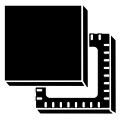
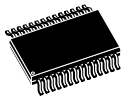
Flash-memory based TPM 2.0 device with an I²C interface



VFQFPN32
(5 × 5 mm)



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

Product status link

ST33TPHF20I2C

STSAFE-TPM

Features

TPM features

- Flash-memory-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 138 and TCG PC Client Specific TPM Platform Specifications 1.03
- Compliant with the Trusted Computing Group (TCG) Trusted Platform Module (TPM) I²C Interface Specification defined in PTP 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
- I²C support up to 400 kHz
- Support for software and hardware physical presence for TPM2.0

Hardware features

- Arm® SecurCore® SC300™ 32-bit RISC core
- Highly reliable Flash memory technology
- Extended temperature range: −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 and clock)
- 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 compliance

- TPM 2.0 compliant with the TCG test suites

1 Description

The ST33TPHF20I2C 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 138 ([TPM 2.0 P1 r138], [TPM 2.0 P2 r138], [TPM 2.0 P3 r138], [TPM 2.0 P4 r138]) and errata version 1.4 [TPM 2.0 rev138 Err .4]. It is also based on the TCG PC client-specific TPM Platform specifications rev 1.03 [PTP 2.0 r1.03] and [Errata sheet]. [TPM 2.0 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 certification

This product is CC certified according to TPM 2.0 at EAL4+.

It obtained FIPS 140-2 level 1 and level 2 certifications.

1.2 Hardware features

The ST33TPHF20I2C 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 ST33TPHF20I2C offers an Inter-Integrated Circuit (I²C) interface capable of supporting the TGC TPM I2C specification based on the TCG PC Client TPM Profile 1.03 in TPM 2.0 mode [PTP 2.0 r1.03] and [Errata sheet].

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

The ST33TPHF20I2C operates in the −25 to +85 °C commercial temperature range (see Section 8 Ordering information) with a supply and I/O voltage of 1.8 V or 3.3 V.

The ST33TPHF20I2C operates in the −40 to +105 °C commercial temperature range (see Section 8 Ordering information) with a supply and I/O voltage of 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 product status are available at: www.st.com. 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 ST33TPHF20I2C products

This document covers the functionality of firmware 4A.41 (74.65 in decimal) preloaded on ST TPM hardware with marking: PEAHC3 with “V2” in the J marking area.

The firmware version is retrieved with the `TPM_GetCapability` or `TPM2_GetCapability` command. The firmware digest, which is a cryptographic footprint, also uniquely identifies the firmware loaded on the product.

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

2.2 Firmware image

The ST33TPHF20I2C datasheet describes the functionality of the firmware image 4A.41 (74.65 in decimal) loaded on ST TPM hardware with markings:

- P68HAHB9
- PEAHC3 (J marking area is empty)

