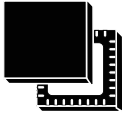


STSAFE-TPM trusted platform module 2.0 with a SPI or I²C interface



UFQFPN32 (5 × 5 × 0.55 mm)



Product status

ST33KTPM2X

Features

TPM features

- Flash-memory-based trusted platform module (*TPM*)
- Compliant with Trusted Computing Group (*TCG*) trusted platform module (*TPM*) Library specifications 2.0, revision 1.59 errata version 1.4 and *TCG* PC Client Platform *TPM* Profile (*PTP*) for *TPM* 2.0 Version 1.05
- 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:
 - Common Criteria EAL4+ in compliance with the *TPM* 2.0 protection profile (augmented with AVA_VAN.5, resistant to high-potential attacks)
 - FIPS 140-3
 - *TCG* certification
- SPI communication bus running at up to 66 MHz
- I²C communication bus running at up to 1 Mb/s

Hardware features

- Highly reliable flash memory with error correction code
- Extended temperature range: -40 °C to 105 °C
- Electrostatic discharge (ESD) protection up to 4 kV (HBM)
- 1.8 V or 3.3 V supply voltage range

Security features

- Active shield
- Monitoring of environmental parameters
- Hardware and software protection against fault injection and side channel attacks
- *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, 3072 and 4096 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
 - 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's targeted compliance

- Compliant with Microsoft® Windows® 10 and 11
- Compliant with Linux® drivers
- Compliant with Intel® vPro® technology
- Compliant with 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.

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.

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

The STSAFE-TPM devices target Common Criteria, TCG, and FIPS certifications.

The [ST33KTPM2X](#) offers a slave serial peripheral interface (SPI) or a target I²C interface, both 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 [ST33KTPM2X](#) operates in the -40 °C to 105 °C extended temperature range.

The device is offered in the UFQFPN32 ECOPACK2 package. ECOPACK is an ST trademark.



2 UFQFPN32 pin and signal description

The figure below gives the pinout of the UFQFPN32 package in which the devices are delivered. The table describes the associated signals.

Figure 1. UFQFPN32 pinout

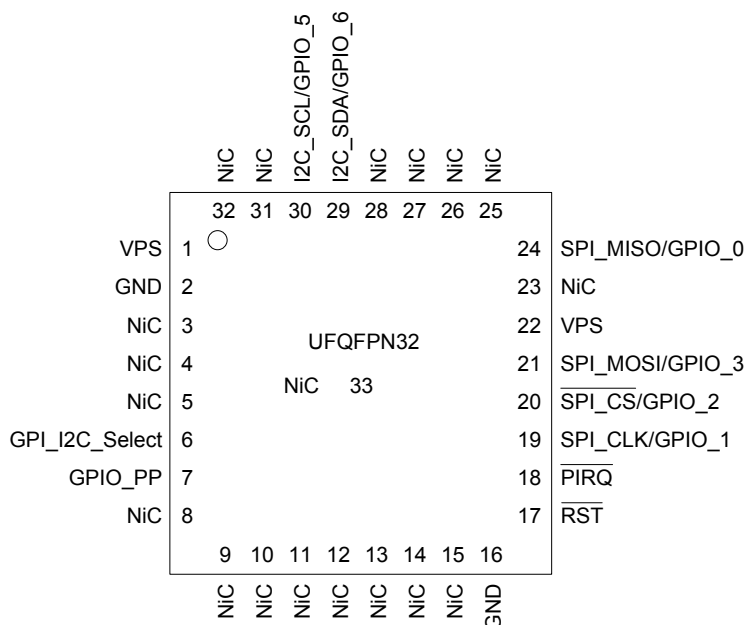


Table 1. Pin descriptions

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	Ground, has to be connected to the main motherboard ground.
RST	Input	Reset, active low, used to re-initialize the device. Must not be unconnected. External pull-up resistor 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)
SPI_CS	Input	SPI Chip (or Slave) Select, internal pull-up (active low; output from master)
PIRQ	Output	IRQ, active low, open drain, used by the TPM to generate an interrupt
GPIO_PP	Input	Physical Presence, active high, internal pull-down. Used to indicate Physical Presence to the TPM. The GPIO function could be modified by activating the GPIOs mapped with the NV storage index feature.
GPI_I2C_Select	Input	This pin must be connected to an external pull-down resistor to activate the I ² C protocol during product boot time. It can remain unconnected for the SPI protocol. This pin is internal pull-up by default and becomes internal floating after I ² C activation.
NiC	-	Not internally connected: not connected to the die. May be left unconnected but no impact on TPM if connected.
GPIO_X	Input/Output	The GPIO function could be modified by activating the GPIOs mapped with the NV storage index feature. GPIO availability is dependent of bus interface (for example, GPIO_5 and GPIO_6 are available with the SPI interface activated).

