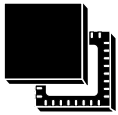
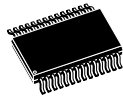


Flash-memory-based device combining TPM 1.2 and TPM 2.0 with an SPI interface



VFQFPN32
(5 × 5 mm)



TSSOP28
(4.4 mm body width)

Features

TPM features

- Flash-memory-based Trusted Platform Module (TPM)
- Supporting two modes exclusively with either the TPM 1.2 or the TPM 2.0 command set
- Supporting dynamic switch from one mode to another and capability to lock one mode irreversibly
- For TPM 1.2, compliant with Trusted Computing Group (TCG) Trusted Platform Module (TPM) Main specifications 1.2, Level 2, Revision 116 and TCG PC Client Specific TPM Interface Specifications 1.3
- For TPM 2.0, compliant with Trusted Computing Group (TCG) Trusted Platform Module (TPM) Library specifications 2.0, Level 0, Revision 138 and TCG PC Client Specific TPM Platform Specifications 1.03
- TPM firmware code can be upgraded thanks to a persistent Flash-memory loader application to support new standard evolutions
- Common Criteria (CC) certification according to the TPM 1.2 and TPM 2.0 protection profiles at EAL4+
- FIPS 140-2 level 1 certification for both modes and level 2 for mode TPM2.0
- SPI support for up to 33 MHz in FIFO and CRB protocol modes
- Support for software and hardware physical presence for TPM 1.2 and TPM 2.0

Hardware features

- Arm® SecurCore® SC300™ 32-bit RISC core
- Highly reliable Flash memory technology
- Extended temperature range: -40 °C to 105 °C
- ESD (electrostatic discharge) protection up to 4 kV (HBM)
- 1.8 V or 3.3 V supply voltage range
- 28-lead thin shrink small outline and 32-lead very thin fine pitch quad flat pack ECOPACK packages

Security features

- Active shield and environmental sensors
- Memory protection unit (MPU) used to segregate TPM assets between TPM 1.2 and TPM 2.0 modes
- Monitoring of environmental parameters (power)
- Hardware and software protection against fault injection
- FIPS compliant RNG built on an SP800-90A compliant SHA256 DRBG and an AIS-31 Class PTG2 compliant true random number generator (TRNG)
- Cryptographic algorithms:
 - RSA key generation (1024 or 2048 bits)
 - RSA signature and encryption
 - HMAC SHA-1 & SHA-256
 - AES-128-192-256
 - ECC 224 & 256 bits

Product status link

[ST33TPHF2ESPI](#)



Product compliance

- TPM 1.2 compliant with Microsoft® Windows® 7, 8.1 and 10
- TPM 2.0 compliant with Microsoft Windows 10
- Compliant with Intel® TXT for TPM1.2 and TPM 2.0 in SPI FIFO mode
- TPM 1.2 and TPM 2.0 compliant with the respective TCG test suites

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.

They embed an Arm® SecurCore SC300™ processor with additional security features to help protect against advanced forms of attack.

The ST33TPHF2ESPI offers a slave serial peripheral interface (SPI) compliant with the TCG PC Client TPM Profile specifications.

The ST33TPHF2ESPI supports two exclusive modes that support either TPM 1.2 or TPM 2.0 commands. The product can be locked irreversibly in TPM 1.2 or TPM 2.0 mode during provisioning, or only after provisioning to provide a smooth migration between TPM 1.2 and TPM 2.0.

The ST33TPHF2ESPI operates in the –25 to +85 °C commercial temperature range with a supply and I/O voltage of 1.8 V, or in the –40 °C to 105 °C extended temperature range with a supply and I/O voltage of 3.3 V.

The device is offered in TSSOP28 and VFQFPN32 ECOPACK2 packages. ECOPACK is an ST trademark.

Note: Arm is a registered trademark of Arm Limited (or its subsidiaries) in the US and/or elsewhere.

arm



2 Data brief scope

2.1 ST33TPHF2ESPI products

This document covers the functionality of firmware version 49.08 (73.08 in decimal) preloaded on ST TPM hardware with markings:

- PEAHC0

The information to order the supporting platforms is provided in [Section 8 Ordering information](#).

2.2 Firmware image

The firmware image version 49.08 can be loaded to the ST TPM hardware of the [ST33TPHF2ESPI](#) products, identifiable by their firmware version, which is of the form 49.xx. The ordering codes of the products upgradable to firmware version 49.08 are the following:

- ST33HTPH2ExxAAF0 and ST33HTPH2ExxAAF1 (FW 49.00)
- ST33HTPH2ExxAHB3 and ST33HTPH2ExxAHB4 (FW 49.04)

3 Pin and signal description

The two figures below give the pinouts of the two packages in which the devices are delivered. The table describes the associated signals.

