Summary Data Sheet

6657 V0.05

QVAULT TPM

SEAL SQ
semiconductors + quantum

Table of Contents

1 Product Overview

The QVault TPM is a high-security, flash-memory-based Trusted Platform Module (TPM) compliant with the Trusted Computing Group (TCG) TPM 2.0 specifications, revision 1.83

It is Post Quantum Cryptography (PQC) capable and can be firmware upgraded on the field to enable such features.

Designed for PC, embedded and IoT applications, it provides essential cryptographic services for data confidentiality, integrity, and authentication, with interfaces for I²C and SPI communication.

Key Applications:

- Trusted Boot: Ensures system integrity during startup
- Device attestation: Protecting 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

2 Certifications

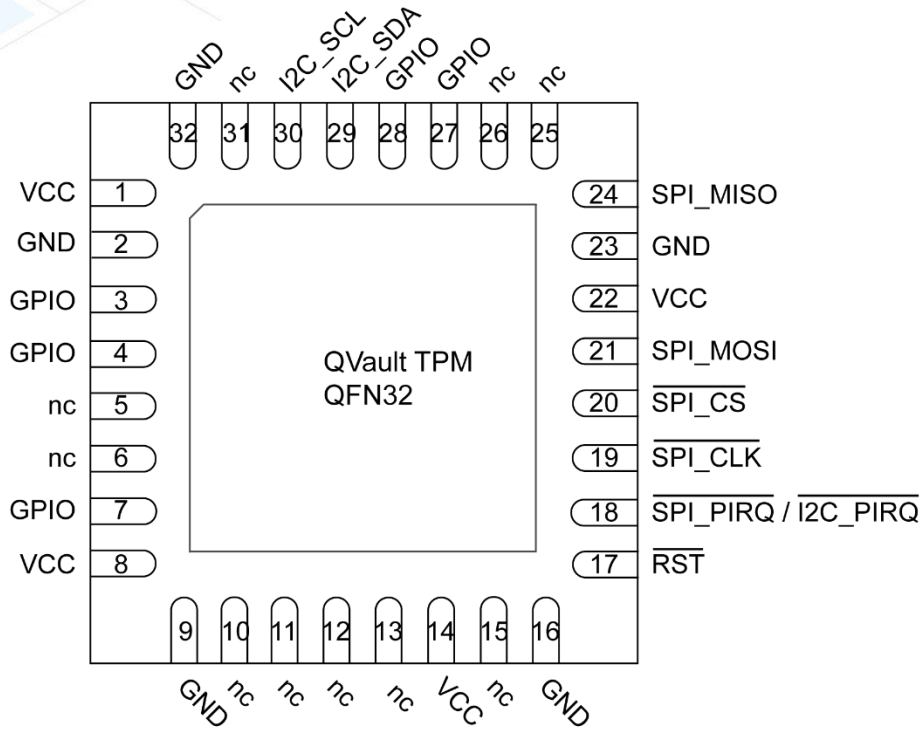
- Common Criteria EAL4+
- FIPS 140-3
- TCG TPM 2.0 Certification

3 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 Entropy Source for TRNG
- Endorsement Keys:
  - Pre-provisioned with three EK & Certificates (RSA 2048, ECC NIST P-256, ECC NIST P-384)
  - Pre-provisioned with three 2048-bit RSA key pairs
  - Pre-provisioned with PQC Keys for Future Use (ML-KEM-1024 & ML-DSA-87)
- Fault-tolerant firmware loader for safe updates

4 Pinout

- QVault TPM's pinout is compliant with the TCG Specifications and provides both I²C & SPI Interfaces.



nc = not internally connected

The exposed pad is not internally connected (floating).
It is recommended, but not mandatory, to connect it to the board GND

5 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 (256/384/512), SHA3 (256/384/512), SHAKE128, SHAKE256
- Message Authentication:
  - HMAC using SHA1, SHA2, and SHA3

