIDEN

CardOS V8 PQC customer benefits

ICAO-compliant eID/ePassport solution

Certified multi-application eID solution

eIDAS QSCD / QSealCD

PQC based signature application

Optional support of FIDO2 and OpenPGP, based on PQC

Standards and technical specifications

- Dual Interface / contactless / contact-based version
- Contactless interface according to ISO14443 Type A and B
- Dual Interface hardware platform based on 28nm technology TEGRION™: IFX chip SLC27GDA
- NFC support
- ICAO and eID functionality (BAC, EACv1, EACv2, RI, PACE, AA)
- Optional Packages for FIDO2 and OpenPGP
- Crypto algorithms:
  - 3DES, AES (256 bit)
  - RSA (up to 4096 Bit key size)
  - SHA-1, SHA-2 (up to 512 bit)
  - ECDSA (up to 521 bit)
  - Post-quantum cryptography (ML-DSA / CRYSTALS-Dilithium, ML-KEM / CRYSTALS-Kyber)
- RNG according to DRG.4 / PTG.3
- EAL 5+ Common Criteria certification according to ICAO PPs EAC/PACE (PP-0056v2, PP-0068v2), BAC (PP-0055) and SSCD-PPs (PP-0059, PP-0071, PP-0072) with certified patch management
- EAL 6+ Common Criteria certification of IFX chip platform according to PP-0084
- Modules COM10.8, COM8.4, S-MFC8.8 (DI), MCS8 (CL)

More information:

20260122