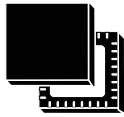


## STSAFE-TPM trusted platform module 2.0 with a SPI or I<sup>2</sup>C interface



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 1.5 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
- *I<sup>2</sup>C* 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
- *NIST* SP800-90A
- *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-PKCS1v1\_5*)
  - *RSA* encryption (*RSAS-ES*, *RSAS-ES-PKCS1v1\_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 **ST33KTPM2X** offers a slave serial peripheral interface (*SPI*) or a target *I<sup>2</sup>C* 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 **ST33KTPM2X** devices are offered in the UFQFPN32 Ecopack2 packages.



## 2 Firmware description

The table below lists the features newly implemented in *TPM* firmware version 0x00.09.02.00 (9.512) compared to the previous *TPM* firmware version.

**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 <i>LMS</i> signature besides <i>ECC NIST P-384</i> for future firmware loading
Configurable background <i>RSA</i> key generation	Background key generation becomes configurable and supports <i>RSA 4096</i> .
<i>FIPS 140-3</i> level 2	Optional mode to support <i>FIPS 140-3</i> level 2 authentication requirements

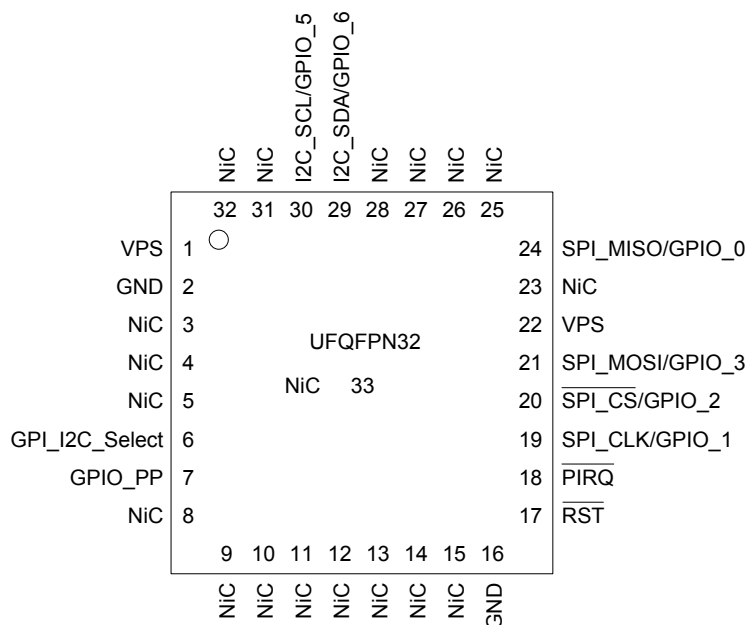
**Table 2. List of changes for parts shipped with factory firmware 9.512**

Item	Description
<i>RSA 3072 EK</i> and <i>EK</i> certificate	<i>RSA 3072 EK</i> and <i>EK</i> 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



DT70357V2

Table 3. UFQFPN32 pin descriptions

Signal	Type	Description
VPS	Input	<b>Power supply.</b> This pin must be connected to 1.8 V or 3.3 V DC power rail supplied by the motherboard.
GND	Input	<b>Ground,</b> has to be connected to the main motherboard ground.
RST	Input	<b>Reset,</b> 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	<b>SPI master input, slave output</b> (output from slave)
SPI_MOSI	Input	<b>SPI master output, slave input</b> (output from master)
SPI_CLK	Input	<b>SPI serial clock</b> (output from master)
SPI_CS	Input	<b>SPI chip (or slave) select,</b> internal pull-up (active low; output from master)
PIRQ	Output	<b>IRQ,</b> active low, open drain, used by the <i>TPM</i> to generate an interrupt
GPIO_PP	Input	<b>Physical presence (PP),</b> active high, internal very weak pull down. Used to indicate physical presence to the <i>TPM</i> . The <i>GPIO</i> function could be modified by activating the <i>GPIOs</i> mapped with the <i>NV</i> storage index feature.
GPI_I2C_Select	Input	This pin must be connected to an external pull-down resistor to activate the <i>I<sup>2</sup>C</i> protocol during product boot time. It can remain unconnected for the <i>SPI</i> protocol. This pin is internal weak pull-up by default and becomes internal floating after <i>I<sup>2</sup>C</i> activation.
NiC	-	<b>Not internally connected:</b> not connected to the die. May be left unconnected but no impact on <i>TPM</i> if connected.
GPIO_X	Input/output	The <i>GPIO</i> function could be modified by activating the <i>GPIOs</i> mapped with the <i>NV</i> storage index feature. <i>GPIO</i> availability is dependent of bus interface (for example, <i>GPIO_5</i> and <i>GPIO_6</i> are available with the <i>SPI</i> interface activated).
I2C_SDA/GPIO_6	Input/output	<b>Bidirectional I<sup>2</sup>C serial data</b> (open drain without a weak pull-up resistor) / General-purpose input/output if <i>SPI</i> is activated <sup>1</sup>
I2C_SCL/GPIO_5	Input	<b>Input I<sup>2</sup>C serial clock</b> (open drain without a weak pull-up resistor) / General-purpose input/output if <i>SPI</i> is activatedGeneral-purpose input/output <sup>1</sup>

