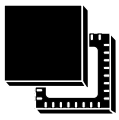
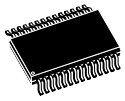
ST33TPHF20SPI

Data brief

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



VFQFPN32
(5 × 5 mm)



TSSOP28
(9.7 × 6.4 mm,
4.4 mm body width)

Product status link
ST33TPHF20SPI

STSAFE-TPM

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 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 2.0 protection profiles at EAL4+
- FIPS 140-2 level 2 certification
- SPI support for up to 33 MHz in FIFO and CRB protocol modes
- Support for software and hardware physical presence

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
- Monitoring of environmental parameters (power)
- Hardware and software protection against fault injection
- FIPS-compliant random-number generator (RNG) built on an SP800-90A compliant SHA256 deterministic random bit generator (DRBG) and an AIS-31 Class PTG2 compliant true random number generator (TRNG)
- Cryptographic algorithms:
  - RSA (Rivest-Shamir-Adleman) key generation (1024 or 2048 bits)
  - RSA signature and encryption
  - Hash-based message authentication code (HMAC) SHA-1 & SHA-256
  - Advanced Encryption Standard (AES)-128-192-256
  - Elliptic curve cryptography (ECC) 224 & 256 bits
  - Elliptic curve Diffie–Hellman (ECDH) 224 & 256 bits
  - Elliptic curve direct anonymous attestation (ECDAA)

Product compliance

- TPM 2.0 compliant with Microsoft® Windows® 8.1 and 10
- Compliant with Intel® TXT
- TPM 2.0 compliant with the corresponding 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 ST33TPHF20SPI offers a slave serial peripheral interface (SPI) compliant with the TCG PC Client TPM Profile specifications.

The ST33TPHF20SPI supports TPM 2.0 commands exclusively, and offers 112 Kbytes of user-dedicated non-volatile memory.

The ST33TPHF20SPI 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.

2 Data brief scope

2.1 ST33TPHF20SPI products

This document covers the functionality of the ST33TPHF20SPI product family, the most recent of which has firmware version 4A.40 (74.64 in decimal) preloaded on ST TPM hardware with markings:

- P0AHD1

The information to order the supporting platforms is provided in Section 8 Ordering information.

2.2 Firmware image

The firmware image version 4A.40 can be loaded to the ST TPM hardware of the ST33TPHF20SPI products, identifiable by their firmware version, which is of the form 4A.xx. The ordering codes of the products upgradable to firmware version 4A.40 are the following:

- ST33HTPH2ExxAAF3 (FW 4A.00)
- ST33HTPH2ExxAHC1 (FW 4A.08)

See Section 9 Firmware image overview for an overview of the available firmware images.

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

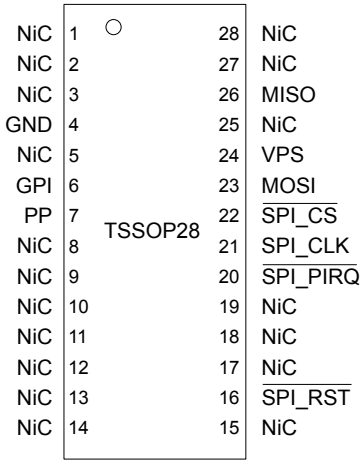


Figure 2. VQFN32 pinout

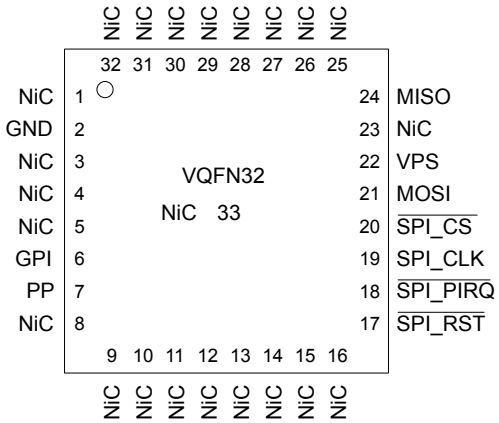


Table 1. Pin descriptions

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.
$\overline{\text{SPI\_RST}}$	Input	**SPI Reset,** active low, used to re-initialize the device. Must not be unconnected. External pull-up resistor 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)
$\overline{\text{SPI\_CS}}$	Input	**SPI Chip (or Slave) Select**, internal pull-up (active low; output from master)

Signal	Type	Description
$\overline{\text{SPI\_PIRQ}}$	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`). If this feature is not used, connect an external pull-up resistor (10 kΩ) to this pad.
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.

