Technical Datasheet
(PRELIMINARY)

TPR1003A

# QVAULT TPM 183
# TECHNICAL DATASHEET



SEAL SQ
semiconductors + quantum

# Table of Contents

# 1. Product Overview

The QVault TPM 183 is a Trusted Platform Module (TPM) compliant with the Trusted Computing Group (TCG) TPM 2.0 specifications, revision 1.83.

It provides essential cryptographic services for data confidentiality, integrity, and authentication, with interfaces for I²C and SPI communication.

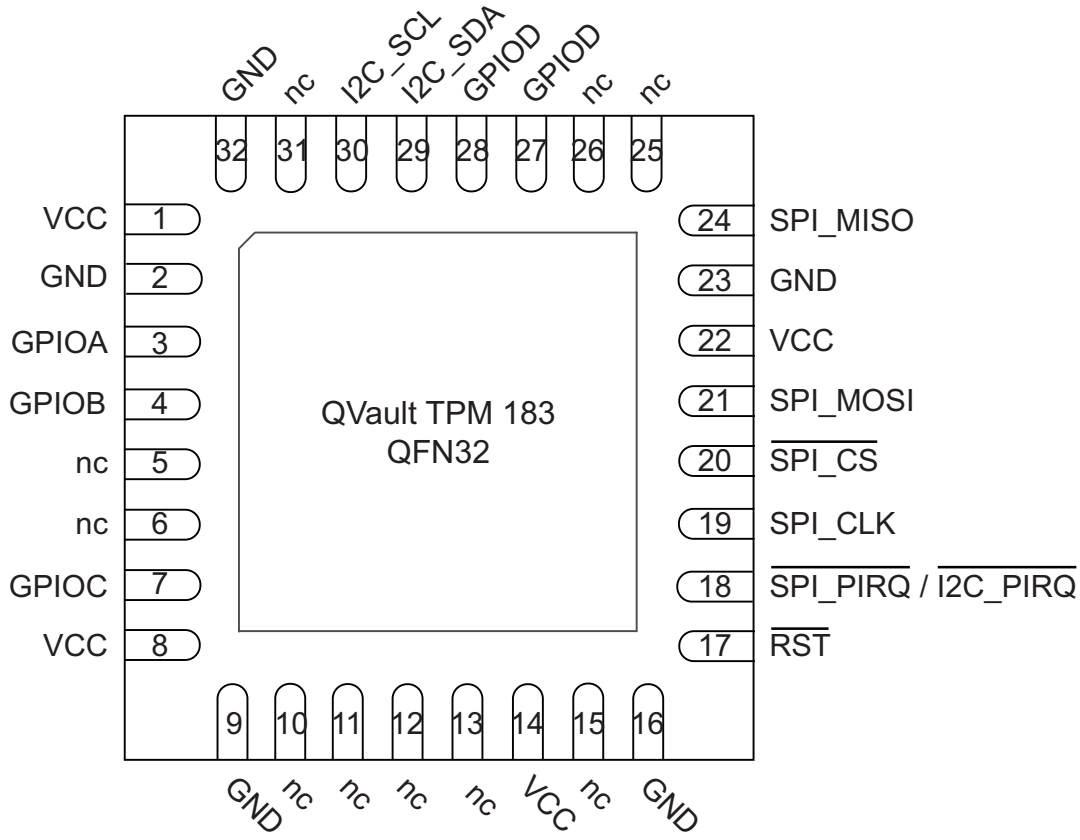
- **Key Applications:**
  - **Trusted Boot: ensures system integrity during startup**
  - **Device attestation: protects against alterations of identity & device integrity**
  - **Secure Authentication: for devices, users, and platforms**
  - **IoT Device Security: protects connected devices from unauthorized access**
  - **Cryptographic Key Management: secure generation, storage, and management of cryptographic keys**
  - **Data Integrity Protection: ensures data integrity and authenticity**
- **Certifications**
  - **Common Criteria EAL4+**
  - **FIPS 140-3**
  - **TCG TPM 2.0**
- **Security Features**
  - **Physical and Environmental Protections**
  - **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)**
  - **Fault-tolerant firmware loader for safe & secure updates**
    - **Firmware can only be updated with a TCG certified & SEALSQ authenticated new image**
- **Memory and Storage**
  - **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**
- **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 2kV (HBM)**
- **Ordering information**

**Table 1-1.** Part numbers

| Reference | Description |
|---|---|
| QVault TPM-022-Z | QFN32 production QVault TPM 183 |
| QVAULTTPM_RPI_STK | Development kit for QVault TPM 183 - Raspberry Pi header |

# 2. Pinout and package

The QVault TPM 183 is available in QFN32 package, is pinout 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