Signal	Type	Description
I2C_SDA	Input/Output	Bidirectional I ² C serial data (open drain without a weak pull-up resistor).
I2C_SCL	Input	Input I ² C serial clock (open drain without a weak pull-up resistor).

Note: The UFQFPN32 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.

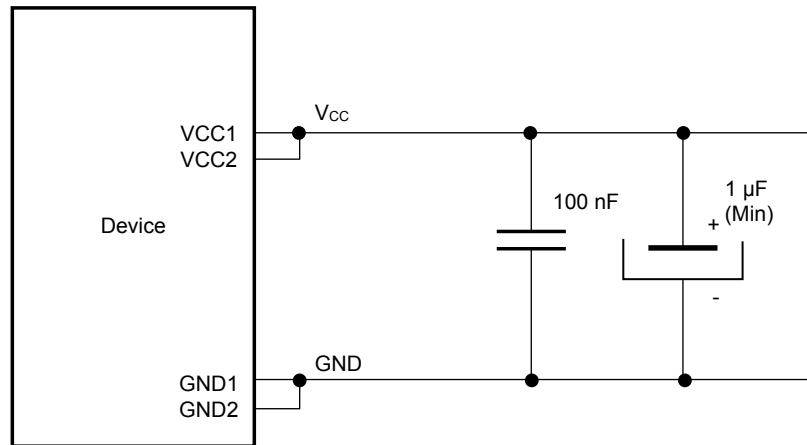
3 Electrical integration guidance

This section gives some guidance on how to integrate the ST33KTPM2X device in an application.

3.1 Recommended power supply filtering

The power supply of the device should be filtered using the circuit shown in the figure below.

Figure 2. Recommended filtering capacitors on V_{CC}



DT64224V1

Table 2. V_{CC} rising slope

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

Symbol	Parameter	Min.	Typ.	Max.	Unit
S _{VCC}	V _{CC} rising slope	2	-	2 · 10 ³	V/ms

Note: Measurement must be done between 1.36 V and 1.62 V. If V_{CC} rising slope requirement is unreachable for the concerned platform or if there is any other noisy environment at boot, a "power-on reset and warm reset sequence" must be run.

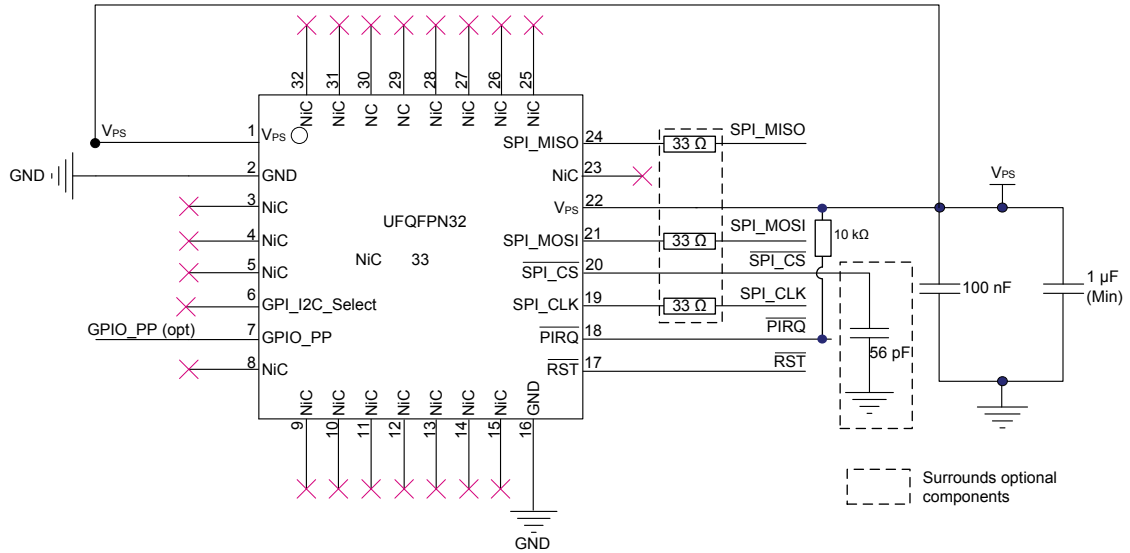
3.2 SPI_CS optional filtering

Recommendation for SPI_CS integration: It is mandatory that SPI_CLK is at the low logic level when the falling edge occurs on the SPI_CS signal. An external capacitance of 56 pF is recommended on SPI_CS for that purpose. This capacitor might not be required depending on the intrinsic line capacitance, the SPI bus frequency, or both.