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.

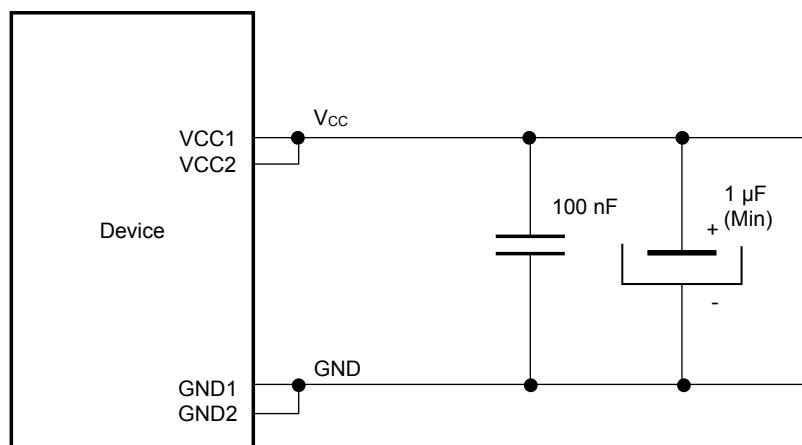
## 4 Electrical integration guidance

This section gives some guidance on how to integrate the ST33KTPM2X 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<sub>CC</sub>**



DT64224V1

**Table 4. V<sub>CC</sub> rising slope**

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

Symbol	Parameter	Min.	Typ.	Max.	Unit
S <sub>VCC</sub>	V <sub>CC</sub> rising slope	2	-	2 · 10 <sup>3</sup>	V/ms

**Note:** Measurement must be done between 1.36 V and 1.62 V. If V<sub>CC</sub> 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.

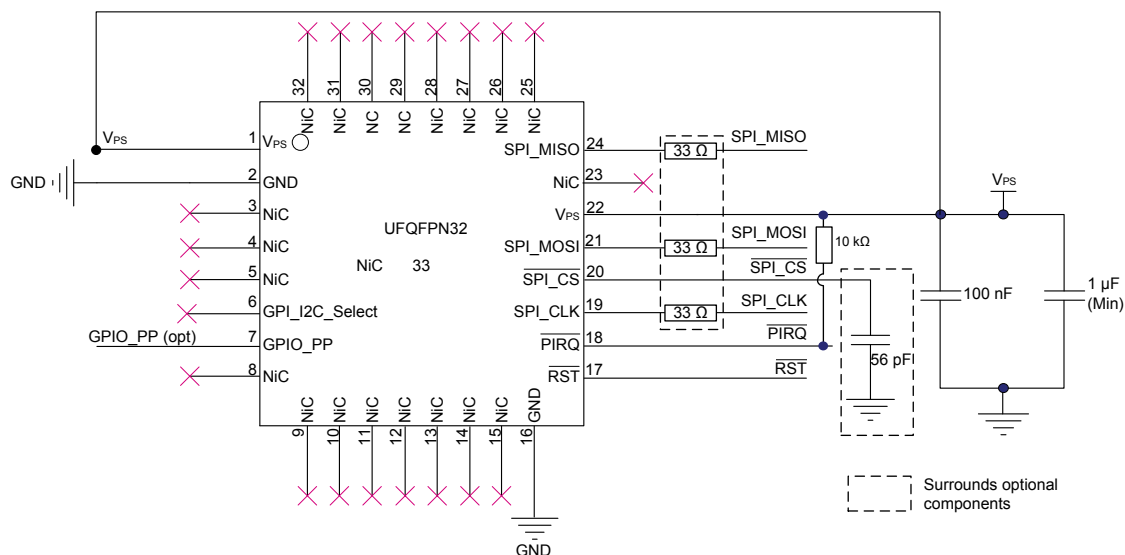
### 4.2 SPI\_CS optional filtering

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 ST33KTPM2X device for SPI communication.

