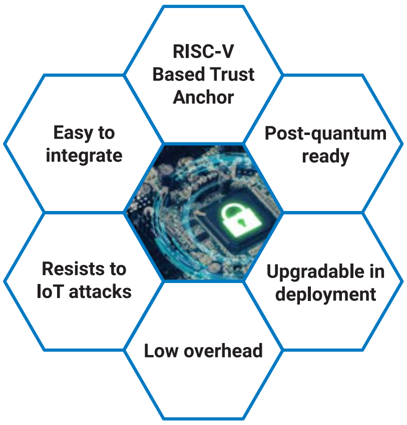
Sustainable IoT Trust Anchor

Enabling security in cost-constrained markets

Sustainable IoT Trust Anchor (TAn) that enables future-proof cryptography (post-quantum included) to secure IoT solutions over a long lifespan, with a small footprint and with remotely upgradable features

General description

CSEM's TAn solution is a security module that protects credentials for markets, such as wearables and IoT end nodes in agriculture, industry, and healthcare. It enforces secure execution of state-of-the-art cryptographic operations in System-on-Chips (SoC).



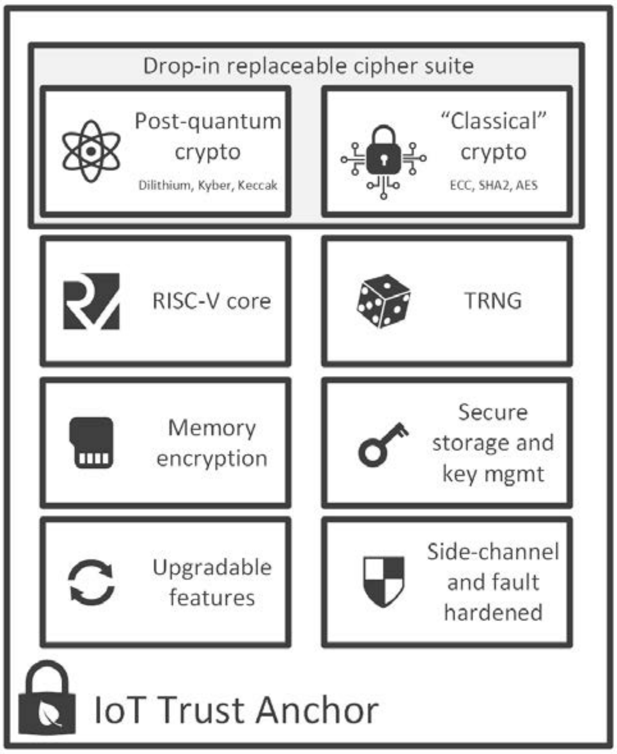
Why a new TAn ?

Existing Trust Anchors are generally designed to withstand the highest level of malicious threats, therefore, incurring an overhead (e.g., chip surface, latency). These are either inefficient or oversized for low-cost IoT solutions and, consequently, are not adapted to securing IoT communications. Furthermore, security modules are rarely designed to be regularly upgraded to adapt to the evolving threat landscape.

- Optimized performance
- Low cost
- Upgradable features
- Low Integration complexity
- Post-quantum crypto

Key features

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, let us know what you think about this solution in this two-minute survey.