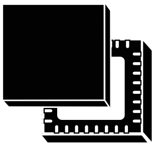
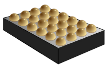
ST33KTPM2I

Data brief

STSAFE-TPM for consumer and industrial applications



UFQFPN32 WF (5 × 5 × 0.55 mm)



WLCSP24 (1.81 × 2.59 × 0.31 mm)

Product status link
ST33KTPM2I

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 1.06
- 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

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
- *SPI* support at up to 48 MHz
- *I²C* support at up to 1 MHz

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, Brainpool P_256/384/512_R1, BN P_256, Curve448)
  - *ECC* secret sharing (*ECDH*, X448)
  - *ECC* signature (*ECDSA*, ECSchnorr, *ECDAA*, Ed448)
- 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 all Common Criteria (EAL4+), and *FIPS* 140-3 certification.

The ST33KTPM2I, by default, offers two exclusive configurations:

- a slave serial peripheral interface (*SPI*)
- a target I^2C interface.

Both of these configurations are 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 ST33KTPM2I operates in the –40 °C to 105 °C extended temperature range.

The ST33KTPM2I devices are qualified for industrial and consumer applications and are offered in TCG standardized UFQFPN32 wettable flanks and WLCSP24 packages.

LICENSED
DPA
COUNTERMEASURES™

2 Firmware description

The table below lists the features newly implemented in *TPM* firmware version 0x00.0A.02.00 (10.512) compared to the previous *TPM* firmware version.

Table 1. **List of new features supported by firmware version 10.512**

Item	Description
PTP 1.06	Compliance with *TCG* Pc Client *TPM* Profile 1.06
ECC NIST P-521	Support of *NIST* P-521 curve
SHA-512	Support of SHA-512
Ed448	Support of Ed448 signature algorithm
X448	Support of X448 key agreement algorithm
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.
Brainpool	Support Brainpool curves P256_R1, P384_R1 and P512_R1
Hibernate power state	Support of hibernate state
FIPS 140-3 level 2	Optional mode to support *FIPS* 140-3 level 2 evaluation requirements

Table 2. **List of changes for parts shipped with factory firmware 10.512**

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

3 Pin and signal description

3.1 TCG standard package

3.1.1 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

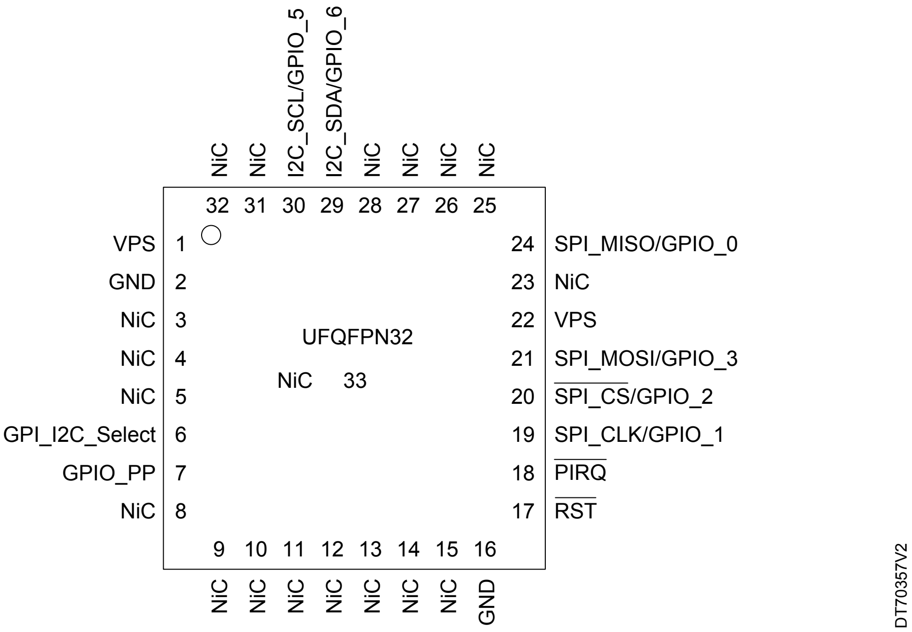


Table 3. **UFQFPN32 pin descriptions**

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/GPIO_0	Output[1]	***SPI* master input, slave output** (output from slave) / General-purpose input/output if I^{2}C is activated
SPI_MOSI/GPIO_3	Input[1]	***SPI* master output, slave input** (output from master) / General-purpose input/output if I^{2}C is activated
SPI_CLK/GPIO_1	Input[1]	***SPI* serial clock** (output from master) / General-purpose input/output if I^{2}C is activated
$\overline{\text{SPI\_CS}}$/GPIO_2	Input[1]	***SPI* chip (or slave) select**, internal pull-up (active low; output from master) / General-purpose input/output if I^{2}C is activated
$\overline{\text{PIRQ}}$	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*.
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 weak 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.
I2C_SDA/GPIO_6	Input/ output[1]	**Bidirectional *I^{2}C* serial data** (open drain without a weak pull-up resistor) / General-purpose input/output if *SPI* is activated
I2C_SCL/GPIO_5	Input[1]	**Input *I^{2}C* serial clock** (open drain without a weak pull-up resistor) / General-purpose input/output if *SPI* is activated

[1] *In GPIO configuration, this signal is Input/output.*

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.*

3.2 Optimized packages

3.2.1 WLCSP24 ballout and signal description

The figures below show the WLCSP24 ballout, and Table 4 provides the ball description.

This package is available for the ST33KTPM2I device.