Figure 1. TSSOP28 pinout

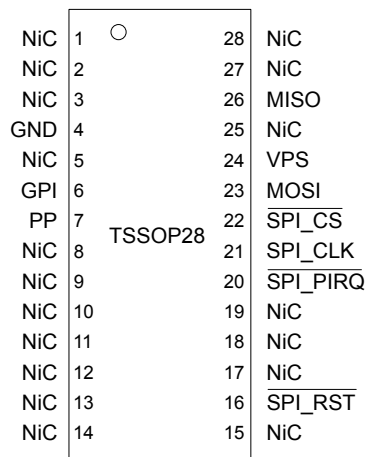


Figure 2. VQFN32 pinout

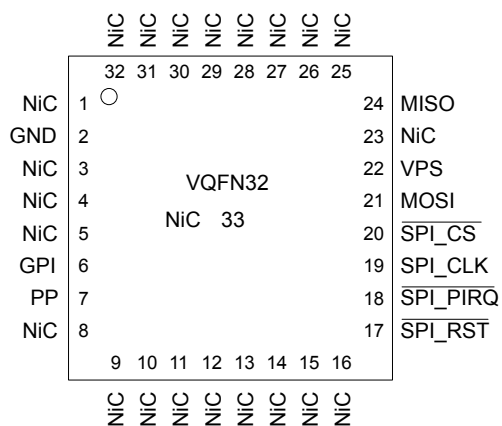


Table 1. Pin descriptions

| Signal | Type | Description |
|----------|--------|--|
| VPS | Input | Power supply. This pin must be connected to 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, internal pull-up, used to re-initialize the device. Must not be unconnected. External pull-up required if it cannot be driven. |
| MISO | Output | SPI Master Input, Slave Output (output from slave) |
| MOSI | Input | SPI Master Output, Slave Input (output from master) |
| SPI_CLK | Input | SPI Serial Clock (output from master) |
| SPI_CS | 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 |
| PP | Input | Physical Presence, active high, internal pull-down. Used to indicate Physical Presence. |
| GPI | Input | Used for activation and deactivation of the TPM Standby mode (TPMLowPowerByGPIO) |
| NiC | - | Not internally connected: not connected to the die. May be left unconnected but no impact on 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.

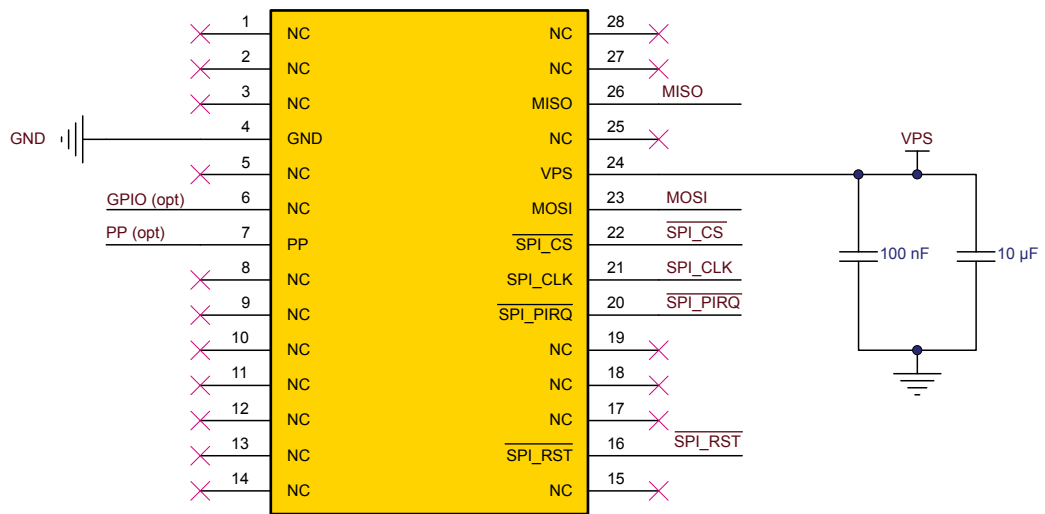
4 Integration guidance

4.1 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 in the case of the TSSOP28 package. The same implementation is also valid for the TSSOP28 and QFN32 packages.

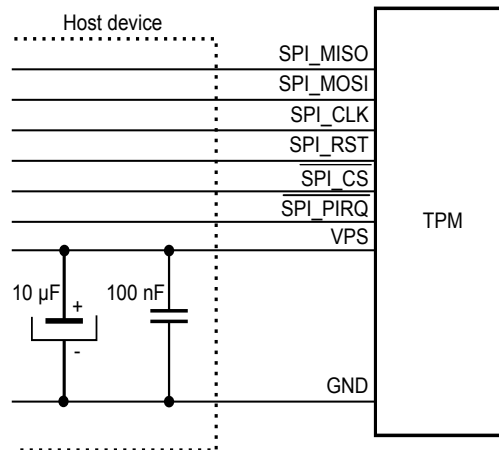
Figure 3. Typical hardware implementation (TSSOP28 package)



4.2 Power supply filtering

As mentioned in [Section 3 Pin and signal description](#), the power supply of the circuit must be filtered using the circuit shown in the figure below.

Figure 4. 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).