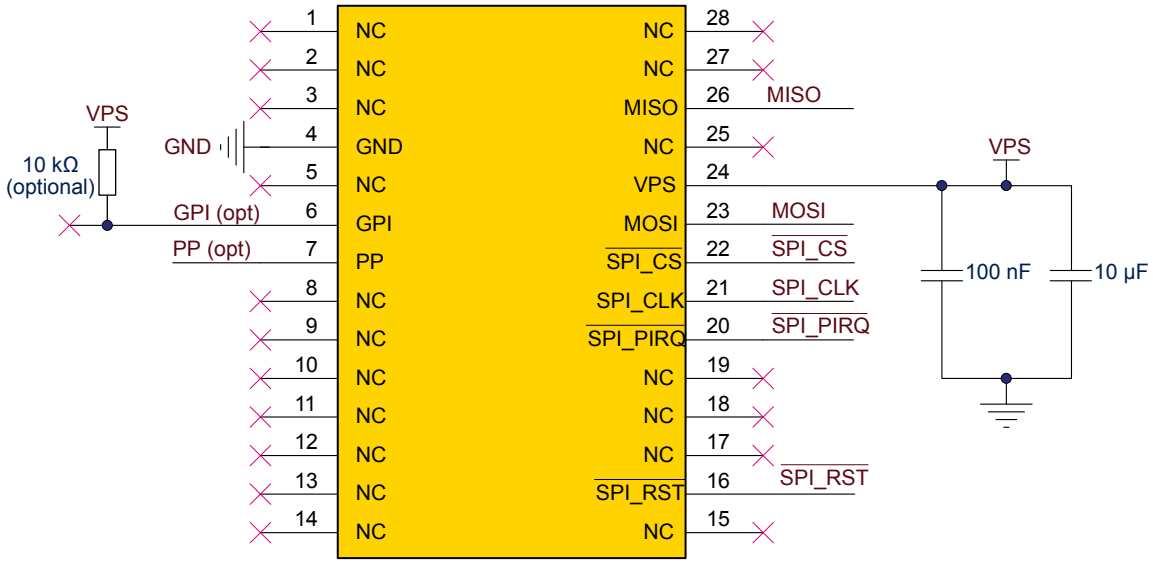
4 Integration guidance

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.

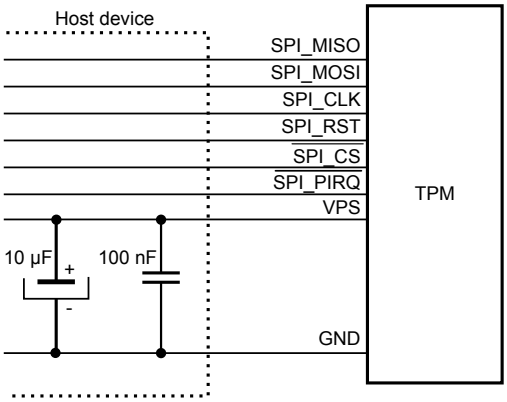
Figure 3. Typical hardware implementation (TSSOP28 package)



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).

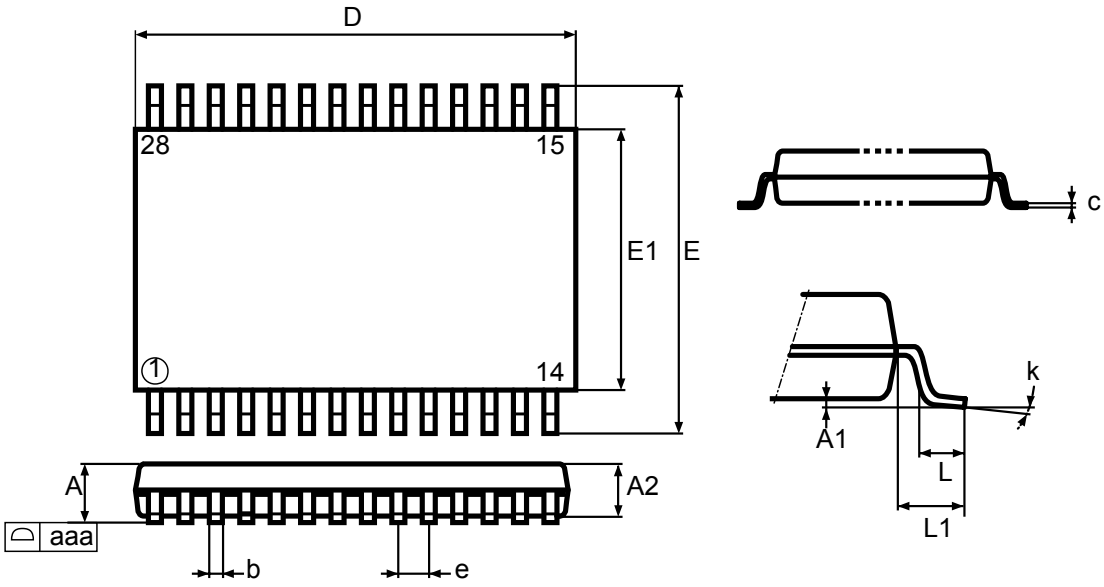
5 Package information

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 TSSOP28 package information

