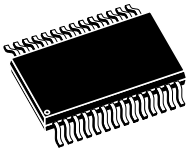
# ST33TPHF20SPI

## Flash-based TPM 2.0 device with an SPI interface

**Data brief**



TSSOP28

VFQFPN32

## Features

### TPM features

- Flash based Trusted Platform Module (TPM)
- For TPM 2.0, compliant with Trusted Computing Group (TCG) Trusted Platform Module (TPM) Library specifications 2.0, Level 0, Revision 116 and TCG PC Client Specific TPM Platform Specifications 0.43 and errata
- TPM firmware code can be upgraded thanks to a persistent Application Flash Loader to support new standard evolutions
- CC certification according to TPM 2.0 PP at EAL4+
- SPI support at up to 33 MHz

### Hardware features

- ARM® SecurCore® SC300™ 32-bit RISC core
- Highly reliable Flash memory technology
- Extended temperature ranges: -40 °C to 105 °C
- ESD 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
- 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
  - ECDH 224 & 256 bits
  - ECDAA

### Product compliance

- Compliant with Microsoft® Windows 8.1 and Windows 10
- Compliant with Intel® TXT for TPM 2.0
- Compliant with TCG test suite for TPM 2.0

# Contents

# 1 Description

The ST33TPHF20SPI is a cost-effective and high performance trusted platform module (TPM) targeting PC, server platforms and embedded systems.

The product implements the functions defined by the Trusted Computing Group (www.trustedcomputinggroup.org) in the TCG Trusted Platform Module Library Specifications version 2.0 Level 0 Revision 116 (*[TPM 2.0 P1 r116]*, *[TPM 2.0 P2 r116]*, *[TPM 2.0 P3 r116]*, *[TPM 2.0 P4 r116]*) and errata version 1.3 *[TPM 2.0 rev116 Err 1.3]*.It is also based on the TCG PC Client specific TPM Platform specifications rev0.43 *[PTP 2.0 r0.43]* and *[Errata sheet]*. *[TPM 20 PP]* specifies the protection profile.

The product also supports the ability to upgrade the TPM firmware thanks to a persistent application Flash loader to support new standard evolutions.

## 1.1 Security certifications

This product is CC certified according to TPM 2.0 PP at EAL4+. It also targets FIPS 140-2 certification.

## 1.2 Hardware features

The ST33TPHF20SPI is based on a smartcard-class secure MCU that incorporates the most recent generation of ARM® processors for embedded secure systems. Its SecurCore® SC300™ 32-bit RISC core is built on the Cortex® M3 core with additional security features to help to protect against advanced forms of attacks.

The ST33TPHF20SPI offers a fast slave serial peripheral interface (SPI) supported by an embedded hardware communication engine compliant with TCG PC Client TPM Profile 0.43 *[PTP 2.0 r0.43]*.

The product features hardware accelerators for advanced cryptographic functions. The AES peripheral provides a secure AES (Advanced Encryption Standard) algorithm implementation, while the NESCRYPT crypto-processor efficiently supports the public key algorithms.

The ST33TPHF20SPI operates in the -25 to +85 °C commercial temperature range or the -40 °C to 105 °C extended temperature range with a supply and I/O voltage of 1.8 V or 3.3 V.

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 device status are available at: *www.st.com*.

ECOPACK® is an ST trademark.


# 2 Pin and signal descriptions

*Figure 1* and *Figure 2* give the pinouts of the two packages in which the devices are delivered. *Table 1* describes the associated signals.

