



Summary Data Sheet

6657 V0.05

QVAULT TPM



Table of Contents

1	<i>Product Overview.....</i>	3
2	<i>Certifications</i>	3
3	<i>Security Features</i>	3
4	<i>Package.....</i>	6
5	<i>Pinout.....</i>	3
6	<i>Cryptographic Services</i>	4
7	<i>Memory and Storage.....</i>	5
8	<i>Interfaces and Communication.....</i>	5
9	<i>Electrical Characteristics</i>	5



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

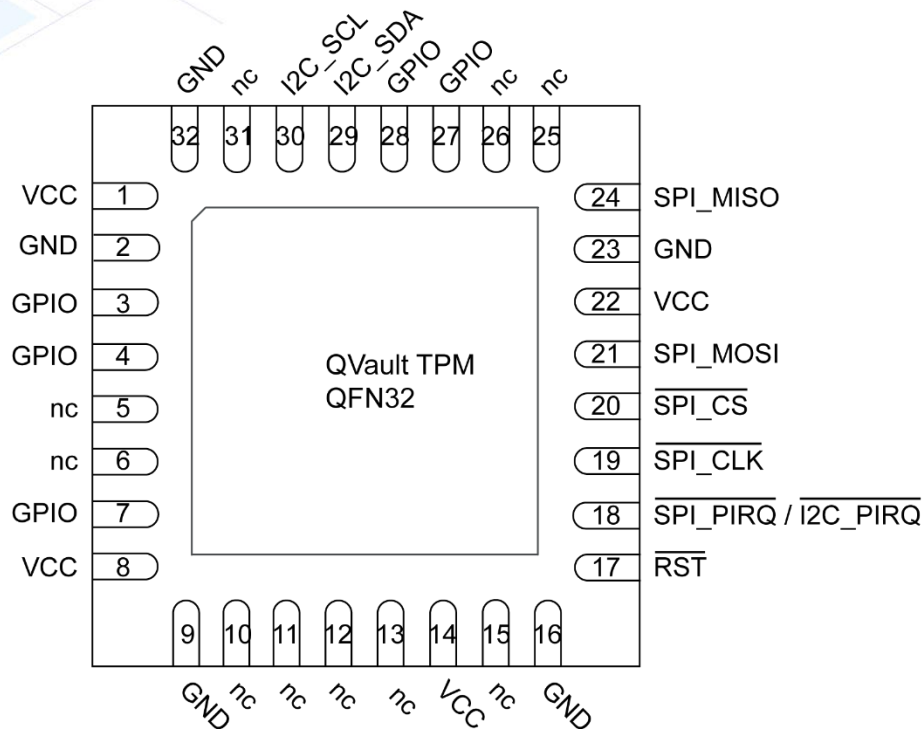
- Common Criteria EAL4+
- FIPS 140-3
- TCG TPM 2.0 Certification

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

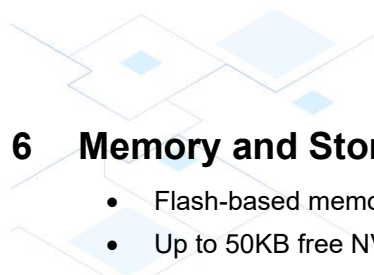
The exposed pad is not internally connected (floating).