TSSOP28 is a 28-pin, 9.7 × 6.4 mm, 4.4 mm body width, 0.65 mm pitch, thin shrink small outline package.
Unless otherwise specified, general tolerance is ± 0.1 mm.

Figure 5. TSSOP28 - outline



1. Drawing is not to scale.

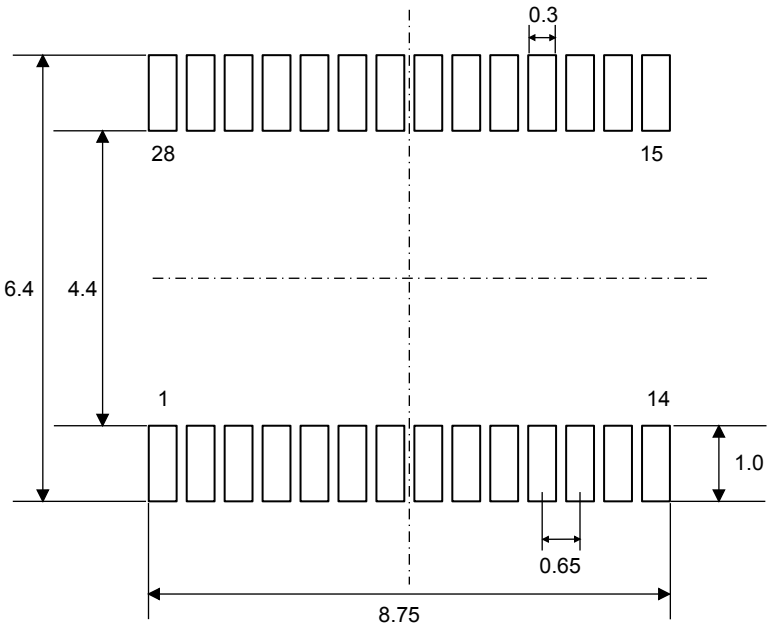
Table 2. TSSOP28 - mechanical data

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	-

Symbol	millimeters			inches [1]		
	Min.	Typ.	Max.	Min.	Typ.	Max.
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. TSSOP28 - recommended footprint

