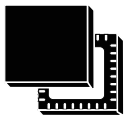
ST33KTPM2XSPI

Data brief

STSAFE-TPM trusted platform module 2.0 with a SPI interface



UFQFPN32 (5 × 5 × 0.55 mm)

Product status link
ST33KTPM2XSPI

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 1.5 and *TCG* PC Client Platform *TPM* Profile (*PTP*) for *TPM* 2.0 Version 1.06
- Fault-tolerant firmware loader that keeps the *TPM* fully functional when the loading process is interrupted
- Firmware image signed with *ECDSA* and *PQC* signature *LMS* (SP800-208)
- 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 with physical security level 3
  - *TCG* certification
- *SPI* communication bus running at up to 66 MHz

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
- *NIST* SP800-90A and AIS20-compliant deterministic random-bit generator (DRBG)
- *NIST* 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*-1v1_5)
  - *RSA* encryption (*RSAES*-OAEP, RSAES-1-v1_5)
  - SHA-1, SHA-2 (256, 384 and 512 bits), SHA-3 (256 and 384 bits)
  - *HMAC* SHA-1, SHA-2, and SHA-3
  - AES-128, 192, and 256 bits
  - *ECC* key generation (*NIST* P_256/384/521, BN P_256)
  - *ECC* secret sharing (*ECDH*)
  - *ECC* signature (*ECDSA*, ECSchnorr, *ECDAA*)
  - PQC protected firmware update mechanism with *LMS* (SP800-208)
- Device provided with four endorsement keys (*EK*) and *EK* certificates (RSA2048, RSA3072, *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 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. 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.

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* certification.

The ST33KTPM2XSPI offers a slave serial peripheral interface (*SPI*) 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 ST33KTPM2XSPI operates in the –40 °C to 105 °C extended temperature range.

The ST33KTPM2XSPI devices are offered in the UFQFPN32 Ecopack2 packages.

2 Product and firmware description

Table 1 lists the features newly implemented in TPM firmware version 0x00.09.02.00 (9.512) compared to the previous *TPM* firmware versions.

Table 1. List of new features supported by firmware version 9.512

Item	Description
Firmware update mechanism	Automatic copy of second firmware instance after one flashable image loading. Autorepair in case the firmware instance integrity is corrupted.
ECC NIST P-521	Support of NIST P-521 curve
SHA-512	Support of SHA-512
Hibernate power state	Support of hibernate state
PQC firmware upgrade	Firmware upgrade requires an additional SP800-208 *LMS* signature besides *ECC NIST* P-384 for future firmware loading
Configurable background *RSA* key generation	Background key generation becomes configurable and supports RSA 4096.
FIPS 140-3 level 2	Optional mode to support *FIPS* 140-3 level 2 authentication requirements

Table 2 lists the factory provisioning features supported exclusively by part numbers ST33KTPM2X32DKJ5 and ST33KTPM32DKJ0.

Table 2. List of changes for parts ST33KTPM2X32DKJ5 and ST33KTPM2X32DKJ0

Item	Description
RSA 3072 *EK* and *EK* certificate	*RSA* 3072 *EK* and *EK* certificate loaded during manufacturing.

3 UFQFPN32 pin and signal description

The figure below gives the pinout of the UFQFPN32 package in which the devices are delivered. Table 3 describes the associated signals.