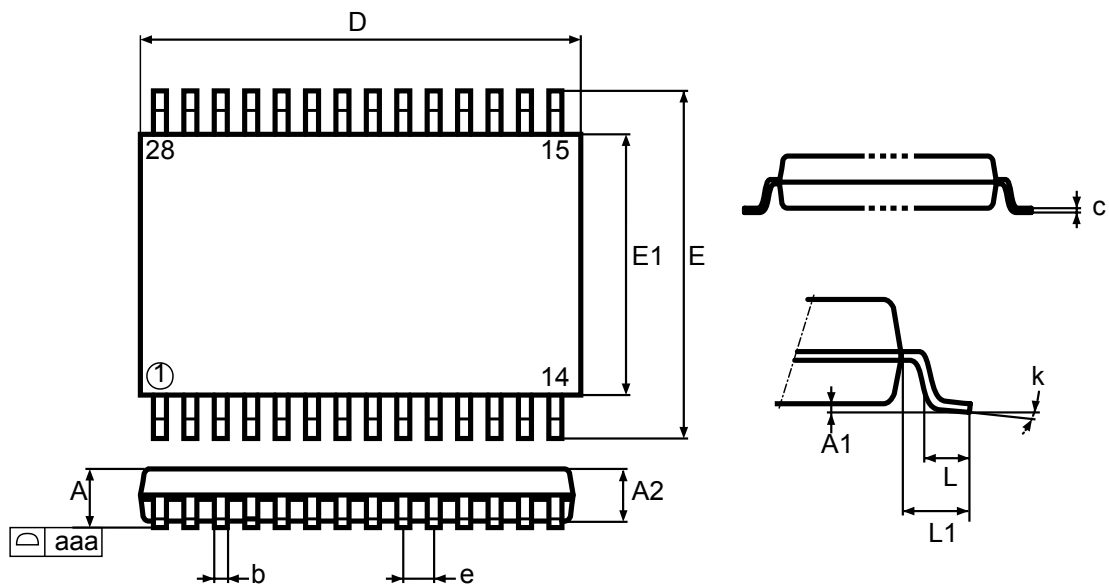
5 Package information

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.

5.1 28-pin thin shrink small outline package information

Dimensional features of the TSSOP28 package: Body width 4.4 mm. Pitch 0.65 mm.
Unless otherwise specified, general tolerance is ± 0.1 mm.

Figure 5. 28-lead thin shrink small outline package outline



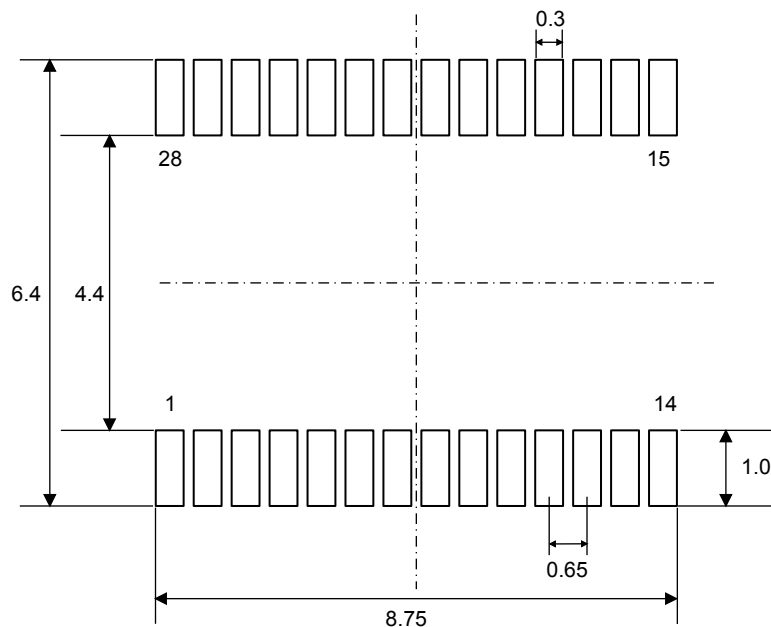
1. Drawing is not to scale.

Table 2. 28-lead thin shrink small outline package mechanical data

| Symbol | millimeters | | | inches ⁽¹⁾ | | |
|--------|-------------|-------|-------|-----------------------|--------|--------|
| | Min. | Typ. | Max. | Min. | Typ. | Max. |
| A | - | - | 1.200 | - | - | 0.0472 |
| A1 | 0.050 | - | 0.150 | 0.0020 | - | 0.0059 |
| A2 | 0.800 | 1.000 | 1.050 | 0.0315 | 0.0394 | 0.0413 |
| b | 0.190 | - | 0.300 | 0.0075 | - | 0.0118 |
| c | 0.090 | - | 0.200 | 0.0035 | - | 0.0079 |
| D | 9.600 | 9.700 | 9.800 | 0.3780 | 0.3819 | 0.3858 |
| E | 6.200 | 6.400 | 6.600 | 0.2441 | 0.2520 | 0.2598 |
| E1 | 4.300 | 4.400 | 4.500 | 0.1693 | 0.1732 | 0.1772 |
| e | - | 0.650 | - | - | 0.0256 | - |
| L | 0.450 | 0.600 | 0.750 | 0.0177 | 0.0236 | 0.0295 |
| L1 | - | 1.000 | - | - | 0.0394 | - |
| k | 0° | - | 8° | 0° | - | 8° |
| aaa | - | - | 0.100 | - | - | 0.0039 |