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

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

3 Pin and signal description

Figure 1. **TSSOP28 pinout**

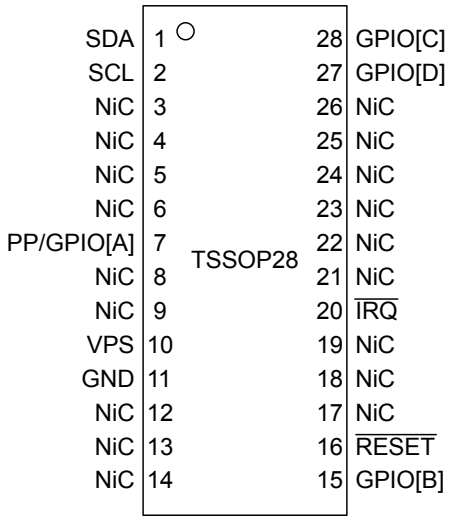


Figure 2. **VQFN32 pinout**

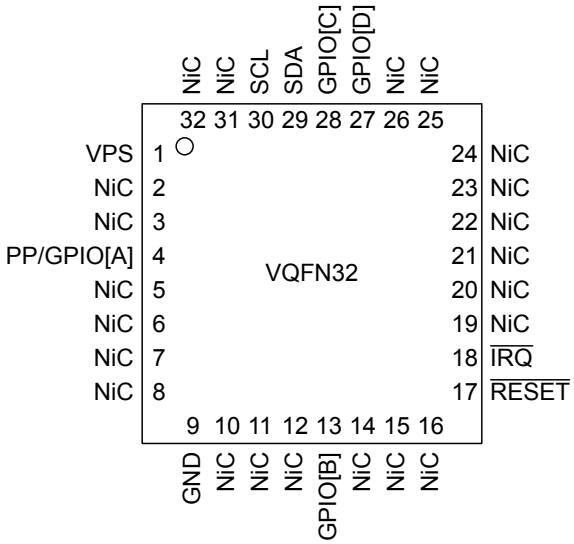


Table 1. **Pin descriptions**

Signal	Type	Description
VPS	Input	**Power supply**. This pin must be connected to 1.8 V or 3.3 V DC power rail on the motherboard.
GND	Input	GND has to be connected to the main motherboard ground.
SDA	Bidir	I2C serial data (open drain with no weak pull-up resistor)
SCL	Input	I2C serial clock (open drain with no weak pull-up resistor)
IRQ	Output	IRQ used by the TPM to generate an interrupt

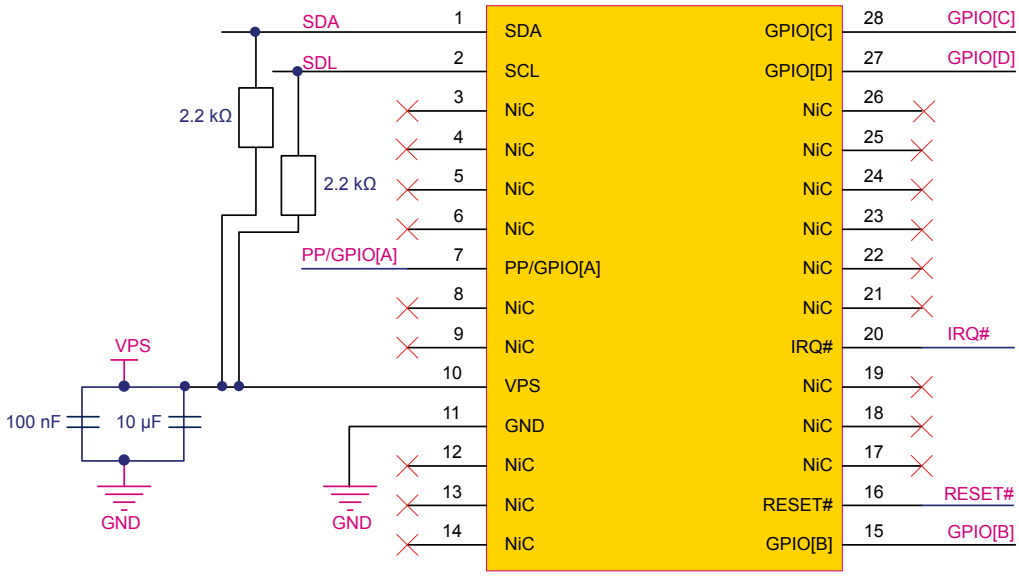
Signal	Type	Description
RESET	Input	Reset used to re-initialize the device
GPIO[A..D]	Input/ output	General-purpose input/output. Defaults to low.
PP	Input	**Physical Presence**, active high, internal pull-down. Used to indicate Physical Presence to the TPM.
NiC	-	**Not internally connected**: not connected to the die. May be left unconnected but has no impact on the TPM if connected.

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.

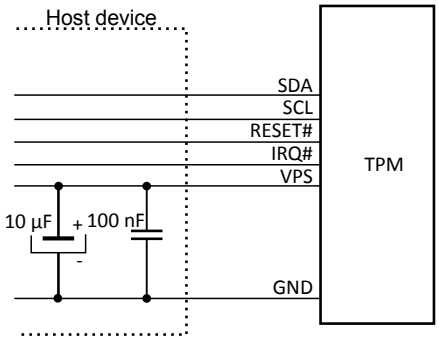
Figure 3. Typical hardware implementation (TSSOP28 package)



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).