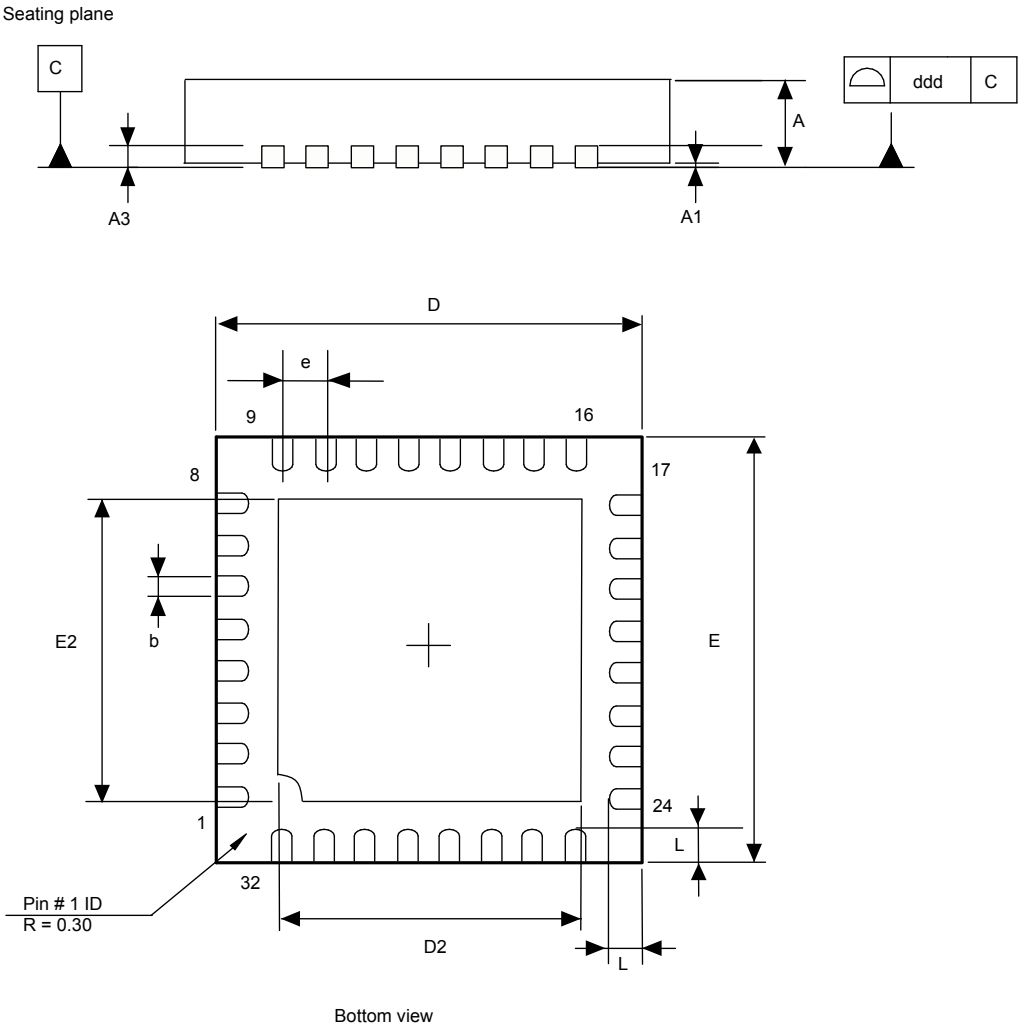


1. All dimensions are in millimeters.

5.2 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 7. VFQFPN32 - outline



1. Drawing is not to scale.

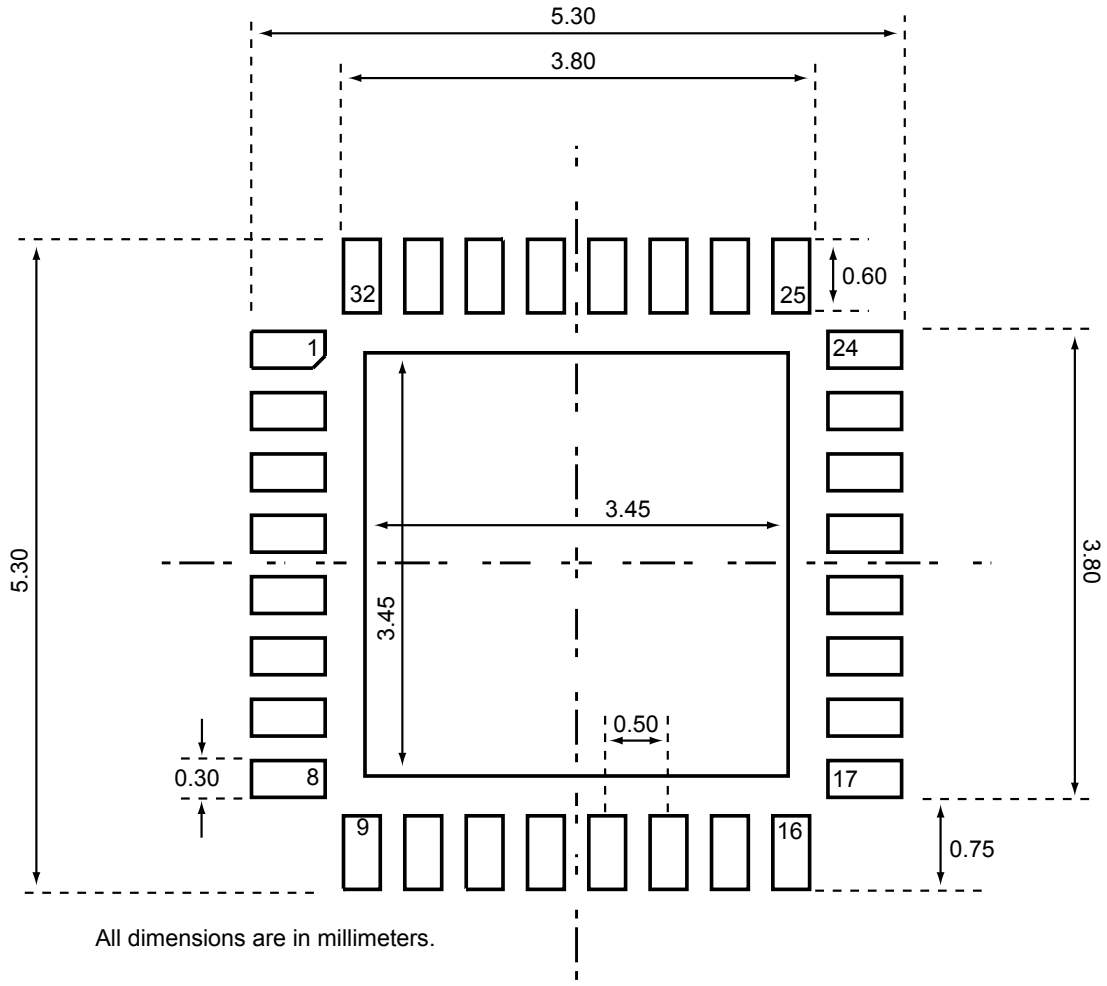
Table 3. VFQFPN32 - mechanical data

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