3.3 Device integration for SPI communication

The figure below shows the typical hardware implementation of the ST33KTPM2X device for SPI communication.

Figure 3. Typical hardware implementation for SPI communication (UFQFPN32 package)



DT688966V1

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. Its use is mandatory to avoid disturbance of the ramp-up and ramp-down signals.

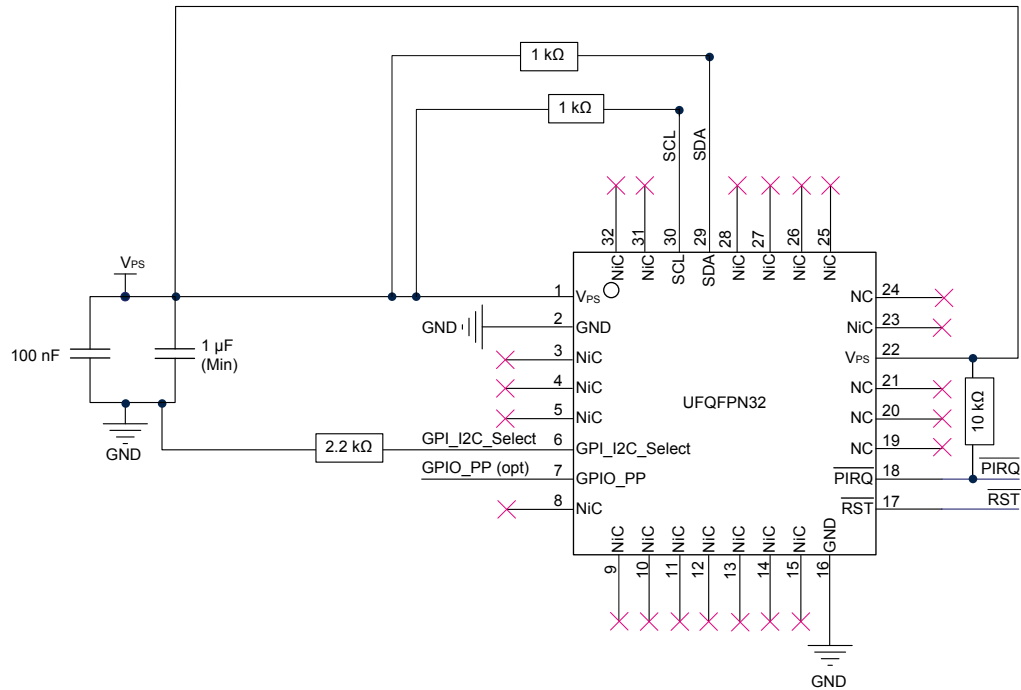
Note: The capacitor on $\overline{\text{SPI_CS}}$ is optional (see Section 3.2 $\overline{\text{SPI_CS}}$ optional filtering).

Note: The pull-up resistor on the PIRQ line is mandatory to optimize the power consumption in standby mode.

3.4 Device integration for I²C communication

The figure below shows the typical hardware implementation of the ST33KTPM2X device for I²C communication.

Figure 4. Typical hardware implementation for I²C communication (UFQFPN32 package)



DT68867V2

Note: The pull-up resistor on the PIRQ line is mandatory to optimize the power consumption in standby mode.