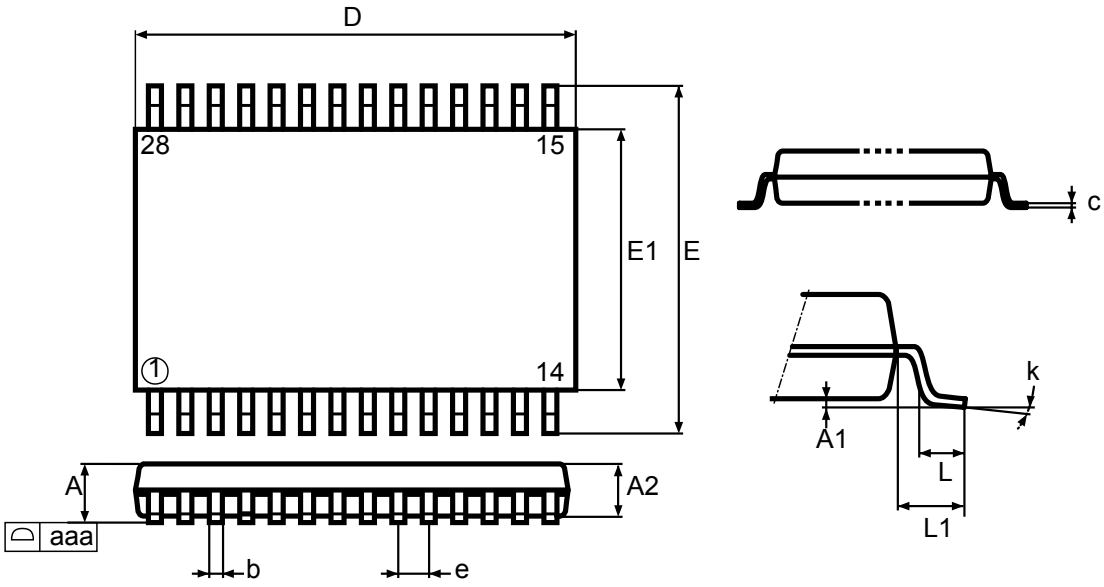
5 Package information

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.