Figure 2. WLCSP 24 ballout - bottom view (balls side)

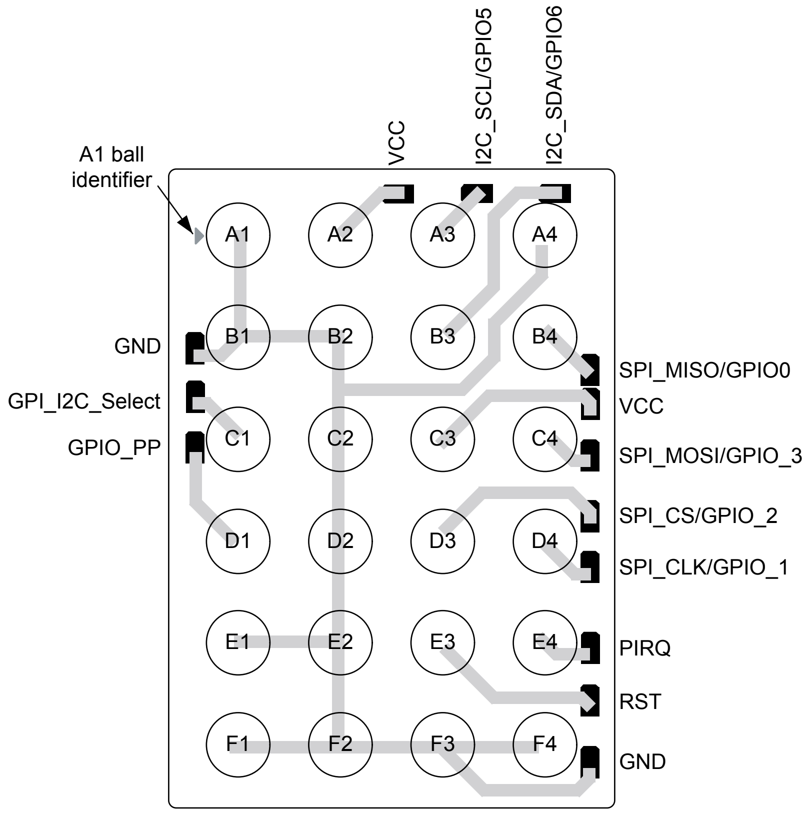


Table 4. **WLCSP24 ball description**

Ball number	Signal	Type	Description
A1	GND	Input	**Ground**, has to be connected to the main motherboard ground.
A2	VCC	Input	**Power supply**. This pin must be connected to 1.8 V or 3.3 V DC power rail supplied by the motherboard.
A3	I2C_SCL/ GPIO_5	Input[1]	**Input *I^2C* serial clock** (open drain without a weak pull-up resistor) / General-purpose input/output if *SPI* is activated
A4	GND	Input	**Ground**, has to be connected to the main motherboard ground.
B1	GND	Input	**Ground**, has to be connected to the main motherboard ground.
B2	GND	Input	**Ground**, has to be connected to the main motherboard ground.
B3	I2C_SDA/ GPIO_6	Input/output[1]	**Bidirectional *I^2C* serial data** (open drain without a weak pull-up resistor) / General-purpose input/output if *SPI* is activated
B4	SPI_MISO/ GPIO_0	Output	***SPI* master input, slave output** (output from slave) / General-purpose input/output if I^2C is activated
C1	GPI_I2C_Select	Input	This pin must be connected to an external pull-down resistor to activate the *I^2C* protocol during product boot time. It can remain unconnected for the *SPI* protocol. This pin is internal weak pull-up by default and becomes internal floating after *I^2C* activation.
C2	GND	Input	**Ground**, has to be connected to the main motherboard ground.
C3	VCC	Input	**Power supply**. This pin must be connected to 1.8 V or 3.3 V DC power rail supplied by the motherboard.
C4	SPI_MOSI/ GPIO_3	Input[1]	***SPI* master output, slave input** (output from master) / General-purpose input/output if I^2C is activated
D1	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.
D2	GND	Input	**Ground**, has to be connected to the main motherboard ground.
D3	$\overline{\text{SPI\_CS}}$/ GPIO_2	Input[1]	***SPI* chip (or slave) select**, internal pull-up (active low; output from master) / General-purpose input/output if I^2C is activated
D4	SPI_CLK/ GPIO_1	Input[1]	***SPI* serial clock** (output from master) / General-purpose input/output if I^2C is activated
E1	GND	Input	**Ground**, has to be connected to the main motherboard ground.
E2	GND	Input	**Ground**, has to be connected to the main motherboard ground.
E3	$\overline{\text{RST}}$	Input	**Reset**, active low, used to re-initialize the device. Must not be unconnected. External pull-up resistor required if it cannot be driven.
E4	$\overline{\text{PIRQ}}$	Output	**IRQ**, active low, open drain, used by the *TPM* to generate an interrupt
F1	GND	Input	**Ground**, has to be connected to the main motherboard ground.
F2	GND	Input	**Ground**, has to be connected to the main motherboard ground.
F3	GND	Input	**Ground**, has to be connected to the main motherboard ground.
F4	GND	Input	**Ground**, has to be connected to the main motherboard ground.

[1] *In GPIO configuration, this signal is Input/output.*

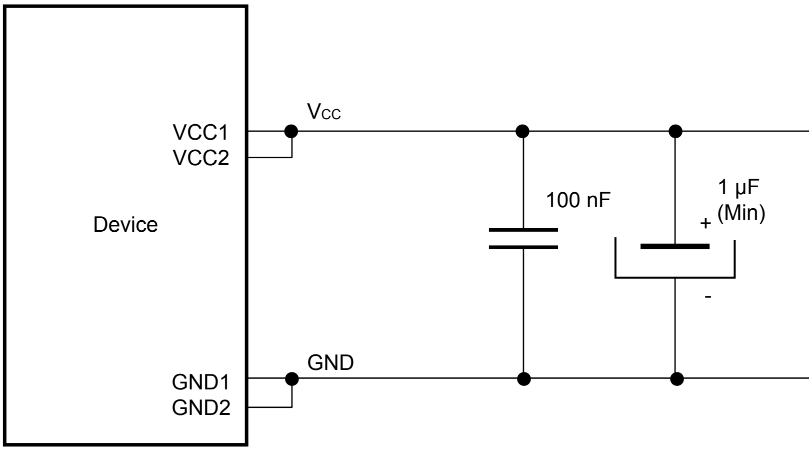
4 Electrical integration guidance

This section gives some guidance on how to integrate the ST33KTPM2I 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 3. Recommended filtering capacitors on V_{CC}



DT64224V1

Table 5. 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.

