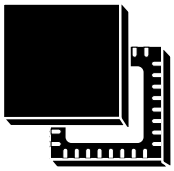
STSAFE-TPM ST33TPHF2XSPI: TPM 2.0 device with an SPI interface



VFQFPN32

5 × 5 mm

Product status link
ST33TPHF2XSPI

Features

TPM features

- Flash-memory-based trusted platform module (TPM)
- Compliant with Trusted Computing Group (TCG) Trusted Platform Module (TPM) Library specifications 2.0, Level 0, Revision 159 – errata 1.1 and TCG PC Client Specific TPM Platform Specifications 1.05 rev 14
- Fault-tolerant firmware loader that keeps the TPM fully functional when the loading process is interrupted (self-recovery)
- SP800-193 compliant for protection, detection and recovery requirements
- Targeted certifications:
  - CC according to TPM 2.0 PP at EAL4+ (augmented with AVA_VAN.5 and ALC_FLR.1)
  - FIPS 140-2 level 2 (physical security level 3)
  - TCG certification
- SPI support at up to 33 MHz

Hardware features

- Highly reliable Flash memory technology
- Extended temperature range: −40 °C to 105 °C
- ESD protection up to 4 kV (HBM) and 750 V (CDM)
- 1.8 V or 3.3 V supply voltage range

Security features

- Active shield and environmental sensors
- Monitoring of environmental parameters (power)
- Hardware and software protection against fault injection
- FIPS SP800-90A and AIS20-compliant deterministic random-bit generator (DRBG)
- FIPS SP800-90B and AIS31-compliant true random-number generator (TRNG)
- Cryptographic algorithms:
  - RSA key generation (1024, 2048 or 3072 bits)
  - RSA signature (RSASSA-PSS, RSASSA-PKCS1v1_5)
  - RSA encryption (RSAES-OAEP, RSAESPKCS1-v1_5)
  - SHA-1, SHA-2 (256 and 384 bits), SHA-3 (256 and 384 bits)
  - HMAC SHA-1, SHA-2, and SHA-3
  - AES-128, 192, and 256 bits
  - TDES 192 bits
  - ECC (NIST P-256, P-384 curves): key generation, ECDH, and ECDSA, ECSchnorr
  - ECDAA (BN-256 curve)
- Device provided with 3 endorsement keys (EK) and EK certificates (RSA2048, ECC NIST P_256 and ECC NIST P_384)
- Device provisioned with three 2048-bit RSA key pairs to reduce the TPM provisioning time

Product compliance

- Compliant with Microsoft® Windows® 10 and 11
- Compliant with Linux® drivers
- Compliant with Intel® vPro® technology
- Compliant with the TCG test suite for TPM 2.0
- Compliant with the open-source TCG TPM 2.0 TSS implementation

1 Description

The STSAFE-TPM (trusted platform module) family of products offers a broad portfolio of standardized solutions for embedded, PC, mobile and computing applications. STSAFE is an ST trademark.

It includes turnkey products compliant with the Trusted Computing Group (TCG) standards that provide services to protect the confidentiality, integrity and authenticity of information and devices.

These devices are easy to integrate thanks to the variety of supported interfaces and the availability of TPM ecosystem software solutions.

The STSAFE-TPM devices are all Common Criteria (EAL4+) and FIPS certified.

The ST33TPHF2XSPI offers a slave serial peripheral interface (SPI) compliant with the TCG PC Client TPM Profile specifications.

It offers resilience services during the TPM firmware upgrade process, and self-recovery of TPM firmware and critical data upon failure detection.

The ST33TPHF2XSPI operates in the –25 to +85 °C commercial temperature range at 1.8 V, or in the –40 °C to 105 °C extended temperature range at 3.3 V.

The device is offered in the VFQFPN32 ECOPACK2 package. ECOPACK is an ST trademark.

1.1 Security certifications

The list of certified products can be consulted on the Common Criteria website: https://www.commoncriteriaportal.org/, the NIST website: https://csrc.nist.gov/, and the TCG website https://trustedcomputinggroup.org/.

2 Pin and signal description

The figure below gives the pinout of the VFQFPN32 package in which the devices are delivered. The table below describes the associated signals.

Figure 1. VQFN32 pinout

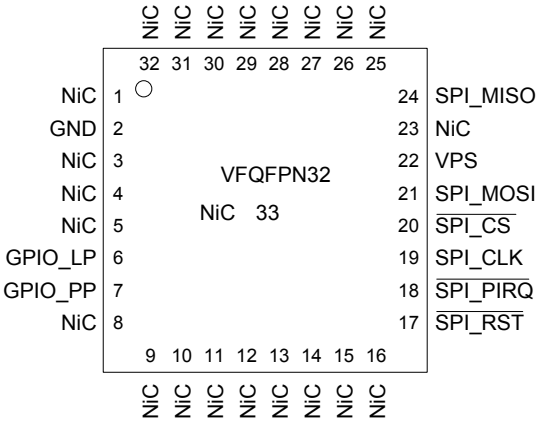


Table 1. Pin descriptions

Signal	Type	Description
VPS	Input	**Power supply**. This pin must be connected to the 1.8 V or 3.3 V DC power rail supplied by the motherboard.
GND	Input	GND has to be connected to the main motherboard ground.
SPI_RST	Input	**SPI Reset,** active low, used to re-initialize the device. Must not be unconnected. External pull-up required if it cannot be driven.
SPI_MISO	Output	**SPI Master Input, Slave Output** (output from slave)
SPI_MOSI	Input	**SPI Master Output, Slave Input** (output from master)
SPI_CLK	Input	**SPI Serial Clock** (output from master)
$\overline{\text{SPI\_CS}}$ (or $\overline{\text{SPI\_NSS}}$)	Input	**SPI Chip (or Slave) Select**, internal pull-up (active low; output from master)
SPI_PIRQ	Output	**SPI IRQ**, active low, open drain, used by TPM to generate an interrupt
GPIO_PP	Input	**Physical Presence**, active high, internal pull-down. Used to indicate Physical Presence to the TPM. GPIO Function could be modified by activating GPIO mapped with NV storage Indices feature.
GPIO_LP	Input	By default: Used for activation and deactivation of the TPM Standby mode (TPMLowPowerByGpio). The GPIO function could be modified by activating GPIOs mapped on the NV storage index feature.
NiC	-	**Not internally connected**: not connected to the die. May be left unconnected, but has no impact on the TPM if connected.

Note: The VQFN32 package has a central pad (PIN33) on the bottom, which is not connected to the die. This pin does not impact the TPM, be it connected or not.

3 Serial peripheral interface (SPI) and TPM registers

The SPI interface implemented in this device complies with the TCG PC Client-specific TPM Platform specifications [PTP 2.0 r1.05] for the TPM 2.0 library.

The SPI supports only one clock mode (CPOL=0, CPHA=0).

Data is transferred serially between master and slave; the most significant bit (msb) first, least significant bit (lsb) last.

Addresses and commands are transferred msb first for the entire field, e.g. the 24-bit address is transferred by sending b23 first, then b22 all the way up to b0.

The TPM drives data on the falling edge of the SPI clock.

The TPM samples data on the rising edge of the SPI clock.

The TPM will always decode a 24-bit address in the 0xD4_xxxx range when the TPM's $\overline{\text{SPI\_CS}}$ pin is asserted.

The ST33TPHF2XSPI supports an interrupt interface line directly from the TPM to the main platform MCU. This interrupt is supported using a dedicated GPIO ($\overline{\text{SPI\_PIRQ}}$, active low). The device detects a change in the TPM status when the TPM triggers a falling edge on pin $\overline{\text{SPI\_PIRQ}}$.

3.1 SPI communication protocol flow control

3.1.1 SPI communication

The TPM flow control mechanism operates on a transaction basis and can transfer data of various sizes. The TPM can transfer or receive 1 up to 32 bytes of data per transaction.

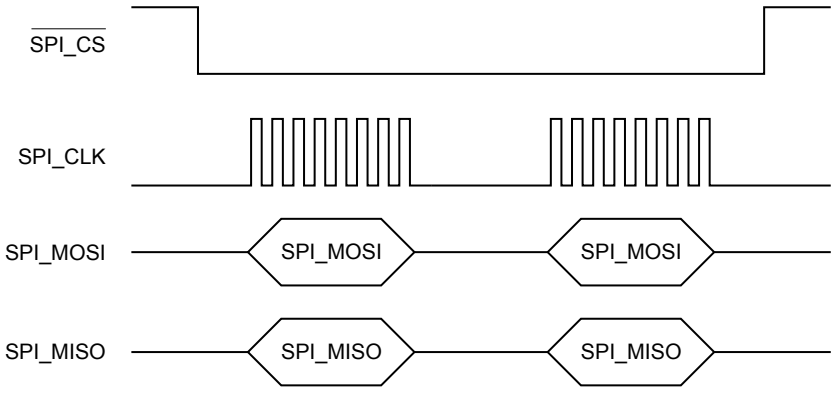
Because the SPI does not support any acknowledge signal, a specific way to synchronize between the host and the TPM has been defined.

In order to synchronize the start of a command, the SPI master must set low the $\overline{\text{SPI\_CS}}$ pin when sending a command and set the $\overline{\text{SPI\_CS}}$ pin back to high at the end of the transaction.