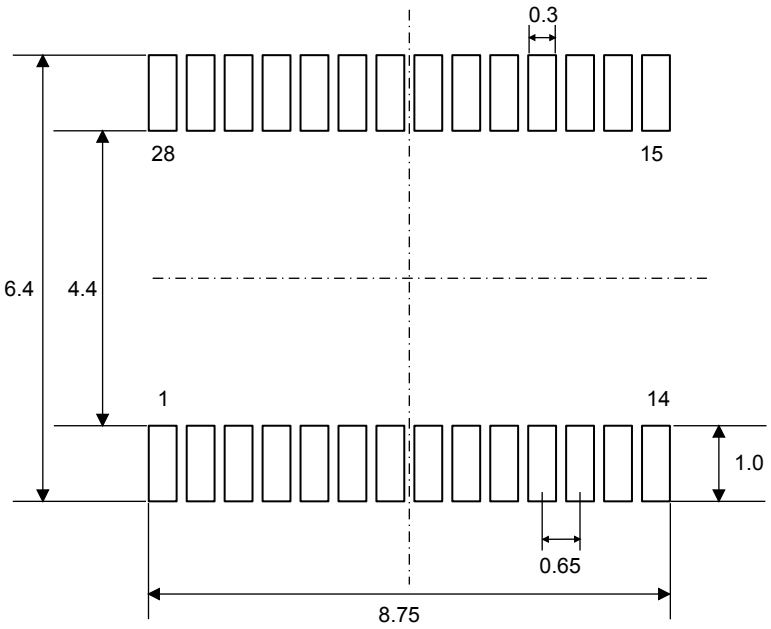
Table 2. TSSOP28 - mechanical data

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

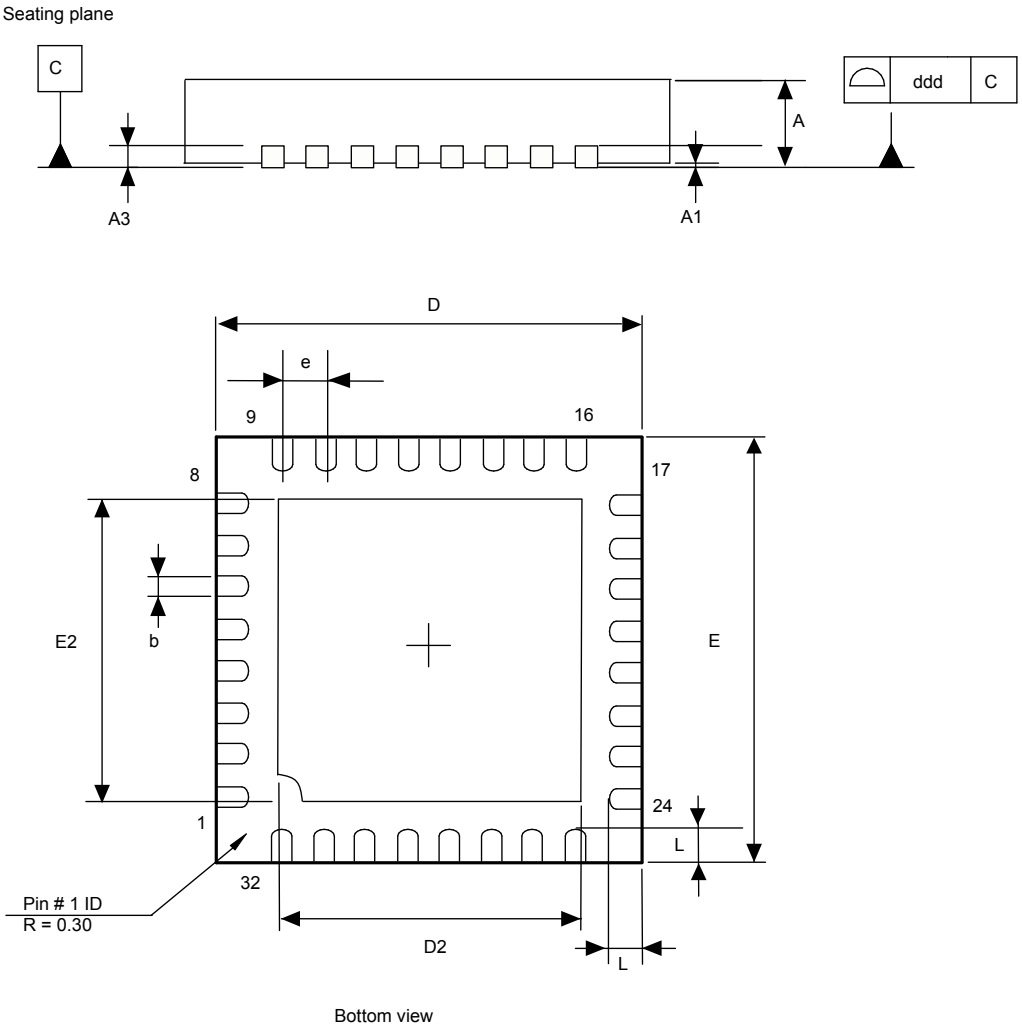


1. All dimensions are in millimeters.

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.