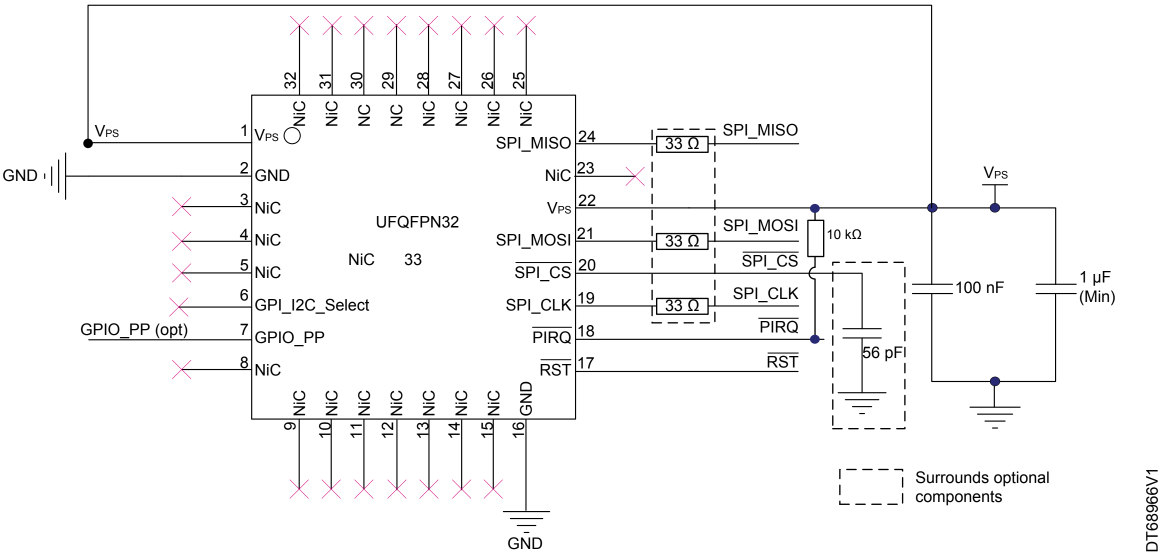
4.2 $\overline{\text{SPI\_CS}}$ optional filtering

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 ST33KTPM2I device for *SPI* communication.

Figure 4. 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.*

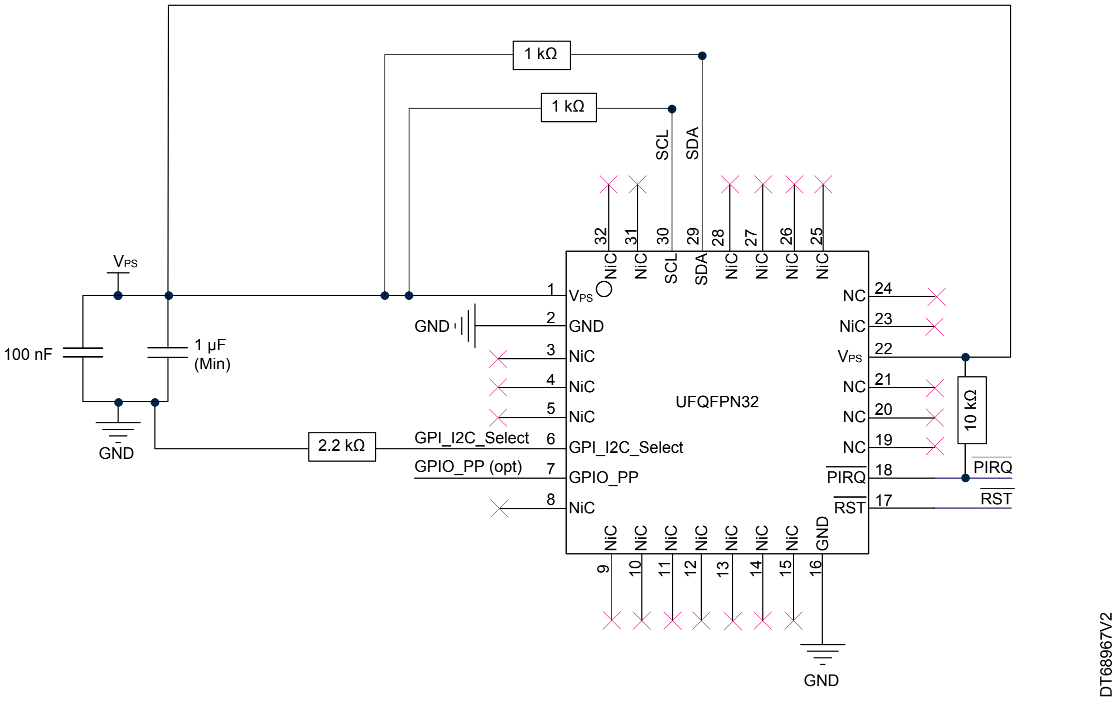
Note: *The capacitor on $\overline{\text{SPI\_CS}}$ is optional (see $\overline{\text{SPI\_CS}}$ optional filtering).*

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

4.4 Device integration for I²C communication

The figure below shows the typical hardware implementation of the ST33KTPM2I device for *I²C* communication.