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

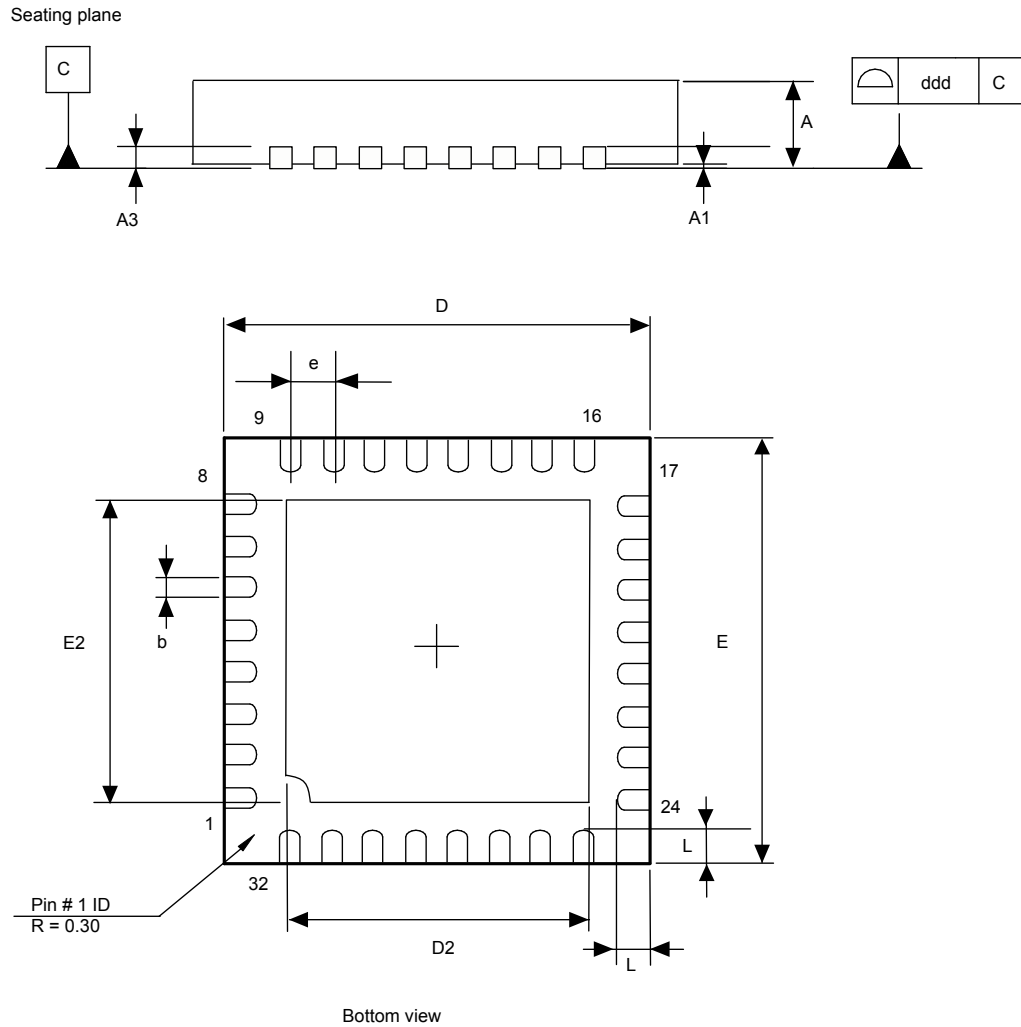
Figure 6. 28-lead thin shrink small outline package footprint



1. All dimensions are in millimeters.

5.2 32-lead very thin fine pitch quad flat pack no-lead (VFQFPN) package information