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 8. VFQFPN32 - recommended 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 at 0 lfpm (1)
	Junction to case thermal resistance	θ_{JC}	1.48 at 0 lfpm(1)
	Junction to board thermal resistance	θ_{JB}	13.9 at 0 lfpm(1)

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

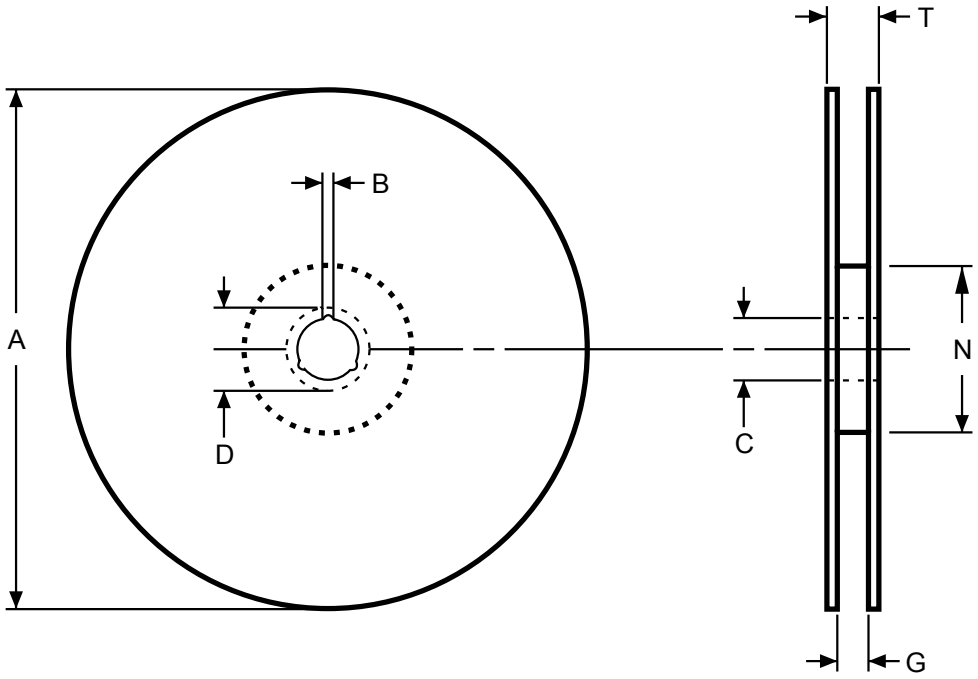
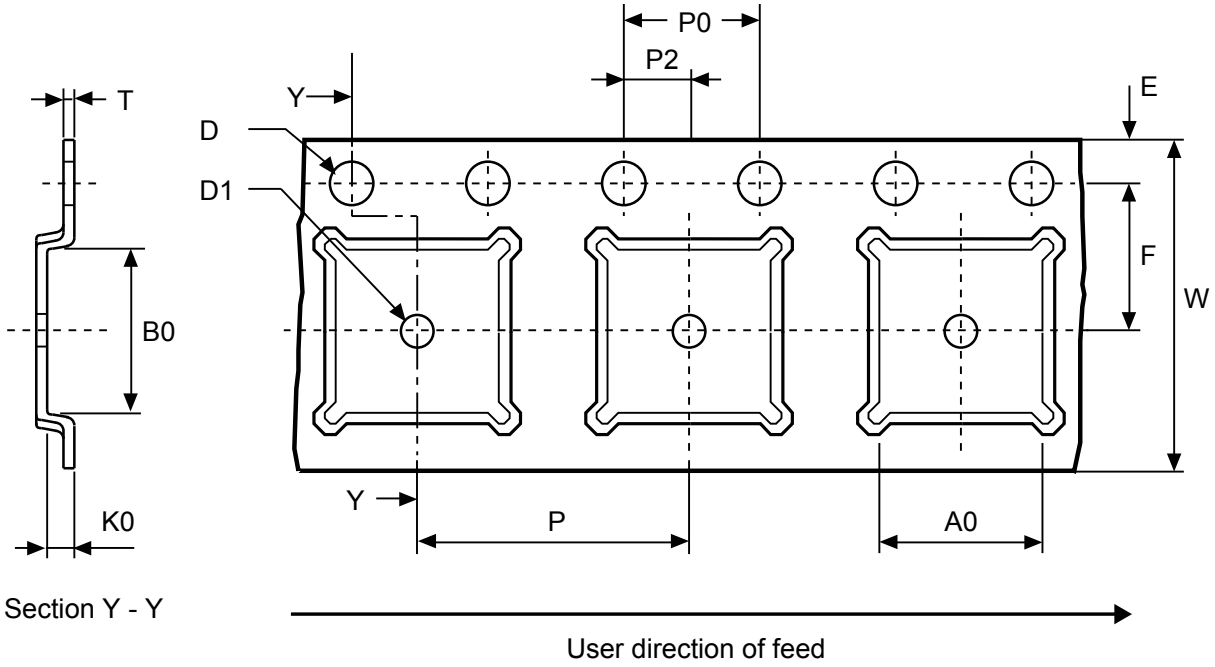