Figure 5. Typical hardware implementation for *I²C* communication (UFQFPN32 package)



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

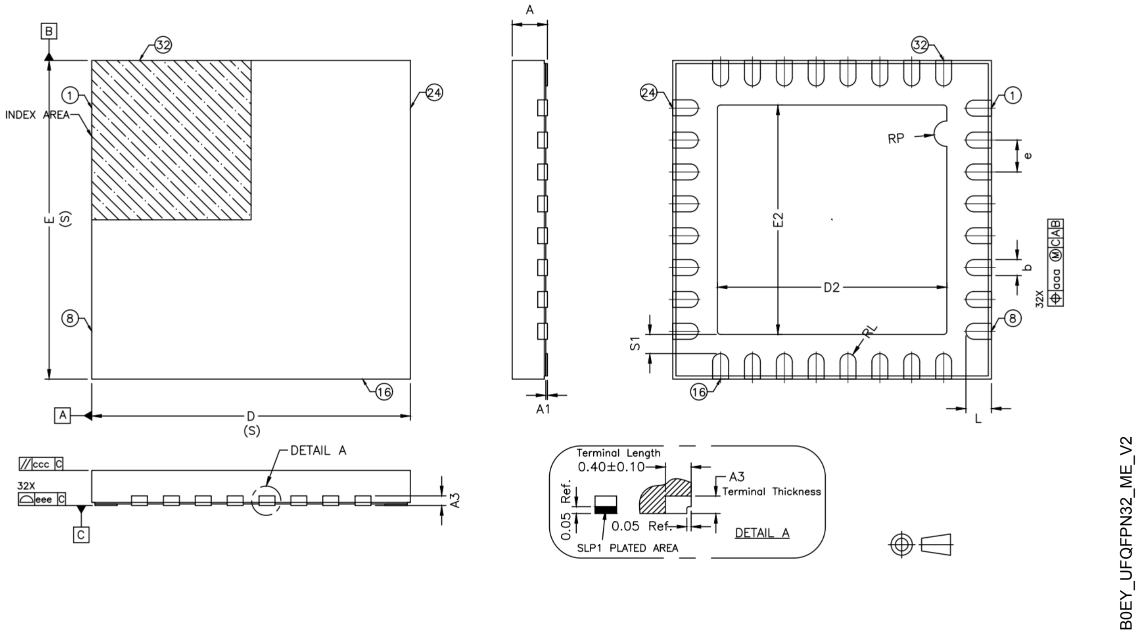
5 Package information

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 lead wettable flank, 5x5 mm, 0.5 mm pitch ultra thin fine pitch quad flat package.

Figure 6. UFQFPN32 - Outline



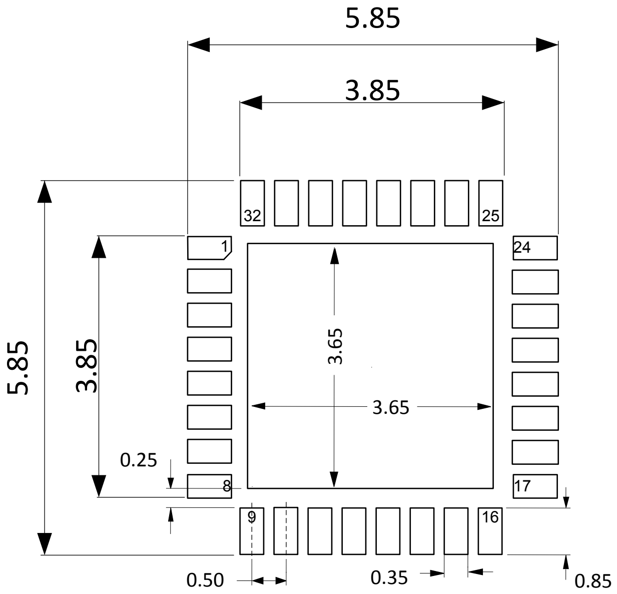
1. *Drawing is not to scale.*
2. *Coplanarity applies to the exposed pad as well as the terminal.*

Table 6. **UFQFPN32 - Mechanical data**

Symbol	millimeters			inches[1]		
	Min	Typ	Max	Min	Typ	Max
A	0.50	0.55	0.65	0.0197	0.0217	0.0256
A1	-	0.05	-	-	0.0020	-
A3	0.152 ref.			0.0060 ref.		
L	0.30	0.40	0.50	0.0118	0.0157	0.0196
b	0.18	0.25	0.30	0.0071	0.0098	0.0118
D	5.00 BSC			0.1968 BSC		
E	5.00 BSC			0.1968 BSC		
e	0.50 BSC			0.0197 BSC		
D2	3.50	3.65	3.80	0.1377	0.1437	0.1496
E2	3.50	3.65	3.80	0.1377	0.1437	0.1496
S1	0.30 ref.			0.0118 ref.		
N[2]	32					
bbb	-	0.10	-	-	0.0039	-
ccc	-	0.10	-	-	0.0039	-
eee	-	0.08	-	-	0.0031	-

1. *Values in inches are converted from mm and rounded to 4 decimal digits.*
2. *Total number of terminals.*

Figure 7. **UFQFPN32 - PCB footprint example**



B0EY_UFQFPN32_FP_V2

1. *Dimensions are expressed in millimetres.*
2. *Pin 1 is identified in the PCB footprint example. The location of this pin must be identified using the customer manufacturing process.*

5.1.1 UFQFPN32 thermal characteristics of packages

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

Table 7. **Thermal characteristics**

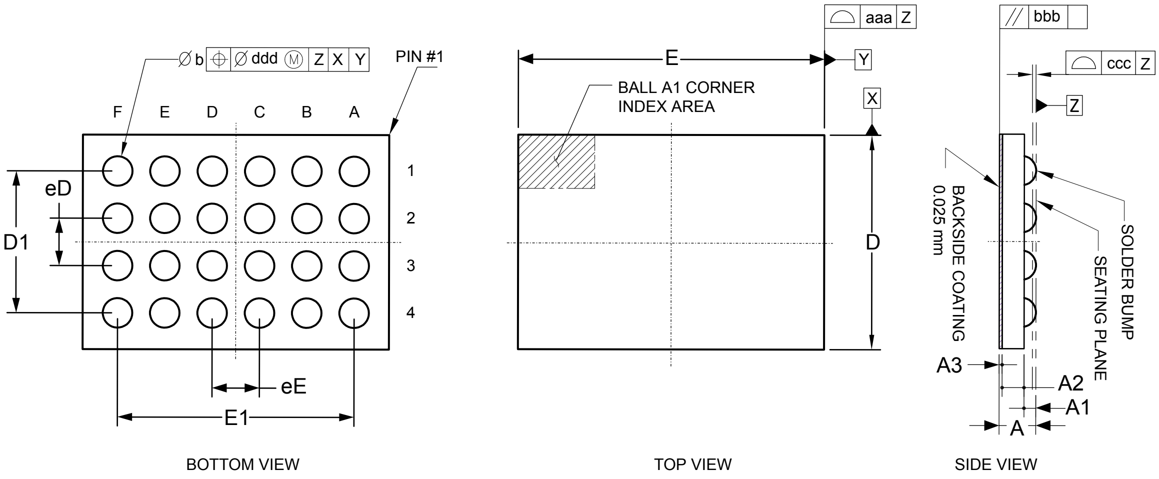
Parameter		Symbol	Value
Recommended operating temperature range	Ambient temperature	T_A	−40 to 105 °C
	Case temperature	T_C	-
	Junction temperature	T_J	−37 to 108 °C
Absolute maximum junction temperature		-	125 °C
Maximum power dissipation		-	66 mW
Theta-JA, -JB and -JC	Junction to ambient thermal resistance	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