**Table 2-1.** Pin description

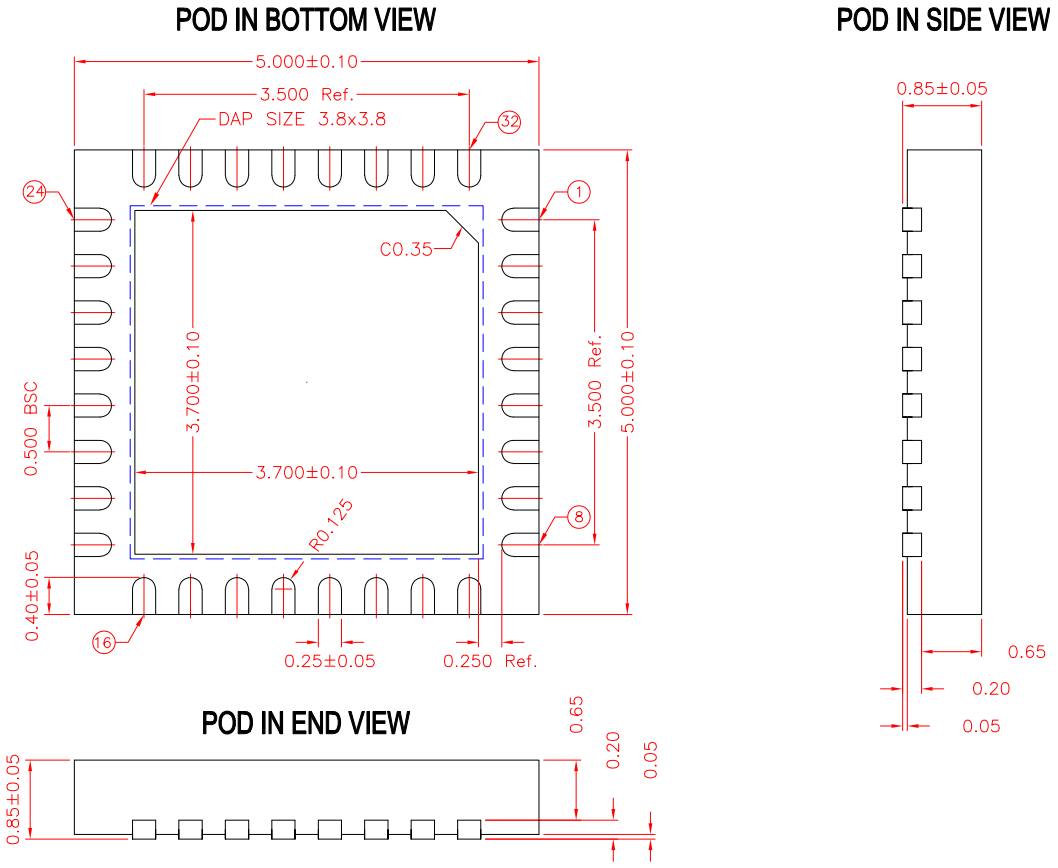
| Pin | Type | Description |
|---|---|---|
| VCC | Power supply | Power supply |
| GND | Power supply | Ground |
| GPIO A, B, C and D | I/O | General purpose input output |
| $\overline{\text{RST}}$ | Input | Device reset, active low |
| $\overline{\text{SPI\_PIRQ}}$ / $\overline{\text{I2C\_PIRQ}}$ | Output | SPI or I2C interrupt, active low, open drain |
| SPI_CLK | Input | SPI clock signal |

**Table 2-1.** Pin description

| Pin | Type | Description |
|---|---|---|
| $\overline{\text{SPI\_CS}}$ | Input | SPI chip select |
| SPI_MOSI | Input | SPI data input |
| SPI_MISO | Output | SPI data output |
| I2C_SDA | I/O | $I^2C$ data pin signal - open drain |
| I2C_SCL | Input | $I^2C$ clock signal |

**Figure 2-1.** Product marking - top view

**Figure 2-2.** QFN32 (RoHS compliant) 5mm x 5mm x 0.85mm outline




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

# 3. Implementation details

The QVault TPM 183 follows the Trusted Computing Group (TCG) TPM 2.0 specifications, revision 1.83 ([R1] [R2] [R3] [R4]) and the PC Client Platform TPM Profile for TPM 2.0 version 1.06 ([R5]). In these specifications some features are optional and others are vendor-specific. This section details what is actually implemented on the QVault TPM 183.

## 3.1 TPM attributes and cryptographic capabilities

### 3.1.1 QVault TPM properties implementation

The fixed properties of the QVault TPM 183 are defined in the Table 3-1. These properties can be read on the device thanks to the TPM2_Get_Capability query.

**Table 3-1.** TPM fixed properties

| Capability Name | Returned Value | Description |
|---|---|---|
| TPM2_PT_HR_TRANSIENT_MIN | 3 | The number of transient objects that can be held in the QVault TPM RAM.<br>QVault TPM supports 2 RSA 3072-bit keys. |
| TPM2_PT_HR_PERSISTENT_MIN | 7 | The number of persistent objects that can be held in QVault TPM NV Memory.<br>QVault TPM supports 2 persistent RSA 3072-bit keys. |
| TPM2_PT_HR_LOADED_MIN | 3 | The number of authorization sessions that can be held in QVault TPM RAM. |
| TPM2_PT_ACTIVE_SESSIONS_MAX | 64 | The number of authorization sessions that can be active concurrently. |
| TPM2_PT_MANUFACTURER | 0x5345414C | This field is set to ‘SEAL’. |
| TPM2_PT_VENDOR_STRING_1 | 0x51566175 | This field is set to 'QVau'. |
| TPM2_PT_VENDOR_STRING_2 | 0x6C742054 | This field is set to 'lt T'. |
| TPM2_PT_VENDOR_STRING_3 | 0x504D0000 | This field is set to 'PM' (+ 2 null bytes). |
| TPM2_PT_VENDOR_STRING_4 | 0x00000000 | This field is left empty (4 null bytes). |
| TPM2_PT_FIRMWARE_VERSION_1 | 0xMMMMmmmm | The TPM firmware version - part 1:<br>Firmware version MMMM.mmmm.PP<br>(PP is in TPM_PT_FIRMWARE_VERSION_2)<br>For example:<br>MMMM = 0x0010<br>mmmm = 0x000A<br>PP = 0x03<br>Version is 16.10.3 |
| TPM2_PT_FIRMWARE_VERSION_2 | 0xPPUUuuRR | PP is a part of the firmware version, as explained above.<br>Upgrader version UU.uu<br>RR is reserved for internal use. |
| NV_MEMORY_SIZE | 51200 | 50 * 1024. |
| TPM2_PT_NV_INDEX_MAX | 2048 | The maximum size of an NV Index data area. |
| TPM2_PT_NV_BUFFER_MAX | 1024 | The maximum data size in one NV write, NV read, NV extend, or NV certify command. |
| TPM2_PT_NV_COUNTERS_MAX | 0 | No limitation on the number of NV indexes that are allowed to have the TPMA_NV_COUNTER attribute SET. |

### 3.1.2 Supported algorithms

The QVault TPM supports the algorithms listed in the following table.