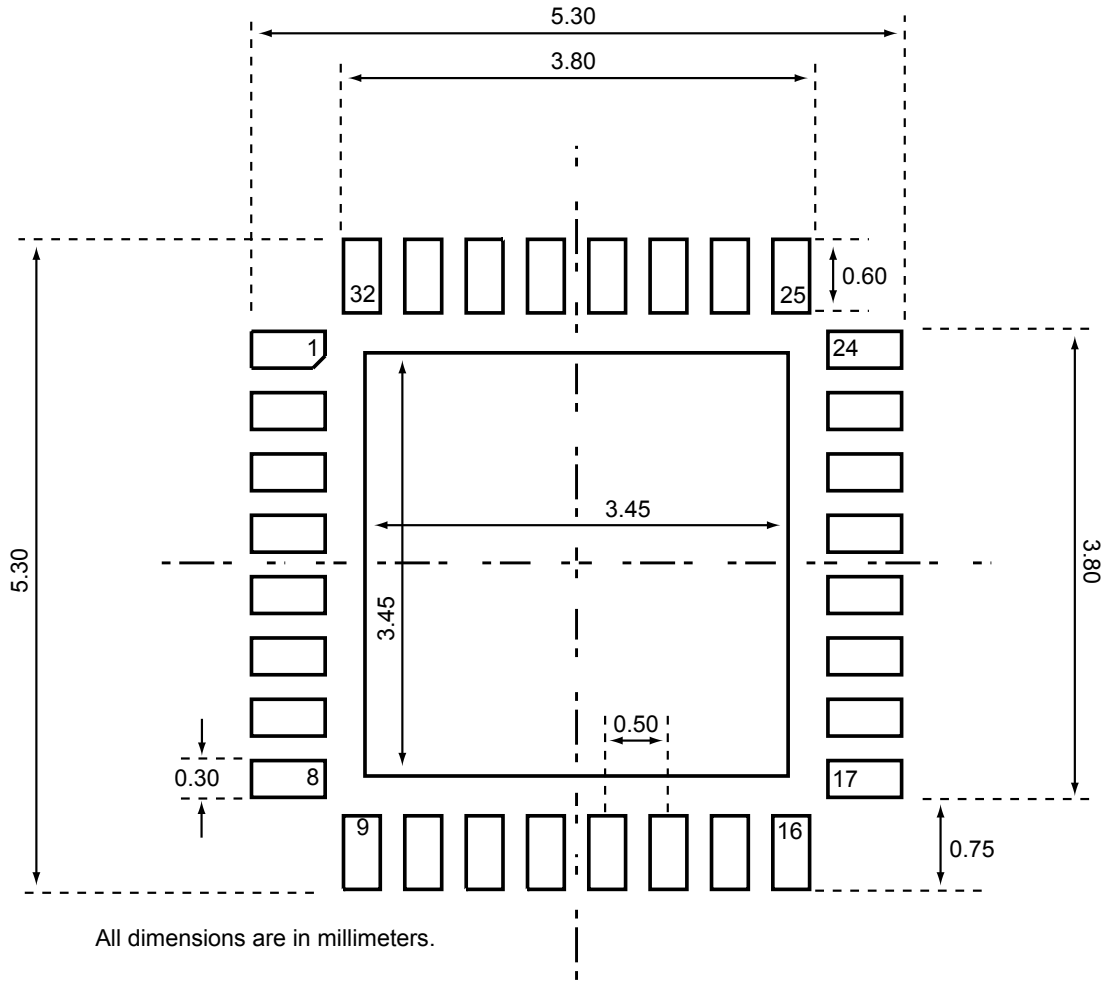
Table 3. VFQFPN32 - mechanical data

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

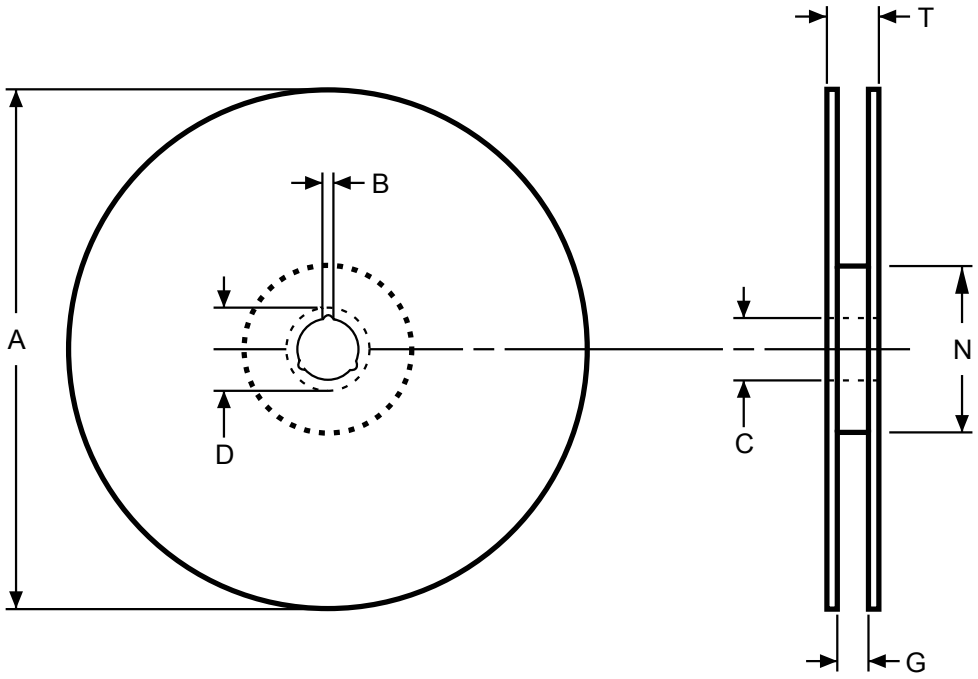
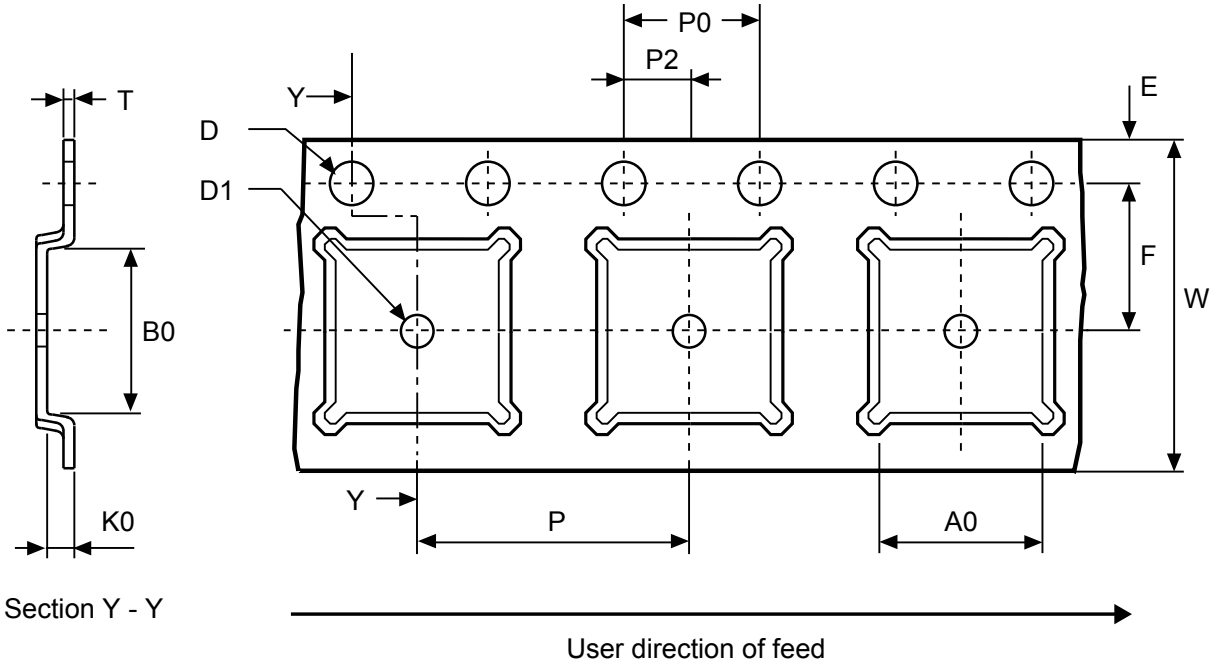