An SPI start of frame is detected when the $\overline{\text{SPI\_CS}}$ signal goes low. This causes the TPM to drive the SPI_MISO signal low. An end of frame is detected when the $\overline{\text{SPI\_CS}}$ line goes to the high voltage level.

The transmit sequence begins when the TPM receives the SPI_CLK signal, the $\overline{\text{SPI\_CS}}$ signal goes low and the most significant bit of the data is present on the SPI_MOSI pin.

Figure 2. SPI transmit sequence



The TPM host initiates every command by transmitting a single byte on the SPI_MOSI pin that tells the TPM if it is a read or write operation in a register. This byte also contains the size of the transfer including the 1st byte. The command processing continues with the transfer of three more bytes containing the address of the targeted register.

At this time, depending on the targeted register, the TPM is able to insert 1 or more Wait states before acknowledging the transfer. A Wait state is a Low state (0) sent on the SPI_MISO pin by the TPM. An Acknowledgment is a byte, whose last bit is ‘1’, sent on the SPI_MISO pin by the TPM.

In the case of a register read command, the TPM sends on the SPI_MISO pin the number of requested bytes from the requested register.

In the case of a register write command, the TPM reads on the SPI_MOSI pin the number of bytes previously declared and modifies accordingly the TPM state machine.

Table 2. SPI bit protocol

Bit transfer order on SPI_MISO/SPI_MOSI pins	Byte on SPI_MISO/SPI_MOSI pins	Usage	Notes
RFU	67 for 64B transactions 11 for 8B transactions	future use for larger register sizes	-
57-63 – last bits on wire	7	Data[30:24]	-
56		Data[31]	msb of 4th LSB
49-55	6	Data[22:16]	-
48		Data[23]	msb of 3rd LSB
41-47	5	Data[14:8]	-
40		Data[15]	msb of 2nd LSB
33-39	4	Data[6:0]	-
32		Data[7]	msb of 1st LSB
Optional flow control can be done in this window. See Section 3.1.2 Protocol flow control for SPI read access and Section 3.1.3 Protocol flow control for SPI write access for details. This is the only place in the bit transfers where flow control can be performed.			
31	3	Addr[0]	lsb of address
9-30	1-3	Addr[22] down to Addr[1]	-
8	1	Addr[23]	msb of address
2-7	0	bits[5:0] Size of transfer where bit[5] of this field is the 3rd bit transferred on the wire, and bit [0] is the 8th bit on the wire. This field is 0's based count of the bytes. Any byte count from 1 to 64 is legal.	Bit [5:0] decode '11_1111' = 64 bytes ' etc. for 63 down to 6 bytes '00_0100' = 5 bytes '00_0011' = 4 bytes '00_0010' = 3 bytes '00_0001' = 2 bytes '00_0000' = 1 byte
1		Reserved; bit[6]	-
0 – first bit on wire		Byte0, bit[7] Read/Write	1=read, 0 = write

3.1.2 Protocol flow control for SPI read access

Following the standard specification, depending on the targeted register, the TPM is authorized to insert 1 Wait state before acknowledging the read access. A Wait state is a Low state (0) sent on the SPI_MISO pin by the TPM. An Acknowledgment is a byte, whose last bit is '1', sent on the SPI_MISO pin by the TPM.

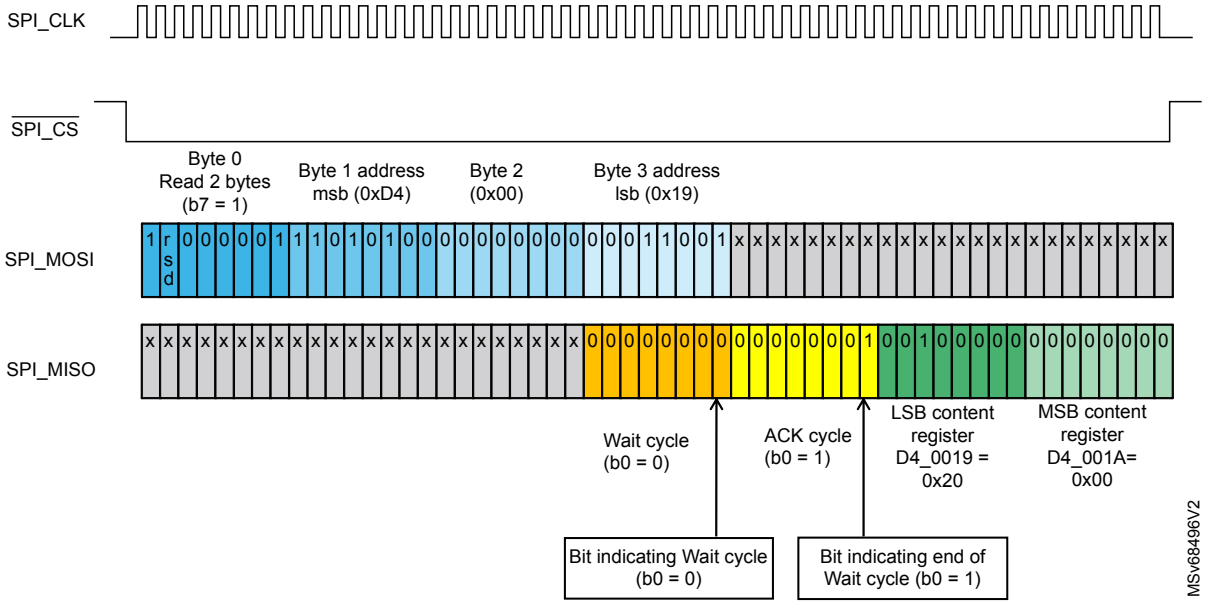
The ST TPM uses only one wait state for SPI read access.

On read access, if the data are not available, the ST TPM uses the dedicated bits defined by the standard specification:

- stsValid (bit 7 in the Status register): This bit indicates whether TPM_STS_x.dataAvail and TPM_STS_x.Expect are valid. They are valid when stsValid = 1.
- tpmRegValidSts (bit 7 in the Access register): This bit indicates whether all other bits in this register contain valid values. All values are valid when tpmRegValidSts = 1.

The Host should repeat read access and consider that the TPM is out of order only after TIMEOUT_B (2 seconds) of no data availability.

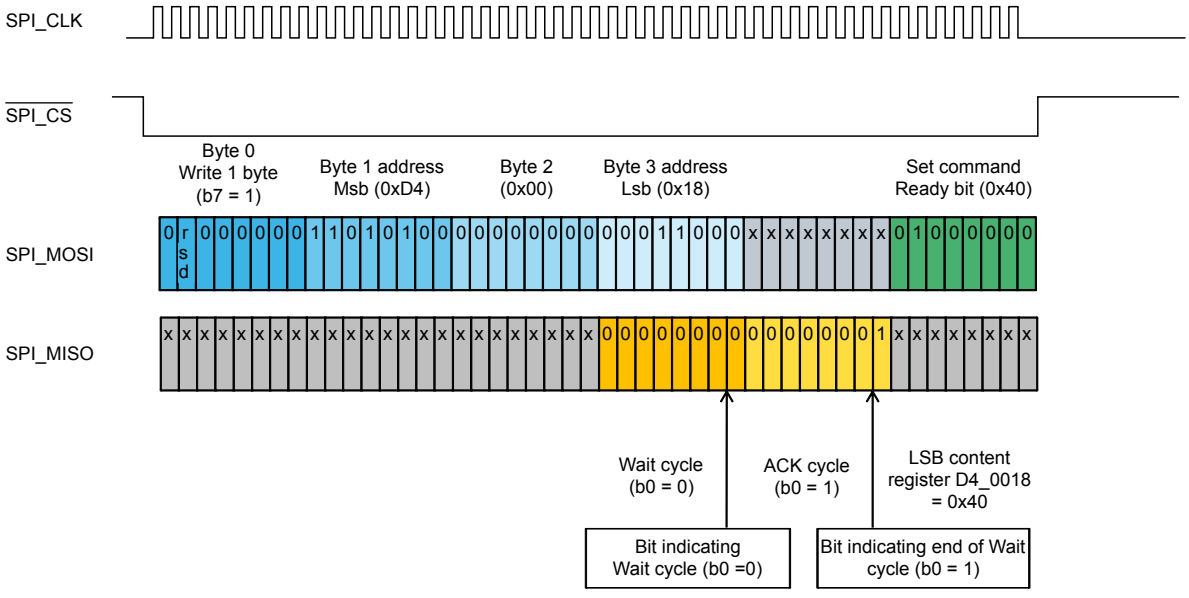
Figure 3. **SPI Read register example**



3.1.3 Protocol flow control for SPI write access

Following the standard specification, the TPM is authorized to insert 1 or more Wait states before acknowledging the write access. A Wait state is low state (0) sent on the SPI_MISO pin by the TPM. An Acknowledgment is a byte, whose last bit is '1', sent on the SPI_MISO pin by the TPM.

Figure 4. **SPI write register example**



3.2 Register space addresses

The following table shows TPM register space starting from the base address 0xD4_0000.