**Table 3-2.** Supported algorithms

| Algorithm ID | PC client 1.06 status<br>(M)andatory<br>(R)ecommended<br>(D)eprecated<br>(O)ptional<br>(N)ot allowed | QVault TPM support status |
|---|---|---|
| TPM_ALG_RSA | N<br>M<br>M<br>O | RSA 1024-bit keys are not supported<br>RSA 2048-bit keys are supported<br>RSA 3072-bit keys are supported<br>RSA 4096-bit keys are not supported |
| TPM_ALG_TDES | N | Not supported |
| TPM_ALG_SHA1 | O | Supported |
| TPM_ALG_HMAC | M | Supported |
| TPM_ALG_AES | N<br>O<br>O<br>O<br>M | ECB mode is not supported.<br>CTR mode is supported<br>OFB mode is supported<br>CBC mode is supported<br>CFB mode is supported |
| TPM_ALG_MGF1 | M | Supported |
| TPM_ALG_KEYEDHASH | M | Supported |
| TPM_ALG_XOR | M | Supported |
| TPM_ALG_SHA256 | M | Supported |
| TPM_ALG_SHA384 | M | Supported |
| TPM_ALG_SHA512 | O | Supported |
| TPM_ALG_SM3_256 | O | Not supported |
| TPM_ALG_SM4 | O | Not supported |
| TPM_ALG_RSASSA | M | Supported |
| TPM_ALG_RSAES | M | Supported |
| TPM_ALG_RSAPSS | M | Supported |
| TPM_ALG_OAEP | M | Supported |
| TPM_ALG_ECDSA | M | Supported |
| TPM_ALG_ECDH | M | Supported |
| TPM_ALG_ECDAA | O | Supported |
| TPM_ALG_SM2 | O | Not Supported |
| TPM_ALG_ECSCHNORR | O | Not Supported |
| TPM_ALG_ECC | M | Supported see Section 3.1.3 |
| TPM_ALG_ECMQV | O | Not Supported |
| TPM_ALG_SYMCIPHER | M | Supported |
| TPM_ALG_CAMELLIA | O | Not Supported |

**Table 3-2.** Supported algorithms

| | | |
|---|---|---|
| TPM_ALG_SHA3_256 | O | Not Supported |
| TPM_ALG_SHA3_384 | O | Not Supported |
| TPM_ALG_SHA3_512 | O | Not Supported |

### 3.1.3 Supported curves

The ECC curves supported in QVault TPM are detailed in the following table.

**Table 3-3.** Supported curves

| Curve Identifier | PC client 1.06 status (M)andatory (O)ptional (U)ndocumented | Support status |
|---|---|---|
| TPM_ECC_NIST_P256 | M | Supported |
| TPM_ECC_NIST_P384 | M | Supported |
| TPM_ECC_NIST_P521 | U | Supported |
| TPM_ECC_BN_P256 | O | Supported |
| TPM_ECC_SM2_P256 | O | Not Supported |

## 3.2 TPM commands

The table below lists all TPM2 commands described in the PC Client Platform specification and their support status on QVault TPM.

**Table 3-4.** Command list

| Command | PC client 1.06 status (M)andatory (O)ptional (U)ndocumented | QVault TPM support status |
|---|---|---|
| **Signals / Indications** | | |
| _TPM_INIT | M | Supported |
| _TPM_Hash_Start | M | Supported |
| _TPM_Hash_Data | M | Supported |
| _TPM_Hash_End | M | Supported |
| **Startup** | | |
| TPM2_Startup | M | Supported |
| TPM2_Shutdown | M | Supported |
| **Testing** | | |
| TPM2_IncrementalSelfTest | M | Supported |
| TPM2_SelfTest | M | Supported |
| TPM2_GetTestResult | M | Supported |
| **Session Commands** | | |
| TPM2_StartAuthSession | M | Supported |
| TPM2_PolicyRestart | M | Supported |
| **Object Commands** | | |
| TPM2_Create | M | Supported |
| TPM2_Load | M | Supported |
| TPM2_LoadExternal | M | Supported |
| TPM2_ReadPublic | M | Supported |
| TPM2_ActivateCredential | M | Supported |
| TPM2_MakeCredential | M | Supported |
| TPM2_Unseal | M | Supported |
| TPM2_ObjectChangeAuth | M | Supported |
| TPM2_CreateLoaded | O | Supported |
| **Duplicate Commands** | | |
| TPM2_Duplicate | M | Supported |
| TPM2_Rewrap | O | Not supported |
| TPM2_Import | M | Supported |
| **Asymmetric Primitives** | | |
| TPM2_RSA_Encrypt | M | Supported |
| TPM2_RSA_Decrypt | M | Supported |
| TPM2_ECDH_KeyGen | M | Supported |
| TPM2_ECDH_ZGen | M | Supported |

**Table 3-4.** Command list

| | | |
|---|---|---|
| TPM2_ECC_Parameters | M | Supported |
| TPM2_ZGen_2Phase | O | Not supported |
| **Symmetric Primitives** | | |
| TPM2_EncryptDecrypt | O | Not supported |
| TPM2_EncryptDecrypt2 | O | Supported |
| TPM2_Hash | M | Supported |
| TPM2_HMAC | M | Supported |
| TPM2_MAC | O | Not supported |
| **Random Number Generator** | | |
| TPM2_GetRandom | M | Supported |
| TPM2_StirRandom | M | Supported |
| **Hash/HMAC/Event Sequences** | | |
| TPM2_HMAC_Start | M | Supported |
| TPM2_MAC_Start | O | Not supported |
| TPM2_HashSequenceStart | M | Supported |
| TPM2_SequenceUpdate | M | Supported |
| TPM2_SequenceComplete | M | Supported |
| TPM2_EventSequenceComplete | M | Supported |
| **Attestation Commands** | | |
| TPM2_Certify | M | Supported |
| TPM2_CertifyCreation | M | Supported |
| TPM2_Quote | M | Supported |
| TPM2_GetSessionAuditDigest | M | Supported |
| TPM2_GetCommandAuditDigest | O | Not supported |
| TPM2_GetTime | M | Supported |
| TPM2_CertifyX509 | O | Not Supported |
| **Anonymous Attestation** | | |
| TPM2_Commit | O | Supported |
| TPM2_EC_Ephemeral | O | Not supported |
| **Signature Verification** | | |
| TPM2_VerifySignature | M | Supported |
| TPM2_Sign | M | Supported |
| **Command Audit** | | |
| TPM2_SetCommandCodeAuditStatus | O | Not supported |
| **Integrity Collection (PCR)** | | |
| TPM2_PCR_Extend | M | Supported |
| TPM2_PCR_Event | M | Supported |
| TPM2_PCR_Read | M | Supported |
| TPM2_PCR_Allocate | M | Supported |
| TPM2_PCR_SetAuthPolicy | O | Not supported |