**Figure 1. TSSOP28 pinout**

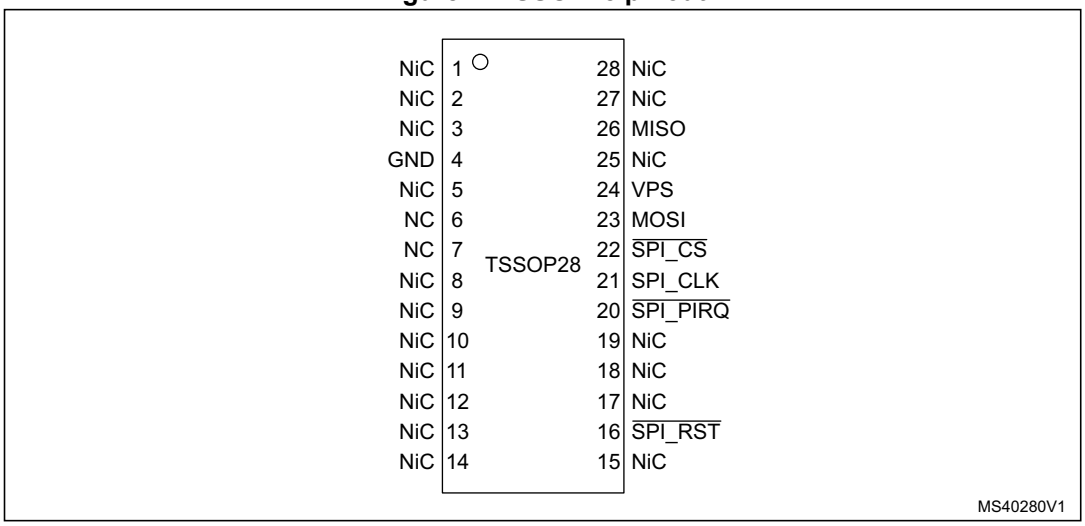



**Figure 2. VQFN32 pinout**

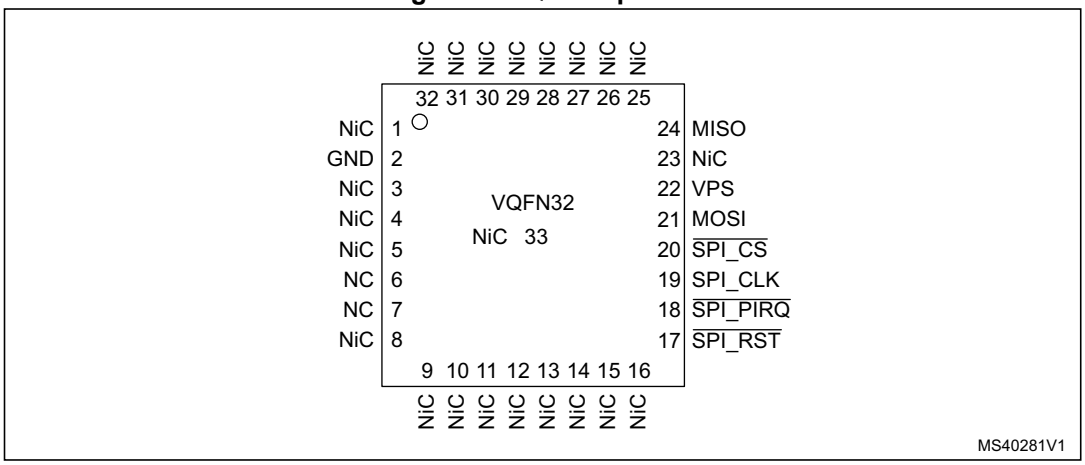


**Table 1. Pin descriptions**

| 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. |
| $\overline{\text{SPI\_RST}}$ | Input | **SPI Reset** used to re-initialize the device |
| 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) |
| $\overline{\text{SPI\_CS}}$ | Input | **SPI** Slave Select (active low; output from master) |
| $\overline{\text{SPI\_PIRQ}}$ | Output | **SPI IRQ** used by TPM to generate an interrupt |
| NiC | - | **Not internally connected**: not connected to the die. May be left unconnected but no impact on TPM if connected. |
| NC | - | **Not Connected**: connected to the die but not usable. May be left unconnected. Internal pull down. |

*Note: The VQFN32 package has an 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.*

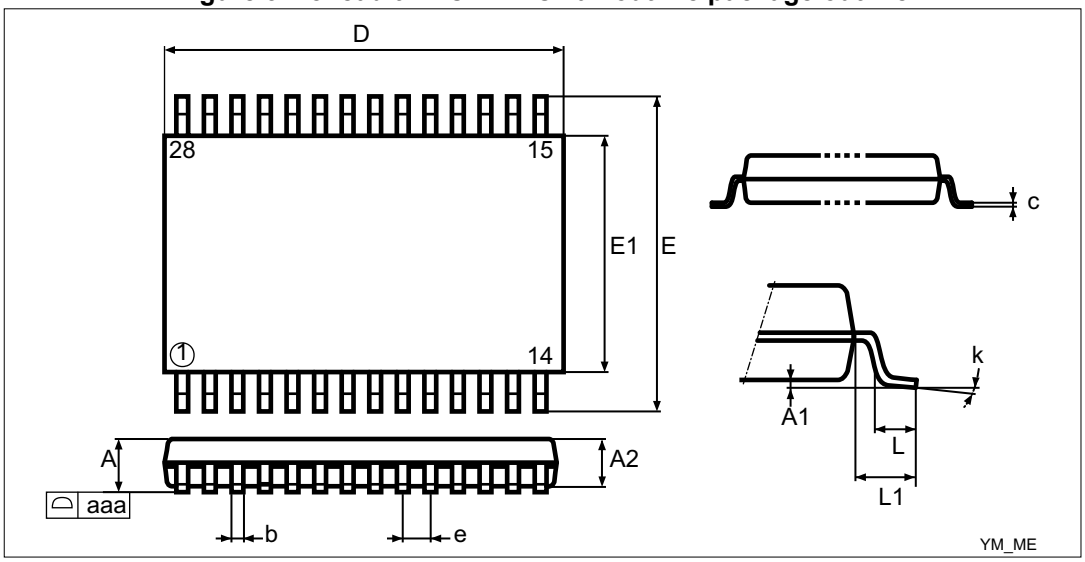
# 3 Package information

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.