Figure 1. UFQFPN32 pinout

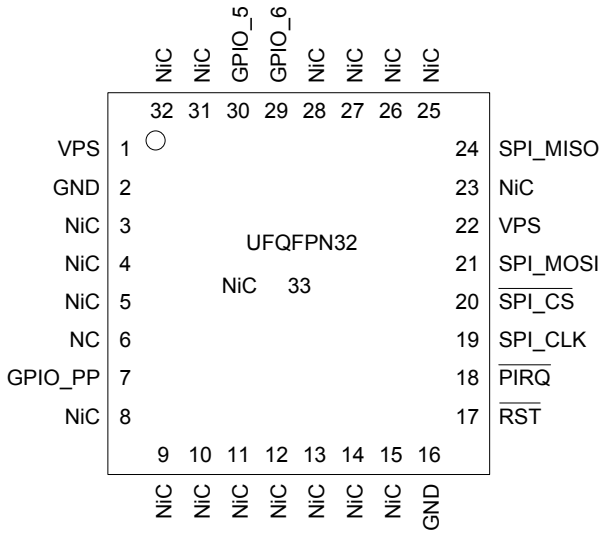


Table 3. UFQFPN32 pin descriptions

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.
$\overline{\text{RST}}$	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)
$\overline{\text{SPI\_CS}}$	Input	***SPI* chip (or slave) select**, internal pull-up (active low; output from master)
$\overline{\text{PIRQ}}$	Output	**IRQ**, active low, open drain, used by the *TPM* to generate an interrupt
GPIO_PP	Input	**Physical presence** (*PP*), active high, internal very weak pull down. Used to indicate physical presence to the *TPM*. The *GPIO* function could be modified by activating the *GPIO*s mapped with the *NV* storage index feature.
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 unused. Must be left unconnected.
GPIO_6	Input/output	General-purpose input/output(1)
GPIO_5	Input/output	General-purpose input/output(1)

1. *The GPIO function could be modified by activating the GPIOs mapped with the NV storage index feature.*

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.

4 Electrical integration guidance

This section gives some guidance on how to integrate the ST33KTPM2XSPI device in an application.

4.1 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}

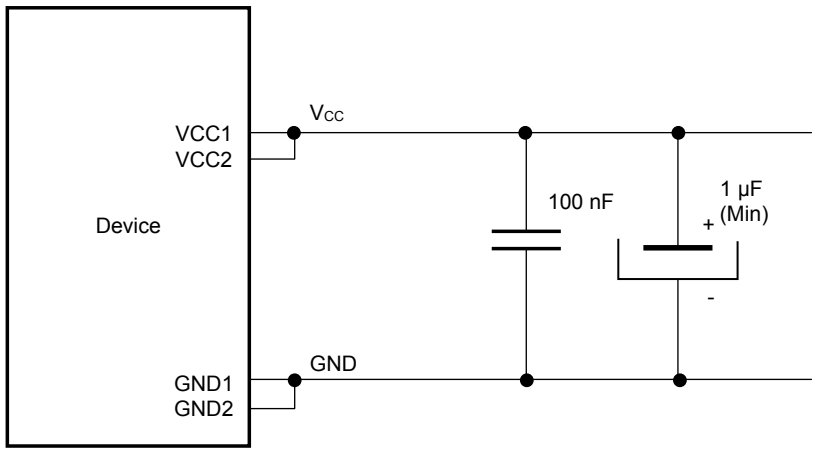


Table 4. V_{CC} rising slope

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	-	$2 \cdot 10^3$	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.

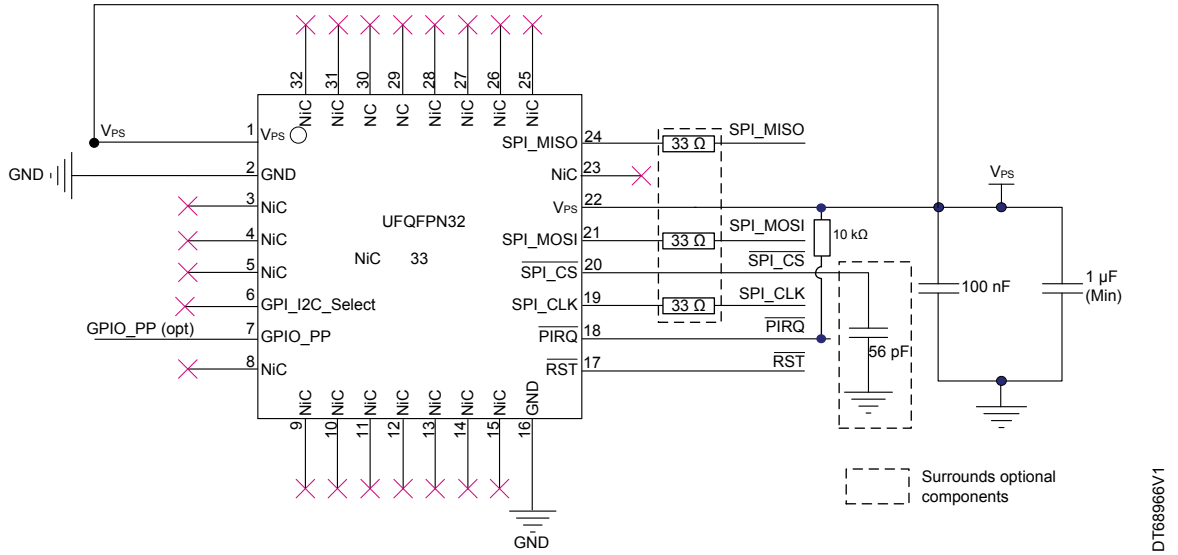
4.2 $\overline{\text{SPI\_CS}}$ optional filtering