**Table 3-4.** Command list

| | | |
|---|---|---|
| TPM2_PCR_SetAuthValue | O | Not supported |
| TPM2_PCR_Reset | M | Supported |
| **Enhanced Authorization (EA)** | | |
| TPM2_PolicySigned | M | Supported |
| TPM2_PolicySecret | M | Supported |
| TPM2_PolicyTicket | M | Supported |
| TPM2_PolicyOR | M | Supported |
| TPM2_PolicyPCR | M | Supported |
| TPM2_PolicyLocality | M | Supported |
| TPM2_PolicyNV | M | Supported |
| TPM2_PolicyCounterTimer | M | Supported |
| TPM2_PolicyCommandCode | M | Supported |
| TPM2_PolicyPhysicalPresence | O | Not supported |
| TPM2_PolicyCpHash | M | Supported |
| TPM2_PolicyNameHash | M | Supported |
| TPM2_PolicyDuplicationSelect | M | Supported |
| TPM2_PolicyAuthorize | M | Supported |
| TPM2_PolicyAuthValue | M | Supported |
| TPM2_PolicyPassword | M | Supported |
| TPM2_PolicyGetDigest | M | Supported |
| TPM2_PolicyNvWritten | M | Supported |
| TPM2_PolicyTemplate | M | Supported |
| TPM2_PolicyAuthorizeNV | M | Supported |
| TPM2_PolicyCapability | U | Not supported |
| TPM2_PolicyParameters | U | Not supported |
| TPM2_Policy_AC_SendSelect | U | Not supported |
| **Hierarchy Commands** | | |
| TPM2_CreatePrimary | M | Supported |
| TPM2_HierarchyControl | M | Supported |
| TPM2_SetPrimaryPolicy | M | Supported |
| TPM2_ChangePPS | O | Supported (required for FIPS) |
| TPM2_ChangeEPS | O | Supported (required for FIPS) |
| TPM2_Clear | M | Supported |
| TPM2_ClearControl | M | Supported |
| TPM2_HierarchyChangeAuth | M | Supported |
| **Dictionary Attack Functions** | | |
| TPM2_DictionaryAttackLockReset | M | Supported |
| TPM2_DictionaryAttackParameters | M | Supported |
| **Miscellaneous Management Functions** | | |
| TPM2_PP_Commands | O | Not supported |

**Table 3-4.** Command list

| | | |
|---|---|---|
| TPM2_SetAlgorithmSet | O | Not supported |
| **Field Upgrade** | | |
| TPM2_FieldUpgradeStart | O | Not supported |
| TPM2_FieldUpgradeData | O | Not supported |
| TPM2_FirmwareRead | O | Not supported |
| **Context Management** | | |
| TPM2_ContextSave | M | Supported |
| TPM2_ContextLoad | M | Supported |
| TPM2_FlushContext | M | Supported |
| TPM2_EvictControl | M | Supported |
| **Clocks and Timers** | | |
| TPM2_ReadClock | M | Supported |
| TPM2_ClockSet | M | Supported |
| TPM2_ClockRateAdjust | M | Supported |
| **Capability Commands** | | |
| TPM2_GetCapability | M | Supported |
| TPM2_TestParms | M | Supported |
| TPM2_SetCapability | U | Not supported |
| **Non-volatile Storage** | | |
| TPM2_NV_DefineSpace | M | Supported |
| TPM2_NV_UndefineSpace | M | Supported |
| TPM2_NV_UndefineSpaceSpecial | M | Supported |
| TPM2_NV_ReadPublic | M | Supported |
| TPM2_NV_Write | M | Supported |
| TPM2_NV_Increment | M | Supported |
| TPM2_NV_Extend | M | Supported |
| TPM2_NV_SetBits | M | Supported |
| TPM2_NV_WriteLock | M | Supported |
| TPM2_NV_GlobalWriteLock | O | Not supported |
| TPM2_NV_Read | M | Supported |
| TPM2_NV_ReadLock | M | Supported |
| TPM2_NV_ChangeAuth | M | Supported |
| TPM2_NV_Certify | M | Supported |
| **Attached Component Commands** | | |
| TPM2_AC_GetCapability | O | Not supported |
| TPM2_AC_Send | O | Not supported |
| TPM2_Policy_AC_Send | O | Not supported |
| TPM2_NV_DefineSpace2 | U | Not supported |
| TPM2_NV_ReadPublic2 | U | Not supported |

**Table 3-4.** Command list

| | | |
|---|---|---|
| **Authenticated Countdown Timer** | | |
| TPM2_ACT_SetTimeout | O | Not supported |
| **Vendor Specific** | | |
| TPM2_Vendor_LockEPS | U | Supported |
| TPM2_Vendor_FieldUpgradeStart | U | Supported |
| TPM2_Vendor_FieldUpgradeData | U | Supported in field upgrade mode (FUM)<br>See Firmware Upgrade |

## 3.3 Provisioned EK certificates

By default the QVault TPM 183 is provisioned with the following EK certificates (see [R8]):

**Table 3-5.** EK certificates

| NV index | EK certificate | Range |
|---|---|---|
| 0x1C000002 | RSA 2048 | Low range |
| 0x1C00000a | ECC P256 | Low range |
| 0x1C000016 | ECC P384 | High Range |

## 3.4 General Purpose I/O (GPIO)

Four GPIO pins can be mapped to ordinary NV indexes with the corresponding handle values listed in the table below.