## 3.1 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 3. 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**

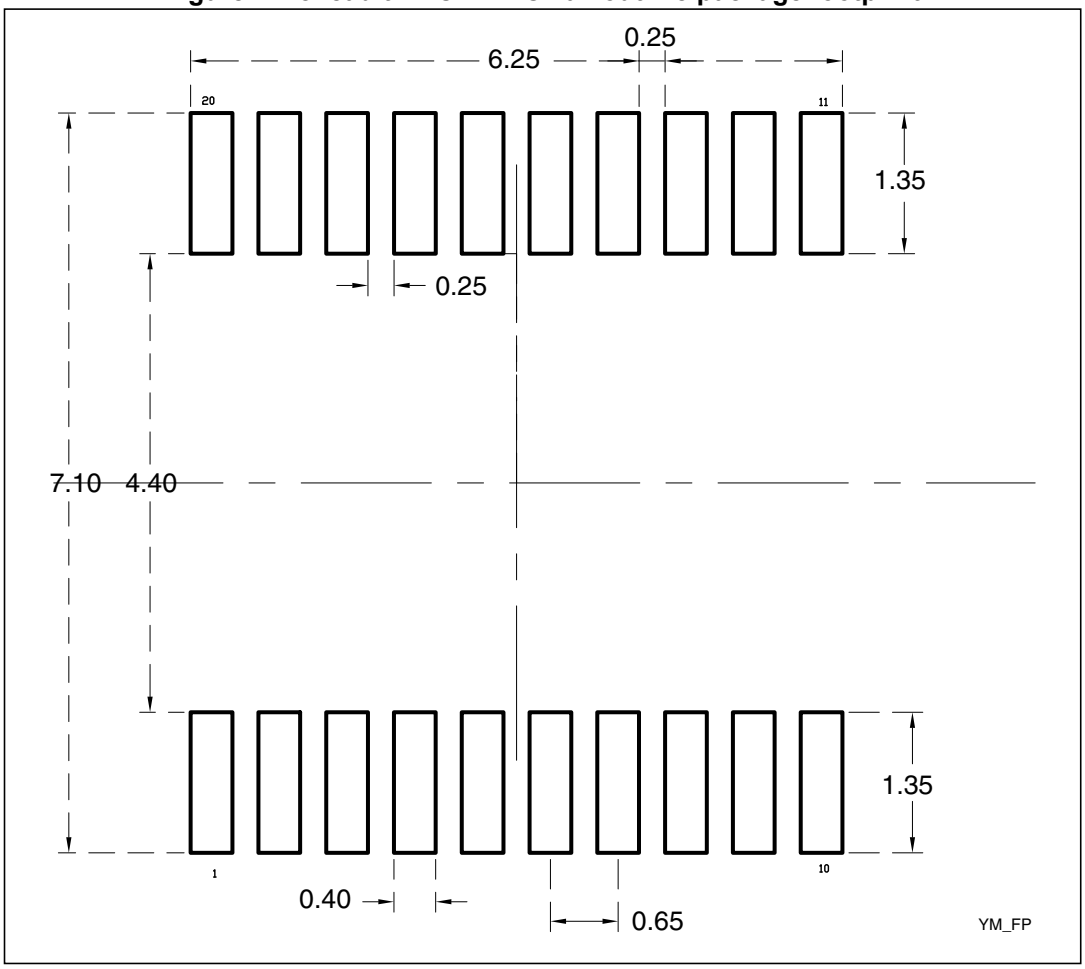
| Symbol | millimeters | | | inches(1) | | |
|---|---|---|---|---|---|---|
| | Min. | Typ. | Max. | Min. | Typ. | Max. |
| A | - | - | 1.20 | - | - | 0.047 |
| A1 | 0.05 | - | 0.15 | 0.002 | - | 0.006 |
| A2 | 0.80 | 1.00 | 1.05 | 0.031 | 0.040 | 0.041 |
| b | 0.19 | - | 0.30 | 0.007 | - | 0.012 |
| c | 0.09 | - | 0.20 | 0.004 | - | 0.008 |
| D | 9.60 | 9.70 | 9.80 | 0.378 | 0.382 | 0.386 |
| E | 6.20 | 6.40 | 6.60 | 0.244 | 0.252 | 0.260 |
| E1 | 4.30 | 4.40 | 4.50 | 0.170 | 0.173 | 0.177 |
| e | - | 0.65 | - | - | 0.026 | - |
| L | 0.45 | 0.60 | 0.75 | 0.018 | 0.024 | 0.0230 |
| L1 | - | 1.00 | - | - | 0.040 | - |