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.

4.3 Device integration for SPI communication

The figure below shows the typical hardware implementation of the ST33KTPM2XSPI device for *SPI* communication.

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



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 $\overline{SPI\_CS}$ is optional (see $\overline{SPI\_CS}$ optional filtering).

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

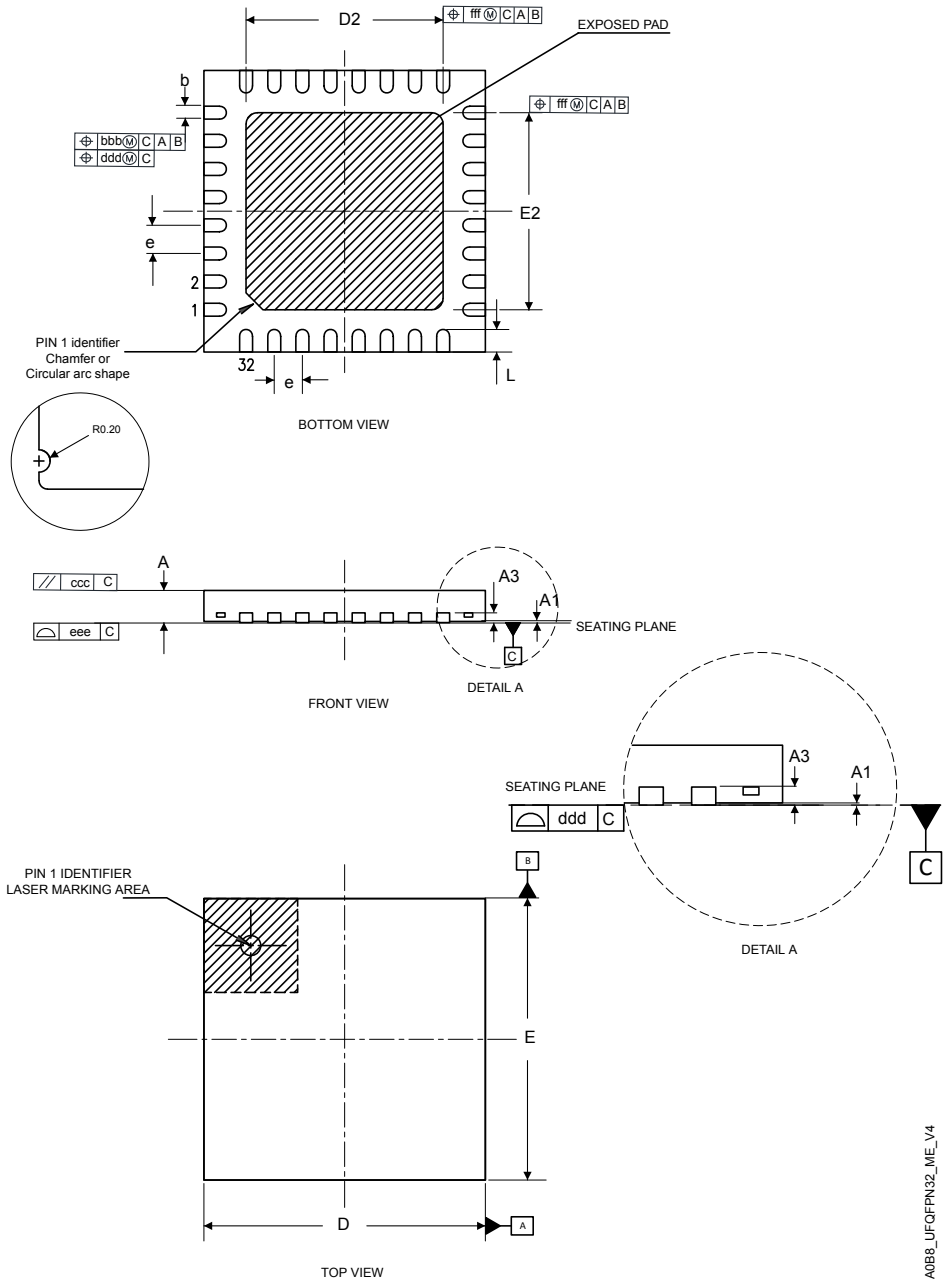
5 Package information

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 UFQFPN32 package information

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

Figure 4. UFQFPN32 - Outline



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.*

3. *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 5. 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	-	-

1. *All dimensions are in millimetres. Dimensioning and tolerancing schemes are conform to ASME Y14.5M-2018 except European .*
2. *Values in inches are converted from mm and rounded to 4 decimal digits.*
3. *UFQFPN stands for Ultra thin Fine pitch Quad Flat Package No lead: A ≤ 0.60mm / Fine pitch e ≤ 1.00mm.*