Table 6. Reel dimensions

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**

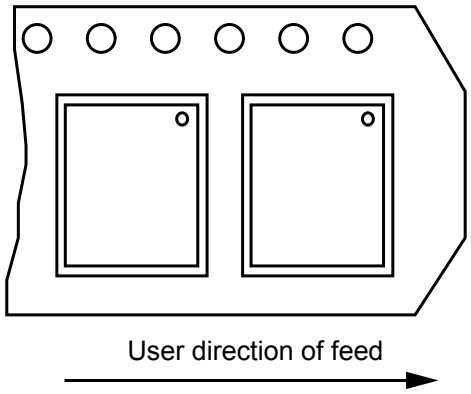
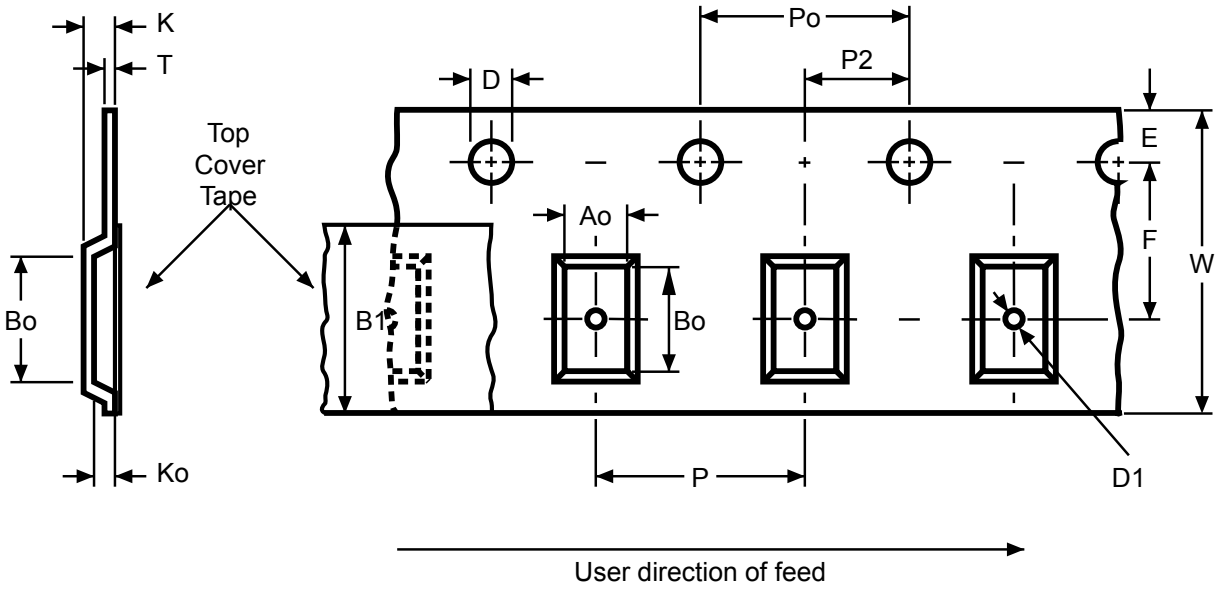