**Table 2. 28-lead thin shrink small outline package mechanical data (continued)**

| Symbol | millimeters | | | inches[1] | | |
|---|---|---|---|---|---|---|
| | Min. | Typ. | Max. | Min. | Typ. | Max. |
| k | 0° | - | 8° | 0° | - | 8° |
| aaa | - | - | 0.10 | - | - | 0.004 |

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

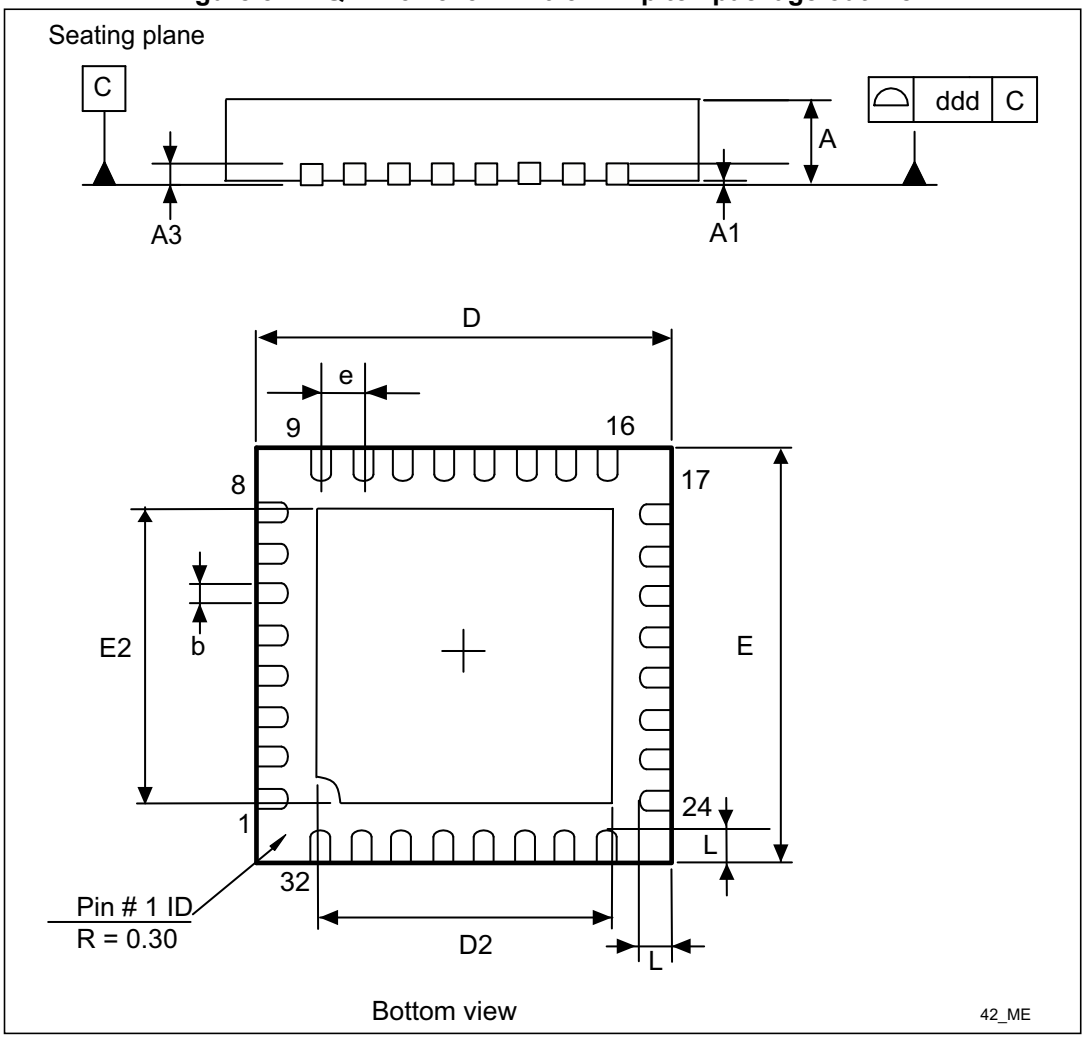
**Figure 4. 28-lead thin shrink small outline package footprint**