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



**Note:** The use of a low-value resistor (typically 33  $\Omega$ ) 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 SPI\_CS is optional (see [SPI\\_CS optional filtering](#)).

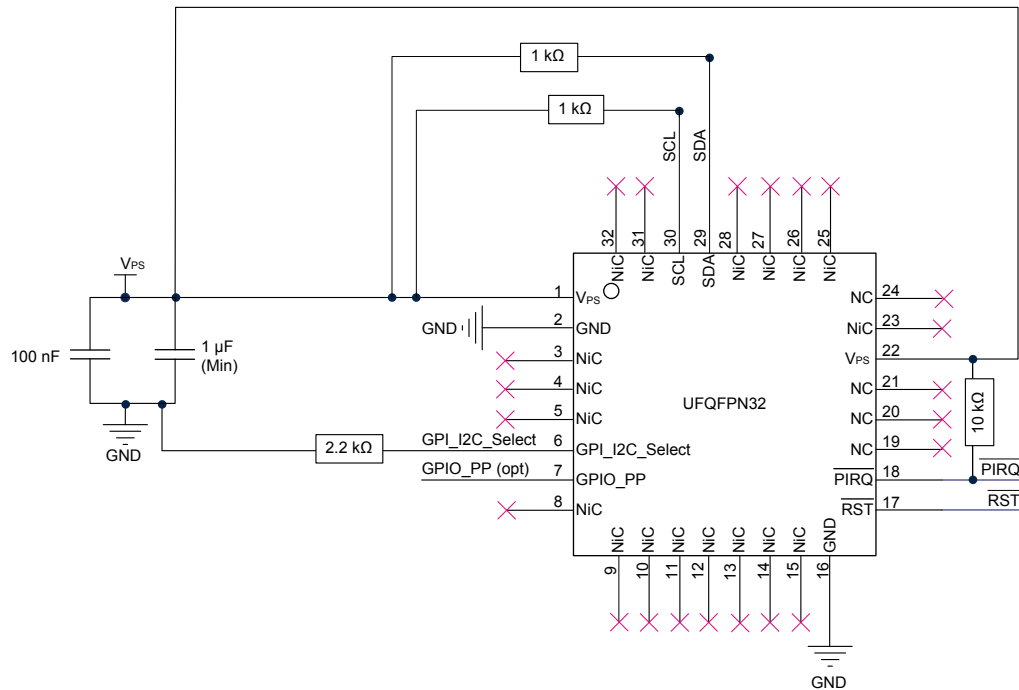
**Note:** The pull-up resistor on the PIRQ line is mandatory to optimize the power consumption in standby mode.



## 4.4 Device integration for I<sup>2</sup>C communication

The figure below shows the typical hardware implementation of the ST33KTPM2X device for I<sup>2</sup>C communication.