Figure 7. VFQFPN32 5x5 mm 0.5 mm pitch package outline

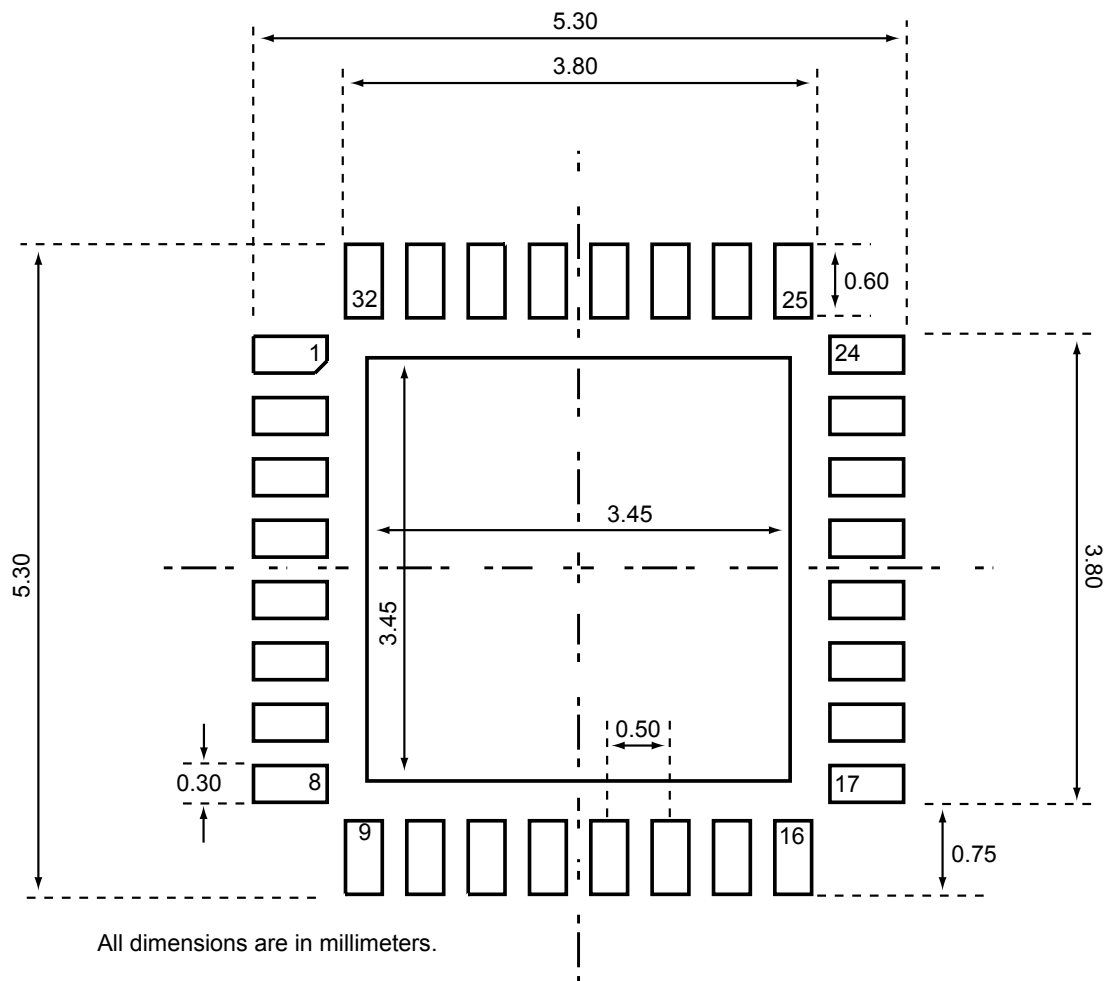


1. Drawing is not to scale.

Table 3. VFQFPN32 5x5 mm package 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 8. VFQFPN32 5x5 mm 0.5 mm pitch package footprint


5.3 Thermal characteristics of packages

The table below provides the thermal characteristics of the TSSOP28 and VFQFPN32 packages.

Table 4. 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} | 35.8 @ 0 lfpm ⁽¹⁾ |
| | Junction to case thermal resistance | θ_{JC} | - |
| | Junction to board thermal resistance | θ_{JB} | - |

1. Linear feet per minute.

6 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 to the EIA 481-A standard specification.

Table 5. Packages on tape and reel

| Package | Description | Tape width | Tape pitch | Reel diameter | Quantity per reel |
|-----------|---|------------|------------|---------------|-------------------|
| TSSOP 28 | Thin shrink small outline package | 16 mm | 8 mm | 13 in. | 2500 |
| VFQFPN 32 | Very thin fine pitch quad flat pack no-lead package | 12 mm | 8 mm | 13 in. | 3000 |

Figure 9. Reel diagram

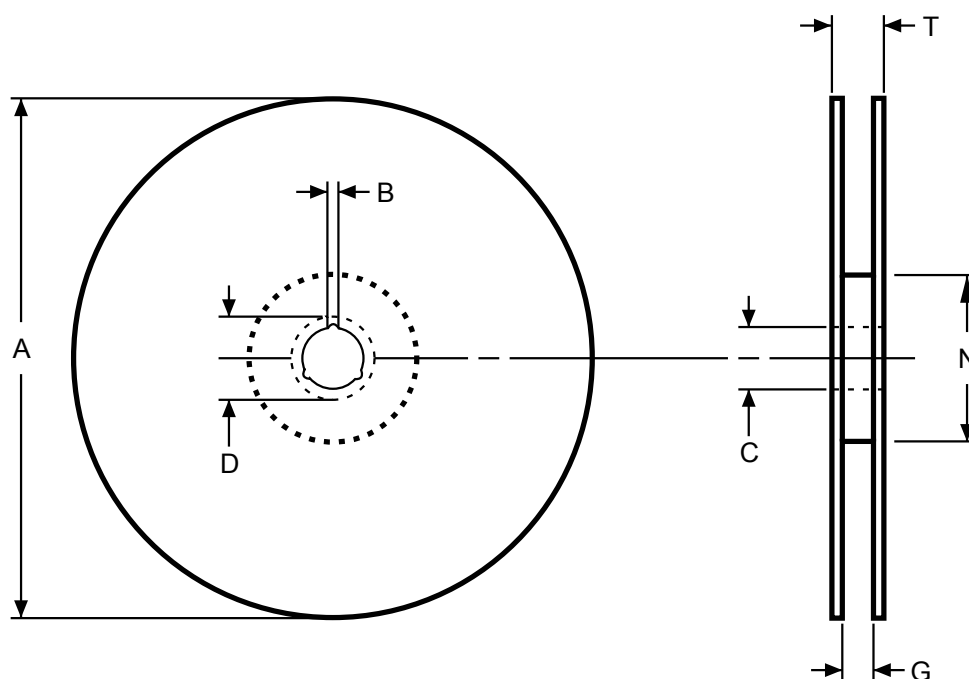
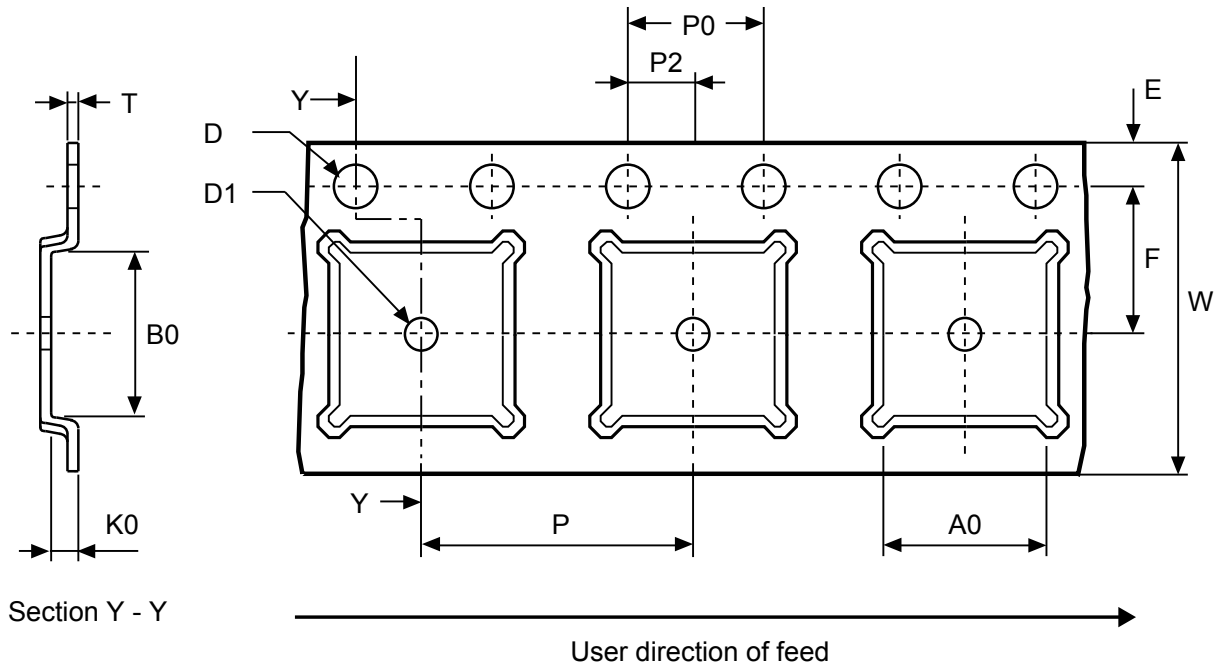