4. *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.*
5. *A1 is the vertical distance from the bottom surface of the plastic body to the nearest metallized package feature.*
6. *A3 is the distance from the seating plane to the upper surface of the terminals.*
7. *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.*
8. *Dimensions D and E do not include mold protrusion, not to exceed 0,15mm.*
9. *BSC stands for BASIC dimensions. It corresponds to the nominal value and has no tolerance. For tolerances refer to Table 6*
10. *N represents the total number of terminals.*

Table 6. Tolerance of form and position

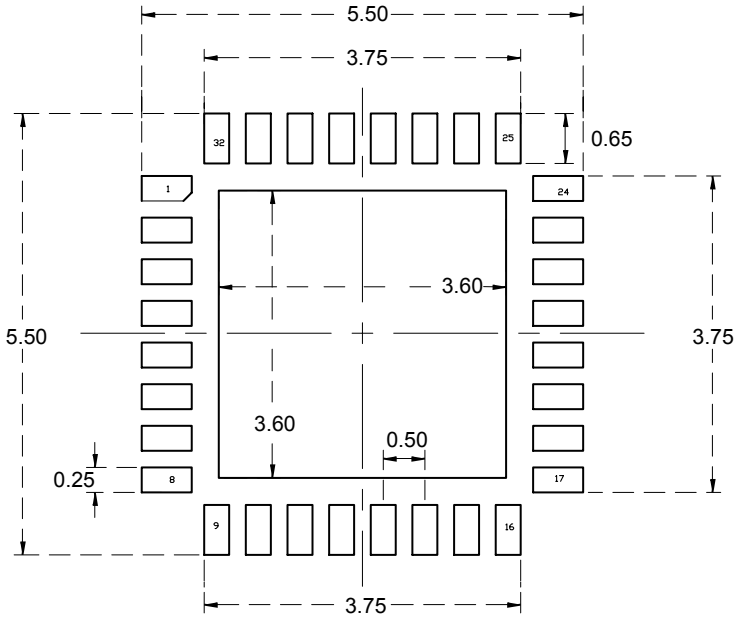
Symbol(1)	Tolerance of form and position(2) In millimeters	Tolerance of form and position(3) In inches
aaa	0.15	0.006
bbb	0.10	0.004
ccc	0.10	0.004
ddd	0.05	0.002
eee	0.10	0.004
fff	0.10	0.004

1. *For the tolerance of form and position definitions see Table 7.*
2. *All dimensions are in millimetres. Dimensioning and tolerancing schemes are conform to ASME Y14.5M-2018 except European .*
3. *Values in inches are converted from mm and rounded to 4 decimal digits.*

Table 7. 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 5. UFQFPN32 - Footprint example