**Figure 4. Typical hardware implementation for I<sup>2</sup>C communication (UFQFPN32 package)**



DT68967V2

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

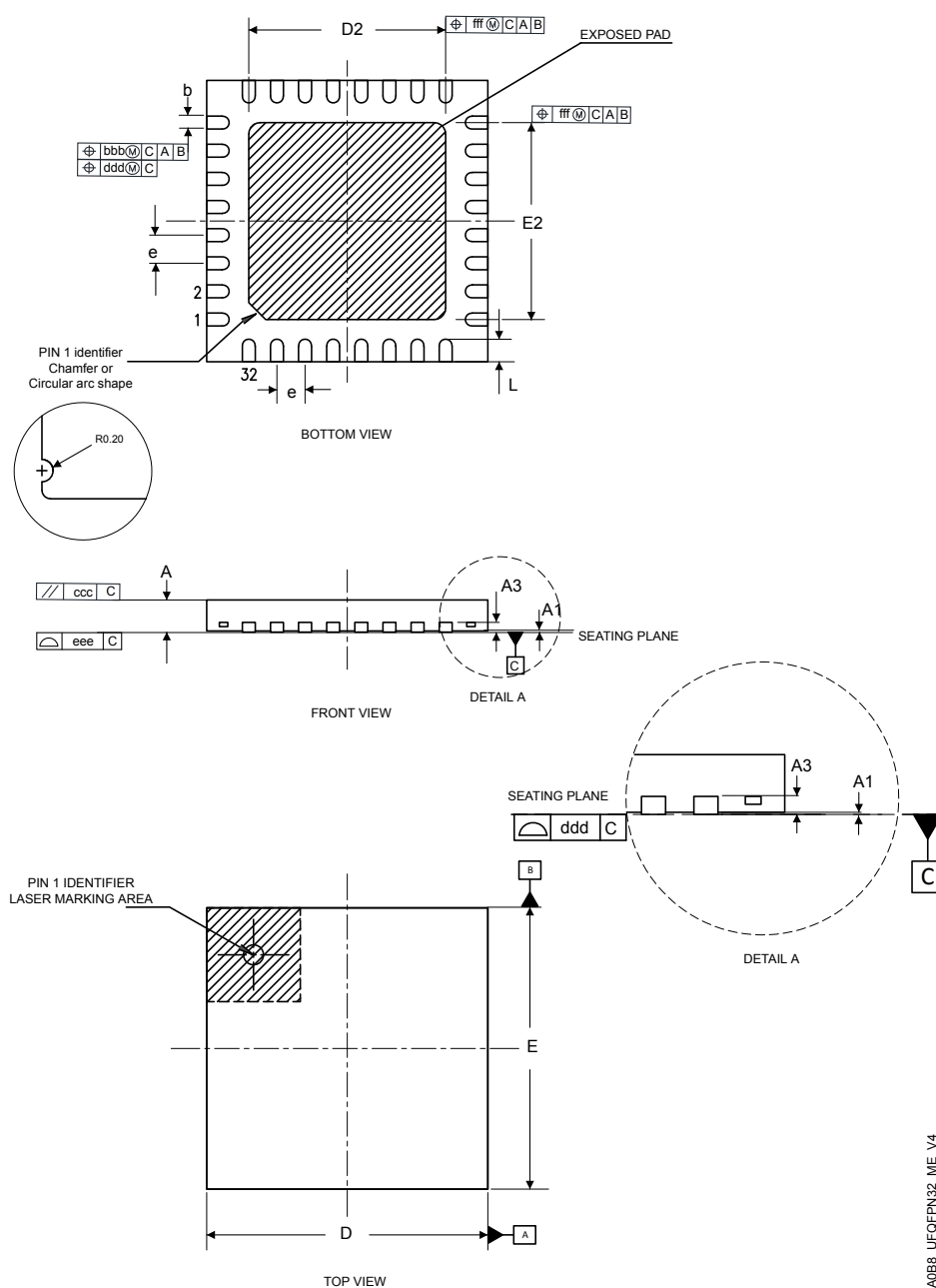
## 5 Package information

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](http://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 5. 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.*

- 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 <sup>(1)</sup>			inches <sup>(2)</sup>		
	Min	Typ	Max	Min	Typ	Max
A <sup>(3)(4)</sup>	0.50	0.55	0.60	0.0197	0.0217	0.0236
A1 <sup>(5)</sup>	0.00	-	0.05	0.000	-	0.0020
A3 <sup>(6)</sup>	-	0.15	-	-	0.0060	-
b <sup>(7)</sup>	0.18	0.25	0.30	0.0071	0.010	0.0118
D <sup>(8)(9)</sup>	5.00 BSC			0.1969 BSC		
D2	3.50	3.60	3.70	0.139	0.143	0.147
E <sup>(8)(9)</sup>	5.00 BSC			0.1969 BSC		
E2	3.50	3.60	3.70	0.139	0.143	0.147
e <sup>(9)</sup>	-	0.50	-	-	0.02	-
N <sup>(10)</sup>	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 6
- N represents the total number of terminals.