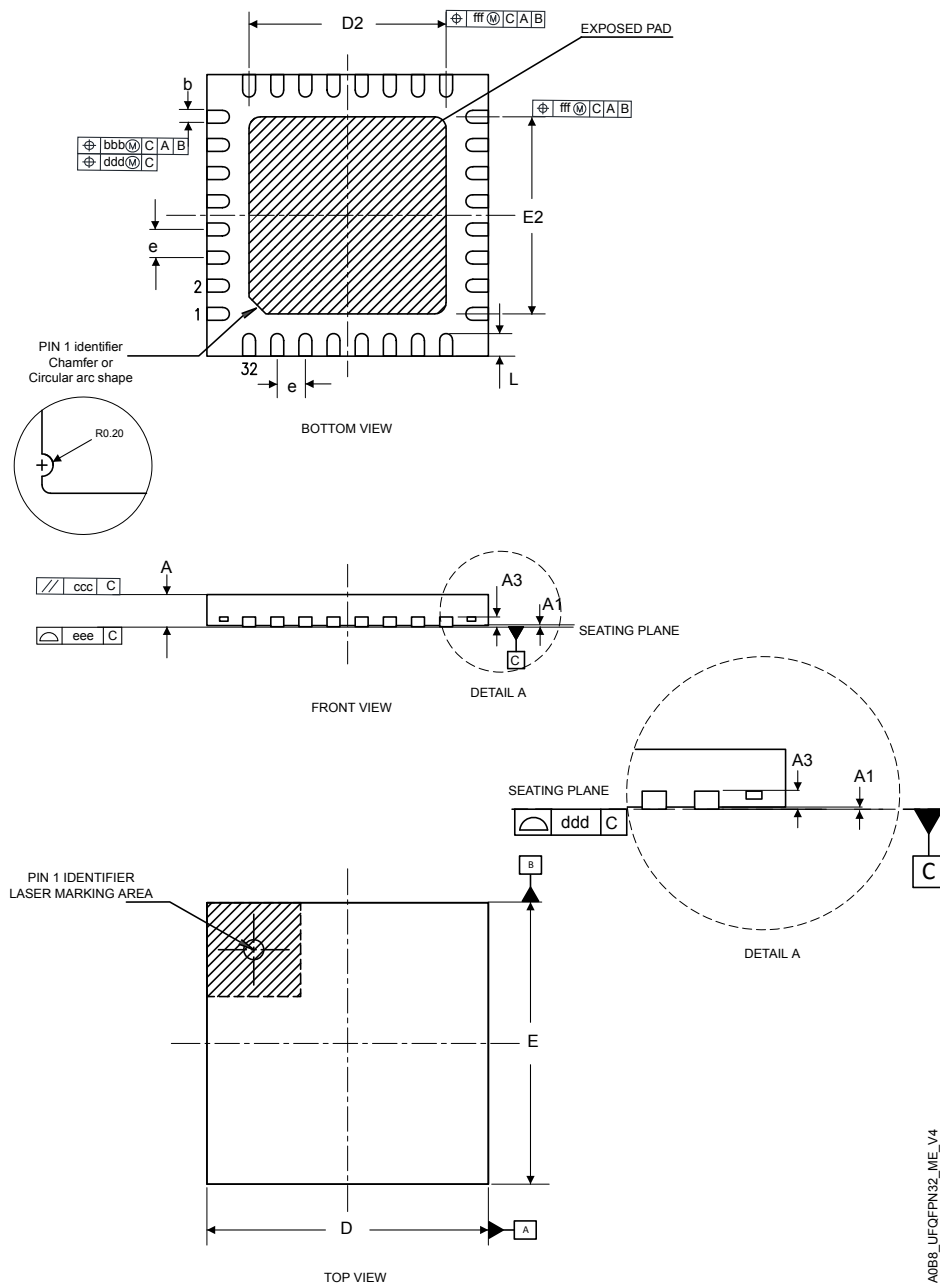
4 Package information

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.

4.1 UFQFPN32 package information

This UFQFPN is a 32 pins, 5x5 mm, 0.5 mm pitch ultra thin fine pitch quad flat package.

Figure 5. UFQFPN32 - Outline



A0B8_UFQFPN32_ME_V4

1. Drawing is not to scale.
2. All leads/pads should also be soldered to the PCB to improve the lead/pad solder joint life.

- There is an exposed die pad on the underside of the UFQFPN package. It is recommended to connect and solder this backside pad to PCB ground.

Table 3. UFQFPN32 - Mechanical data

Symbol	millimeters ⁽¹⁾			inches ⁽²⁾		
	Min	Typ	Max	Min	Typ	Max
A ⁽³⁾⁽⁴⁾	0.50	0.55	0.60	0.0197	0.0217	0.0236
A1 ⁽⁵⁾	0.00	-	0.05	0.000	-	0.0020
A3 ⁽⁶⁾	-	0.15	-	-	0.0060	-
b ⁽⁷⁾	0.18	0.25	0.30	0.0071	0.010	0.0118
D ⁽⁸⁾⁽⁹⁾	5.00 BSC			0.1969 BSC		
D2	3.50	3.60	3.70	0.139	0.143	0.147
E ⁽⁸⁾⁽⁹⁾	5.00 BSC			0.1969 BSC		
E2	3.50	3.60	3.70	0.139	0.143	0.147
e ⁽⁹⁾	-	0.50	-	-	0.02	-
N ⁽¹⁰⁾				32		
K	0.15	-	-	0.006	-	-
L	0.30	-	0.50	0.0119	-	0.0199
R	0.09	-	-	0.004	-	-