3.2.1 FIFO interface

Table 3. List of FIFO register space addresses

Locality 0	Register name	Locality 1	Register name	Locality 2	Register name	Locality 3	Register name	Locality 4	Register name	Register description
0x0000	TPM_ACCESS_0	0x1000	TPM_ACCESS_1	0x2000	TPM_ACCESS_2	0x3000	TPM_ACCESS_3	0x4000	TPM_ACCESS_4	Used to gain ownership of the TPM for this particular Locality
0x000B-0x0008	TPM_INT_ENABLE_0	0x100B-0x1008	TPM_INT_ENABLE_1	0x200B-0x2008	TPM_INT_ENABLE_2	0x300B-0x30008	TPM_INT_ENABLE_3	0x400B-0x4008	TPM_INT_ENABLE_4	Interrupt Configuration Register
0x000C	TPM_INT_VECTOR_0	0x100C	TPM_INT_VECTOR_1	0x200C	TPM_INT_VECTOR_2	0x300C	TPM_INT_VECTOR_3	0x400C	TPM_INT_VECTOR_4	SIRQ vector to be used by the TPM (SIRQ pin not available)
0x0013-0x0010	TPM_INT_STATUS_0	0x1013-0x1010	TPM_INT_STATUS_1	0x2013-0x2010	TPM_INT_STATUS_2	0x3013-0x3010	TPM_INT_STATUS_3	0x4013-0x4010	TPM_INT_STATUS_4	Shows which interrupt has occurred
0x0017-0x0014	TPM_INTF_CAPABILITY_0	0x1017-0x1014	TPM_INTF_CAPABILITY_1	0x2017-0x2014	TPM_INTF_CAPABILITY_2	0x3017-0x3014	TPM_INTF_CAPABILITY_3	0x4017-0x4014	TPM_INTF_CAPABILITY_4	Provides the information about supported interrupts and the characteristic of the burstCount register of the particular TPM.
0x001A-0x0018	TPM_STS_0	0x101A-0x1018	TPM_STS_1	0x201A-0x2018	TPM_STS_2	0x301A-0x3018	TPM_STS_3	0x401A-0x4018	TPM_STS_4	Status Register. Provides status of the TPM
-	-	-	-	-	-	-	-	0x4020	TPM_HASH_END	This signals the end of the hash operation in Locality 4.
0x00027-0x0024	TPM_DATA_FIFO_0	0x1027-0x1024	TPM_DATA_FIFO_1	0x2027-0x2024	TPM_DATA_FIFO_2	0x3027-0x3024	TPM_DATA_FIFO_3	0x4027-0x4024	TPM_HASH_DATA / TPM_DATA_FIFO_4	ReadFIFO or WriteFIFO, depending on the current bus cycle (read or write). These four addresses are aliased to one inside the TPM. In Locality 4, it is the HASH_DATA FIFO.
-	-	-	-	-	-	-	-	0x4028	TPM_HASH_START	This signals the start of the hash operation in Locality 4.
0x0080-0x0083	TPM_XDATA_FIFO_0	0x1080-0x1083	TPM_XDATA_FIFO_1	0x2080-0x2083	TPM_XDATA_FIFO_2	0x3080-0x3083	TPM_XDATA_FIFO_3	0x4080-0x4083	TPM_XDATA_FIFO_4	Extended ReadFIFO or WriteFIFO, depending on the current bus cycle (read or write). Transactions to this address may be any size from 1B to maxTransferCapability identified in the capability register.
0x00BF-0x0084	Reserved	0x10BF-0x1084	Reserved	0x20BF-0x2084	Reserved	0x30BF-0x3084	Reserved	0x40BF-0x4084	Reserved	-
0x0F03-0x0F00	TPM_DID_VID_0	0x1F03-0x1F00	TPM_DID_VID_1	0x2F03-0x2F00	TPM_DID_VID_2	0x3F03-0x3F00	TPM_DID_VID_3	0x4F03-0x4F00	TPM_DID_VID_4	Vendor and device ID
0x0F04	TPM_RID_0	0x1F04	TPM_RID_1	0x2F04	TPM_RID_2	0x3F04	TPM_RID_3	0x4F04	TPM_RID_4	Revision ID
0x0F7F-0x0F05	Reserved	0x1F7F-0x1F05	Reserved	0x2F7F-0x2F05	Reserved	0x3F7F-0x3F05	Reserved	0x4F7F-0x4F05	Reserved	-

3.2.2 Command response buffer interface

Table 4. List of CRB register space addresses

Locality 0	Register name	Locality 1	Register name	Locality 2	Register name	Locality 3	Register name	Locality 4	Register name
0x0003-0x0000	TPM_LOC_STATE_0	0x1003-1000	TPM_LOC_STATE_1	0x2000-0x2003	TPM_LOC_STATE_2	0x3000-0x3003	TPM_LOC_STATE_3	0x4000-0x4003	TPM_LOC_STATE_4
0x000B-0x0008	TPM_LOC_CTRL_0	0x100B-1008	TPM_LOC_CTRL_1	0x200B-0x2008	TPM_LOC_CTRL_2	0x300B-0x30008	TPM_LOC_CTRL_3	0x400B-0x4008	TPM_LOC_CTRL_4
0x000F-0x000C	TPM_LOC_STS_0	0x100F-100C	TPM_LOC_STS_1	0x200F-0x200C	TPM_LOC_STS_2	0x300F-0x300C	TPM_LOC_STS_3	0x400F-0x400C	TPM_LOC_STS_4
0x002F-0x0010	Reserved	0x102F-1010	Reserved	0x202F-0x2010	Reserved	0x302F-0x3010	Reserved	0x402F-0x4010	Reserved
0x0037-0x0030	TPM_INTERFACE_ IDENTIFIER_0	0x1037-1030	TPM_INTERFACE_ IDENTIFIER_1	0x2037-0x2030	TPM_INTERFACE_ IDENTIFIER_2	0x3037-0x3030	TPM_INTERFACE_ IDENTIFIER_3	0x4037-0x4030	TPM_INTERFACE_ IDENTIFIER_4
0x003F-0x0038	TPM_CRB_CTRL_EXT_0	0x103F-0x1038	Reserved	0x203F-0x2038	Reserved	0x303F-0x3038	Reserved	0x403F-0x4038	Reserved
0x0043-0x0040	TPM_CRB_CTRL_REQ_0	0x1043-0x1040	TPM_CRB_CTRL_REQ_1	0x2043-0x2040	TPM_CRB_CTRL_REQ_2	0x3043-0x3040	TPM_CRB_CTRL_REQ_3	0x4043-0x4040	TPM_CRB_CTRL_REQ_4
0x0047-0x0044	TPM_CRB_CTRL_STS_0	0x1047-0x1044	TPM_CRB_CTRL_STS_1	0x2047-0x2044	TPM_CRB_CTRL_STS_2	0x3047-0x3044	TPM_CRB_CTRL_STS_3	0x4047-0x4044	TPM_CRB_CTRL_STS_4
0x004B-0x0048	TPM_CRB_CTRL_ CANCEL_0	0x104B-0x1048	TPM_CRB_CTRL_ CANCEL_1	0x204B-0x2048	TPM_CRB_CTRL_ CANCEL_2	0x304B-0x3048	TPM_CRB_CTRL_ CANCEL_3	0x404B-0x14048	TPM_CRB_CTRL_ CANCEL_4
0x004F-0x004C	TPM_CRB_CTRL_ START_0	0x104F-0x104C	TPM_CRB_CTRL_ START_1	0x204F-0x204C	TPM_CRB_CTRL_ START_2	0x304F-0x304C	TPM_CRB_CTRL_ START_3	0x404F-0x404C	TPM_CRB_CTRL_ START_4
0x0057-0x0050	TPM_CRB_CTRL_INT_0	0x1057-0x1050	TPM_CRB_CTRL_INT_1	0x2057-0x2050	TPM_CRB_CTRL_INT_2	0x3057-0x3050	TPM_CRB_CTRL_INT_3	0x4057-0x4050	TPM_CRB_CTRL_INT_4
0x005B-0x0058	TPM_CRB_CTRL_CMD_ SIZE_0	0x105B-0x1058	TPM_CRB_CTRL_CMD_ SIZE_1	0x205B-0x2058	TPM_CRB_CTRL_CMD_ SIZE_2	0x305B-0x3058	TPM_CRB_CTRL_CMD_ SIZE_3	0x405B-0x4058	TPM_CRB_CTRL_CMD_ SIZE_4
0x005F-0x005C	TPM_CRB_CTRL_CMD_ LADDR_0	0x105F-0x105C	TPM_CRB_CTRL_CMD_ LADDR_1	0x205F-0x205C	TPM_CRB_CTRL_CMD_ LADDR_2	0x305F-0x305C	TPM_CRB_CTRL_CMD_ LADDR_3	0x405F-0x405C	TPM_CRB_CTRL_CMD_ LADDR_4
0x0063-0x0060	TPM_CRB_CTRL_CMD_ HADDR_0	0x1063-0x1060	TPM_CRB_CTRL_CMD_ HADDR_1	0x2063-0x2060	TPM_CRB_CTRL_CMD_ HADDR_2	0x3063-0x3060	TPM_CRB_CTRL_CMD_ HADDR_3	0x4063-0x4060	TPM_CRB_CTRL_CMD_ HADDR_4
0x0067-0x0064	TPM_CRB_CTRL_RSP_ SIZE_0	0x1067-0x1064	TPM_CRB_CTRL_RSP_ SIZE_1	0x2067-0x2064	TPM_CRB_CTRL_RSP_ SIZE_2	0x3067-0x3064	TPM_CRB_CTRL_RSP_ SIZE_3	0x4067-0x4064	TPM_CRB_CTRL_RSP_ SIZE_4
0x006F-0x0068	TPM_CRB_CTRL_RSP_ ADDR_0	0x106F-0x1068	TPM_CRB_CTRL_RSP_ ADDR_1	0x206F-0x2068	TPM_CRB_CTRL_RSP_ ADDR_2	0x306F-0x3068	TPM_CRB_CTRL_RSP_ ADDR_3	0x406F-0x4068	TPM_CRB_CTRL_RSP_ ADDR_4
0x007F-0x0070	Reserved	0x107F-0x1070	Reserved	0x207F-0x2070	Reserved	0x307F-0x3070	Reserved	0x407F-0x4070	Reserved
0x0880-0x0080	TPM_CRB_DATA_ BUFFER_0	0x1880-0x1080	TPM_CRB_DATA_ BUFFER_1	0x2880-0x2080	TPM_CRB_DATA_ BUFFER_2	0x3880-0x3080	TPM_CRB_DATA_ BUFFER_3	0x4880-0x4080	TPM_CRB_DATA_ BUFFER_4
0x0FFF-0x0881	Reserved	0x1FFF-0x1881	Reserved	0x2FFF-0x2881	Reserved	0x3FFF-0x3881	Reserved	0x4FFF-0x4881	Reserved

