Post-quantum transition for IoT

Quantum threat

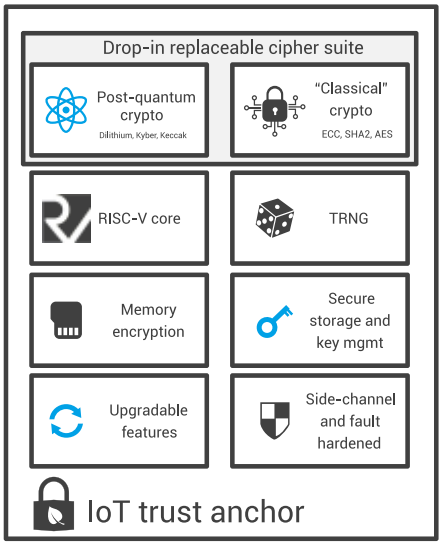
Quantum computers will render the current industry-standard public key cryptography insecure. US gov. contractors must use new Post-Quantum Crypto (PQC) standard as default from 2025 and fully switch to PQC by 2035. Europe is following suite.

PQC transition

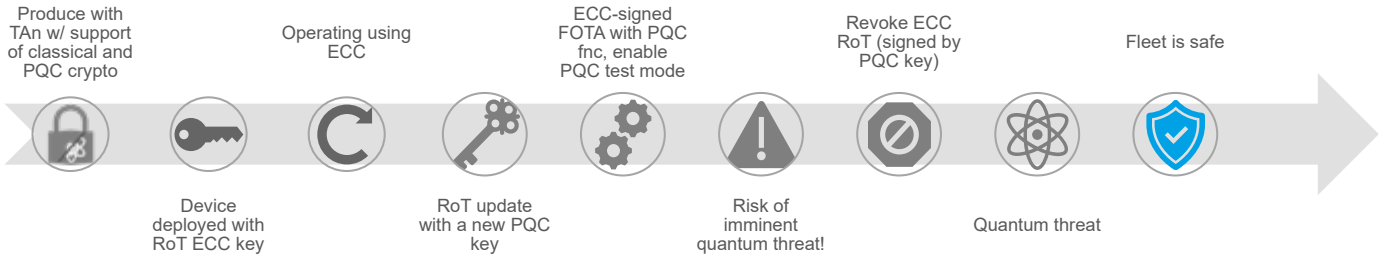
Making an IoT fleet post-quantum ready implies a backward non-compatible replacement of cryptographic keys and implementations in all devices. CSEM is designing the software, the hardware and other technology for a smooth post-quantum Iot transition deployed over the air, minimizing costs and complications.

IoT trust anchor

CSEM's proposed solution is a low-footprint TAn (hard macro and associated firmware) offering state-of-the-art cryptographic accelerators designed to resist low-skilled to medium-level attacks (e.g., AVA_VAN2/3) throughout the lifespan of a typical low-cost IoT solution. Our architecture is RISC-V based and supports post-quantum cryptography and TAn reconfiguration over-the-air mechanisms to ensure sustainability. Resultantly, our TAn embeds the necessary tools to secure IoT solutions over a long life span (≥ 20 years).



We would love to hear your thoughts! Please, contact us by following the QR code below.



Post-Quantum transition over the air