Table 6. Reel dimensions

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**

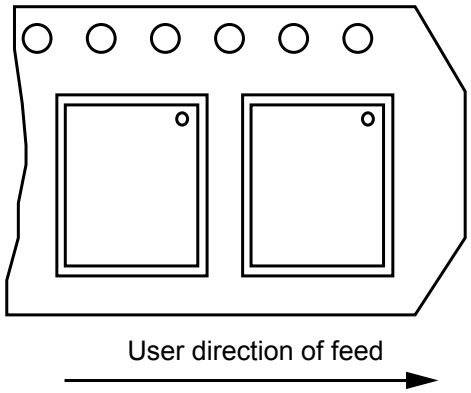
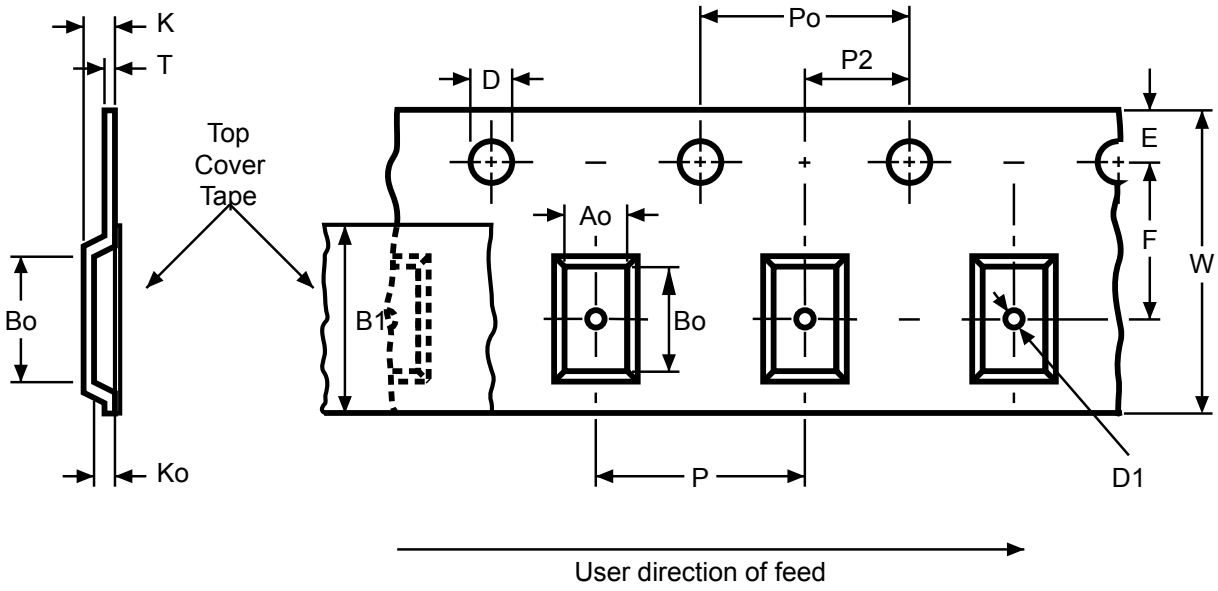