3.3 Register descriptions

Detailed descriptions of each register can be found in TCG PC Client Specific Platform TPM Profile for [PTP 2.0 r1.05].

3.4 Additional information

- The TPM implement a PIRQ but does not implement an SIRQ pin.
- Any write operation to the TPM_ACCESS_x register with more than one field set to a '1' is not accepted.
- Interface capability:
  - TPM_STS_x.burstCount is dynamic.
  - Interrupt detection mode "Level low" is supported (other modes "Level high" and "Edge" are not supported).
  - Interrupts localityChange and dataAvailable are supported (Interrupt stsValid and commandReady are not supported).
- Transaction size:
  - The TPM accepts transactions to offset 0x0024-0x0027 which are of lengths from 1 to 32 bytes (legacy FIFO).
  - The TPM accepts transactions to offset 0x0081-0x0083 which are of lengths from 1 to 32 bytes (extended FIFO).
- Vendor and Device ID for the TPM
  - TPM_DID_VID_X = 0x0000104A; // DID = 0x0000 and VID = 0x104A (id of STMicroelectronics defined by TCG)
- Revision ID for the TPM
  - TPM_RID_X = 0xFFFFFF4E; // 0xFFFFFF = reserved

3.5 Recommendations

For optimized performance results, the use of an extended data FIFO with 32-byte burst is mandatory.

When the falling edge occurs on the $\overline{\text{SPI\_CS}}$ signal, SPI_CLK must be at the low logic level as defined in Figure 7. SPI slave timing diagram - SPI_CLK low (by default).

If the device does not show this behavior, add a 56 pF capacitor (example value) on the $\overline{\text{SPI\_CS}}$ line to slow the falling edge on $\overline{\text{SPI\_NSS}}$ or $\overline{\text{SPI\_CS}}$.

3.6 Integration requirements

- When the falling edge occurs on the $\overline{\text{SPI\_CS}}$ signal, SPI_CLK must be at the low logic level as defined in Figure 7. SPI slave timing diagram - SPI_CLK low (by default).
  If the device does not show this behavior, add a 56 pF capacitor (example value) on the $\overline{\text{SPI\_CS}}$ line to slow the falling edge on $\overline{\text{SPI\_NSS}}$ or $\overline{\text{SPI\_CS}}$.
- The duration of TPM_HASH_DATA exceeds 250 µs if SHA384 and Dual bank management are implemented.
- In Windows 10 or 11, for using a 3072-bit RSA key, update the following, if it exists in the registry editor:
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TPM]
  "TimeoutCommandCreate"=dword:00493E0

4 Electrical characteristics

This section summarizes the operating and measurement conditions, and the DC and AC characteristics of the device. The parameters in the DC and AC characteristic tables that follow are derived from tests performed under the measurement conditions summarized in the relevant tables. Users should check that the operating conditions in their circuit match the measurement conditions when relying on the quoted parameters.

4.1 Absolute maximum ratings

Table 5. Absolute maximum ratings

Symbol	Parameter	Value	Unit
V_{PS}	Supply voltage	–0.3 to 3.6	V
V_{IO}	Input or output voltage relative to ground	–0.3 to V_{PS} +0.3	V
T_A	Ambient operating temperature	–25 to +85	°C
		–40 to +105(1)	
T_{STG}	Storage temperature (refer to [AN2639])	–65 to +150	°C
V_{ESD}	Electrostatic discharge voltage according to JESD22-A114, human body model	4000	V
	Electrostatic discharge voltage according to ANSI ESD STM5.3.1, charged device model	750	V

1. *For the 3.3 V voltage range only.*

Note: Stresses listed above may cause permanent damage to the device. This is a stress rating only and functional operation of the device at these or any other conditions above those indicated in the operational sections of the specification is not implied.

Exposure to absolute maximum rating conditions for extended periods may affect device reliability.

4.2 DC and AC characteristics

T_A = −40 to 105 °C (for the 3.3 V voltage range only) and T_A = −25 to 85 °C (for the 1.8 V and 3.3 V voltage ranges).

The voltage (V_{PS}) must be in one of the two authorized ranges: 1.8 V ±10% or 3.3 V ±10%.

The voltage on all inputs or outputs must not exceed V_{PS} + 0.3 V or be lower than V_{PS} - 0.3 V.

Table 6. DC characteristics (V_{PS} = 1.8 V or 3.3 V ± 10%)

Symbol	Parameter	Condition	Min.	Typ.	Max.	Unit
V_{IL}	Input low voltage	-	–0.3	-	0.2 × V_{PS}	V
V_{IH}	Input high voltage	-	0.7 × V_{PS}	-	V_{PS} + 0.3	V
I_{IL}	Input low current in high Impedance mode	0 V < V_{IL} < 0.2 × V_{PS}	–10	-	10	µA
	Input low current in Weak Pull-up mode (V_{PS} = 1.8 V±10%)	0 V < V_{IL} < 0.2 × V_{PS}	–500	-	1000	
	Input low current in Weak Pull-up mode (V_{PS} = 3.3 V±10%)	0 V < V_{IL} < 0.2 × V_{PS}	–500	-	-	
I_{IH}	Input high current in high Impedance mode	0.7 × V_{PS} < V_{IH} < V_{PS}	–10	-	10	µA
	Input high current in Weak Pull-down mode (V_{PS} = 1.8 V±10%)	0.7 × V_{PS} < V_{IH} < V_{PS}	–20	-	20	
	Input high current in Weak Pull-down mode (V_{PS} = 3.3 V±10%)	0.7 × V_{PS} < V_{IH} < V_{PS}	–30	-	30	

Symbol	Parameter	Condition	Min.	Typ.	Max.	Unit
V_{OH}	Output high voltage	I_{OH} = −1 mA	0.75 × V_{PS}	-	V_{PS}	V
V_{OL}	Output low voltage (V_{PS} = 1.8 V±10%)	I_{OL} = 500 µA	0	-	0.15 × V_{PS}	V
	Output low voltage (V_{PS} = 3.3 V±10%)	I_{OL} = 1 mA	0	-	0.15 × V_{PS}	
POR	Power on reset voltage(1)	-	-	1.45	1.61	V
PD_R	Pull-down resistor	-	-	10	-	kΩ
PU_R	Pull-up resistor	-	-	100	-	kΩ

1. *V_{PS} voltage from which the device starts to run or V_{PS} voltage below which the device starts to switch off during a shutdown.*

4.3 Overshoot

The TPM has been tested in accordance with JEDEC standard JESD78D.

- Tolerated overshoot: 1.5 ×V_{PS}
- Maximum time during overshoot: 10 ms.

4.4 Performance and power consumption characteristics

The values provided in the table below were measured at T_A = −40 to 105 °C (for the 3.3 V voltage range only) and T_A = −25 to 85 °C (for the 1.8 V and 3.3 V voltage ranges).

Table 7. Power-on and warm reset timing characteristics

Symbol	Parameter	Condition	Min.	Typ.	Max.	Unit
t_{WL}	$\overline{\text{RESET}}$ pin low state pulse width for reset	-	1	-	-	ms
t_{INIT}	Minimum time for TPM_ACCESS_x registers to contain valid data from TPM reset	-	-	-	500	µs
t_{CMD}	Time required before sending first TPM command from TPM reset	-	-	-	50	ms
t_{POR_RST}	POR to SPI_RST time	C_{LOAD} = 30 pF	-	200	-	µs
t_{Init_stb}	Wakeup time from Standby	-	-	-	150	µs

Table 8. Power consumption characteristics

The values provided in the table below were measured at T_A = 25 °C.