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

5.2 WLCSP24 package information

This WLCSP is a 24-ball, 1.812 × 2.589 mm, 0.40 mm pitch, wafer level chip scale package.

Figure 8. **WLCSP24 - Outline**



1. *Drawing is not to scale.*
2. *Dimension is measured at the maximum bump diameter parallel to primary datum Z.*
3. *Primary datum Z and seating plane are defined by the spherical crowns of the ball.*
4. *Ball position designation as per JESD 95-1, SPP-010.*

Table 8. **WLCSP24 - Mechanical data**

Symbol	Millimeters			Inches[1]		
	Min.	Typ.	Max.	Min.	Typ.	Max.
A	0.290	0.310	0.330	0.0114	0.0122	0.0129
A1	0.090	0.100	0.100	0.0035	0.0039	0.0039
A2	0.173	0.185	0.198	0.0068	0.0072	0.0078
A3[2]	-	0.025	-	-	0.0010	-
b[3]	0.225	0.250	0.275	0.0088	0.0098	0.0108
D	1.787	1.812	1.837	0.0703	0.0713	0.0723
E	2.564	2.589	2.614	0.101	1.0102	0.103
eD	-	0.400	-	-	0.0157	-
eE	-	0.400	-	-	0.0157	-
D1	-	1.200	-	-	0.0472	-
E1	-	2.000	-	-	0.0787	-
aaa	-	-	0.030	-	-	0.0012
bbb	-	-	0.060	-	-	0.0023
ccc	-	-	0.050	-	-	0.0020
ddd	-	-	0.015	-	-	0.0006

1. *Values in inches are converted from mm and rounded to 3 decimal digits.*
2. *Back side coating.*
3. *Dimension is measured at the maximum bump diameter parallel to primary datum Z.*

5.2.1 PCB design and reflow recommendations

The recommendations provided in this section apply to the WLCSP package only and must be considered as development guidance for PCB designer. It is linked to ST's package development and qualification procedure; as a result, it must be fine-tuned and adapted according to customer process.

Figure 9. **PCB landing pattern**

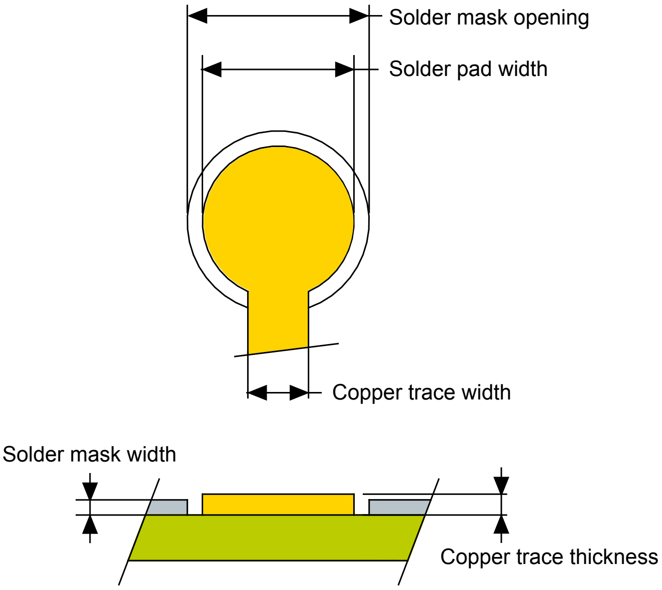


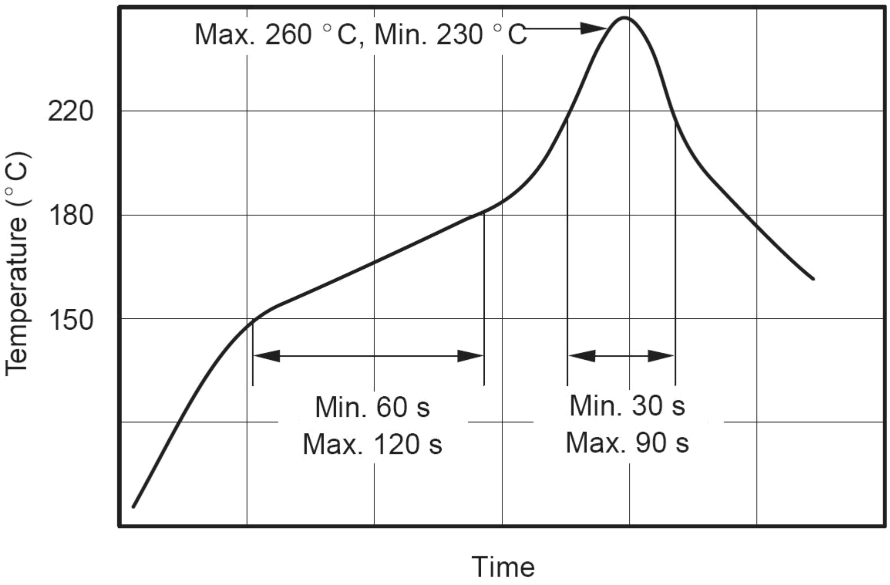
Table 9. **WLCSP24 - Recommended PCB design rules**

Dimension	Recommended values
Pitch	0.400 mm
Solder pad width	0.225 mm
Solder mask opening	0.275 mm
Solder mask thickness	0.025 mm
Copper trace thickness	0.030 mm
Copper trace width	0.080 mm

This package is compliant with the IPC/JEDEC J-STD-020D specifications.