Table 7. **Carrier tape dimensions for VFQFPN 5 × 5 mm**

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

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**

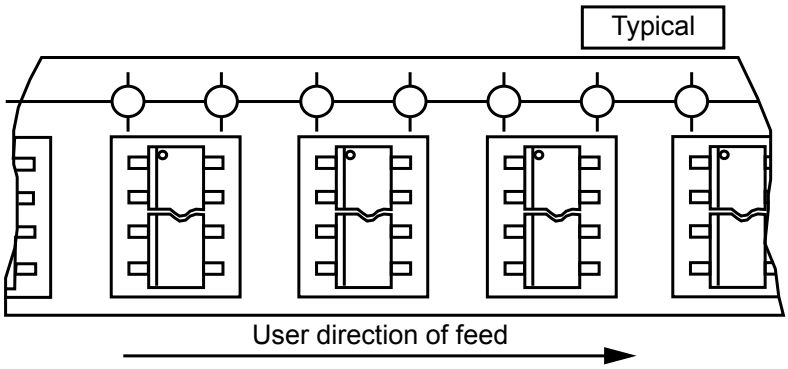


Table 8. **Carrier tape constant dimensions for TSSOP 4.4 mm body width**

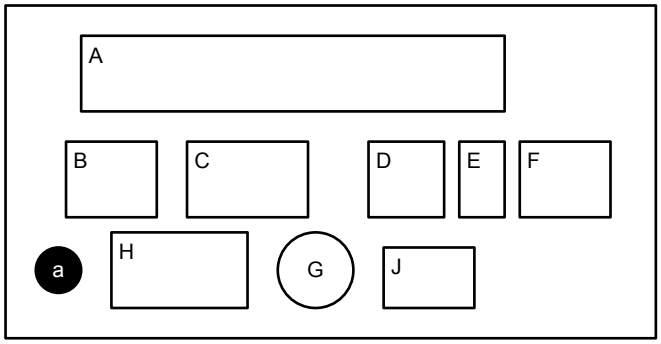
Tape size	Ao, Bo, Ko (1)	D	E	Po	T Max.	Unit
16 mm	See note.	1.5 +0.1 / −0	1.75 ±0.1	4 ±0.1	0.4	mm

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

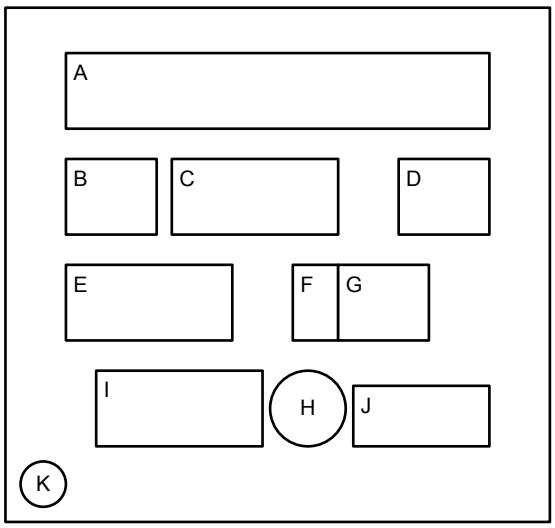
The two figures below illustrate the typical markings of the TSSOP28 and the VQFN32 device packages, respectively.

Figure 14. TSSOP28 device package marking area



A: Marking area
B: Assembly plant
C: BE sequence
D: Diffusion plant
E: Assembly year
F: Assembly week
G: ECOPACK level
H: ST logo
J: Marking area - 2 digits
a: Dot

Figure 15. VQFN32 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: ECOPACK
I: ST logo
J: Marking area - 2 digits
K: Dot

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

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

8 Ordering information

Table 9. Ordering information for ST33TPHF20SPI products

Ordering code	TPM library revision & firmware version	Operating temperature range (1)	Maximum SPI clock frequency	Package	Marking area A	Product status
ST33HTPH2028AHD1	TPM2.0 Rev 1.38 0x00 0x4A 0x00 0x40 (74.64)	−40 °C to +105 °C	33 MHz	TSSOP28	P0AHD1	Active
ST33HTPH2032AHD1				VQFN32		
ST33HTPH2028AHC9	TPM2.0 Rev 1.38 0x00 0x4A 0x00 0x10 (74.16)	−40 °C to +105 °C	33 MHz	TSSOP28	P0AHC9	NRND (not recommended for new design)
ST33HTPH2032AHC9				VQFN32		
ST33HTPH2028AHC1	TPM2.0 Rev 1.38 0x00 0x4A 0x00 0x08 (74.08)	−40 °C to +105 °C	33 MHz	TSSOP28	P0AHC1	NRND (not recommended for new design)
ST33HTPH2032AHC1				VQFN32		
ST33HTPH2028AAF3	TPM2.0 Rev 1.16 0x00 0x4A 0x00 0x00 (74.00)	−40 °C to +105 °C	33 MHz	TSSOP28	P68HAAF3	NRND (not recommended for new design)
ST33HTPH2032AAF3				VQFN32		