Table 6. Reel dimensions

| 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 10. Embossed carrier tape for VFQFPN 5 × 5 mm



1. Drawing is not to scale.

Figure 11. Chip orientation in the embossed carrier tape for VFQFPN 5 × 5 mm

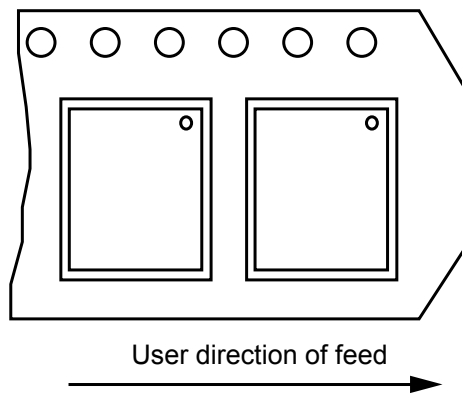
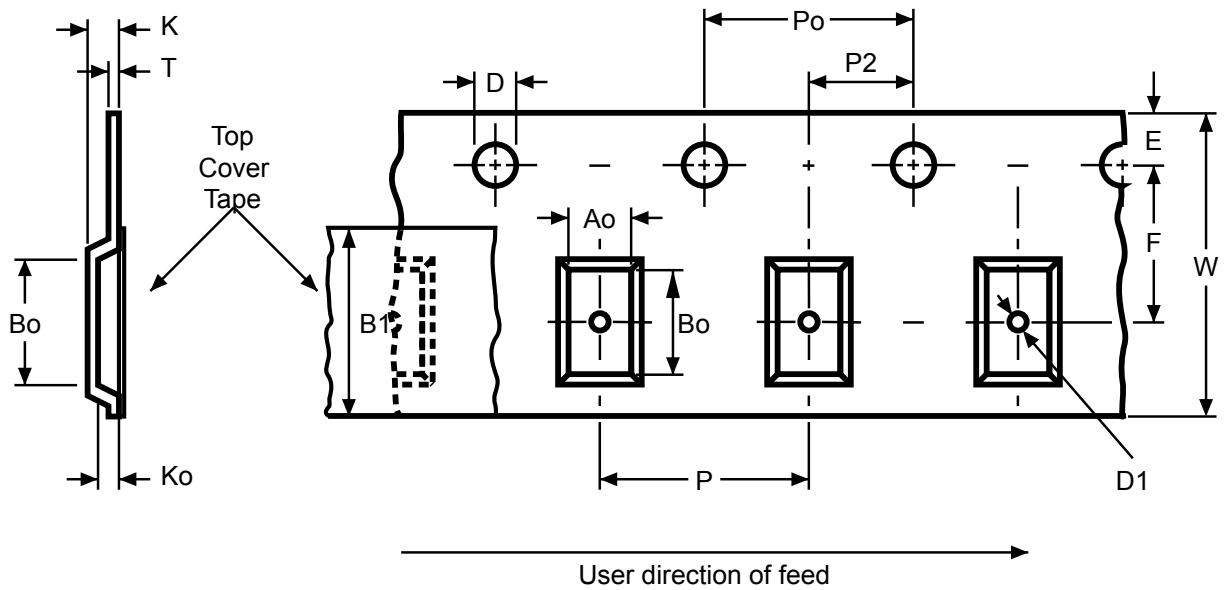


Table 7. Carrier tape dimensions for VFQFPN 5 × 5 mm

| Package | A0 | B0 | K0 | D1 Min. | P | P2 | D | P0 | E | F | W | T Max. | Unit |
|------------|-----------|-----------|----------|---------|--------|--------|------------|--------|-----------|----------|---------|-----------|------|
| VFQFPN 5x5 | 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 |

Figure 12. Embossed carrier tape for TSSOP28 4.4 mm body width



1. Drawing is not to scale.

Figure 13. Chip orientation in the embossed carrier tape for TSSOP28 4.4 mm body width