**Table 6. Tolerance of form and position**

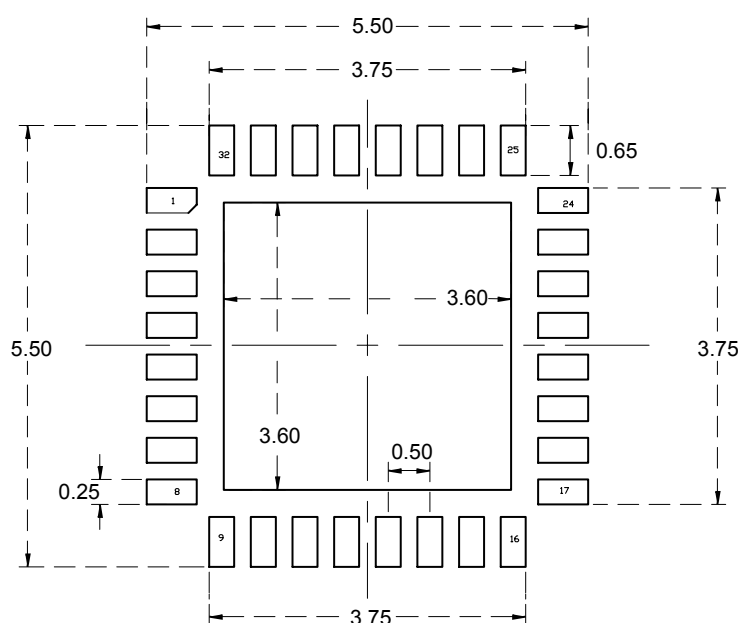
Symbol <sup>(1)</sup>	Tolerance of form and position <sup>(2)</sup>	Tolerance of form and position <sup>(3)</sup>
	In millimeters	In inches
aaa	0.15	0.006
bbb	0.10	0.004
ccc	0.10	0.004
ddd	0.05	0.002
eee	0.10	0.004
fff	0.10	0.004

- For the tolerance of form and position definitions see Table 7.
- 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 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 6. UFQFPN32 - Footprint example**



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	$\theta_{JA}^{(1)}$	35 °C/W
	Junction to case thermal resistance	$\theta_{JC}$	5 °C/W
	Junction to board thermal resistance	$\theta_{JB}$	20 °C/W

1. According to JE5D51-2 (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.

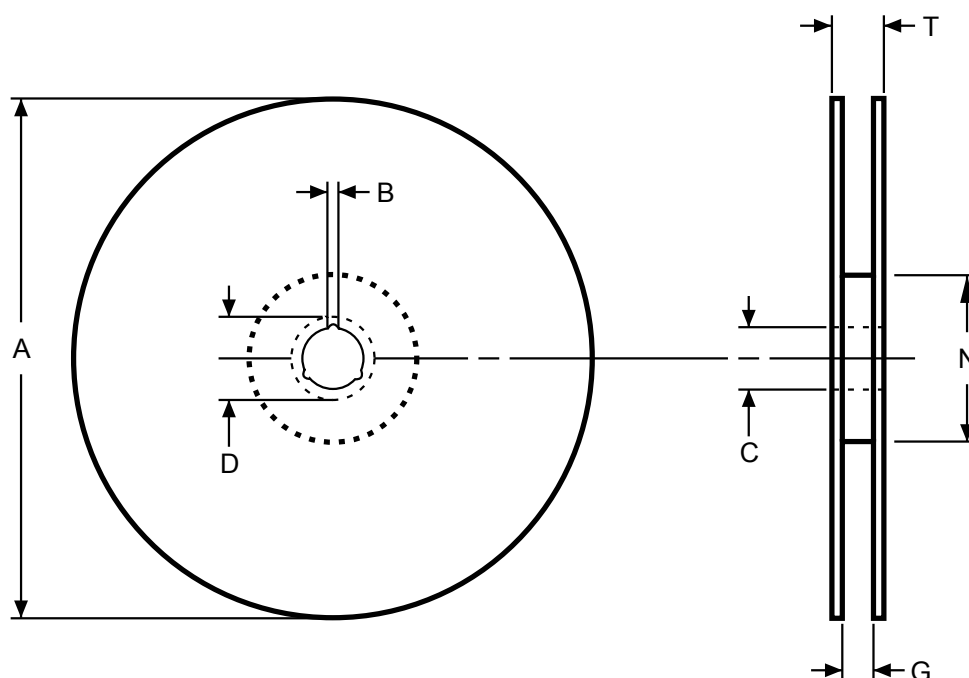
The devices are positioned in the cavities with the identifying pin (normally pin "1") on the same side as the sprocket holes in the tape.