**Table 3-6.** Mapping of GPIO NV indexes

| GPIO Name | QFN32 Pin | TPM_NV_INDEX |
|---|---|---|
| GPIO_A | 3 | 0x01C40000 |
| GPIO_B | 4 | 0x01C40001 |
| GPIO_C | 7 | 0x01C40002 |
| GPIO_D | 27/28 | 0x01C40003 |

The NV GPIO complies with [R5] section 4.5.5. Operations on GPIO pins as described hereafter.


By default, GPIO pins are not configured and cannot be used by the TPM.

In this case, the pins are electrically configured as input pins with a built-in pull-up resistor and may remain unconnected.

### 3.4.1 GPIO Configuration

To use a GPIO pin, the related NV index must be first created by using the TPM2_NV_DefineSpace command with the following parameters:

- nvIndex handle must be set to a handle value defined in Table 3-6.
- dataSize must be 2
- index type must be TPM_NT_ORDINARY
- attribute TPMA_NV_WRITEALL must be cleared

Note

For all other NV index attributes, the behavior is the same as for a standard NV index.

Once created, GPIO configuration is done by using the TPM2_NV_Write command. First TPM2_NV_Write command must write 2 bytes at address 0.

The first byte defines the GPIO state in case of an output configuration (see GPIO usage). The second byte defines the GPIO configuration as described in the following table.

**Table 3-7.** Configuration of GPIO pins

| Byte value | Configuration |
|---|---|
| 1 | Output |
| 2 | Input |
| 3 | Input with pull-down (value in Table 5-4) |
| 4 | Input with pull-up (value in Table 5-4) |
| others | Input with pull-down (value in Table 5-4) |

Note

**Configuration cannot be changed**.

To change a GPIO behavior, undefine and create again the related NV index.

### 3.4.2 GPIO usage

GPIO pins configured as output can be set by using the TPM2_NV_Write command. In this case (any write after the gpio configuration), only the first byte is accessible. The command must write 1 byte only at address 0:

- data = 1 will set the GPIO output to high level (1)
- data = 0 will set the GPIO output to low level (0)

Note

It is not possible to write a GPIO pin set as input.

In this case, the TPM2_NV_Write command will return the TPM_RC_HANDLE error code.

The current state of any GPIO pins can be read by using the TPM2_NV_Read command. The command must read 1 byte at address 0. The responseCode gives the pin value:

- responseCode == TPMI_YES: GPIO is at high level (1)
- responseCode == TPMI_NO: GPIO is at low level (0)

### 3.4.3 GPIO Release

TPM2_NV_UndefineSpace will undefine the NV index used to access the GPIO pin.

After TPM2_UndefineSpace, the GPIO pin will be in the same state than after a power on.

## 3.5 Other TPM features

### 3.5.1 Identification registers

The registers DID,VID,RID have the values defined in the following table:

**Table 3-8.** Identification registers

| Register | Value | Description and details |
|---|---|---|
| TPM_DID_VID | 0x00832406 | Device ID = 0x83<br>Vendor ID = 0x2406 |
| TPM_RID | 0x02 | Revision ID |

### 3.5.2 Locality

The QVault TPM 183 supports 5 localities (0-4).

### 3.5.3 PCR implementation

The QVault TPM 183 supports four banks of 24 PCRs (0-23) with SHA-1 (deprecated, therefore not recommended for new developments), SHA-256, SHA-384 and SHA-512.

By default SHA-256 and SHA-384 are activated, other configurations can be activated using the TPM2_PCR_Allocate command.

### 3.5.4 Power Management

The power management is automatically done by the TPM software depending on its state. Typical consumption can be found in Table 5-7 on page 23.

### 3.5.5 Authenticated Countdown Timer (ACT)

Not supported by the QVault TPM 183.

### 3.5.6 Physical Presence

Not supported by the QVault TPM 183.

## 3.6 Firmware Upgrade

The QVault TPM 183 supports firmware upgrade.

The vendor specific command TPM2_Vendor_FieldUpgradeStart initiates the upgrade process.

This command includes a digest protected by a hybrid signature (ECC and MLDSA) to ensure that the upgrade is initiated by the TPM manufacturer.

Once the field upgrade process has been started, the QVault TPM switches to the field upgrade mode (FUM) and only supports the command TPM2_Vendor_FieldUpgradeData.

If the firmware upgrade process is interrupted (power off, reboot, etc.), the QVault TPM will remain in field upgrade mode (FUM); only the command TPM2_Vendor_FieldUpgradeData is available, until the firmware program flow is started again and completed.

Upgrade does not allow roll-back, it is not possible to revert a firmware to a previous version.

## 3.7 I²C Interface implementation

### 3.7.1 Bus speed

The QVault TPM follows the TCG TPM I²C Interface Specification ([R6], [R7]).

The following speeds are supported:

- Standard Mode (up to 100 kbits/s)
- Fast Mode (up to 400 kbits/s)
- Fast Mode plus (up to 1 Mbits/s)

### 3.7.2 I²C Device address

Address configuration is supported using the TCG defined mechanism (see [R6] section 6.5.15).

The default 7-bit I2C device address of the QVault TPM is 0x2E (following [R5] specification).

## 3.8 Vendor commands

### 3.8.1 TPM2_Vendor_LockEPS

This command locks the TPM2_ChangeEPS command

**Table 3-9.** *TPM2_Vendor_LockEPS command format*

| Type | Name | Description |
|---|---|---|
| TPMI_ST_COMMAND_TAG | tag | TPM_ST_SESSIONS |
| UINT32 | commandSize | |
| TPM_CC | commandCode | TPM_CC_Vendor_LockEPS<br>**0x2000D124** |
| TPMI_RH_PLATFORM | @authorization | TPM_RH_PLATFORM<br>Auth Index: 1<br>Auth Role: ADMIN |
| TPMI_YES_NO | permanent | YES if the lock should be permanent, NO if temporary (locked until next reset) |

Possible response codes are:

***Table 3-10.*** *TPM2_Vendor_LockEPS response code*

| Name | Description |
|---|---|
| TPM_RC_DISABLED | TPM2_ChangeEPS already locked |
| TPM_RC_SUCCESS | operation successful |
| Others | session related error codes |

### 3.8.2 TPM2_Vendor_FieldUpgradeStart

This command starts the firmware upgrade.