6 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

7 Interfaces and Communication

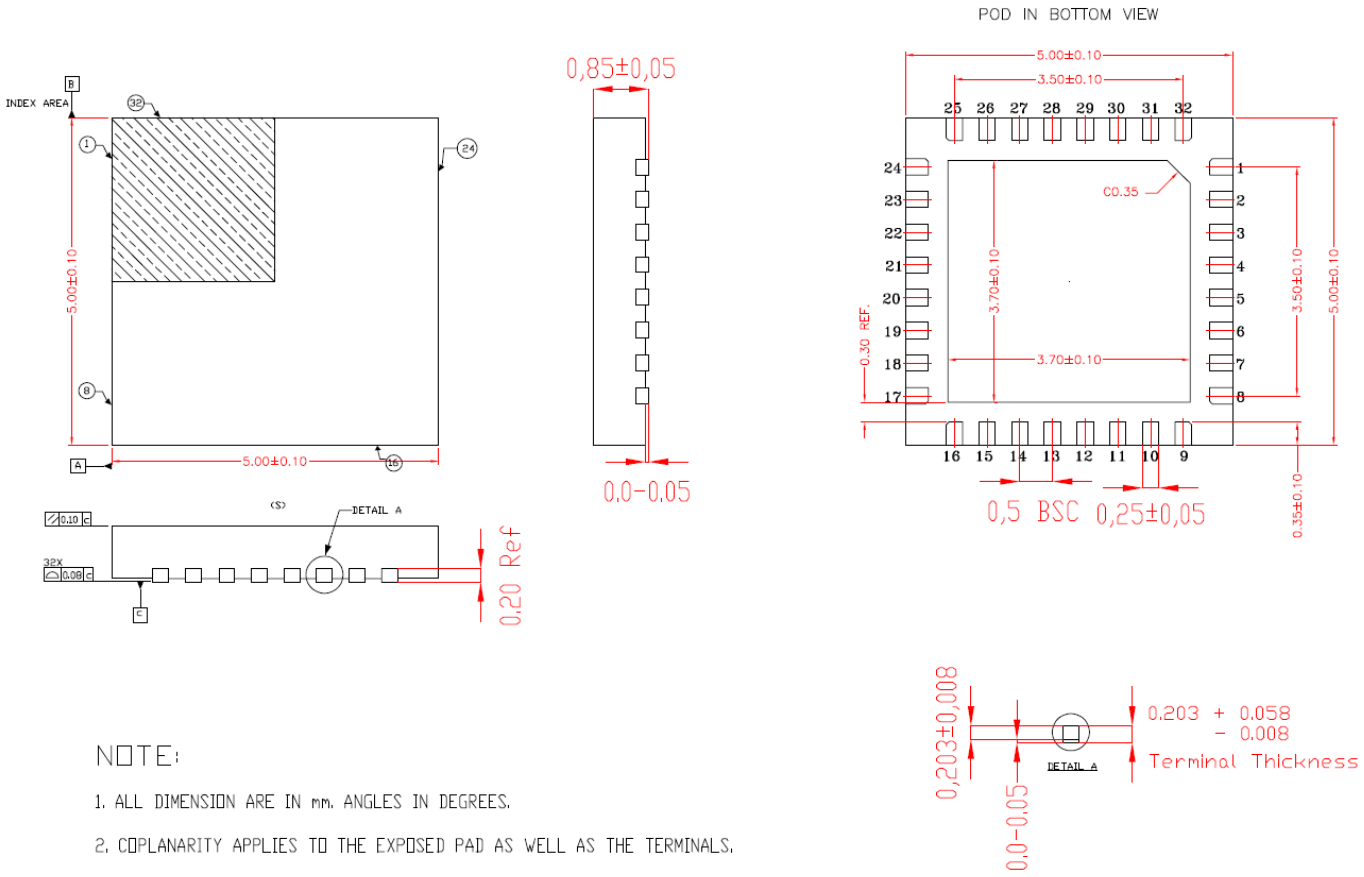
- I²C Interface up to 1 Mb/s
- SPI Interface up to 33 MHz
- Automatic Detection of the Communication Interface
- 4 GPIOs

8 Electrical Characteristics

- 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)

9 Package

- QFN32 (RoHS compliant) 5mm x 5mm x 0.85mm



NOTE:

1. ALL DIMENSION ARE IN mm. ANGLES IN DEGREES.
2. COPLANARITY APPLIES TO THE EXPOSED PAD AS WELL AS THE TERMINALS.
   COPLANARITY SHALL NOT EXCEED 0.08 mm.
3. WARPAGE SHALL NOT EXCEED 0.10 mm.
4. PACKAGE LENGHT / PACKAGE WIDTH ARE CONSIDERED AS SPECIAL CHARACREISTIC. (S)
5. REFER JEDEC MO-220

Headquarters

SEALSQ
Arteparc de Bachasson - Bat A
Rue de la Carrière de Bachasson
CS 70025
13590 Meyreuil - France
Tel: +33 (0)4-42-370-370
Fax: +33 (0)4-42-370-024

Product Contact

Web Site
www.sealsq.com

Technical Support
dl_e-security@sealsq.com

Sales Contact
sales@sealsq.com