A0B8_UFQFPN32_FP_V1

1. *Dimensions are expressed in millimeters.*

5.1.1 UFQFPN32 thermal characteristics of packages

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

Table 8. 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	−37 to 108 °C
Absolute maximum junction temperature		-	125 °C
Maximum power dissipation		-	66 mW
Theta-JA, -JB and -JC	Junction to ambient thermal resistance	θ_{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
Psi-JT	Junction-to-top of the package thermal characterization parameter	Ψ_{JT}	0.2 °C/W

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

6 UFQFPN32 - tape and reel 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 9. UFQFPN32 - Packages on tape and reel

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

Figure 6. UFQFPN32 - Reel diagram

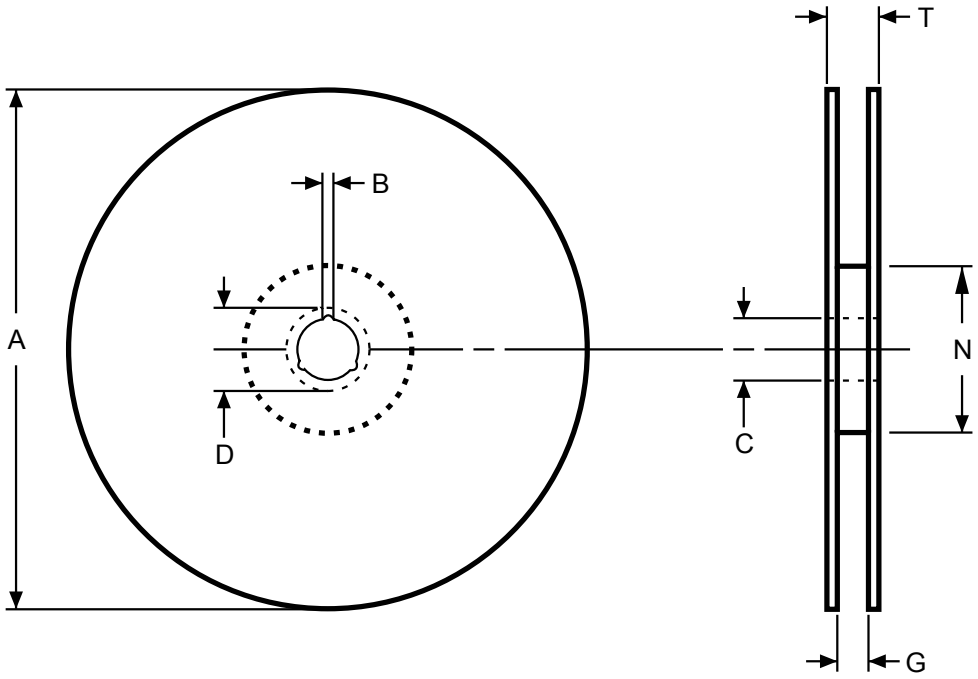
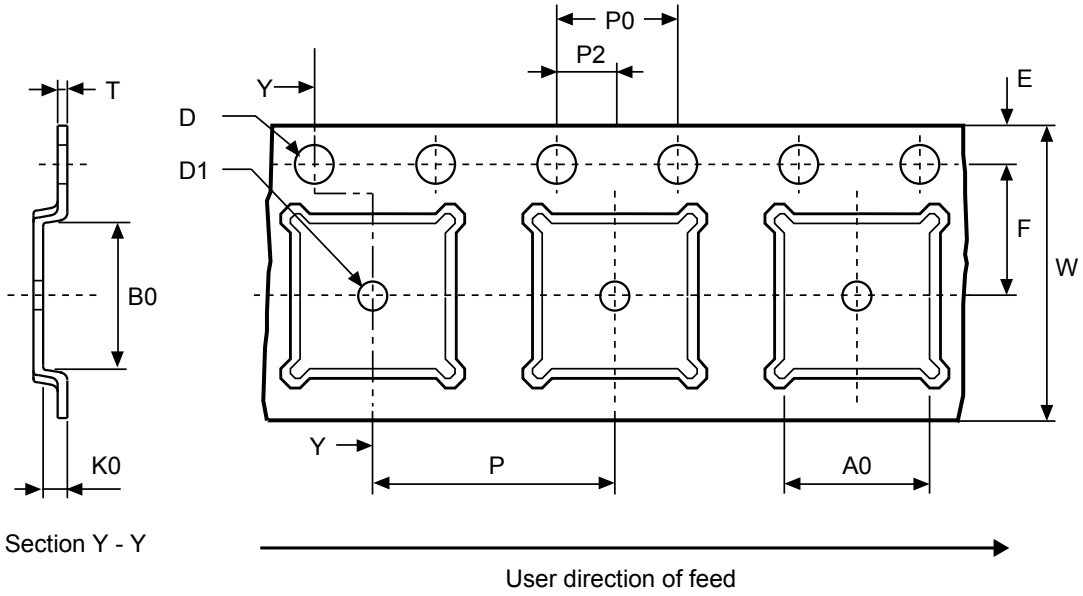