**Table 3-11.** *TPM2_Vendor_FieldUpgradeStart command format*

| Type | Name | Description |
|---|---|---|
| TPMI_ST_COMMAND_TAG | tag | TPM_ST_SESSIONS |
| UINT32 | commandSize | Variable |
| TPM_CC | commandCode | TPM_CC_Vendor_FieldUpgraderStart<br>**0x2000D12F** |
| TPMI_RH_PLATFORM | @authorization | TPM_RH_PLATFORM<br>Auth Index: 1<br>Auth Role: ADMIN |
| TPM2B_DIGEST | | |
| TPMT_SIGNATURE | manifestSignatureECC | signature using the ECC key |
| TPMT_SIGNATURE | manifestSignaturePQC | signature using the PQC key |

### 3.8.3 TPM2_Vendor_FieldUpgradeData

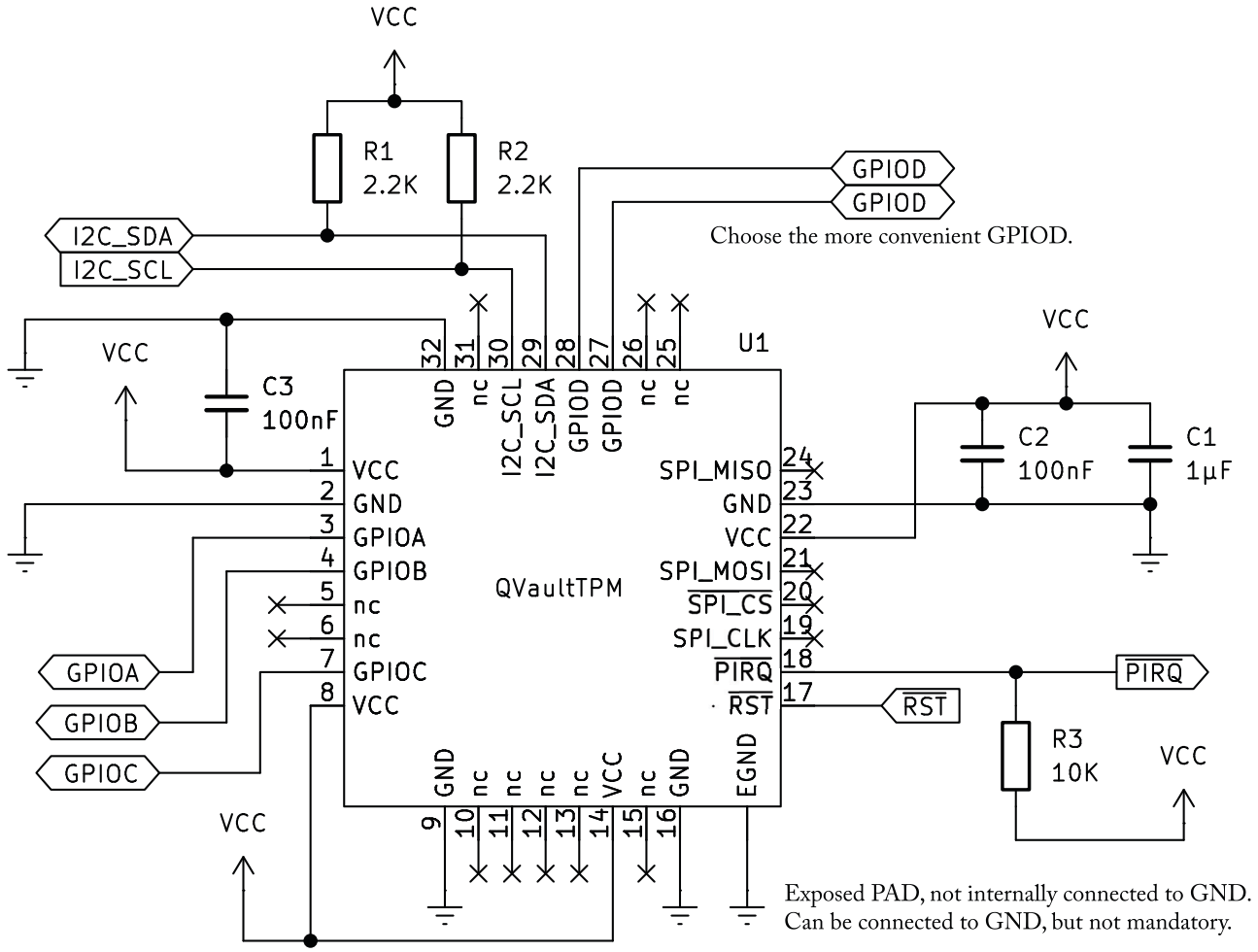
This command loads a new firmware in the QVault TPM.