1. All dimensions are in millimeters.

## 3.2 32-lead very thin fine pitch quad flat pack no-lead (VFQFPN) package information

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




1. Drawing is not to scale.

**Table 3. VFQFPN32 5x5 mm package mechanical data**

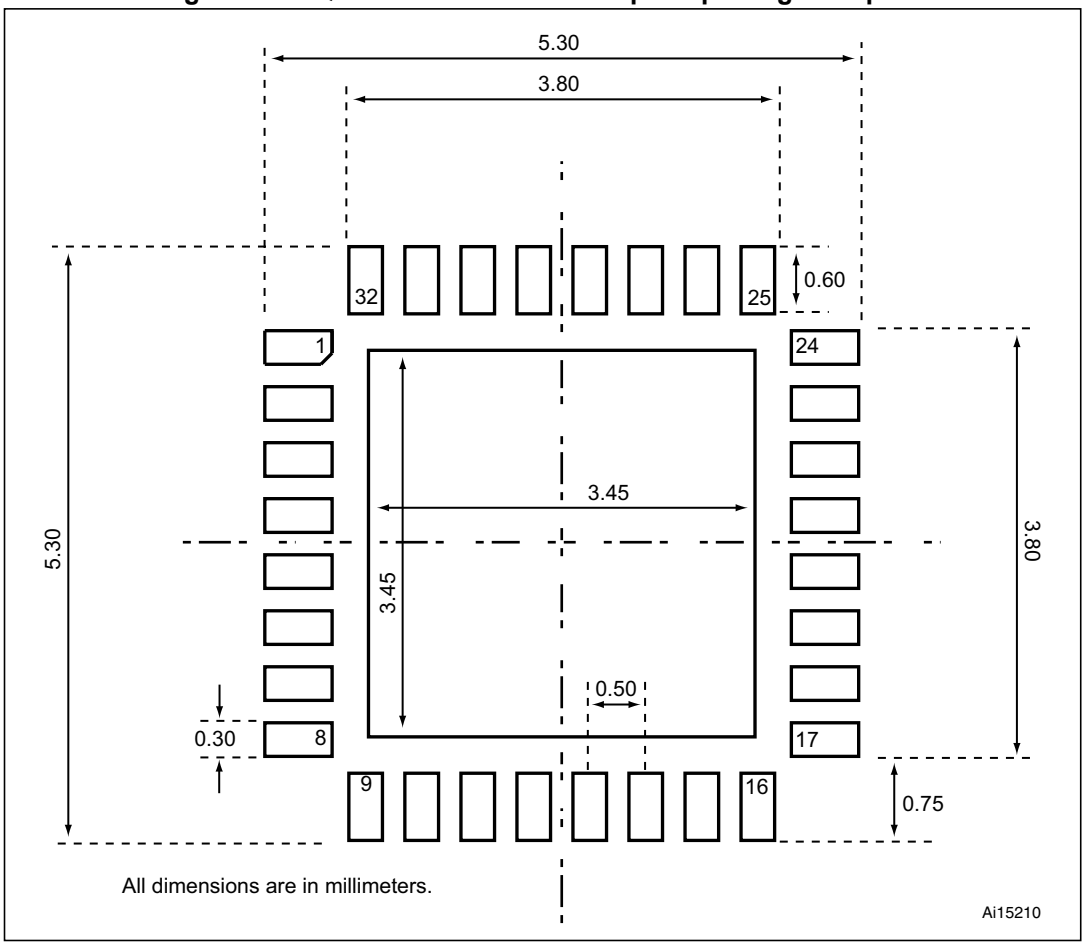
| Symbol | millimeters | | | inches (1) | | |
|---|---|---|---|---|---|---|
| | Min. | Typ. | Max. | Min. | Typ. | Max. |
| A | 0.800 | 0.900 | 1.000 | 0.0315 | 0.0354 | 0.0394 |
| A1 | 0.000 | 0.020 | 0.050 | 0.0000 | 0.0008 | 0.0020 |
| A3 | - | 0.200 | - | - | 0.0079 | - |
| b | 0.180 | 0.250 | 0.300 | 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 |

**Table 3. VFQFPN32 5x5 mm package mechanical data (continued)**

| Symbol | millimeters | | | inches [1] | | |
|---|---|---|---|---|---|---|
| | Min. | Typ. | Max. | Min. | Typ. | Max. |
| 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 6. VFQFPN32 5x5 mm 0.5 mm pitch package footprint**



# 4 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 & Reel specifications are compliant to the EIA 481-A standard specification.