- All dimensions are in millimetres. Dimensioning and tolerancing schemes are conform to ASME Y14.5M-2018 except European.
- Values in inches are converted from mm and rounded to 4 decimal digits.
- UFQFPN stands for Ultra thin Fine pitch Quad Flat Package No lead: $A \leq 0.60\text{mm}$ / Fine pitch $e \leq 1.00\text{mm}$.
- The profile height, A, is the distance from the seating plane to the highest point on the package. It is measured perpendicular to the seating plane.
- A1 is the vertical distance from the bottom surface of the plastic body to the nearest metallized package feature.
- A3 is the distance from the seating plane to the upper surface of the terminals.
- Dimension b applies to metallized terminal. If the terminal has the optional radius on the other end of the terminal, the dimension b must not be measured in that radius area.
- Dimensions D and E do not include mold protrusion, not to exceed 0,15mm.
- BSC stands for BASIC dimensions. It corresponds to the nominal value and has no tolerance. For tolerances refer to Table 4
- N represents the total number of terminals.

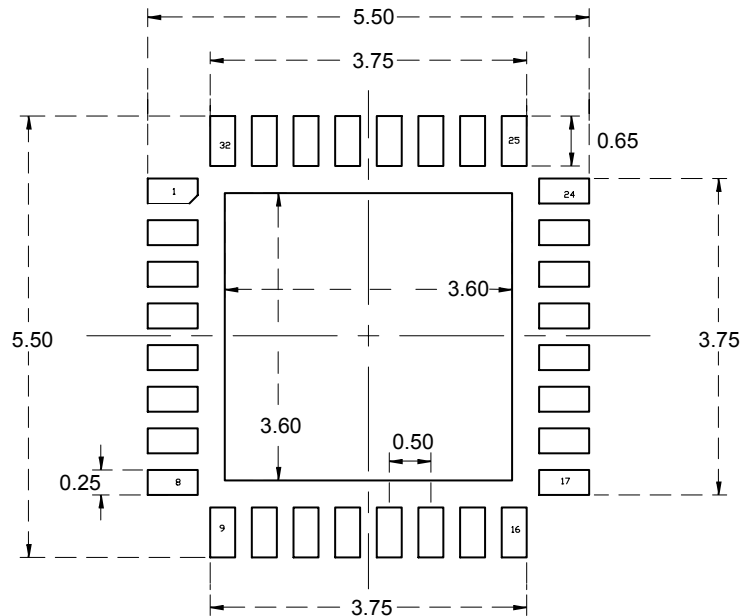
Table 4. Tolerance of form and position

Symbol ⁽¹⁾	Tolerance of form and position ⁽²⁾	Tolerance of form and position ⁽³⁾
	In millimeters	In inches
aaa	0.15	0.006
bbb	0.10	0.004
ccc	0.10	0.004
ddd	0.05	0.002
eee	0.10	0.004
fff	0.10	0.004

- For the tolerance of form and position definitions see Table 5.
- All dimensions are in millimetres. Dimensioning and tolerancing schemes are conform to ASME Y14.5M-2018 except European.
- Values in inches are converted from mm and rounded to 4 decimal digits.

Table 5. Tolerance of form and position symbol definition

Symbol	Definition
aaa	The bilateral profile tolerance that controls the position of the plastic body sides. The centres of the profile zones are defined by the basic dimensions D and E.
bbb	The tolerance that controls the position of the terminals with respect to Datums A and B. The centre of the tolerance zone for each terminal is defined by basic dimension e as related to datums A and B.
ccc	The tolerance located parallel to the seating plane in which the top surface of the package must be located.
ddd	The tolerance that controls the position of the terminals to each other. The centres of the profile zones are defined by basic dimension e.
eee	The unilateral tolerance located above the seating plane wherein the bottom surface of all terminals must be located = coplanarity
fff	The tolerance that controls the position of the exposed metal heat feature. The centre of the tolerance zone is the data defined by the centrelines of the package body

Figure 6. UFQFPN32 - Footprint example


1. Dimensions are expressed in millimeters.

A088_UFQFPN32_FP_V1

4.2 Thermal characteristics of packages

The table below provides the thermal characteristics of the UFQFPN32 package.