Symbol	Parameter	Typ.	Max.	Unit
I_{CC} Run	Normal TPM operation	-	17.5	mA
I_{CC} Idle	Supply current when not processing any commands.	4	-	mA
I_{CC} Standby	Supply current when the device is in Deep Sleep mode(1).	60	-	µA

1. *Activated by default. See Proprietary commands and Technical features.*

Figure 5. Power on and warm reset sequence

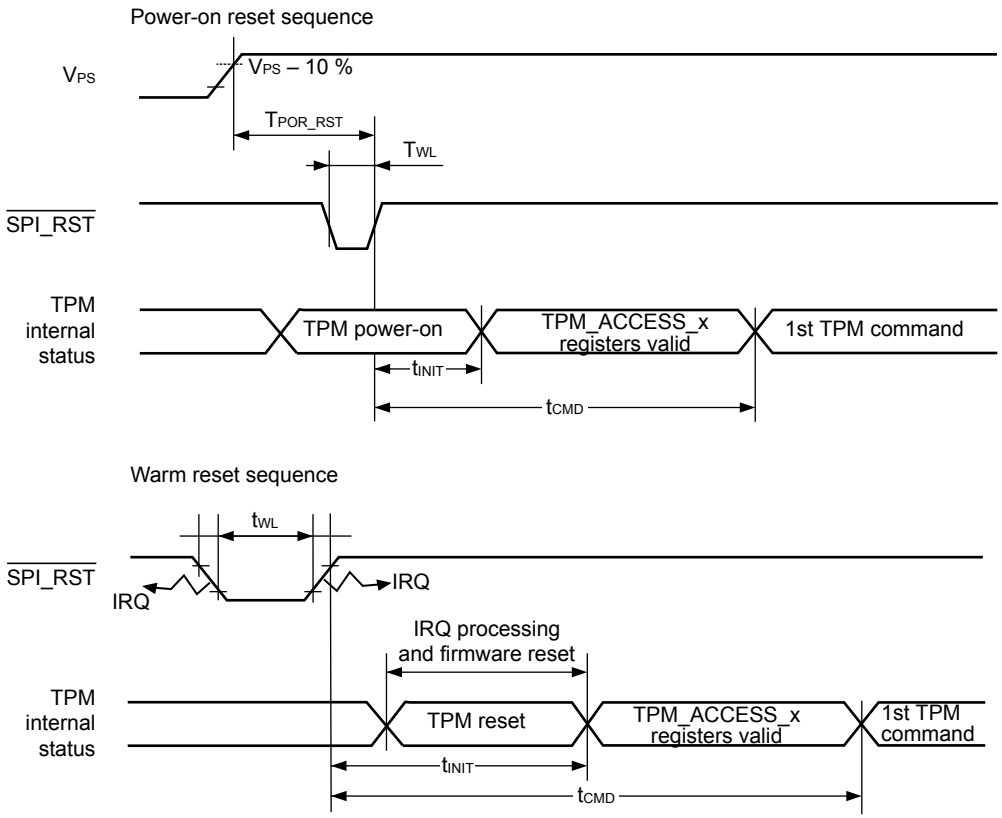
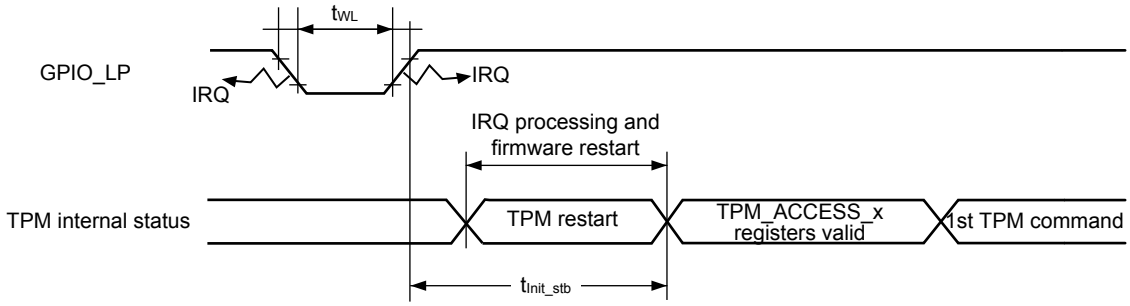


Figure 6. Standby sequence



4.5 SPI characteristics

The SPI latency for the product is 2 bytes.

Table 9. SPI electrical characteristics

Data based on design simulation and/or characterization results, not tested in production.

Symbol	Parameter	Min.	Max.	Unit
f_{SCK}	SPI clock frequency with max baud rate (f/2)	-	34	MHz
$t_{c(SCK)}$	$1/f_{SCK}$	29.4	-	ns
$t_{su(SI)}$	Data input setup time	5	-	ns
$t_{h(SI)}$	Data input hold time	5	-	
$t_{v(SO)}$	Data output valid time		13	
$t_{h(SO)}$	Data output hold time	0	-	
$t_{SU(NSS)}$	Setup time	$5 + 0.5 \times t_{C\ (SPI\_CLK)}$	-	
$t_{h(NSS)}$	Hold time	$5 + 0.5 \times t_{C\ (SPI\_CLK)}$	-	
$t_{dis(SO)}$(1)	Data output disable time	2	10	ns
$t_{a(SO)}$(2)	Data output access time	0	25	ns
t_{delay}	Minimum delay time between SPI_CLK going low and $\overline{SPI\_NSS}$ going low	7	-	ns

1. *The Min. time is the minimum time required to invalidate the data output; the Max. time is the maximum time required for the data output to go to high impedance.*
2. *The Min. time is the minimum time required to drive the data output; the Max. time is the maximum time required to validate the data output.*

Figure 7. SPI slave timing diagram - SPI_CLK low (by default)

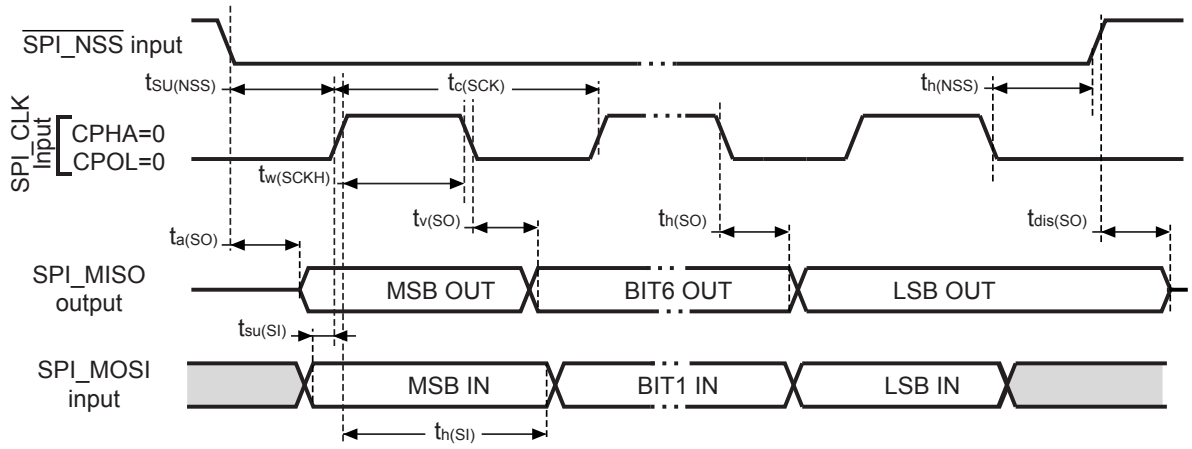
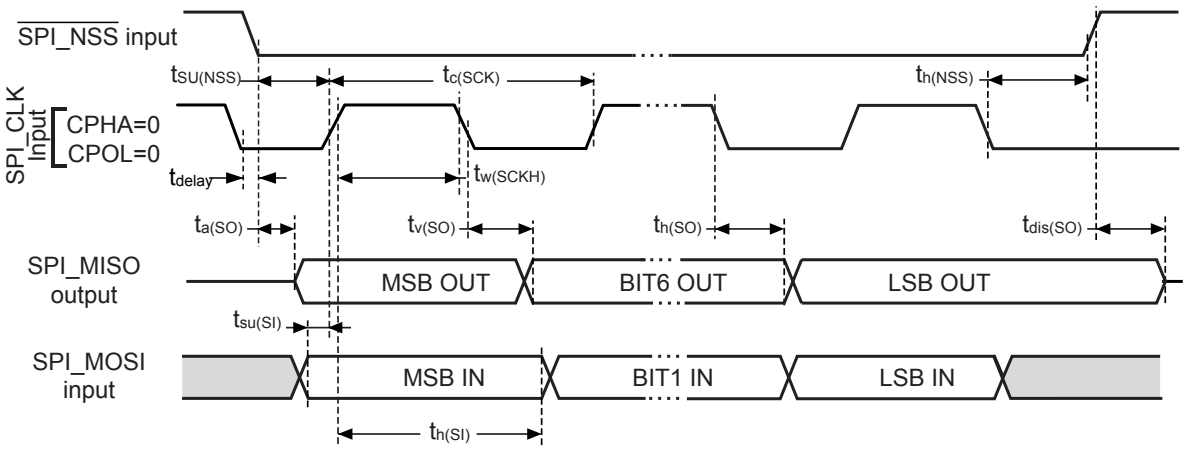


Figure 8. SPI slave timing diagram - SPI_CLK high (by default)



Note: 1. *For both drawings, measurements are made at CMOS levels: 0.3 × V_{PS} and 0.7 × V_{PS}.*

2. *When no communication is ongoing the data output line of the SPI (SPI_MOSI in Master mode, SPI_MISO in Slave mode) has its alternate function capability released. In this case, the pin status depends on the I/O port configuration.*

4.6 AC measurement conditions

Table 10. AC measurement conditions

T_A = −40 to 105 °C (for the 3.3 V voltage range only) and T_A = −25 to 85 °C (for the 1.8 V and 3.3 V voltage ranges).
f = 1 MHz, unless otherwise specified.