**Table 4. 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 7. Reel diagram**

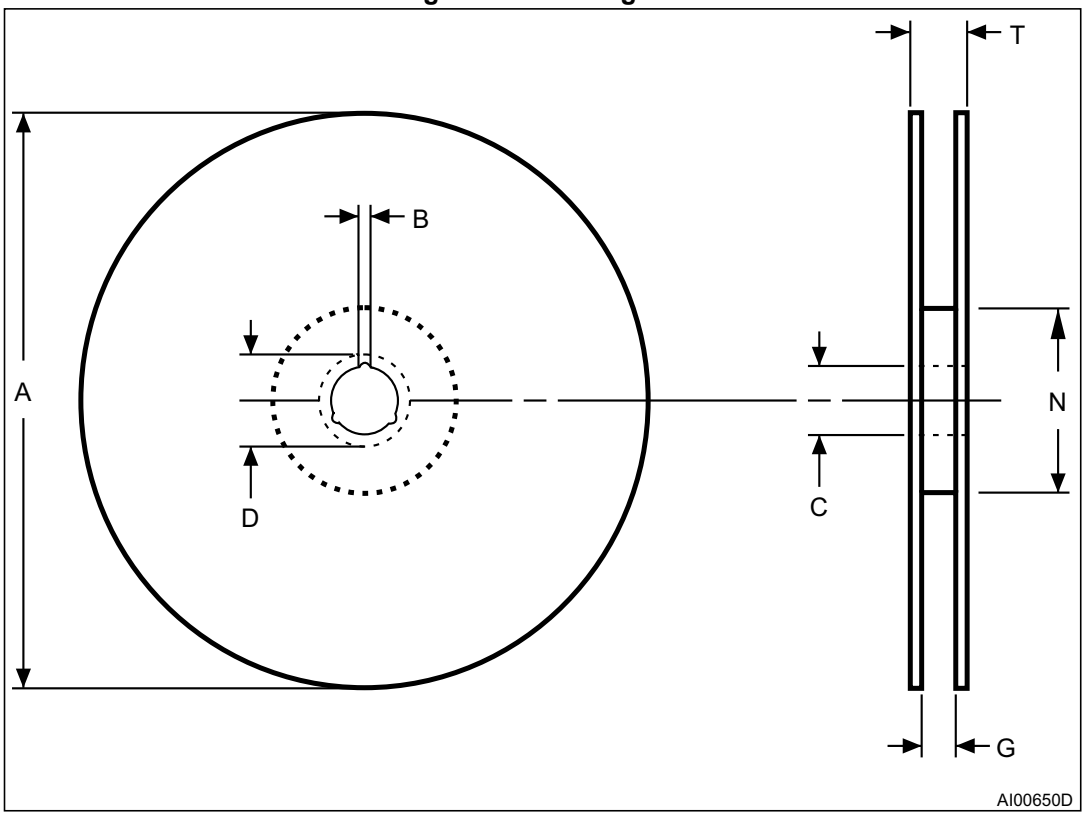
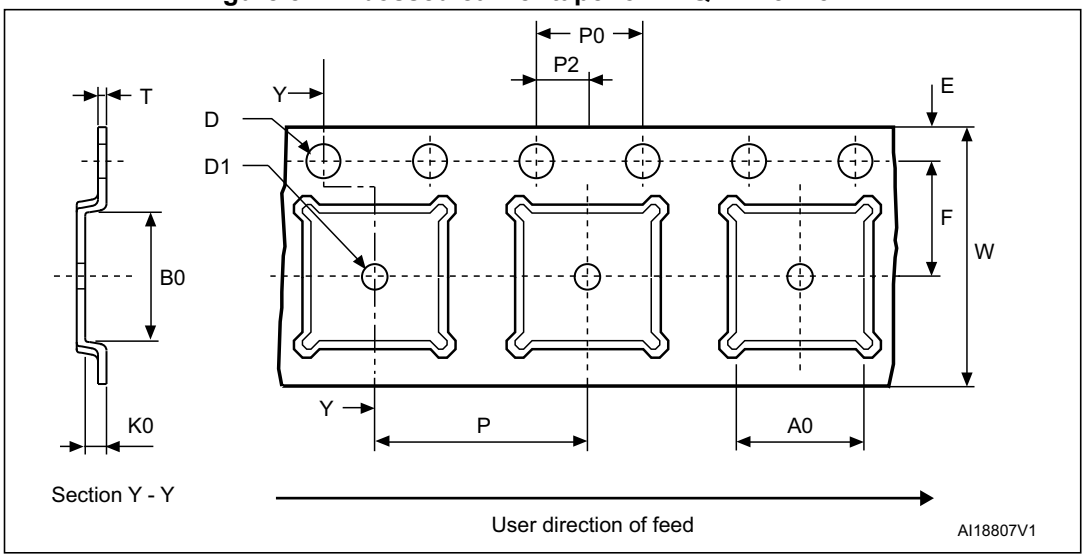


**Table 5. Reel dimensions**

| 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 8. Embossed carrier tape for VFQFPN 5 × 5 mm**