Table 6. 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		-	66 mW
Theta-JA, -JB and -JC	Junction to ambient thermal resistance	$\theta_{JA}^{(1)}$	35 °C/W
	Junction to case thermal resistance	θ_{JC}	5 °C/W
	Junction to board thermal resistance	θ_{JB}	20 °C/W

1. According to JESD51-2 (still air condition).

5 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 7. Packages on tape and reel

Package	Description	Tape width	Tape pitch	Reel diameter	Quantity per reel
UFQFPN32	Ultra thin fine pitch quad flat pack no-lead package	12 mm	8 mm	13 in.	3000

Figure 7. Reel diagram

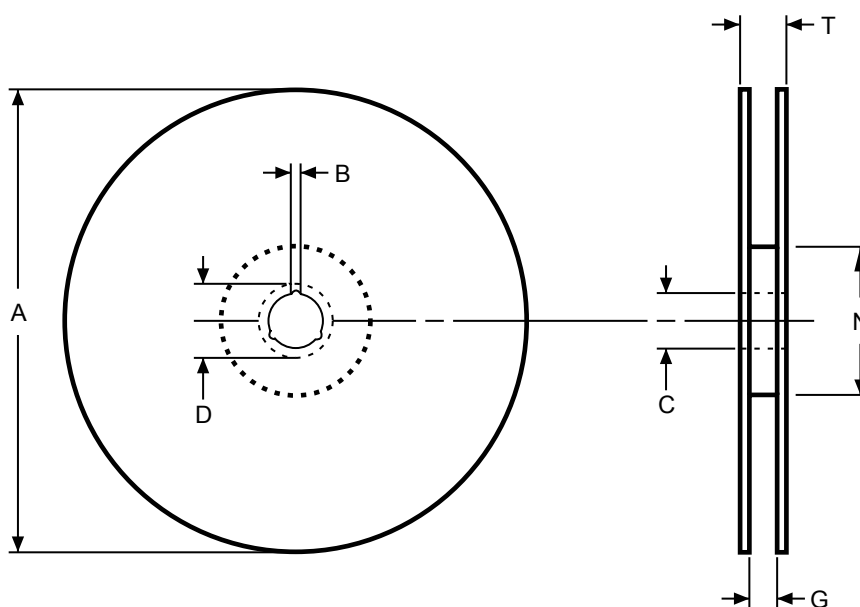
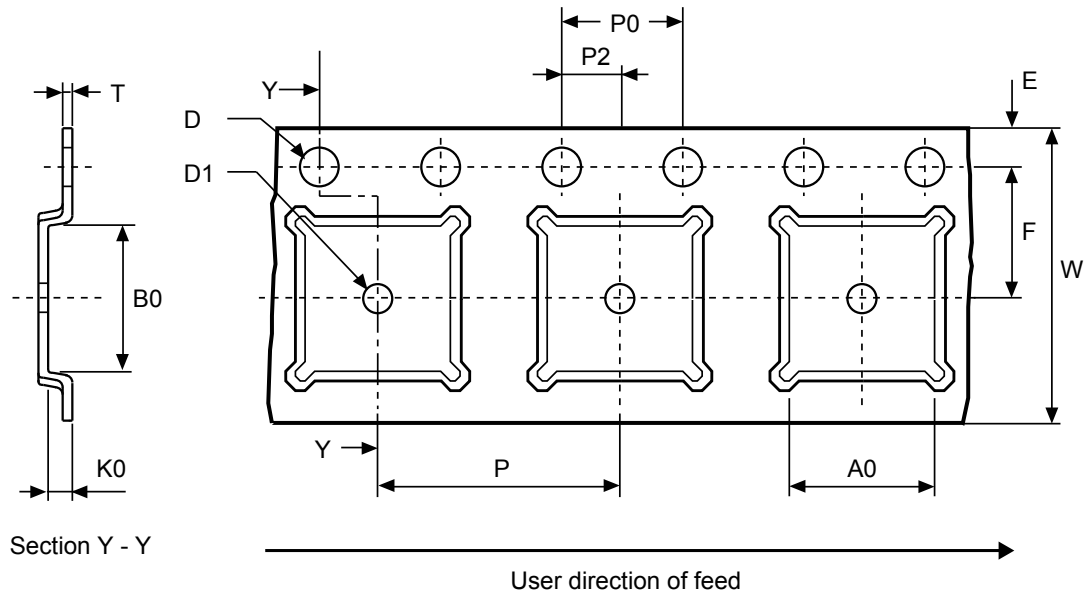