Table 10. UFQFPN32 - Reel dimensions

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 7. UFQFPN32 - Embossed carrier tape



1. *Drawing is not to scale.*

Figure 8. UFQFPN32 - Chip orientation in the embossed carrier tape

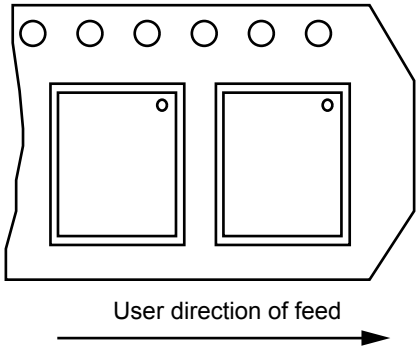


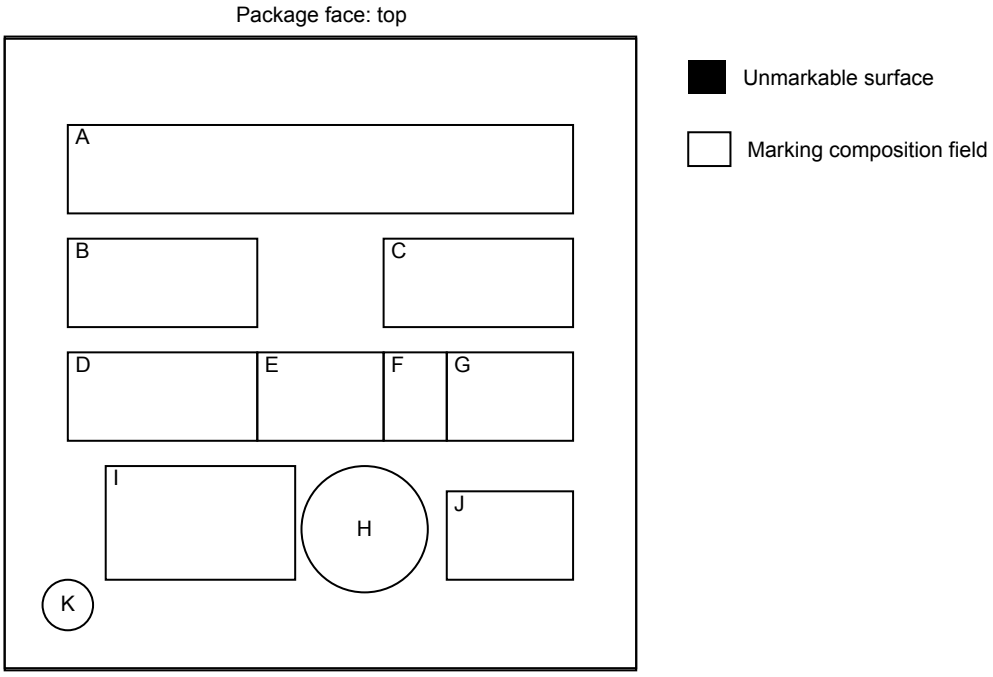
Table 11. UFQFPN32 - Carrier tape dimensions

Package	A0	B0	K0	D1 Min.	P	P2	D	P0	E	F	W	T Max.	Unit
UFQFPN 5×5	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

7 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 9. UFQFPN32 - Standard marking example



Legend:

A: Marking area – Up to 8 digits

B: Marking area – 3 digits

C: BE sequence (LLL)

D: Country of origin (3 characters allowed (max.))