Table 7. **Carrier tape dimensions for VFQFPN 5 × 5 mm**

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**

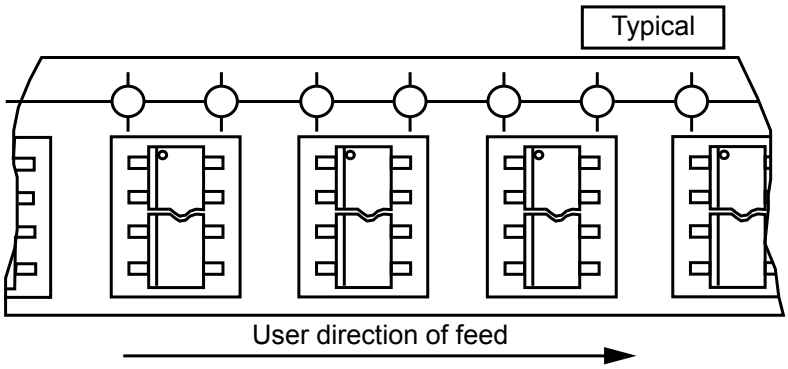


Table 8. **Carrier tape constant dimensions for TSSOP 4.4 mm body width**

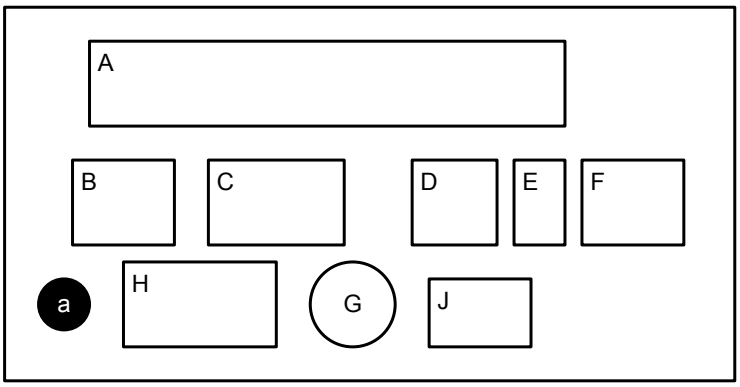
Tape size	Ao, Bo, Ko (1)	D	E	Po	T Max.	Unit
16 mm	See note.	1.5 +0.1 / −0	1.75 ±0.1	4 ±0.1	0.4	mm

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

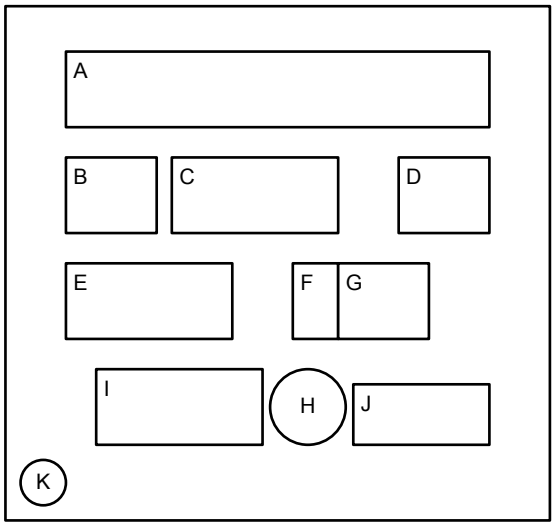
Figure 14. TSSOP28 device package marking area and Figure 15. VQFN32 device package marking area illustrate the typical markings of the TSSOP28 and the VQFN32 device packages, respectively.

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 the two packages, the ‘A’ marking area is either 6 or 8 digits. It is equal to either “PXYZZZ” or “P68XYZZZ” with:

- X = 0
- Y = Hardware revision
- ZZZ = Firmware revision

For both packages, the 2-digit ‘J’ marking area is equal to V2.