Table 8. Reel dimensions

Reel size	Tape width	A Max.	B Min.	C	D Min.	G Max.	N Min.	T Max.	Unit
13"	12	330	1.5	13 ±0.2	20.2	12.6	100	18.4	mm

Figure 8. UFQFPN32 - Embossed carrier tape



1. Drawing is not to scale.

Figure 9. UFQFPN32 - Chip orientation in the embossed carrier tape

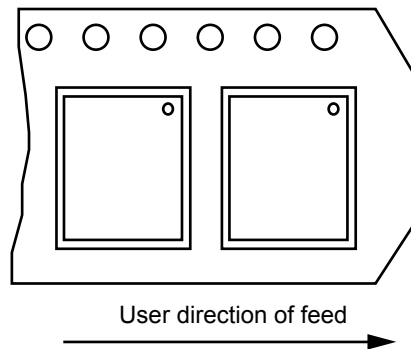


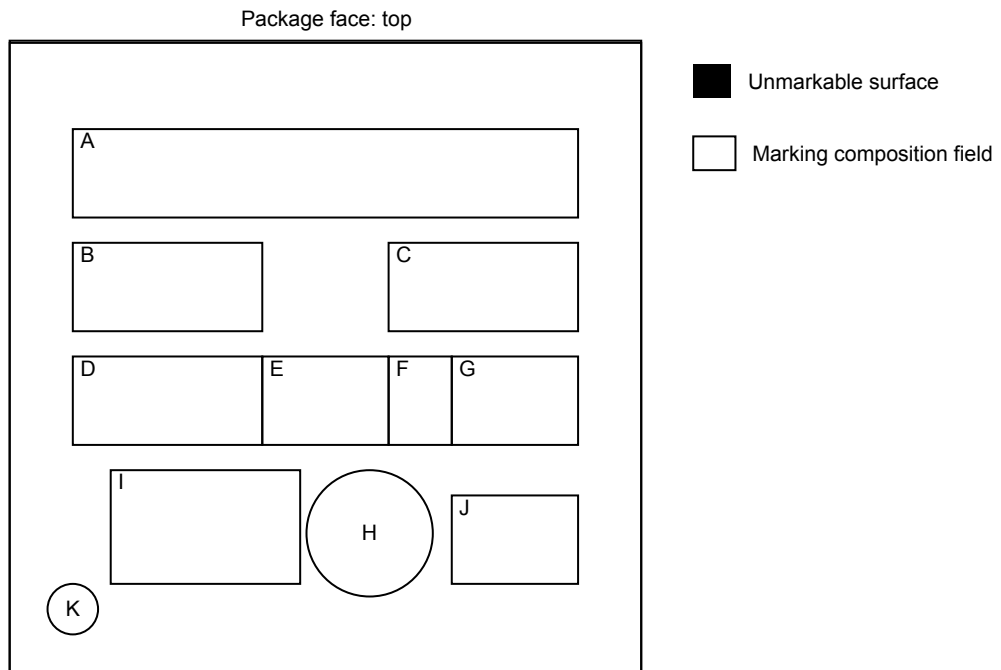
Table 9. UFQFPN32 - Carrier tape dimensions

Package	A0	B0	K0	D1 Min.	P	P2	D	P0	E	F	W	T Max.	Unit
UFQFPN 5x5	5.3 ±0.1	5.3 ±0.1	0.75 ±0.1	1.5	8 ±0.1	2 ±0.05	1.55 ±0.05	4 ±0.1	1.75 ±0.1	5.5 ±0.1	12 ±0.3	0.3 ±0.05	mm

6 UFQFPN32 package marking information

Parts marked as E or ES (for engineering sample) are not yet qualified and therefore not approved for use in production. ST is not responsible for any consequences resulting from such use. In no event will ST be liable for the customer using any of these engineering samples in production. ST's Quality department must be contacted prior to any decision to use these engineering samples to run a qualification activity.