Parameter	Value (1)
Input rise and fall times	10 ns max
Input pulse voltage	V_{IL} to V_{IH}
Input timing reference voltage	0.5 × V_{PS}
Output timing reference voltage	V_{OL} to V_{OH}

1. *Measurement points are at CMOS levels: 0.3 × V_{PS} and 0.7 × V_{PS}.*

Figure 9. AC testing input/output waveforms

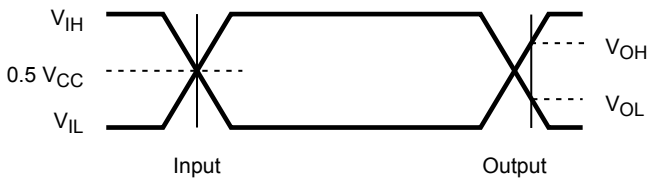
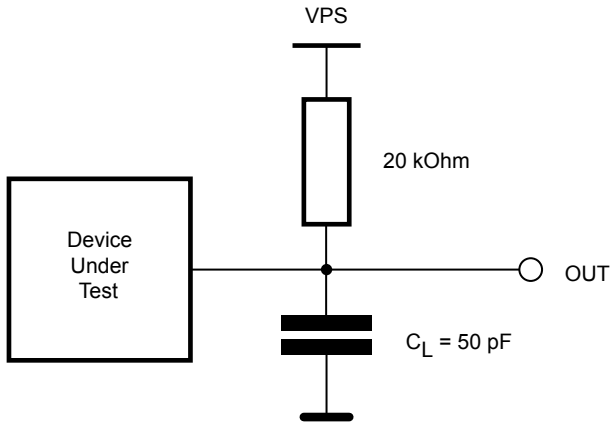


Figure 10. AC testing load circuit



C_L includes JIG capacitance

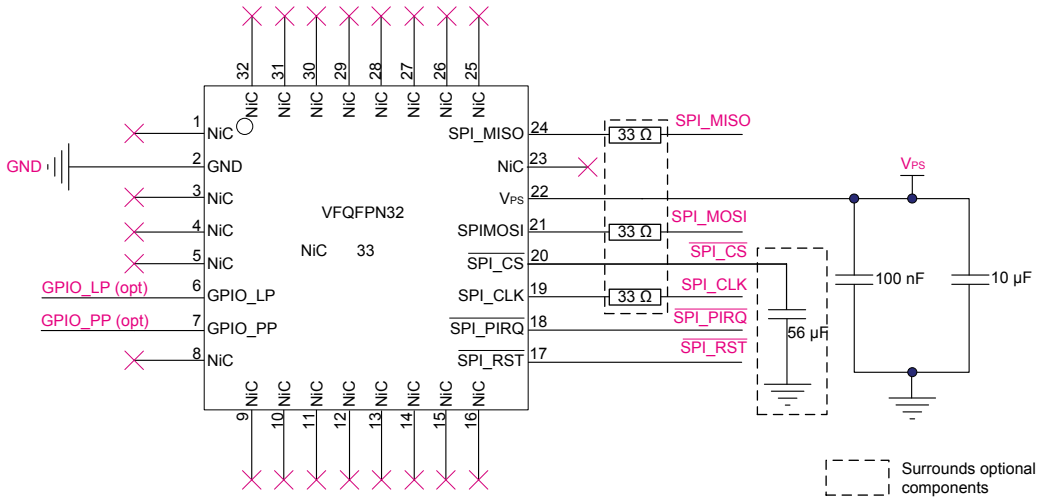
5 Integration guidance

5.1 Typical hardware implementation

The Physical Presence (PP) pin should be connected if platform implementation (at boot level) uses a hardware physical presence function.

The figure below shows the hardware implementation for the VFQFPN32 package.

Figure 11. Typical hardware implementation (VFQFPN32 package)



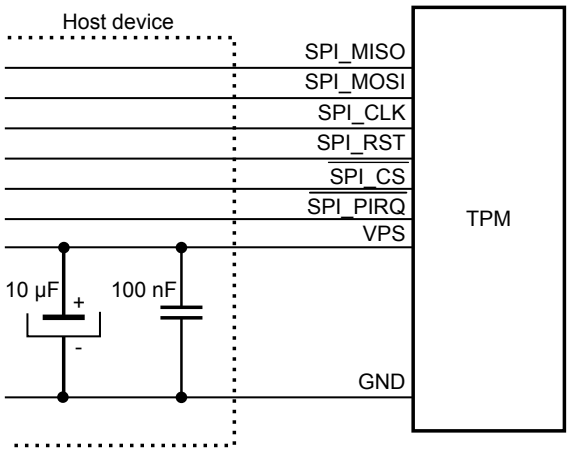
Note: The use of a low-value resistor (typically 33 Ω) on SPI_MISO, SPI_MOSI and SPI_CLK can be recommended for line adaptation when the signals are affected by parasite spikes. It can also be recommended to avoid disturbance of the ramp-up and ramp-down signals.

The capacitor on $\overline{SPI\_CS}$ is optional. Its use is recommended when the SPI_CLK signal is high in SPI mode 0 (see Section 3.6 Integration requirements).

5.2 Power supply filtering

As mentioned in Section 2 Pin and signal description, the power supply of the circuit must be filtered using the circuit shown in the figure below.

Figure 12. Mandatory filtering capacitors on V_{PS}



1. 10 µF and 100 nF are recommended values. The minimum required capacitor value is 2.1 µF (2 µF in parallel with 100 nF).

Table 11. Maximum V_{PS} rising slope

Symbol	Parameter	Value	Unit
S_{VPS}	Maximum VPS rising slope	3.3	V/µs

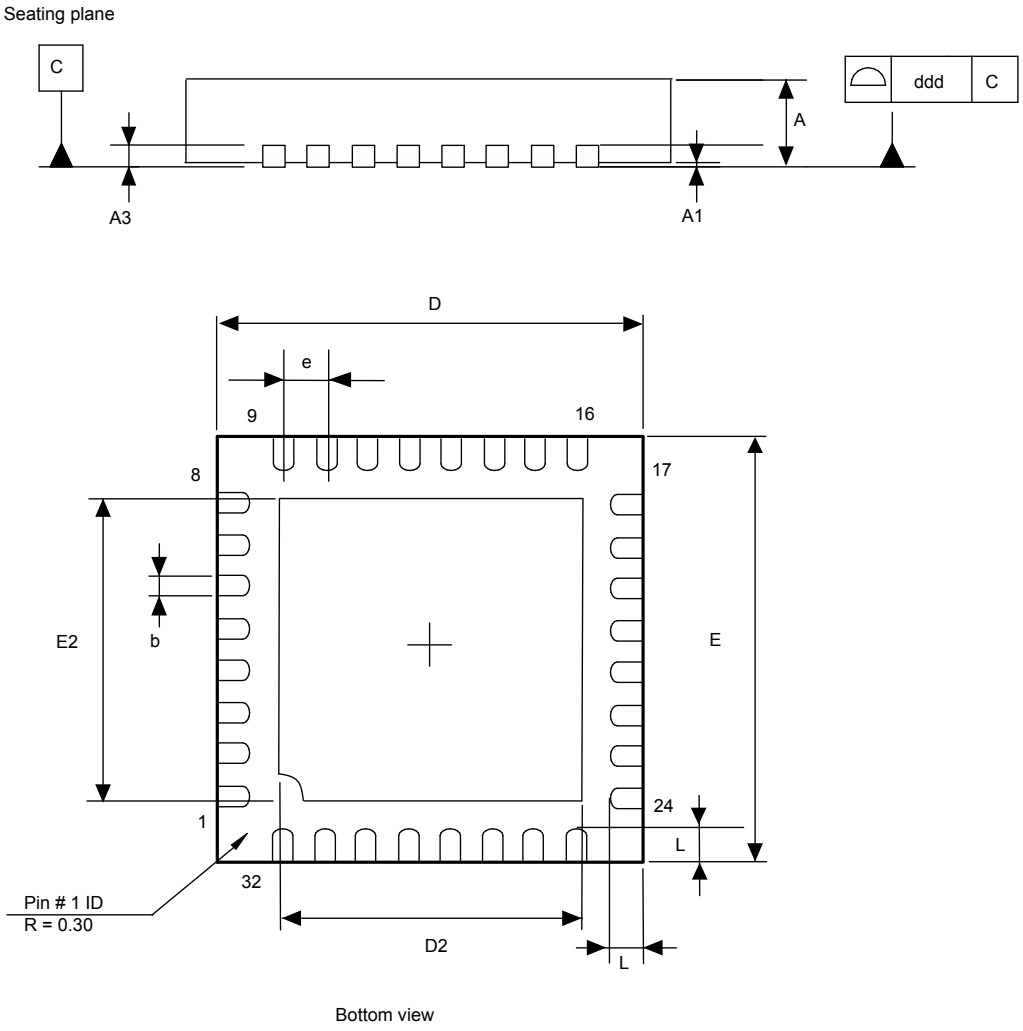
6 Package information

In order to meet environmental requirements, ST offers these devices in different grades of ECOPACK packages, depending on their level of environmental compliance. ECOPACK specifications, grade definitions and product status are available at: www.st.com. ECOPACK is an ST trademark.