1. *Refer to Section 1 Description for the operating voltages associated with the different operating temperature ranges.*

9 Firmware image overview

Table 10. Firmware image overview for the ST33TPHF20SPI products

Firmware version	Firmware version (TPM capability)	TPM 2.0 library revision	Product status
74.00	0x00 0x4A 0x00 0x00	1.16	NRND (not recommended for new design)
74.04	0x00 0x4A 0x00 0x04	1.16	NRND (not recommended for new design)
74.08	0x00 0x4A 0x00 0x08	1.38	NRND (not recommended for new design)
74.16	0x00 0x4A 0x00 0x10	1.38	NRND (not recommended for new design)
74.20	0x00 0x4A 0x00 0x14	1.16	Active
74.64	0x00 0x4A 0x00 0x40	1.38	Active

Table 11. Commercial product supporting the update with firmware image version 74.20

xx = 28 for products delivered in TSSOP28, and 32 for products delivered in QFN32 packages.

Commercial products	Firmware preloaded in factory	TPM2_Clear required before firmware update
ST33HTPH2ExxAAF3	74.00 0x00 0x4A 0x00 0x00	No

Table 12. Commercial product supporting the update with firmware image version 74.64

xx = 28 for products delivered in TSSOP28, and 32 for products delivered in QFN32 packages.

Commercial products	Firmware preloaded in factory	TPM2_Clear required before firmware update
ST33HTPH20xxAAF3	74.00 0x00 0x4A 0x00 0x00	Yes
ST33HTPH20xxAHC1	74.08 0x00 0x4A 0x00 0x08	No
ST33HTPH20xxAHC9	74.16 0x00 0x4A 0x00 0x10	No

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*.

Appendix A Terms and abbreviations

Table 13. List of abbreviations

Term	Meaning
AES	Advanced Encryption Standard
CC	Common Criteria
DES	Data Encryption Standard
DRBG	Deterministic random-bit generator
EAL	Evaluation assurance level
EC	Elliptic curve
ECC	Elliptic curve cryptography
ECDAA	Elliptic curve direct anonymous attestation
ECDH	Elliptic curve Diffie–Hellman
ESD	Electrostatic discharge
FIPS	Federal Information Processing Standard
FW	Firmware
GPI	General-purpose input
HBM	Human body model
HMAC	Keyed-Hashing for message authentication
MPU	Memory protection unit
NIST	National Institute of Standards and Technology
NRND	Not recommended for new design
RNG	Random number generator
RSA	Rivest Shamir Adelman
SHA	Secure Hash algorithm
SPI	Serial Peripheral Interface
ST	STMicroelectronics
TCG	Trusted Computed Group
TIS	TPM interface specification
TPM	Trusted Platform Module
TRNG	True random number generator

Revision history

Table 14. Document revision history

Date	Version	Changes
04-Mar-2016	1	Initial release.
15-Mar-2016	2	Updated TPM features related to certification and updated Section 1.1: Security certifications. Updated references in Section 1: Description. Added Figure 38: Chip orientation in the embossed carrier tape for VFQFPN 5 × 5 mm and Figure 40: Chip orientation in the embossed carrier tape for TSSOP28 4.4 mm body width.
06-Feb-2018	3	Updated Appendix B: Referenced documents. The device is compliant with these revisions of the TCG documentation. The device has obtained FIPS 140-2 level 2 certification. Updated Section 1.1: Security certifications. Updated TPM 2.0 compliance with Microsoft Windows 8.1 and 10. Updated Section 2: Pin and signal description. Added Section 3: Integration guidance. Updated Arm logo and trademark. Reference modified at bottom of pages. Small text changes.
15-Nov-2019	4	Updated document for firmware version 4A.40 (74.64 in decimal): • Updated Section 1 Description. • Added Section 2.1 ST33TPHF20SPI products and Section 2.2 Firmware image. • Changed GPIO pin to GPI in Section 3 Pin and signal description. • Updated Figure 3. Typical hardware implementation (TSSOP28 package). • Added θ_{JC} and θ_{JB} values to Table 4. Thermal characteristics. • Updated Section 7 Package marking information. • Added Section 8 Ordering information. • Added Section 9 Firmware image overview. Added Section 5.3 Thermal characteristics of packages. Updated Section Appendix A Terms and abbreviations. Removed *Referenced documents* section. Small text changes.

Contents

List of tables

List of figures