***Table 3-12.*** *TPM2_Vendor_FieldUpgradeData command format*

| Type | Name | Description |
|---|---|---|
| TPMI_ST_COMMAND_TAG | tag | TPM_ST_NO_SESSIONS |
| UINT32 | commandSize | |
| TPM_CC | commandCode | TPM_CC_Vendor_FieldUpgraderData<br>**0x2000D141** |
| TPM2B_MAX_UPG_BUFFER | fuData | Field upgrade image data |

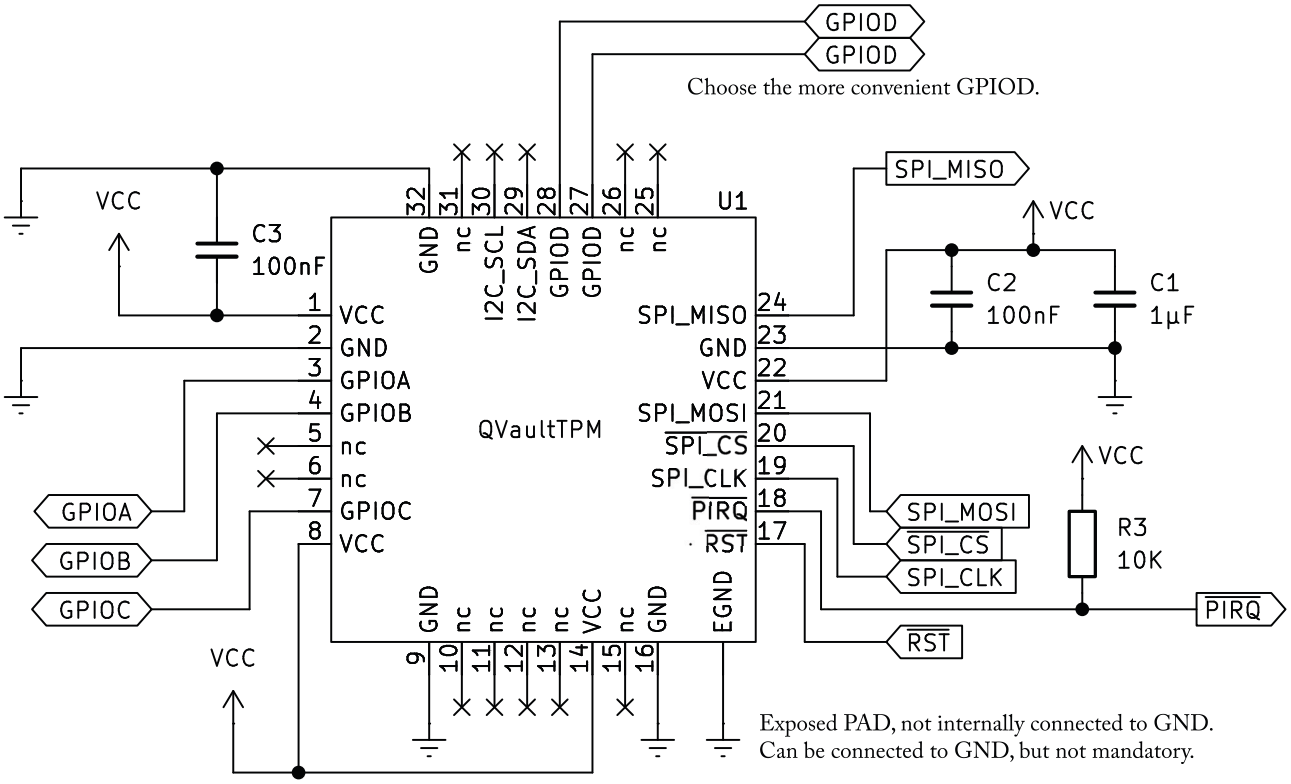
# 4. Typical schematics

## 4.1 I²C




Place the 100nF capacitors near their corresponding VCC.
GPIOA, GPIOB, GPIOC, GPIOD and $\overline{\text{PIRQ}}$ are optional, depending on implementation.

## 4.2 SPI




Place the 100nF capacitors near their corresponding VCC.
GPIOA, GPIOB, GPIOC, GPIOD and $\overline{\text{PIRQ}}$ are optional, depending on implementation.

# 5. AC/DC characteristics

## 5.1 Maximum ratings

**Table 5-1.** Maximum ratings

| Symbol | Parameter | Condition | Min. | Typ. | Max. | Units |
|---|---|---|---|---|---|---|
| $V_M$ | Maximum Voltage | | | | TBD | V |
| $T_S$ | Storage Temperature | | TBD | | TBD | °C |

## 5.2 AC/DC characteristics (1.62V - 3.60V range; T= -40°C to +105°C)

**Table 5-2.** AC/DC characteristics - general

| Symbol | Parameter | Condition | Min. | Typ. | Max. | Units |
|---|---|---|---|---|---|---|
| $T_O$ | Operating Temperature | | -40 | | +105 | °C |
| $V_{CC}$ | Operation Supply Voltage | | 1.62 | | 3.6 | V |
| $V_{MAX}$ | Voltage Monitor: High Level Detection | | | 3.6 | | V |
| $V_{MIN}$ | Voltage Monitor: Low Level Detection | | | 1.62 | | V |
| $T_{MAX}$ | Temperature monitor High Level Detection | | | 105 | | °C |
| $T_{MIN}$ | Temperature monitor Low Level Detection | | | -40 | | °C |

**Table 5-3.** AC/DC characteristics - RST

| Symbol | Parameter | Condition | Min. | Typ. | Max. | Units |
|---|---|---|---|---|---|---|
| $I_{IL}$ | Leakage Current RST | $V_{IN}$=0V | | 0 | | µA |
| $I_{IH}$ | Leakage Current RST | $V_{IN}$=Vcc | | 0 | | µA |
| $V_{IH}$ | Input High Voltage, RST signal | | 0.7Vcc | | Vcc+0.3 | V |
| $V_{IL}$ | Input Low Voltage, RST signal | | -0.3 | | 0.2Vcc | V |
| $R_{PULLUP}$ | RST pin pull-up | | | 105 | | kΩ |
| $R_{PULLDN}$ | RST pin pull-down | | | 1000 | | kΩ |