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

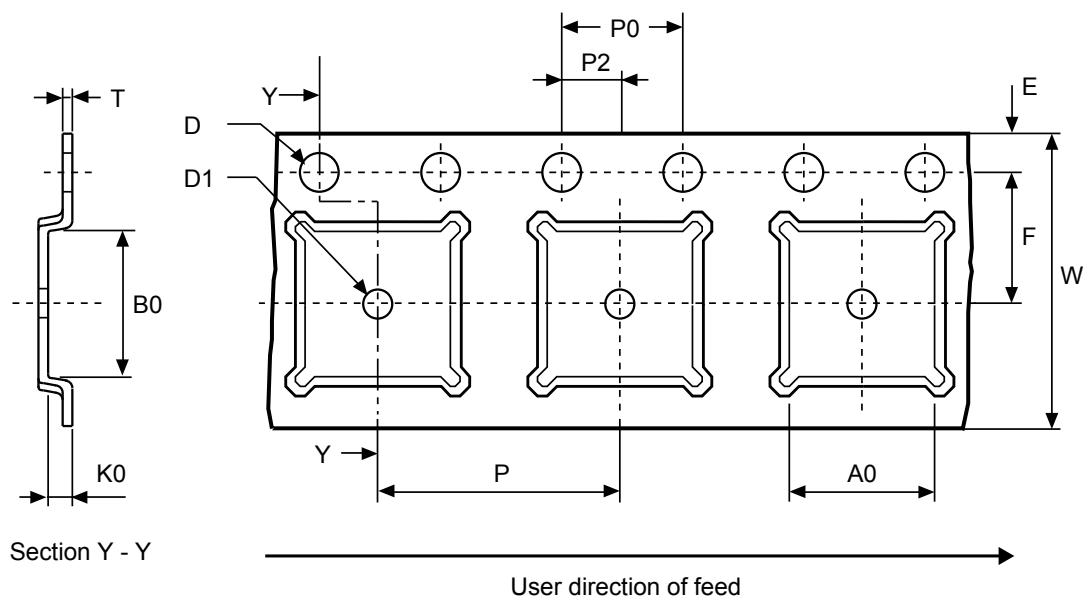
**Figure 7. UFQFPN32 - Reel diagram**



**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 8. UFQFPN32 - Embossed carrier tape



1. Drawing is not to scale.

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

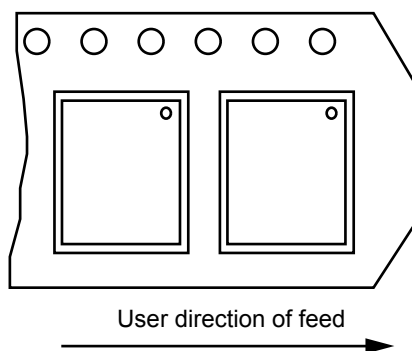


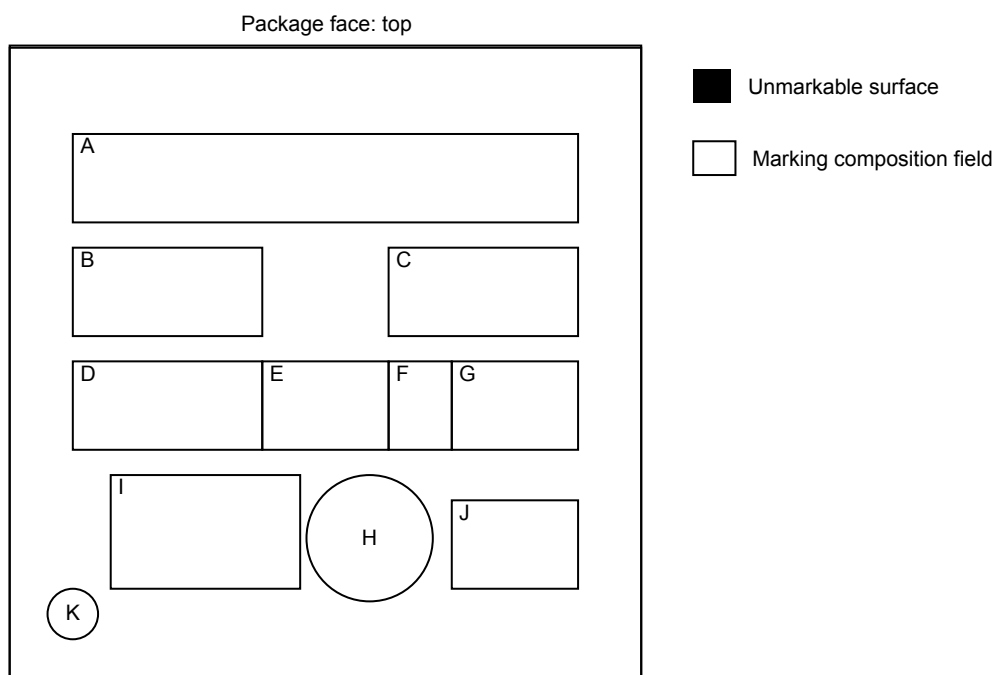
Table 11. UFQFPN32 - Carrier tape dimensions