E: Assembly plant (PP)

F: Assembly year (Y)

G: Assembly week (WW)

H: Second level interconnect

I: Standard STMicroelectronics logo

J: Diffusion traceability plant (WX)

K: Dot(1)

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

8 Ordering information

Table 12. **Ordering information**

Ordering code	Product line	Factory firmware version	Package	Minimum ordering quantity	Marking area A	Marking area B
ST33KTPM2X32DKJ0	ST33KTPM2XSPI	0x00.09.02.00 (9.512)	UFQFPN32	3000	KTPM	KJ0
ST33KTPM2X32DKJ5		0x00.09.01.02 (9.258)				KJ5
ST33KTPM2X32DKG8		0x00.09.01.01 (9.257)				KG8
ST33KTPM2X32CKE2		0x00.09.01.00 (9.256)				KE2

9 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.

[FIPS 186-5]	Digital Signature Standard (DSS), NIST
[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 1.5]	Errata Version 1.5 for Trusted Platform Module Library Family 2.0 Revision 1.59, TCG
[PTP 2.0 r1.06]	TCG PC Client Platform TPM Profile (PTP) for TPM 2.0 Version 1.06, 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
[SP800-208]	Recommendation for Stateful Hash-Based Signature Schemes. October 2020, NIST
[Algorithm registry]	TCG Algorithm Registry Family "2.0", Revision 1.32
[Vendor Registry]	TCG TPM Vendor ID Registry Version 1.02 Revision 1.00
[IG FIPS PUB 140-3]	Implementation guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program

Revision history

Table 13. **Document revision history**

Date	Revision	Changes
10-May-2022	1	Initial release.
27-Jan-2023	2	Updated: • TPM features and Hardware features in cover page • Section 1: Description • UFQFPN32 pin and signal description including Figure 1 and Table 3 • Section 3.1: Recommended power supply filtering including Figure 2. Recommended filtering capacitors on V_{CC} and Table 2. V_{CC} rising slope • Section 3.2: SPI_CS optional filtering • Section 3.3 Device integration for SPI communication inlcuding Figure 3. Typical hardware implementation for SPI communication (UFQFPN32 package) • Section 3.4 Device integration for I²C communication including Figure 4. Typical hardware implementation for I²C communication (UFQFPN32 package) • Section 4.1 UFQFPN32 package information: corrected typo on introduction and on line D2 of Table 3. UFQFPN32 - Mechanical data
30-Jan-2024	3	Changed the scope of the document to limit it to ST33KTPM2XSPI (For information on ST33KTPM2XI2C, refer to DB5191). Updated the following sections: • Section Features • Section 1: Description • Section 2: UFQFPN32 pin and signal description • Section 4.1: UFQFPN32 package information • Section 7: Ordering information • Section 3.1: Recommended power supply filtering Added the following sections: • Section 4.2: Thermal characteristics of packages • Appendix A: Referenced documents
20-Jun-2025	4	Added: • Section 2: Product and firmware description Updated: • Section Features • Section 1: Description • Table 3. UFQFPN32 pin descriptions • Table 8. Thermal characteristics • Table 12. Ordering information • Appendix A: Referenced documents

Glossary

3D Three-dimensional

AES Advanced encryption standard

CA Certification Authority

CC Common Criteria

CRT Chinese remainder theorem

DES Data encryption standard

DRBG Deterministic random bit generator

DXE Driver execution environment

EC Elliptic curve

ECC Elliptic curve cryptography

ECDA Elliptic curve direct anonymous attestation

ECDAA Elliptic curve direct anonymous attestation (algorithm)

ECDH Elliptic curve Diffie–Hellman

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

LMS
Leighton–Micali signatures

NIST National Institute of Standards and Technology

NV Nonvolatile

PP Physical presence

PQC Post quantum cryptography

PSS Probabilistic signature scheme

PTP Platform *TPM* Profile

RSA Public-key cryptosystem (created by Ron Rivest, Adi Shamir and Leonard Adleman)

RSAES Rivest Shamir Adelman encryption/decryption scheme

RSASSA Rivest Shamir Adelman signature scheme with appendix

SHA Secure Hash algorithm

SPI Serial peripheral interface

TCG Trusted Computing Group®

TPM Trusted platform module

TRNG True random number generator

TSS TPM software stack

Contents

List of tables

List of figures