Figure 10. UFQFPN32 - Standard marking example



Legend:

- | | |
|--|--------------------------------------|
| A: Marking area – Up to 8 digits | G: Assembly week (WW) |
| B: Marking area – 3 digits | H: Second level interconnect |
| C: BE sequence (LLL) | I: Standard STMicroelectronics logo |
| D: Country of origin (3 characters allowed (max.)) | J: Diffusion traceability plant (WX) |
| E: Assembly plant (PP) | K: Dot ⁽¹⁾ |
| F: Assembly year (Y) | |

1. The dot on the back side indicates the pin 1 location.

7 Ordering information

Table 10. Ordering information

Ordering code	Product line	Factory firmware version	Package	Minimum ordering quantity	Marking (area A)	Marking (area B)
ST33KTPM2X32DKG9	ST33KTPM2X	0x0x00.09.01.01 (09.257)	UFQFPN32	3000	KTPM	KG9

8 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 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 1.4]	Errata Version 1.4 for Trusted Platform Module Library Family 2.0 Revision 1.59, TCG
[PTP 2.0 r1.05]	TCG PC Client Platform TPM Profile (PTP) for TPM 2.0 Version 1.05 Revision 14, TCG
[PTP 2.0 errata]	Errata version 1.0 for PC Client Platform TPM Profile (PTP) for TPM 2.0 Version 1.05 Revision 0.14, 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 11. Document revision history

Date	Revision	Changes
15-Dec-2023	1	Initial release.

Glossary

3D Three-dimensional	PKCS Public key cryptographic standards
AES Advanced encryption standard	PSS Probabilistic signature scheme
CA Certification Authority	RNG Random number generator
CC Common Criteria	RSA Public-key cryptosystem (created by Ron Rivest, Adi Shamir and Leonard Adleman)
CRT Chinese remainder theorem	RSAES Rivest Shamir Adelman encryption/decryption scheme
DES Data encryption standard	RSASSA Rivest Shamir Adelman signature scheme with appendix
DRBG Deterministic random bit generator	SHA Secure Hash algorithm
DXE Driver execution environment	SPI Serial peripheral interface
EC Elliptic curve	TCG Trusted Computing Group®
ECC Elliptic curve cryptography	TDES Triple DES cryptographic algorithm
ECDA Elliptic curve direct anonymous attestation	TPM Trusted platform module
ECDAA Elliptic curve direct anonymous attestation (algorithm)	TRNG True random number generator
ECDH Elliptic curve Diffie–Hellman	TSS TPM software stack
ECDSA Elliptic curve digital signature algorithm	
EK Endorsement key	
ESD Electrostatic discharge	
FIPS Federal Information Processing Standards	
GPIO General purpose input/output	
HBM Human body model	
HMAC Hash-based message authentication code or keyed-hash message authentication code	
I²C Inter-integrated circuit	
MCU Microcontroller unit	
NIST National Institute of Standards and Technology	
NV Nonvolatile	

Contents

1	Description	3
2	UFQFPN32 pin and signal description	4
3	Electrical integration guidance	6
3.1	Recommended power supply filtering	6
3.2	$\overline{\text{SPI_CS}}$ optional filtering	6
3.3	Device integration for SPI communication	7
3.4	Device integration for I ² C communication	8
4	Package information	9
4.1	UFQFPN32 package information	9
4.2	Thermal characteristics of packages	12
5	Delivery packing	13
6	UFQFPN32 package marking information	15
7	Ordering information	16
8	Support and information	17
	Appendix A Referenced documents	18
	Revision history	19
	List of tables	22
	List of figures	23

List of tables

Table 1.	Pin descriptions	4
Table 2.	V _{CC} rising slope.	6
Table 3.	UFQFPN32 - Mechanical data	10
Table 4.	Tolerance of form and position	10
Table 5.	Tolerance of form and position symbol definition	11
Table 6.	Thermal characteristics.	12
Table 7.	Packages on tape and reel	13
Table 8.	Reel dimensions	13
Table 9.	UFQFPN32 - Carrier tape dimensions	14
Table 10.	Ordering information	16
Table 11.	Document revision history	19

List of figures

Figure 1.	UFQFPN32 pinout	4
Figure 2.	Recommended filtering capacitors on V_{CC}	6
Figure 3.	Typical hardware implementation for SPI communication (UFQFPN32 package)	7
Figure 4.	Typical hardware implementation for I^2C communication (UFQFPN32 package)	8
Figure 5.	UFQFPN32 - Outline	9
Figure 6.	UFQFPN32 - Footprint example	11
Figure 7.	Reel diagram	13
Figure 8.	UFQFPN32 - Embossed carrier tape	14
Figure 9.	UFQFPN32 - Chip orientation in the embossed carrier tape	14
Figure 10.	UFQFPN32 - Standard marking example	15

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.

© 2023 STMicroelectronics – All rights reserved