6.1 VFQFPN32 package information

VFQFPN32 is a 32-lead, 5 × 5 mm, 0.5 mm pitch, very thin fine pitch quad flat pack no-lead package.

Figure 13. VFQFPN32 - outline



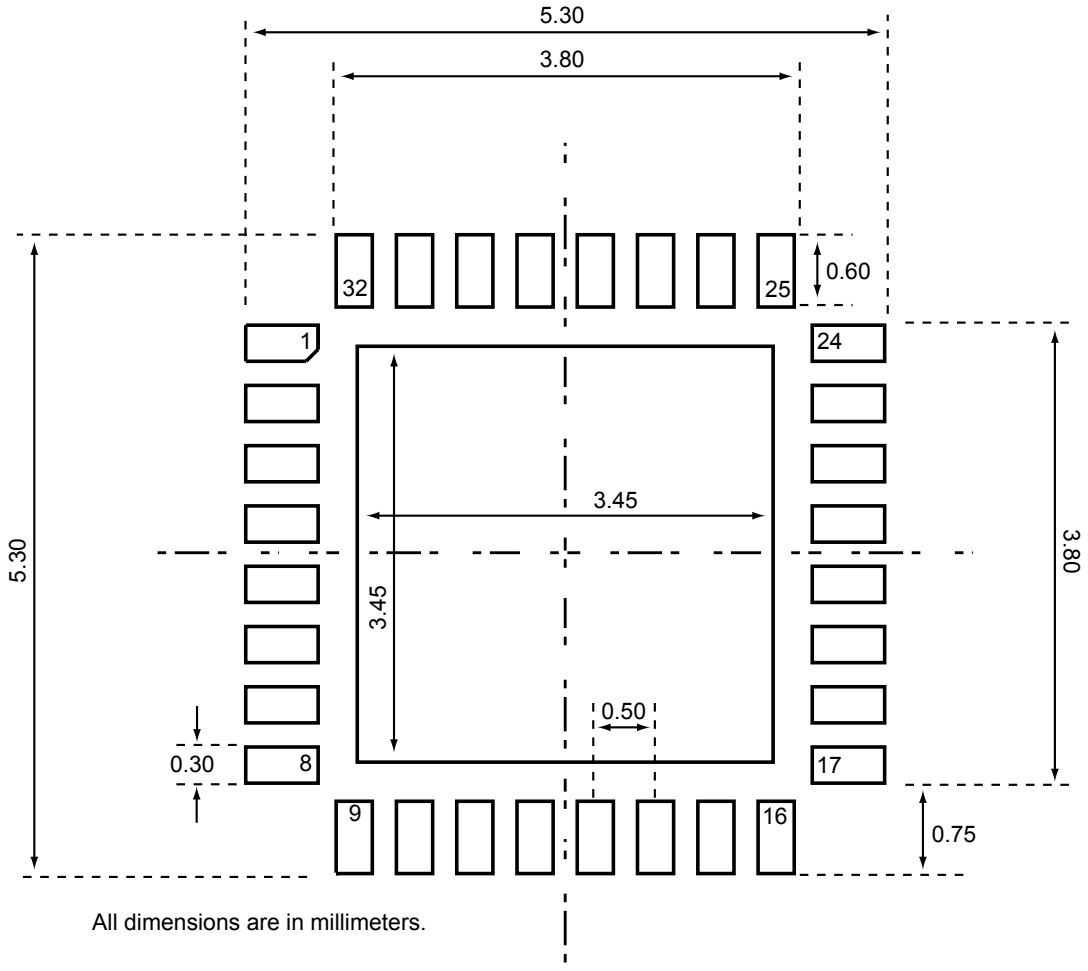
1. Drawing is not to scale.

Table 12. VFQFPN32 - mechanical data

Symbol	millimeters			inches[1]		
	Min.	Typ.	Max.	Min.	Typ.	Max.
A	0.800	0.900	1.000	0.0315	0.0354	0.0394
A1	0.000	0.020	0.050	0.0000	0.0008	0.0020
A3	-	0.200	-	-	0.0079	-
b	0.180	0.250	0.300	0.0071	0.0098	0.0118
D	4.850	5.000	5.150	0.1909	0.1969	0.2028
D2	3.500	3.600	3.700	0.1378	0.1417	0.1457
E	4.850	5.000	5.150	0.1909	0.1969	0.2028
E2	3.500	3.600	3.700	0.1378	0.1417	0.1457
e	-	0.500	-	-	0.0197	-
L	0.300	0.400	0.500	0.0118	0.0157	0.0197
ddd	-	-	0.050	-	-	0.0020

1. *Values in inches are converted from mm and rounded to 4 decimal digits.*

Figure 14. VFQFPN32 - recommended footprint



6.2 Thermal characteristics of packages

The table below provides the thermal characteristics of the VFQFPN32 package.

Table 13. Thermal characteristics

Parameter		Symbol	Value
Recommended operating temperature range	Ambient temperature	T_A	−40 to 105 °C
	Case temperature	T_C	-
	Junction temperature	T_J	−43 to 108 °C
Absolute maximum junction temperature		-	125 °C
Maximum power dissipation		-	63 mW
Theta-JA, -JB and -JC	Junction to ambient thermal resistance	θ_{JA} (1)	35.8 at 0 lfpm (2)
	Junction to case thermal resistance	θ_{JC}	1.48 at 0 lfpm (2)
	Junction to board thermal resistance	θ_{JB}	13.9 at 0 lfpm (2)

1. *According to JESD51-2 (still air condition).*
2. *Linear feet per minute.*

7 Delivery packing

Surface-mount packages can be supplied with tape and reel packing. The reels have a 13" typical diameter.

Reels are in plastic, either anti-static or conductive, with a black conductive cavity tape. The cover tape is transparent anti-static or conductive.

The devices are positioned in the cavities with the identifying pin (normally Pin “1”) on the same side as the sprocket holes in the tape.

The STMicroelectronics tape and reel specifications are compliant with the EIA 481-A standard specification.

Table 14. Packages on tape and reel

Package	Description	Tape width	Tape pitch	Reel diameter	Quantity per reel
VFQFPN32	Very thin fine pitch quad flat pack no-lead package	12 mm	8 mm	13 in.	3000

Figure 15. Reel diagram

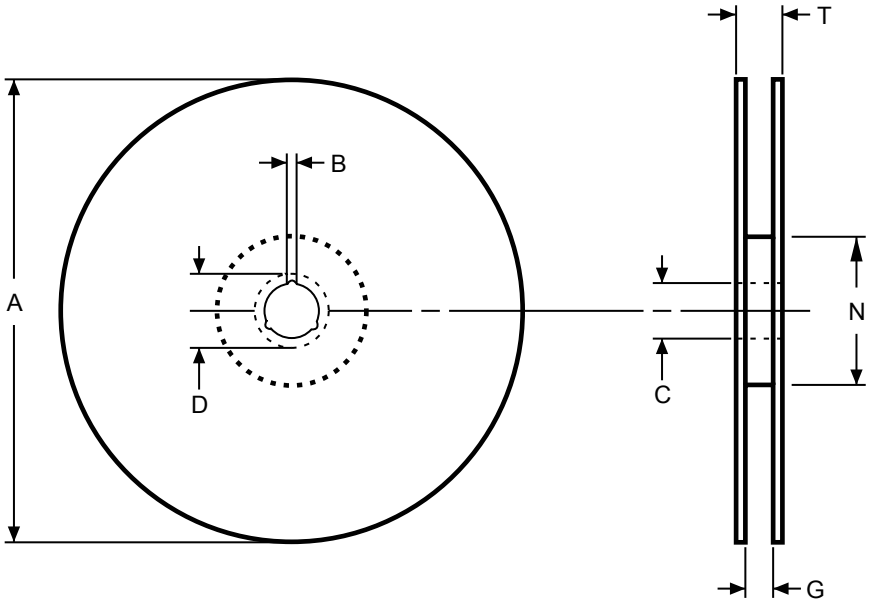
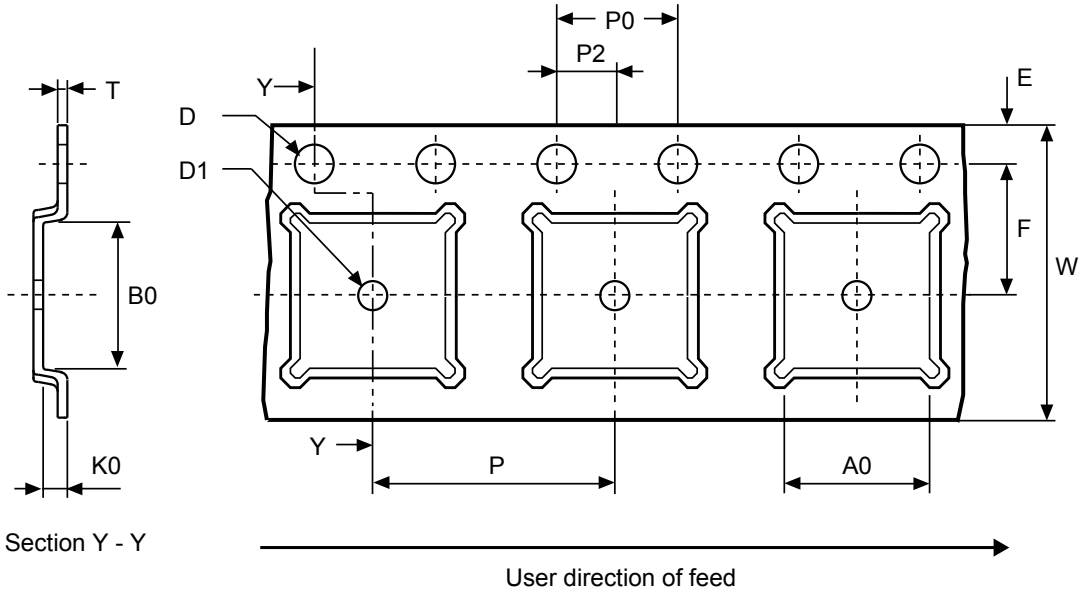