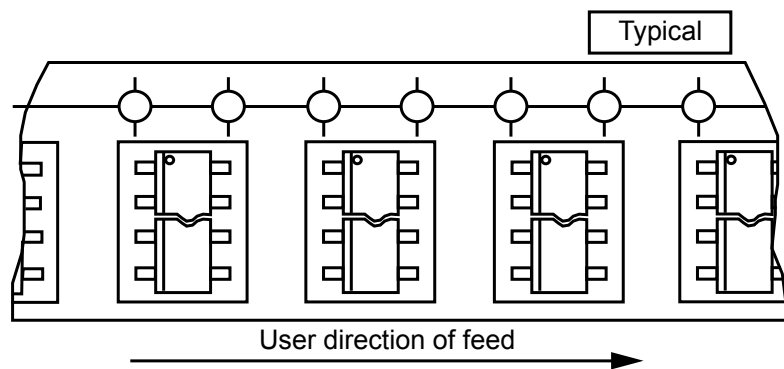


Table 8. Carrier tape constant dimensions for TSSOP 4.4 mm body width

| Tape size | Ao, Bo, Ko ⁽¹⁾ | D | E | Po | T Max. | Unit |
|-----------|---------------------------|---------------|-----------|--------|--------|------|
| 16 mm | See note. | 1.5 +0.1 / -0 | 1.75 ±0.1 | 4 ±0.1 | 0.4 | mm |

1. Ao, Bo, Ko, are determined by components sizes. The clearance between the component and the cavity must be within 0.05 mm (Min.) to 0.90 mm (Max.)

7 Package marking information

The two figure below illustrate the typical markings of the TSSOP28 and the VQFN32 device packages, respectively.

Figure 14. TSSOP28 device package marking area

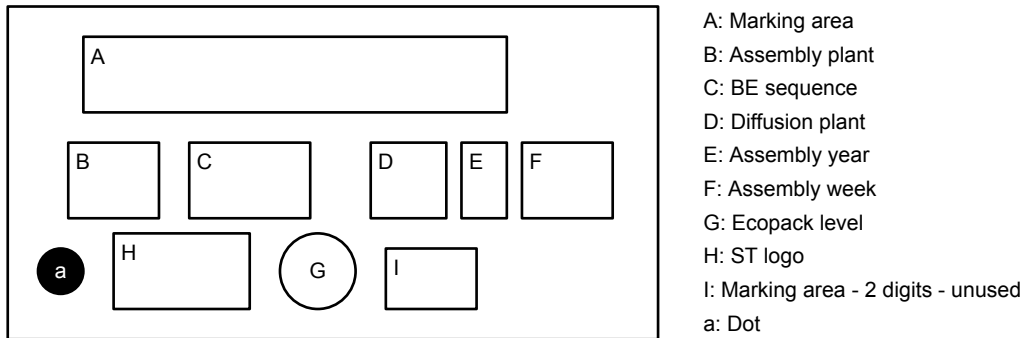
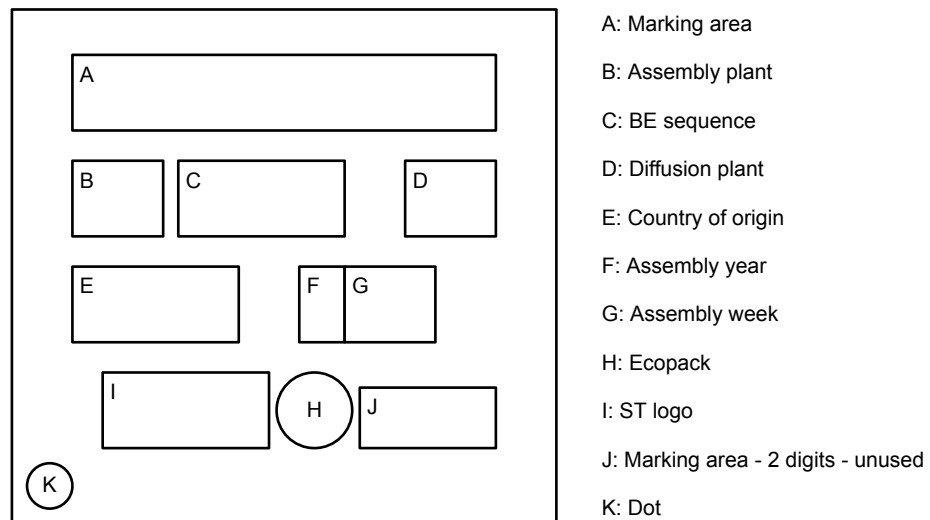


Figure 15. VQFN32 device package marking area



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

- Y = Hardware revision
- ZZZ = Product identifier

8 Ordering information

Table 9. Ordering information for products supporting firmware 49.08 preloaded in factory

| Ordering code | Default TPM Library & Firmware version | Operating temperature range ⁽¹⁾ | Maximum SPI clock frequency | Package | Marking (area A) |
|------------------|--|--|-----------------------------|---------|------------------|
| ST33HTPH2E28AHC0 | TPM 2.0 active | -40 °C to +105 °C | 33 MHz | TSSOP28 | PEAHC0 |
| ST33HTPH2E32AHC0 | 0x00 0x49 0x00 0x08 | | | VQFN32 | |

1. Refer to [Section 1 Description](#) for the operating voltages associated with the different operating temperature ranges.

9 Support and information

Additional information regarding ST TPM devices can be obtained from the website www.st.com.
For any specific support information you can contact STMicroelectronics through the following e-mail:
TPMsupport@list.st.com.