The ST WLCSP is ECOPACK-compliant: In order to meet environmental requirements, ST offers ECOPACK packages. These packages have a lead-free second-level interconnect. The category of second-level interconnect is marked on the package and on the inner box label, in compliance with JEDEC standard JESD97. The maximum ratings related to soldering conditions are also marked on the inner box label. ECOPACK is an ST trademark. ECOPACK specifications are available at www.st.com.

Figure 10. **Reflow soldering temperature profile**



The previous figure shows the Pb-free reflow soldering temperature profile (temperature versus time) and the table below provides the critical reflow parameters (typical values).

Table 10. **Critical reflow parameters**

Parameter	Value (typical)
Process step lead-free solder: Ramp rate	3°C/s
Preheat	150°C to 180°C, 60 to 180 seconds
Time above liquidus (TAL)	220°C, 30 to 90 seconds
Peak temperature	255°C ±5°C
Time within 5°C of peak temperature	10 to 20 seconds
Ramp-down rate	6°C/s maximum

6 Delivery packing

6.1 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 11. 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 11. UFQFPN32 - Reel diagram

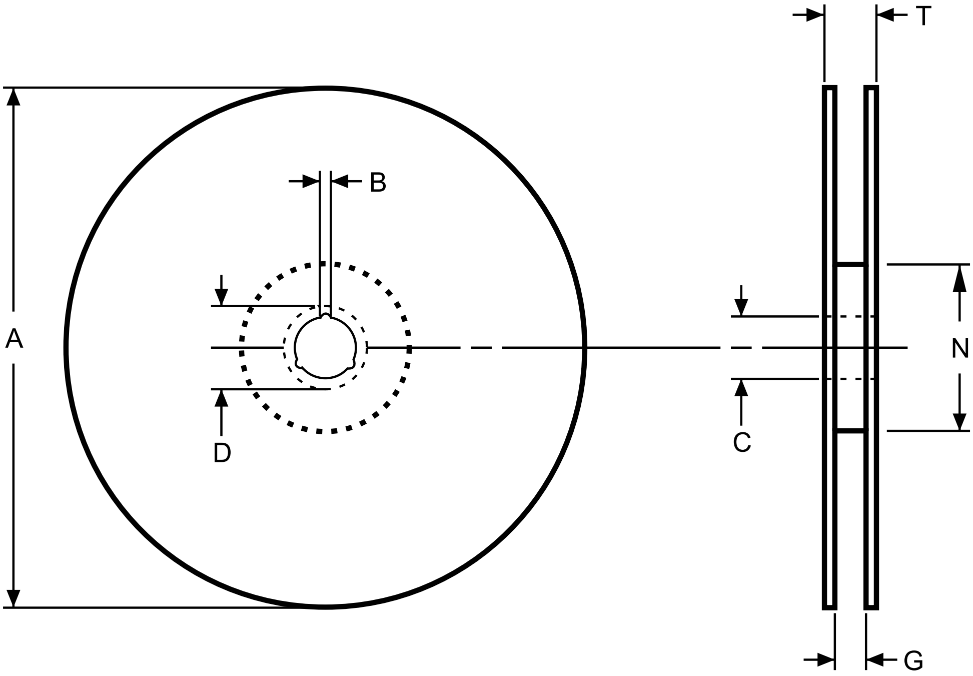
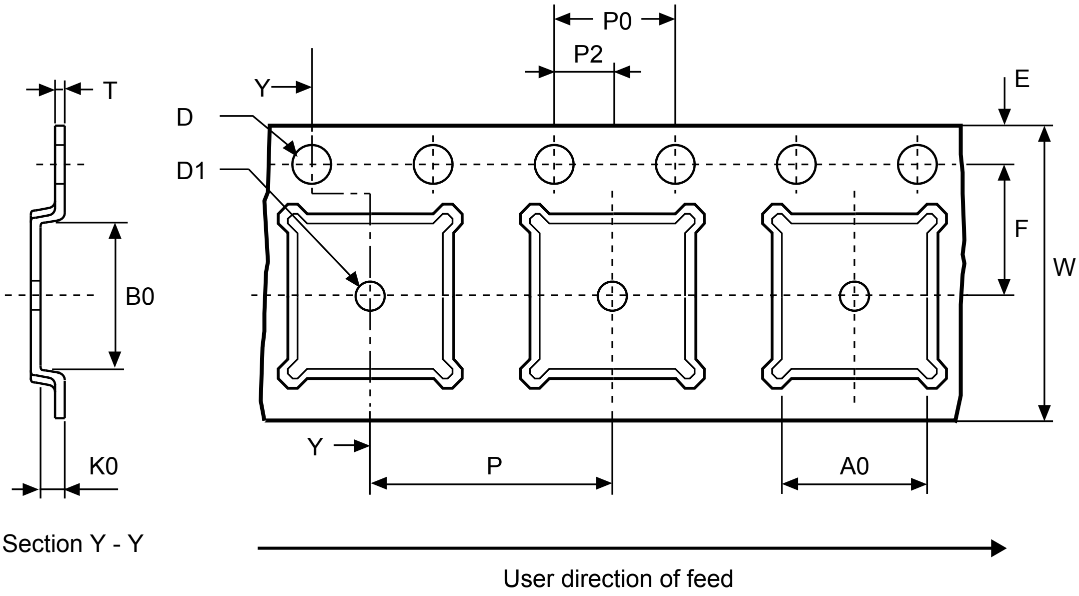


Table 12. UFQFPN32 - Reel dimensions

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 12. UFQFPN32 - Embossed carrier tape



1. *Drawing is not to scale.*

Figure 13. UFQFPN32 - Chip orientation in the embossed carrier tape

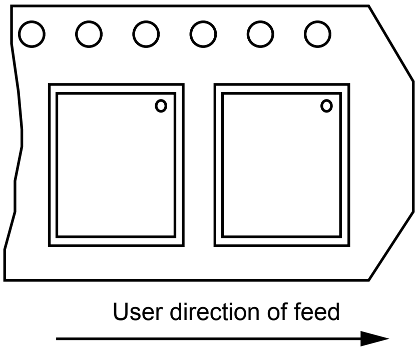


Table 13. UFQFPN32 - Carrier tape dimensions

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

6.2 WLCSP24 tape and reel packing

Surface-mount packages can be supplied with tape and reel packing. The reels have a 13" typical diameter. They contain 5000 devices each.