1. Drawing is not to scale.

**Figure 9. Chip orientation in the embossed carrier tape for VFQFPN 5 × 5 mm**

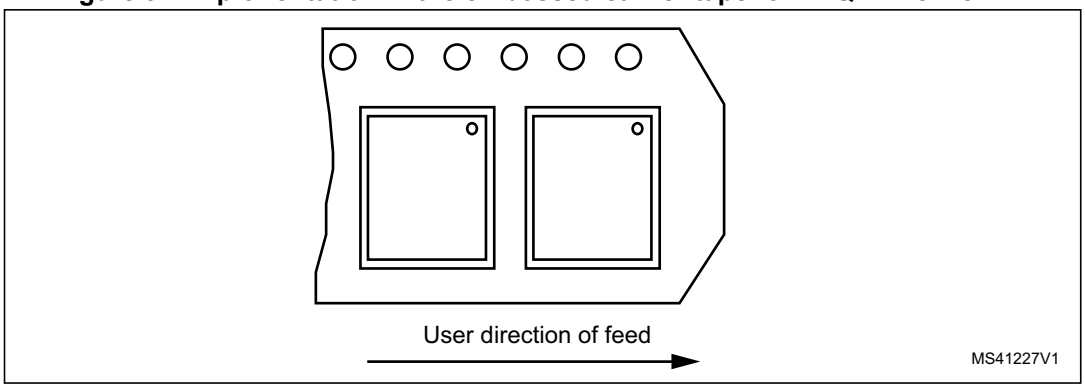
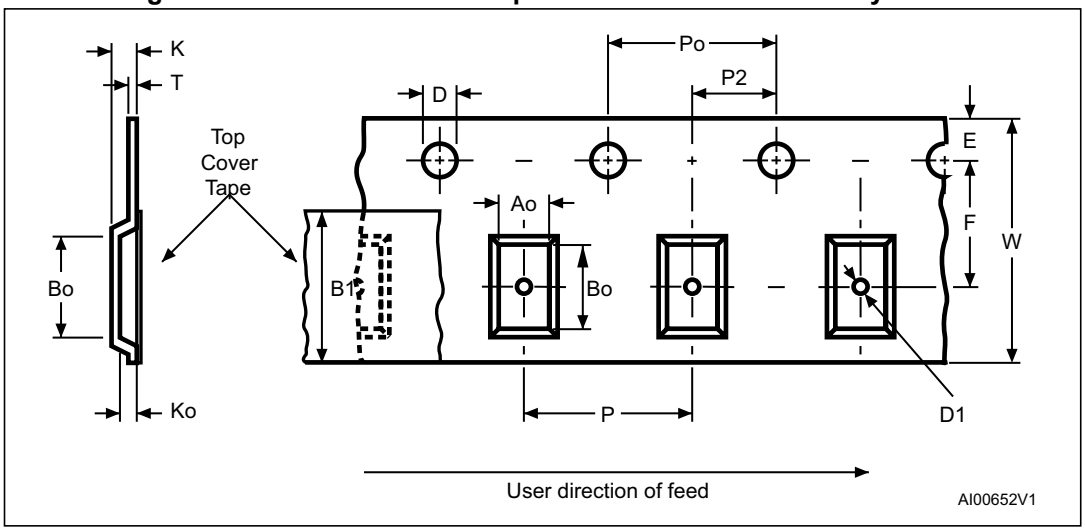



**Table 6. Carrier tape dimensions for VFQFPN 5 × 5 mm**

| Package | A0 | B0 | K0 | D1 Min. | P | P2 | D | P0 | E | F | W | T Max. | Unit |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| FPN 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 10. Embossed carrier tape for TSSOP28 4.4 mm body width**




1. Drawing is not to scale.

**Figure 11. Chip orientation in the embossed carrier tape for TSSOP28 4.4 mm body width**

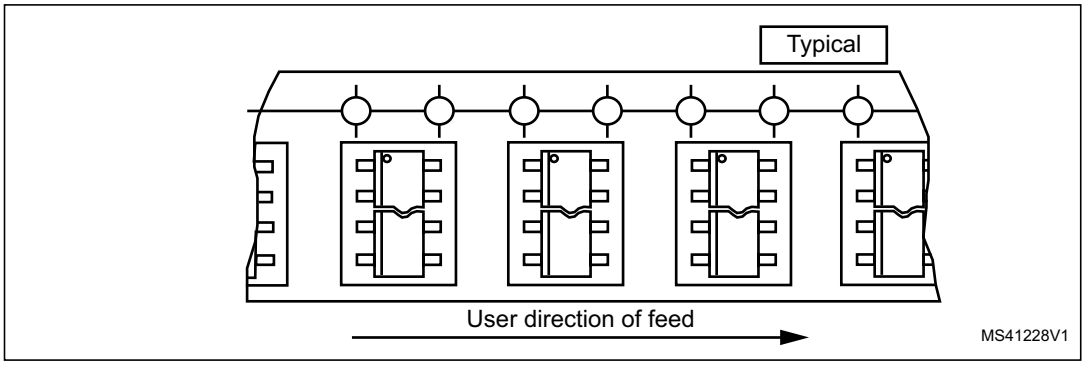



**Table 7. Carrier tape constant dimensions for TSSOP 4.4 mm body width**

| 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.)

