

QVault TPM

Quantum Resistant Certified Trusted Platform Module (TPM)

Quantum Resistant, flash-memory-based, firmware upgradable Trusted Platform Module compliant with TPM 2.0 & FIPS 140-3 requirements. Built on a powerful RISC-V Common Criteria EAL5+ hardware platform.



Trusted Boot

Ensures system integrity during startup



Device Attestation

Protect against alterations of identity & device integrity



Secure Authentication

For devices, users, and platforms



IoT Device Security

Protects connected devices from unauthorized access



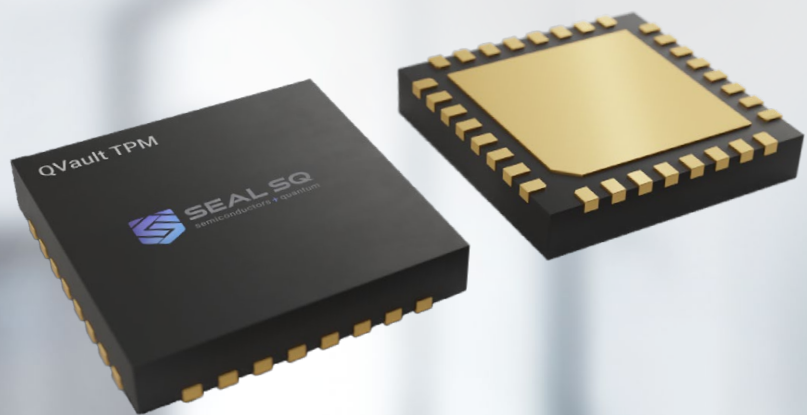
Cryptographic Key Management

Secure generation, storage, and management of cryptographic keys



Data Integrity Protection

Ensures data integrity and authenticity



TPM 2.0



Security Features

- Physical and Environmental Protections:
 - Active shield for physical tamper protection
 - Monitors for voltage, temperature, frequency and light conditions to detect tampering
- Side-Channel Attack Resistance
- Fault Injection Resistance
- Random Number Generation: FIPS SP800-90A DRBG & FIPS SP800-90B TRNG Entropy Source
- Pre-provisioning:
 - Three Endorsement Keys & Certificates (RSA 2048, ECC NIST P-256, ECC NIST P-384)
 - Three 2048-bit RSA key pairs
 - PQC Keys (ML-KEM-1024 & ML-DSA-44)
- Fault-tolerant firmware loader for safe updates

Memory and Storage

- Flash-based memory with error correction
- Up to 50KB free NVM for secure data storage
- Data retention of up to 15 years, with write/erase endurance of 200,000 cycles

Interfaces and Communication

- I²C Interface up to 1 Mb/s
- SPI Interface up to 33 MHz
- Automatic Detection of the Communication Interface
- 4 GPIOs

Cryptographic Services

The QVault TPM provides a broad range of cryptographic services designed to support security needs across multiple industries:

- RSA:
 - Key generation (1024, 2048, 3072, 4096-bit)
 - Encryption: RSAES-OAEP, RSAES-PKCS1-v1_5
 - Signing: RSASSA-PSS, RSASSA-PKCS1-v1_5
- AES
 - 128/192/256-bit encryption, with modes like ECB, CBC, GCM, CFB
- Elliptic Curve Cryptography (ECC):
 - Supported curves: NIST P-256 and P-384
 - Key generation, ECDH (key exchange), ECDSA (signing)
- Hash Functions:
 - SHA1, SHA2 (256/384), and SHA3 (256/384)
- Message Authentication:
 - MAC using SHA1, SHA2, and SHA3

Electrical Characteristic

- Supply Voltage: 1.62 V to 3.6 V
- Operating Temperature Range: -40°C to 105°C
- Electrostatic Discharge (ESD) Protection: Up to 2 kV (HBM)