Reels are in plastic, either antistatic or conductive, with a black conductive cavity tape. The cover tape is transparent antistatic 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 14. WLCSP24 on tape and reel

Package	Description	Tape width	Tape pitch	Reel diameter	Quantity per reel
WLCSP24	Wafer-level chip scale package	12 mm	8 mm	13"	5000

Figure 14. WLCSP24 reel diagram

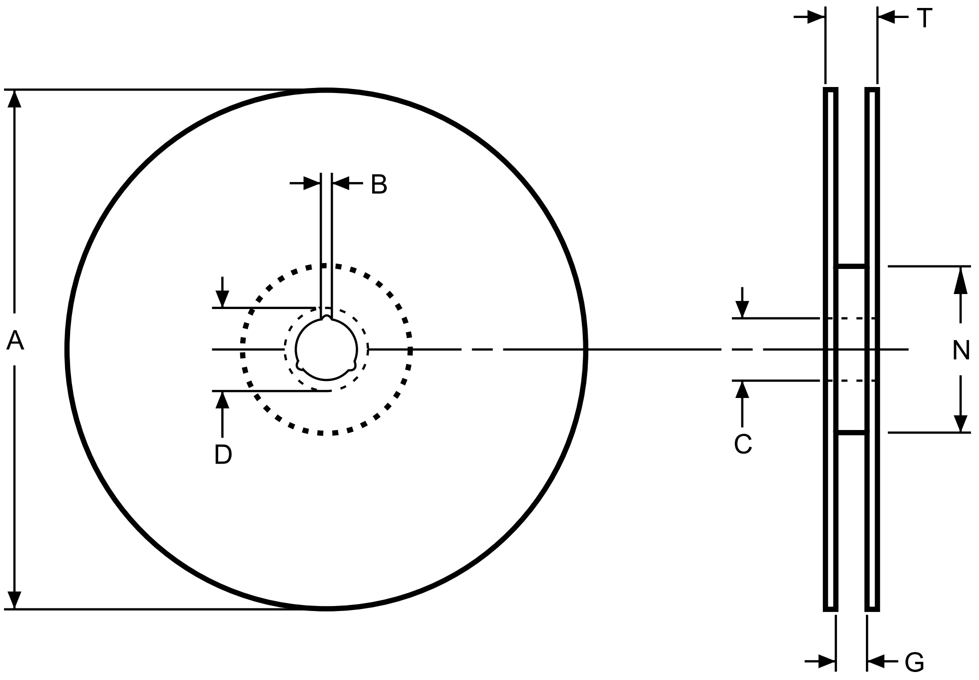
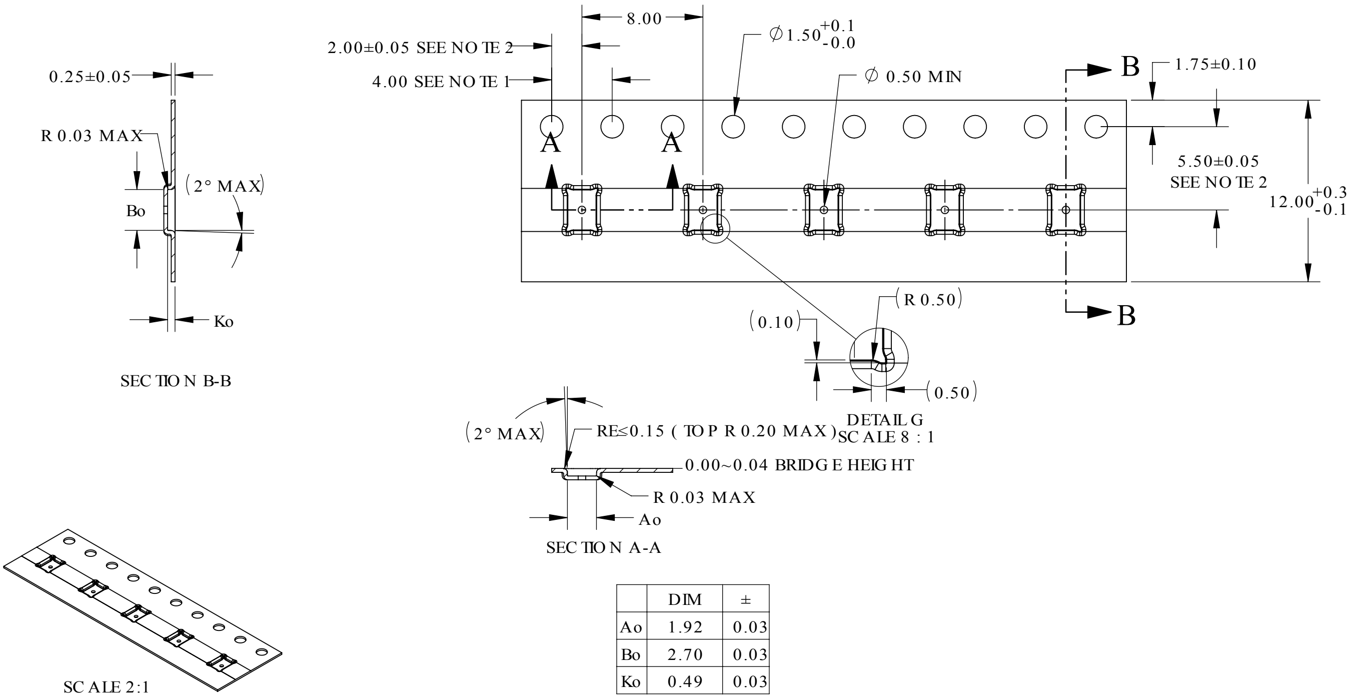