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

## 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 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 <sup>(1)</sup>                |
| F: Assembly year (Y)                               |                                      |

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
ST33KTPM2X32DKJ1	ST33KTPM2X	0x00.09.02.00 (9.512)	UFQFPN32	3000	KTPM	KJ1
ST33KTPM2X32DKG9		0x00.09.01.01 (9.257)				KG9
ST33KTPM2X32CKE3	ST33KTPM2XI2C	0x00.09.01.00 (9.256)				KE3

**Note:** The **ST33KTPM2X** supports exactly the same features as product **ST33KTPM2XI2C** and both support the same firmware images. The **ST33KTPM2XI2C** is re-branded to **ST33KTPM2X** as both products support both the SPI and I<sup>2</sup>C interfaces.

The **ST33KTPM2X** and **ST33KTPM2XI2C** products do not share the same production sites.

## 9 Support and information

---

Additional information regarding ST TPM devices can be obtained from the [www.st.com](http://www.st.com) website.

For any specific support information you can contact STMicroelectronics through the following e-mail:  
*[tpmsupport@list.st.com](mailto: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
15-Dec-2023	1	Initial release.
23-Apr-2024	2	Updated: <ul style="list-style-type: none"> <li>Section 7: Ordering information</li> </ul>
30-May-2025	3	Added: <ul style="list-style-type: none"> <li>Section 2: Firmware description</li> </ul> Updated: <ul style="list-style-type: none"> <li>Section Features</li> <li>Section 1: Description</li> <li>Table 3. UFQFPN32 pin descriptions</li> <li>Section 5.1.1: UFQFPN32 thermal characteristics of packages</li> <li>Section 8: Ordering information</li> <li>Appendix A: Referenced documents</li> </ul>

## Glossary

<b>3D</b> Three-dimensional	<b>MCU</b> Microcontroller unit
<b>AES</b> Advanced encryption standard	<b>NIST</b> National Institute of Standards and Technology
<b>CA</b> Certification Authority	<b>NV</b> Nonvolatile
<b>CC</b> Common Criteria	<b>PKCS</b> Public key cryptographic standards
<b>CRC</b> Cyclic redundancy check	<b>PP</b> Physical presence
<b>CRT</b> Chinese remainder theorem	<b>PQC</b> Post quantum cryptography
<b>DES</b> Data encryption standard	<b>PSS</b> Probabilistic signature scheme
<b>DRBG</b> Deterministic random bit generator	<b>PTP</b> Platform <i>TPM</i> Profile
<b>DXE</b> Driver execution environment	<b>RNG</b> Random number generator
<b>EC</b> Elliptic curve	<b>RSA</b> Public-key cryptosystem (created by Ron Rivest, Adi Shamir and Leonard Adleman)
<b>ECC</b> Elliptic curve cryptography	<b>RSAES</b> Rivest Shamir Adelman encryption/decryption scheme
<b>ECDA</b> Elliptic curve direct anonymous attestation	<b>RSASSA</b> Rivest Shamir Adelman signature scheme with appendix
<b>ECDAA</b> Elliptic curve direct anonymous attestation (algorithm)	<b>SHA</b> Secure Hash algorithm
<b>ECDH</b> Elliptic curve Diffie–Hellman	<b>SPI</b> Serial peripheral interface
<b>ECDSA</b> Elliptic curve digital signature algorithm	<b>TCG</b> Trusted Computing Group®
<b>EK</b> Endorsement key	<b>TDES</b> Triple DES cryptographic algorithm
<b>ESD</b> Electrostatic discharge	<b>TPM</b> Trusted platform module
<b>FIPS</b> Federal Information Processing Standards	<b>TRNG</b> True random number generator
<b>GPIO</b> General purpose input/output	<b>TSS</b> TPM software stack
<b>HBM</b> Human body model	
<b>HMAC</b> Hash-based message authentication code or keyed-hash message authentication code	
<b>I<sup>2</sup>C</b> Inter-integrated circuit	
<b>LMS</b> Leighton–Micali signatures	