# 5 Package marking information

*Figure 12* and *Figure 13* illustrate the typical markings of the TSSOP28 and the VQFN32 device packages, respectively.

**Figure 12. TSSOP28 device package marking area**

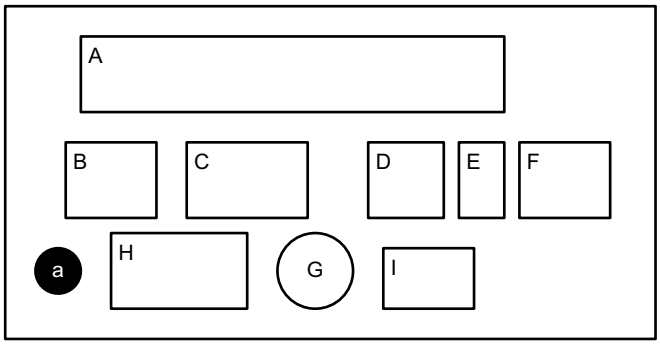
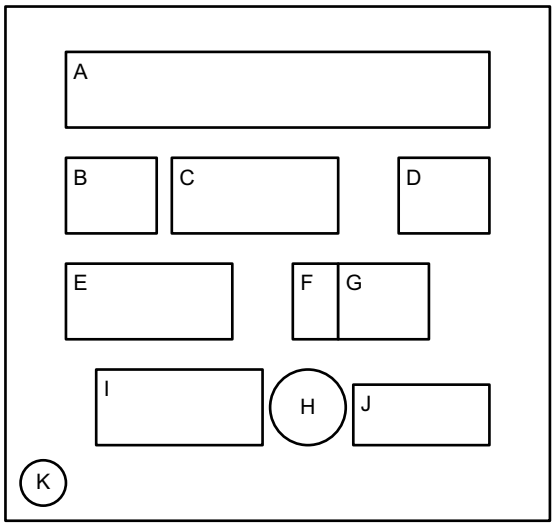



**Figure 13. VQFN32 device package marking area**




For both packages, the 8-digit ‘A’ marking area is equal to “P68XYZZZ” with:

- X = Hardware product
- Y = Hardware revision
- ZZZ = Firmware revision

# 6 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 8. 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 |
| EK | Endorsement Key |
| FIPS | Federal Information Processing Standard |
| GPIO | General Purpose I/O |
| HMAC | Keyed-Hashing for Message Authentication |
| HSM | Hardware security module |
| 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 |

# Appendix B Referenced documents

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

| | |
|---|---|
| [TPM 2.0 P1 r116] | TPM Library, Part 1, Architecture, Family 2.0, rev 1.16, TCG |
| [TPM 2.0 P2 r116] | TPM Library, Part 2, Structures, Family 2.0, rev 1.16, TCG |
| [TPM 2.0 P3 r116] | TPM Library, Part 3, Commands, Family 2.0, rev 1.16, TCG |
| [TPM 2.0 P4 r116] | TPM Library, Part 4, Supporting routines, Family 2.0, rev 1.16, TCG |
| [TPM 2.0 rev116 Err 1.3] | Errata version 1.3 June 16, 2015 for TCG TPM library version 2.0 revision 1.16 October 2014. |
| [PTP 2.0 r0.43] | TCG PC Client Specific Platform TPM Specification (PTP) - Version 2.0 Revision 0.43 |
| [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 |
| [Errata sheet] | PC_Client_Specific_Platform_TPM_Profile_for_TPM_2_0_errata_v1p0.pdf |
| [TCG EK Cre Profile TPM 2.0] | TCG EK credential profile for TPM Family 2.0 Level 0. Specification Version 2.0 Revision 14, November 4, 2014, TCG. |
| [TPM 20 PP] | Protection Profile PC Client Specific TPM, Family 2.0 Level 0 (1.0), December 2014, TCG. |

# Revision history

Table 9. Document revision history

| Date | Revision | Changes |
|---|---|---|
| 04-Mar-2016 | 1 | Initial release. |
| 15-Mar-2016 | 2 | Updated *TPM features* related to certification and updated *Section 1.1: Security certifications*.<br>Updated references in *Section 1: Description*.<br>Added *Figure 9: Chip orientation in the embossed carrier tape for VFQFPN 5 × 5 mm* and *Figure 11: Chip orientation in the embossed carrier tape for TSSOP28 4.4 mm body width*. |