Appendix A Terms and abbreviations

Table 10. List of abbreviations

| Term | Meaning |
|-------------------|--|
| AES | Advanced Encryption Standard |
| 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 |
| EK | Endorsement key |
| FIPS | Federal Information Processing Standard |
| GPIO | General-purpose I/O |
| HLK | Hardware Lab Kit (Windows®) |
| HMAC | Keyed-Hashing for Message Authentication |
| NIST | National Institute of Standards and Technology |
| NV | Non-volatile (memory) |
| OEM | Original equipment manufacturer |
| OIAP | Object-independent authorization protocol |
| OSAP | Object-specific authorization protocol |
| PCR | Platform configuration register |
| RSA | Rivest Shamir Adelman |
| RTM | Root of trust for measurement |
| RTR | Root of trust for reporting |
| SHA | Secure Hash algorithm |
| SPI | Serial Peripheral Interface |
| SRK | Storage root key |
| TCG | Trusted Computed Group |
| 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 |

Revision history

Table 11. Document revision history

| Date | Version | Changes |
|-------------|---------|---|
| 12-Nov-2015 | 1 | Initial release. |
| 26-Apr-2018 | 2 | <p>In Features, updated:</p> <ul style="list-style-type: none"> • TPM features. • Temperature range. • Updated CC and FIPS certification status. • Supported cryptographic algorithms • Product compliance <p>Updated Appendix B: Referenced documents and references in the data brief.</p> <p>Updated Section 1.1: Security certifications.</p> <p>Added Section 2: Data brief scope.</p> <p>Updated Section 3: Pin and signal description.</p> <p>Added Section 4: Integration guidance.</p> <p>Added Section 9: Ordering information.</p> <p>Updated document reference to DB2716.</p> <p>Small text changes.</p> |
| 04-Jul-2019 | 3 | <p>Added STSAFE-TPM logo on cover page.</p> <p>Updated Product compliance.</p> <p>Reorganized Section 1 Description.</p> <p>Updated Section 2.1 ST33TPHF2ESPI products and Section 2.2 Firmware image.</p> <p>Updated product marking. See:</p> <ul style="list-style-type: none"> • Section 2.1 ST33TPHF2ESPI products • Section 7 Package marking information • Section 8 Ordering information <p>Updated Figure 6. 28-lead thin shrink small outline package footprint.</p> <p>Added Section 5.3 Thermal characteristics of packages.</p> <p>Removed list of references.</p> <p>Small text changes.</p> |

Contents

| | | |
|-------------------|---|-----------|
| 1 | Description | 3 |
| 2 | Data brief scope | 4 |
| 2.1 | ST33TPHF2ESPI products | 4 |
| 2.2 | Firmware image | 4 |
| 3 | Pin and signal description | 5 |
| 4 | Integration guidance | 7 |
| 4.1 | Typical hardware implementation | 7 |
| 4.2 | Power supply filtering | 8 |
| 5 | Package information | 9 |
| 5.1 | 28-pin thin shrink small outline package information | 9 |
| 5.2 | 32-lead very thin fine pitch quad flat pack no-lead (VFQFPN) package information | 10 |
| 5.3 | Thermal characteristics of packages | 13 |
| 6 | Delivery packing | 14 |
| 7 | Package marking information | 17 |
| 8 | Ordering information | 18 |
| 9 | Support and information | 19 |
| Appendix A | Terms and abbreviations | 20 |
| | Revision history | 21 |
| | Contents | 22 |
| | List of tables | 23 |
| | List of figures | 24 |

List of tables

| | | |
|------------------|---|----|
| Table 1. | Pin descriptions | 6 |
| Table 2. | 28-lead thin shrink small outline package mechanical data | 10 |
| Table 3. | VFQFPN32 5x5 mm package mechanical data | 12 |
| Table 4. | Thermal characteristics | 13 |
| Table 5. | Packages on tape and reel | 14 |
| Table 6. | Reel dimensions | 14 |
| Table 7. | Carrier tape dimensions for VFQFPN 5 × 5 mm | 15 |
| Table 8. | Carrier tape constant dimensions for TSSOP 4.4 mm body width | 16 |
| Table 9. | Ordering information for products supporting firmware 49.08 preloaded in factory. | 18 |
| Table 10. | List of abbreviations | 20 |
| Table 11. | Document revision history | 21 |

List of figures

| | | |
|-------------------|---|----|
| Figure 1. | TSSOP28 pinout. | 5 |
| Figure 2. | VQFN32 pinout. | 5 |
| Figure 3. | Typical hardware implementation (TSSOP28 package) | 7 |
| Figure 4. | Mandatory filtering capacitors on V_{PS} | 8 |
| Figure 5. | 28-lead thin shrink small outline package outline. | 9 |
| Figure 6. | 28-lead thin shrink small outline package footprint. | 10 |
| Figure 7. | VFQFPN32 5x5 mm 0.5 mm pitch package outline | 11 |
| Figure 8. | VFQFPN32 5x5 mm 0.5 mm pitch package footprint | 12 |
| Figure 9. | Reel diagram | 14 |
| Figure 10. | Embossed carrier tape for VFQFPN 5 × 5 mm | 15 |
| Figure 11. | Chip orientation in the embossed carrier tape for VFQFPN 5 × 5 mm. | 15 |
| Figure 12. | Embossed carrier tape for TSSOP28 4.4 mm body width | 16 |
| Figure 13. | Chip orientation in the embossed carrier tape for TSSOP28 4.4 mm body width | 16 |
| Figure 14. | TSSOP28 device package marking area | 17 |
| Figure 15. | VQFN32 device package marking area | 17 |

IMPORTANT NOTICE – PLEASE 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 acknowledgement.

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, please 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.

© 2019 STMicroelectronics – All rights reserved