## Contents

<b>1</b>	<b>Description .....</b>	<b>3</b>
<b>2</b>	<b>Firmware description .....</b>	<b>4</b>
<b>3</b>	<b>UFQFPN32 pin and signal description.....</b>	<b>5</b>
<b>4</b>	<b>Electrical integration guidance.....</b>	<b>7</b>
4.1	Recommended power supply filtering.....	7
4.2	SPI_CS optional filtering .....	7
4.3	Device integration for SPI communication .....	8
4.4	Device integration for I <sup>2</sup> C communication .....	9
<b>5</b>	<b>Package information.....</b>	<b>10</b>
5.1	UFQFPN32 package information .....	10
5.1.1	UFQFPN32 thermal characteristics of packages.....	13
<b>6</b>	<b>UFQFPN32 - tape and reel delivery packing .....</b>	<b>14</b>
<b>7</b>	<b>UFQFPN32 package marking information .....</b>	<b>16</b>
<b>8</b>	<b>Ordering information .....</b>	<b>17</b>
<b>9</b>	<b>Support and information.....</b>	<b>18</b>
<b>Appendix A</b>	<b>Referenced documents .....</b>	<b>19</b>
	<b>Revision history .....</b>	<b>20</b>
	<b>List of tables .....</b>	<b>23</b>
	<b>List of figures.....</b>	<b>24</b>

## List of tables

<b>Table 1.</b>	List of new features supported by firmware version 9.512 . . . . .	4
<b>Table 2.</b>	List of changes for parts shipped with factory firmware 9.512. . . . .	4
<b>Table 3.</b>	UFQFPN32 pin descriptions . . . . .	6
<b>Table 4.</b>	V <sub>CC</sub> rising slope. . . . .	7
<b>Table 5.</b>	UFQFPN32 - Mechanical data . . . . .	11
<b>Table 6.</b>	Tolerance of form and position . . . . .	11
<b>Table 7.</b>	Tolerance of form and position symbol definition . . . . .	12
<b>Table 8.</b>	Thermal characteristics. . . . .	13
<b>Table 9.</b>	UFQFPN32 - Packages on tape and reel . . . . .	14
<b>Table 10.</b>	UFQFPN32 - Reel dimensions. . . . .	14
<b>Table 11.</b>	UFQFPN32 - Carrier tape dimensions . . . . .	15
<b>Table 12.</b>	Ordering information. . . . .	17
<b>Table 13.</b>	Document revision history . . . . .	20

## List of figures

<b>Figure 1.</b>	UFQFPN32 pinout . . . . .	5
<b>Figure 2.</b>	Recommended filtering capacitors on $V_{CC}$ . . . . .	7
<b>Figure 3.</b>	Typical hardware implementation for SPI communication (UFQFPN32 package). . . . .	8
<b>Figure 4.</b>	Typical hardware implementation for $I^2C$ communication (UFQFPN32 package) . . . . .	9
<b>Figure 5.</b>	UFQFPN32 - Outline . . . . .	10
<b>Figure 6.</b>	UFQFPN32 - Footprint example . . . . .	12
<b>Figure 7.</b>	UFQFPN32 - Reel diagram . . . . .	14
<b>Figure 8.</b>	UFQFPN32 - Embossed carrier tape . . . . .	15
<b>Figure 9.</b>	UFQFPN32 - Chip orientation in the embossed carrier tape . . . . .	15
<b>Figure 10.</b>	UFQFPN32 - Standard marking example . . . . .	16



**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](http://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.

© 2025 STMicroelectronics – All rights reserved