Table 15. Reel dimensions

Reel size	Tape width	A Max.	B Min.	C	D Min.	G Max.	N Min.	T Max.	Unit
13”	16	330	1.5	13 ±0.2	20.2	16.4 +2/–0	100	22.4	mm
	12					12.6		18.4	

Figure 16. Embossed carrier tape for VFQFPN32 5 × 5 mm



1. Drawing is not to scale.

Figure 17. Chip orientation in the embossed carrier tape for VFQFPN32 5 × 5 mm

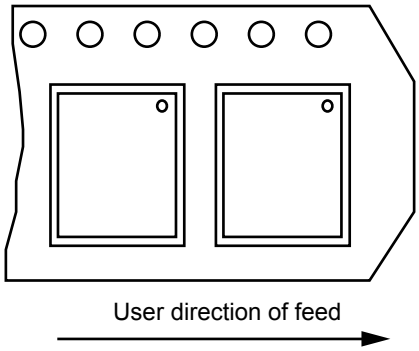


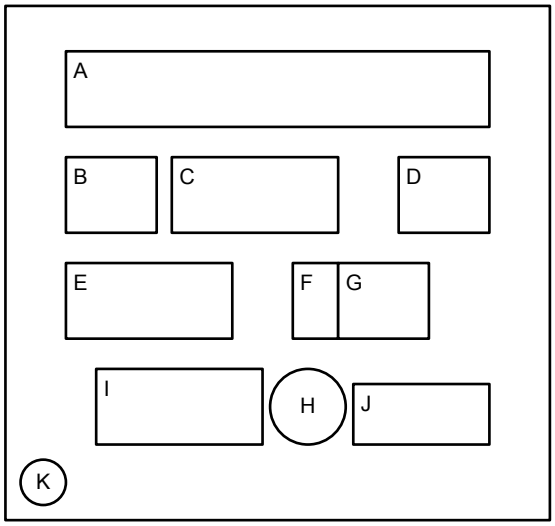
Table 16. Carrier tape dimensions for VFQFPN32 5 × 5 mm

Package	A0	B0	K0	D1 Min.	P	P2	D	P0	E	F	W	T Max.	Unit
VFQFPN 5×5	5.25 ±0.1	5.25 ±0.1	1.1 ±0.1	1.5	8 ±0.1	2 ±0.1	1.55 ±0.05	4 ±0.1	1.75 ±0.1	5.5 ±0.1	12 ±0.3	0.3 ±0.05	mm

8 Package marking information

The figure below illustrates the typical marking of the VFQFPN32 device package.

Figure 18. VFQFPN32 device package marking area



A: Marking area

B: Assembly plant

C: BE sequence

D: Diffusion plant

E: Country of origin

F: Assembly year

G: Assembly week

H: Second-level interconnect (JESD97)

I: ST logo

J: Marking area - 2 digits

K: Dot

For both packages, the 6-digit ‘A’ marking area is equal to "PXYZZZ", with:

- Y = Hardware revision
- ZZZ = Product identifier

9 Ordering information

Table 17. **Ordering information**

Ordering code	Firmware version	TPM Library	Package	Marking A	Product status
ST33HTPH2X32AHE4	0x00.01.03.01 (1.769)	1.59	VFQFPN32	PXAHE4	Active (recommended for new design)
ST33HTPH2X32AHD8	0x00.01.01.02 (1.258)	1.38		PXAHD8	Active
ST33HTPH2X32AHD4	0x00.01.01.01 (1.257)	1.38		PXAHD4	Active

Note: A technical note describing the evolutions between the different firmware versions is available through e-mail support or the sales channels.

10 Support and information

Additional information regarding ST TPM devices can be obtained from the www.st.com website.

For any specific support information you can contact STMicroelectronics through the following e-mail: *TPMsupport@list.st.com*.

STMicroelectronics has put in place a Product Security Incident Response Team (ST PSIRT). We encourage you to report any potential security vulnerability that you might suspect in our products through the ST PSIRT web page: https://www.st.com/psirt.

Appendix A Terms and abbreviations

Table 18. List of abbreviations

Term	Meaning
AES	Advanced Encryption Standard
CA	Certificate authority
CC	Common Criteria
DAM	Dictionary attack mitigation mechanism
Data byte	Byte from the TPM command or answer or register value.
DES	Data Encryption Standard
EC	Elliptic curve
ECC	Elliptic curve cryptography
ECDDA	Elliptic curve direct anonymous attestation
ECDH	Elliptic curve Diffie-Hellman
ECDSA	Elliptic curve digital signature algorithm
ECSchorr	Elliptic curve with Schnorr signature code
EK	Endorsement key
eps	Endorsement primary seed
FIPS	Federal Information Processing Standard
FU	Firmware update
GPIO	General-purpose I/O
HLK	Hardware Lab Kit (Windows®)
HMAC	Keyed-Hashing for Message Authentication
lfpm	Linear feet per minute
HSM	Hardware security module
HWINTF	Hardware interface layer in the TPM's internal firmware; used to drive communication.
NIST	National Institute of Standards and Technology
NV	Non-volatile (memory)
OAEP	Optimal asymmetric encryption padding
OEM	Original equipment manufacturer
OIAP	Object-Independent Authorization Protocol
OSAP	Object Specific Authorization Protocol
PCR	Platform Configuration register
PKCS	Public-key cryptography standards
PKI	Public-key infrastructure
PSS	Probabilistic signature scheme
RSA	Rivest Shamir Adelman
RSAES	Rivest Shamir Adelman encryption/decryption scheme
RSASSA	Rivest Shamir Adelman signature scheme with appendix
RTM	Root of trust for measurement
RTR	Root of trust for reporting
SHA	Secure Hash algorithm

Term	Meaning
SPI	Serial peripheral interface
SRK	Storage root key
TCG	Trusted Computed Group
TDES	Triple data encryption standard
TIS	TPM interface specification
TPM	Trusted Platform Module
TPME	TPM manufacturer
Transaction bytes	All bytes from a TPM command or TPM answer.
TSS	TPM software stack

Appendix B Referenced documents

The following materials are to be used in conjunction with or are referenced by this document.

[TPM 2.0 P1 r159]	TPM Library, Part 1, Architecture, Family 2.0, rev 1.59, TCG
[TPM 2.0 P2 r159]	TPM Library, Part 2, Structures, Family 2.0, rev 1.59, TCG
[TPM 2.0 P3 r159]	TPM Library, Part 3, Commands, Family 2.0, rev 1.59, TCG
[TPM 2.0 P4 r159]	TPM Library, Part 4, Supporting routines, Family 2.0, rev 1.59, TCG
[TPM 2.0 rev159 Err 1.1]	
[PTP 2.0 r1.05]	TCG PC Client Platform TPM Profile (PTP) for TPM 2.0 Version 1.05 Revision 14, TCG
[PKCS#1]	PKCS#1: v2.1 RSA Cryptography Standard, RSA Laboratories
[AN2639]	Application note, Soldering recommendations and package information for Lead-free ECOPACK microcontrollers, STMicroelectronics
[TCG EK Cre Profile TPM 2.3]	TCG EK credential profile for TPM Family 2.0 Level 0. Specification Version 2.3 Revision 2, 23 July 2020, TCG.
[TPM 2.0 PP]	TCG Protection Profile for PC Client Specific TPM 2.0 Library Revision 1.59; Version 1.3
[SP800-90B]	Recommendation for the entropy sources used for random bit generation, January 2018, NIST
[SP800-90Ar1]	Recommendation for random number generation using deterministic random bit generators, June 2015, NIST

Revision history

Table 19. **Document revision history**

Date	Revision	Changes
20-Dec-2022	1	Initial release.

Contents

List of figures

List of tables

IMPORTANT NOTICE – READ CAREFULLY

STMicroelectronics NV and its subsidiaries (“ST”) reserve the right to make changes, corrections, enhancements, modifications, and improvements to ST products and/or to this document at any time without notice. Purchasers should obtain the latest relevant information on ST products before placing orders. ST products are sold pursuant to ST’s terms and conditions of sale in place at the time of order acknowledgment.

Purchasers are solely responsible for the choice, selection, and use of ST products and ST assumes no liability for application assistance or the design of purchasers’ products.

No license, express or implied, to any intellectual property right is granted by ST herein.

Resale of ST products with provisions different from the information set forth herein shall void any warranty granted by ST for such product.

ST and the ST logo are trademarks of ST. For additional information about ST trademarks, refer to www.st.com/trademarks. All other product or service names are the property of their respective owners.

Information in this document supersedes and replaces information previously supplied in any prior versions of this document.