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

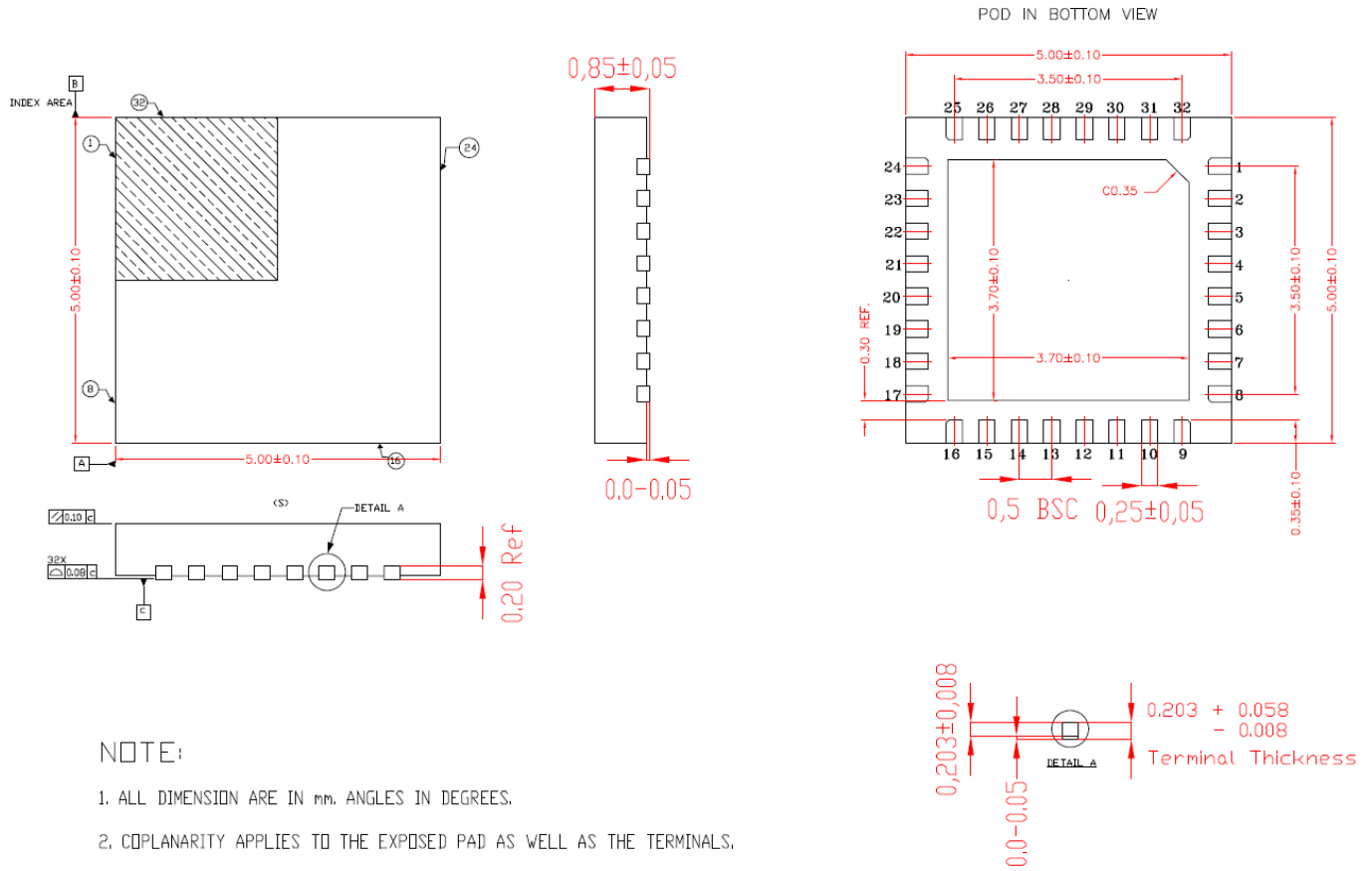
- I²C Interface up to 1 Mb/s
- SPI Interface up to 33 MHz
- Automatic Detection of the Communication Interface
- 4 GPIOs

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)

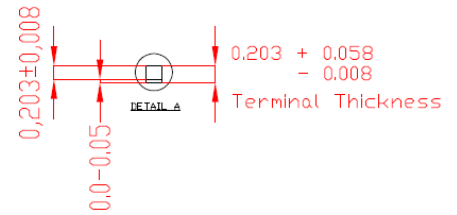
9 Package

- 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

Disclaimer: All products are sold subject to SEALSQ Terms & Conditions of Sale and the provisions of any agreements made between SEALSQ and the Customer. In ordering a product covered by this document the Customer agrees to be bound by those Terms & Conditions and agreements and nothing contained in this document constitutes or forms part of a contract (with the exception of the contents of this Notice). A copy of SEALSQ's Terms & Conditions of Sale is available on request. Export of any SEALSQ product outside of the EU may require an export Licence.

The information in this document is provided in connection with SEALSQ products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SEALSQ products. EXCEPT AS SET FORTH IN SEALSQ'S TERMS AND CONDITIONS OF SALE, SEALSQ OR ITS SUPPLIERS OR LICENSORS ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SEALSQ BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, EXEMPLARY, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, LOSS OF REVENUE, BUSINESS INTERRUPTION, LOSS OF GOODWILL, OR LOSS OF INFORMATION OR DATA) NOTWITHSTANDING THE THEORY OF LIABILITY UNDER WHICH SAID DAMAGES ARE SOUGHT, INCLUDING BUT NOT LIMITED TO CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCTS LIABILITY, STRICT LIABILITY, STATUTORY LIABILITY OR OTHERWISE, EVEN IF SEALSQ HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SEALSQ makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SEALSQ does not make any commitment to update the information contained herein. SEALSQ advises its customers to obtain the latest version of device data sheets to verify, before placing orders, that the information being relied upon by the customer is current. SEALSQ products are not intended, authorized, or warranted for use as critical components in life support devices, systems or applications, unless a specific written agreement pertaining to such intended use is executed between the manufacturer and SEALSQ. Life support devices, systems or applications are devices, systems or applications that (a) are intended for surgical implant to the body or (b) support or sustain life, and which defect or failure to perform can be reasonably expected to result in an injury to the user. A critical component is any component of a life support device, system or application which failure to perform can be reasonably expected to cause the failure of the life support device, system or application, or to affect its safety or effectiveness.

The security of any system in which the product is used will depend on the system's security as a whole. Where security or cryptography features are mentioned in this document this refers to features which are intended to increase the security of the product under normal use and in normal circumstances.

© SEALSQ 2025. All Rights Reserved. SEALSQ ®, SEALSQ logo and combinations thereof, and others are registered trademarks or tradenames of SEALSQ or its subsidiaries. Other terms and product names may be trademarks of others.

The products identified and/or described herein may be protected by one or more of the patents and/or patent applications listed in related datasheets, such document being available on request under specific conditions. Additional patents or patent applications may also apply depending on geographic regions.