8 Ordering information

Table 9. Ordering information for products supporting firmware 4A.41 preloaded in factory

Ordering code	Firmware version	Operating temperature range (1)	Maximum I²C clock frequency	Package	Marking (A area)	Marking (J area)	Product status
ST33HTPH2028AHC3	0x00 0x4A 0x00 0x41 (74.65)	−40 °C to +105 °C	400 kHz	TSSOP28	P0AHC3	V2	Active
ST33HTPH2032AHC3				VQFN32			

1. *Refer to Section 1.2 Hardware features for the operating voltages associated with the different operating temperature ranges.*

Table 10. Products supporting firmware 4A.41 loading

Ordering code	Firmware version	Operating temperature range (1)	Maximum I²C clock frequency	Package	Marking (A area)	Marking (J area)	Product status
ST33HTPH2028AHC3(2)	0x00 0x4A 0x00 0x09	−40 °C to +105 °C	400 kHz	TSSOP28	P0AHC3	-	Obsolete
ST33HTPH2032AHC3(2)				VQFN32			
ST33TPH2E28AHB9	0x00 0x4A 0x00 0x05	−40 °C to +105 °C	400 kHz	TSSOP28	P68HAHB9	-	Not recommended for new design (NRND)
ST33TPH2E32AHB9				VQFN32			

1. *Refer to Section 1.2 Hardware features for the operating voltages associated with the different operating temperature ranges.*
2. *These ordering codes are exclusively available with preloaded 0x00 0x4A 0x00 0x41 firmware. Parts with preloaded 0x00 0x4A 0x00 0x09 firmware are no more available for order.*

9 Firmware image overview

Table 11. Firmware image overview for the ST33TPHF20I2C products

Firmware version	Firmware version (TPM capability)	TPM 2.0 library revision	Product status
74.05	0x00 0x4A 0x00 0x05	1.16	NRND (not recommended for new design)
74.21	0x00 0x4A 0x00 0x15	1.16	Active
74.09	0x00 0x4A 0x00 0x09	1.38	NRND (not recommended for new design)
74.65	0x00 0x4A 0x00 0x41	1.38	Active

Table 12. Commercial product supporting the update with firmware image version 74.21

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

Commercial product	Firmware preloaded in factory	TPM2_Clear required before firmware update
ST33HTPH2ExxAHB9	74.05 0x00 0x4A 0x00 0x05	No

Table 13. Commercial product supporting the update with firmware image version 74.65

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
ST33HTPH2ExxAHB9	74.05 0x00 0x4A 0x00 0x05	Yes
ST33HTPH2ExxAHC3	74.09 0x00 0x4A 0x00 0x09	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*.

11 Terms and abbreviations

Table 14. **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
HMAC	Keyed-Hashing for Message Authentication
I2C	Inter IC interface (Philips protocol)
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
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

12 Referenced documents

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

[TPM 2.0 P1 r138]	TPM Library, Part 1, Architecture, Family 2.0, rev 1.38, TCG
[TPM 2.0 P2 r138]	TPM Library, Part 2, Structures, Family 2.0, rev 1.38, TCG
[TPM 2.0 P3 r138]	TPM Library, Part 3, Commands, Family 2.0, rev 1.38, TCG
[TPM 2.0 P4 r138]	TPM Library, Part 4, Supporting routines, Family 2.0, rev 1.38, TCG
[TPM 2.0 rev138 Err 1.4]	Errata 1.4 January 8, 2018 for TCG TPM library version 2.0 revision 1.38 September, 29 2016.
[PTP 2.0 r1.03]	TCG PC Client Specific Platform TPM Specification (PTP) – Version 2.0 Revision 1.03
[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]	Errata Version 1.1 TCG PC Client Specific Platform TPM Profile for TPM 2.0
[PC Client BIOS]	TCG PC Client Specific Implementation Specification for Conventional BIOS – Version 1.2 Final – Revision 1.00 – July 13, 2005.
[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 2.0 PP]	Protection Profile PC Client Specific TPM, Family 2.0 Level 0 revision 1.38 (1.0), TCG.

Revision history

Table 15. **Document revision history**

Date	Version	Changes
12-Jul-2018	1	Initial release.
19-Nov-2019	2	Updated errata version number (Section 1 Description and Section 12 Referenced documents). Updated Section 2.1 ST33TPHF20I2C products. Added Section 2.2 Firmware image. Removed Section *New features*. Small text changes: • TSSOP28 description (first page), • Section 5.1 TSSOP28 package information, • Section 5.2 VFQFPN32 package information. Updated Section 5.3 Thermal characteristics of packages. Section 7 Package marking information and Section 8 Ordering information. Added Section 9 Firmware image overview.

Contents

List of tables

List of figures