

VaultIC409

Quantum Resistant Secure Element

Our Secure Element VaultIC409, provides all cryptographic algorithms and tamper resistant storage to enable the implementation of state-of-the-art security features in a large panel of devices: Immutable digital identity, Secure communication, Firmware download, Encryption and more...



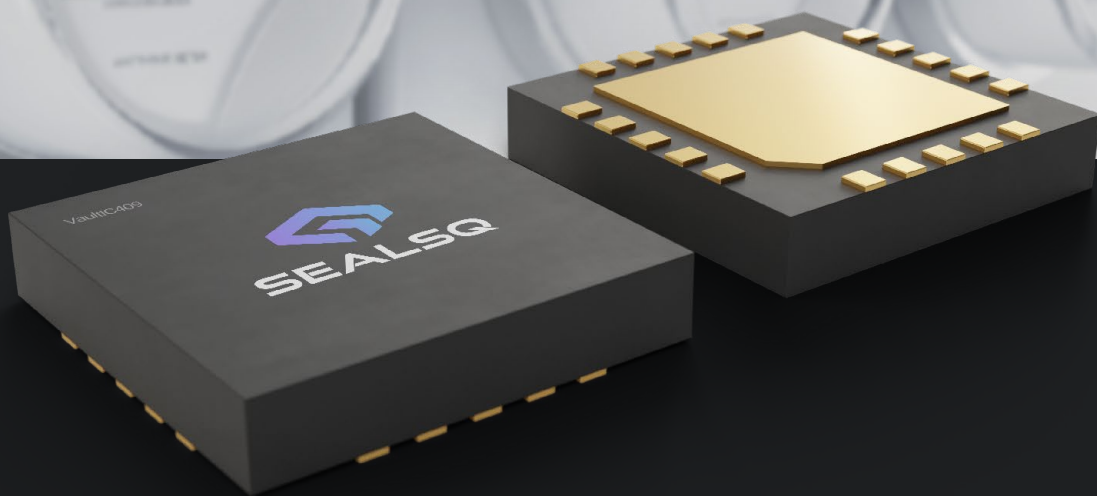
End-to-End Security



**Targeted Certification :
CC EAL5+**

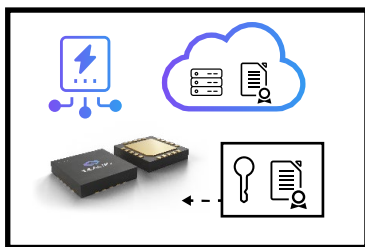
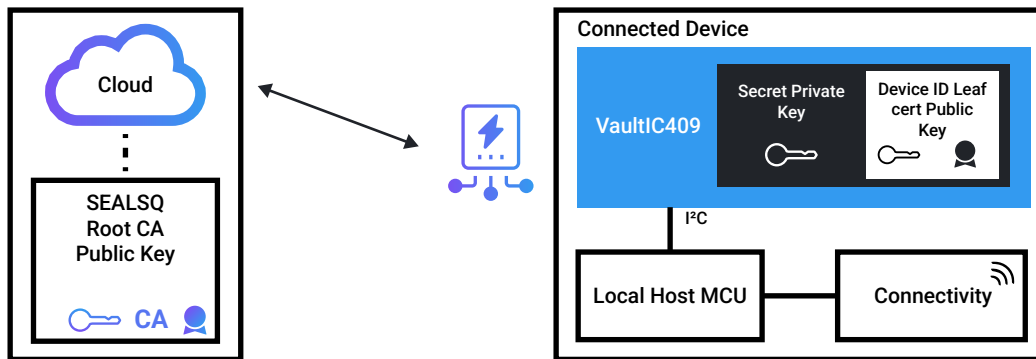


**PQC Accelerator
(Dilithium / Kyber)**

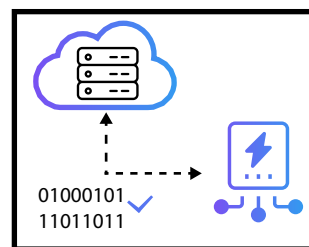


- SHA-3 hardware accelerator
- Hardware Root of Trust for high-risk and long lifecycle products
- Crypto-agility with standard and PQC algorithms for hybrid cryptography
- Security deployment & maintenance with INeS IoT security platform

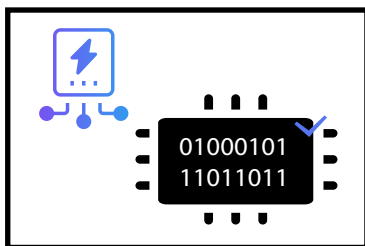
VaultIC409 is preloaded with secrets and X509 certificates to enable strict authentication. It also includes API that implements security protocols for authentication purposes.



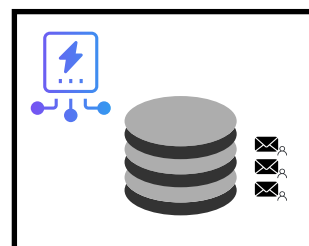
VaultIC409 is delivered with a pre-loaded X509 certificate and the security protocol that authenticate the device.



VaultIC409 ensures the integrity and confidentiality of exchanged data by signing and/or encrypting them.



VaultIC409 ensures that credentials and sensitive data are securely stored in the Secure Element storage and in the non-volatile memory of the device.



VaultIC409 verifies the signature of the device's application firmware, at the initial start as well as when the firmware is updated.

Technical Features

Cryptographic services authentication:

- Elliptic Curve digital signature generation and validation (ECC, GFp) up to 572bits.
- RSA up to 4096 bits .
- Key Establishment ECC-DH, Message encryption AES, Message Digest SHA256, 384 or 512, SHA-3, Strong Authentication Global Platform SCP03
- PQC Keys (ML-KEM- 512, 768, 1024 & ML-DSA-44, 65, 87)
- On-chip key pair generation or VaultiTrust™ data generation and provisioning

Certifications / Standards:

- True RNG: NIST SP 800-90B
- Targeted CC EAL5+
- Targeted NIST FIPS 140-3 Level 3 CMVP

Hardware Platform:

- Flash-based memory with error correction
- Up to 50KB free NVM for secure data storage
- Operating range: 1.62V-3.6V.
- Extended industrial temperature range (-40°C to +105°C).
- Available package: QFN32 (5mm x 5mm).

Interfaces and Communication

- I2C
- SPI
- Automatic Detection of the Communication Interface
- 4 GPIO (for future use)