**Table 5-4.** AC/DC characteristics - GPIO

| Symbol | Parameter | Condition | Min. | Typ. | Max. | Units |
|---|---|---|---|---|---|---|
| $I_{IL}$ | Leakage Current I/O | $V_{IN}$=0 | | 0 | | µA |
| $I_{IH}$ | Leakage Current I/O | $V_{IN}$=Vcc | | 0 | | µA |
| $V_{IH}$ | Input High Voltage, I/O signal | | 0.7Vcc | | Vcc+0.3 | V |
| $V_{IL}$ | Input Low Voltage, I/O signal | | -0.3 | | 0.2Vcc | V |
| $V_{OH}$ | Output High Voltage, I/O signal | $I_{OH}$=20µA<br>$R_{PULLUP}$=20K | 0.7Vcc | | | V |
| $V_{OL}$ | Output Low Voltage, I/O signal | $I_{OL}$<0.5mA | | | 0.15Vcc | V |
| $R_{PULLUP}$ | GPIO pin pull-up | Vcc=1.8V | | 100 | | kΩ |
| | | Vcc=3.3V | | 47 | | |
| $R_{PULLDN}$ | GPIO pin pull-down | Vcc=1.8V | | 90 | | kΩ |
| | | Vcc=3.3V | | 40 | | |

**Table 5-5.** AC/DC characteristics - $I^2C$

| Symbol | Parameter | Condition | Min. | Typ. | Max. | Units |
|---|---|---|---|---|---|---|
| $V_{DD}$ | Voltage applied on SDA and SCL pull-up resistors | | 1.62 | | 5.5 | V |
| $V_{IH}$ | SDA SCL Input High Voltage | | $0.7V_{DD}$ | | | V |
| $V_{IL}$ | SDA SCL Input Low Voltage | | -0.5 | | $0.3V_{DD}$ | V |
| $V_{OL}$ | Output Low Voltage, SDA/SCL | 3 mA sink current; VDD > 2 V | 0 | | 0.4 | V |
| | | 2 mA sink current; VDD ≤ 2 V | 0 | | $0.2V_{DD}$ | |
| $t_{of}$ | Output fall time from $V_{IHmin}$ to $V_{ILmax}$ | | | | TBD | ns |

**Table 5-6.** AC/DC characteristics - SPI

| Symbol | Parameter | Condition | Min. | Typ. | Max. | Units |
|---|---|---|---|---|---|---|
| **SPI input pins - SPI_CLK - $\overline{\text{SPI\_CS}}$ - SPI_MOSI** | | | | | | |
| $V_{IH}$ | Input High Voltage | | 0.7Vcc | | Vcc+0.3 | V |
| $V_{IL}$ | Input Low Voltage | | -0.3 | | 0.2Vcc | V |
| **SPI output pin - SPI_MISO** | | | | | | |
| $V_{OH}$ | Output High Voltage | | 0.7Vcc | | | V |
| $V_{OL}$ | Output Low Voltage | | | | 0.15Vcc | V |
| Tr | Output Rise Time | $C_{out}$ = 30 pF | | | TBD | ns |
| Tf | Output Fall Time | $C_{out}$ = 30 pF | | | TBD | ns |
| **SPI timing** | | | | | | |
| $F_{SPI\_CLK}$ | SPI_CLK frequency | | 1 | | 36 | MHz |
| $D_{SPI\_CLK}$ | SPI_CLK duty cycle | | 40 | | 60 | % |
| $t_{CS}$ | $\overline{\text{SPI\_CS}}$ rising edge to falling edge | | 50 | | | ns |
| $t_{CSS}$ | $\overline{\text{SPI\_CS}}$ low to SPI_CLK starts | | 5 | | | ns |
| $t_{CSH}$ | SPI_CLK stops to $\overline{\text{SPI\_CS}}$ high | | 5 | | | ns |
| $t_{SU}$ | SPI_MOSI setup to SPI_CLK | | 2 | | | ns |
| $t_H$ | SPI_MOSI hold to SPI_CLK | | 3 | | | ns |
| $t_{HO}$ | SPI_MISO hold time | | 0 | | | ns |
| $t_V$ | SPI_MISO valid from SPI_CLK falling edge | | | | TBD | ns |

**Table 5-7.** AC/DC characteristics - consumption

| Symbol | Parameter | Condition | Min. | Typ. | Max. | Units |
|---|---|---|---|---|---|---|
| $I_{SBY}$ | Current consumption in standby mode | No communication, no operation in progress | | TBD | | mA |
| $I_{MAX}$ | Maximum current consumption | | | | TBD | mA |

## Definitions and abbreviations

| | |
|---|---|
| DRBG | Deterministic Random Bit Generator |
| FIPS | Federal Information Processing Standards |
| $I^2C$ | Inter-Integrated Circuit bus |
| LSB / MSB | Least Significant Bit and Most Significant Bit respectively |
| NIST | National Institute of Standards and Technology |
| NVM | Non Volatile Memory |
| PCR | Platform Configuration Register |
| TRNG | True Random Number Generator |
| SHA | Secure Hash Algorithm as defined in FIPS PUB 180-4 [R9] |
| SPI | Serial Peripheral Interface bus |
| TCG | Trusted Computing Group |
| TPM | Trusted Platform Module |

# Reference List


**[R1]** Trusted Platform Module Library Part 1: Architecture - Level 00 Revision 01.83 - January 25, 2024

**[R2]** Trusted Platform Module Library Part 2: Structures - Level 00 Revision 01.83 - January 25, 2024

**[R3]** Trusted Platform Module Library Part 3: Commands - Level 00 Revision 01.83 - January 25, 2024

**[R4]** Trusted Platform Module Library Part 4: Supporting Routines - Level 00 Revision 01.83 - January 25, 2024

**[R5]** PC-Client-Platform-TPM-Profile-for-TPM-2.0-Version-1.06-Revision-32 - 5April24

**[R6]** TCG TPM I2C Interface Specification for TPM 2.0 Revision 1.0 - 2016

**[R7]** Errata version 1.0 - 2017 for TCG TPM I2C Interface Specification for TPM 2.0

**[R8]** TCG EK Credential Profile for TPM 2.0 - Version 2.5 Rev 2 - January 26, 2022

**[R9]** FIPS PUB 180-4. Secure Hash Standard. August 2015.

# Revision History

Document Details

Title: QVault TPM 183 Technical Datasheet

Literature Number: TPR1003A

Date: 30Apr26

- Revision A:
  - First Release

## 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