Table 15. WLCSP24 reel dimensions

Reel size	Tape size	A Max.	B Min.	C	D Min.	G Min.	N Min.	T Max.	Unit
13"	12	330	1.5	13 ±0.25	20.2	12.6	100	18.4	mm

Figure 15. **WLCSP24 carrier tape**



	DIM	±
Ao	1.92	0.03
Bo	2.70	0.03
Ko	0.49	0.03

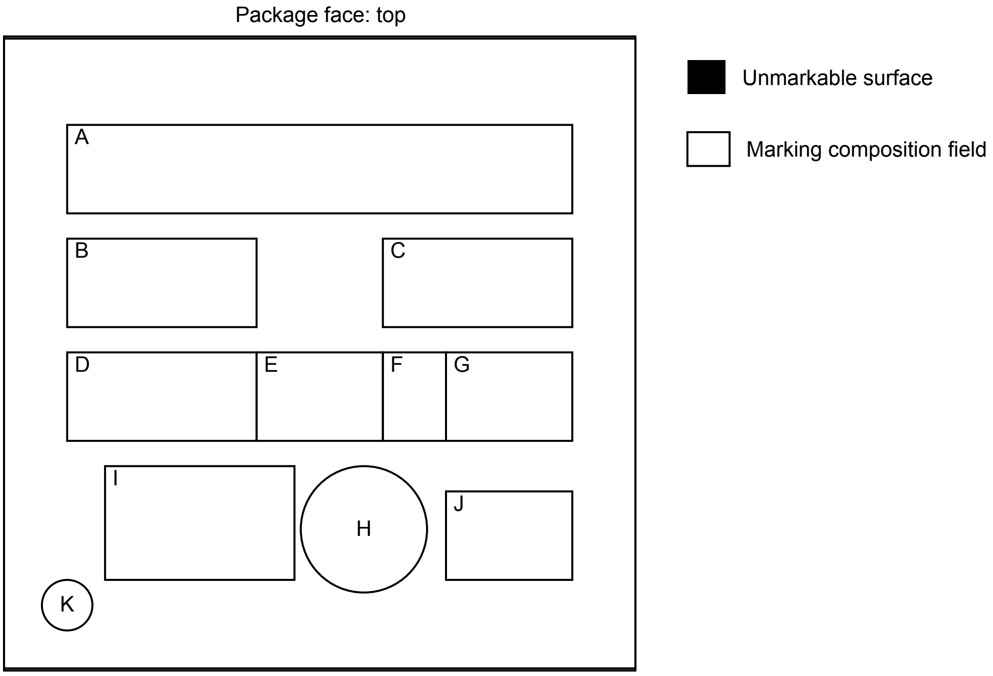
1. *10 sproket hole pitch cumulative tolerance ±0.2*
2. *Pocket position relative to sprocket hole measured as true position of pocket, not pocket hole.*
3. *Ao and Bo are measured on a plane at a distance "R" above the bottom of the pocket.*
4. *Dimensions are in millimeters.*
5. *Tolerances, unless specified: ±0.2 for 1 decimal place; ±0.10 for 2 decimal places.*

7 Package marking information

7.1 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 16. **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)

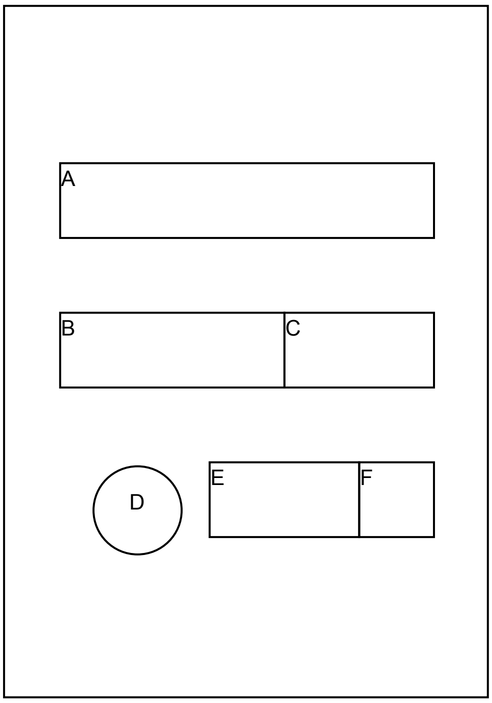
K: Dot[1]

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

7.2 WLCSP24 package marking information

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

Figure 17. **WLCSP24 package standard marking example (top view)**



Caption:

A: Marking area (5 characters)

B: Marking area (3 characters)

C: Assembly plant (PP)

D: Dot (The dot on the marking side indicates the A1 ball location on the ball side.)

E: Assembly week (WW)

F: Assembly year (Y)

8 Ordering information

Table 16. Ordering information

Ordering code	Package	Factory firmware version	Supported interfaces	Marking area A	Marking area B	Minimum ordering quantity
ST33KTPM2IWLBZB1	WLCSP24	10.512	I²C or SPI	KTPMI	ZB1	5000 units
ST33KTPM2I3WBZB1	UFQFPN32 WF					3000 units
ST33KTPM2IWLBZA9	WLCSP24	10.257			ZA9	5000 units
ST33KTPM2I3WBZA9	UFQFPN32 WF					3000 units

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.

[IETF RFC 8032]	Edwards-Curve Digital Signature Algorithm (EdDSA)
[IETF RFC 7748]	Elliptic Curves for Security
[FIPS 186-5]	Digital Signature Standard (DSS), NIST
[TCG Alg. Reg.]	TCG Algorithm Registry Family “2.0”, Revision 1.34
[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
[TCG TPM20 Part3 1.83]	Trusted Platform Module Library Specification, Family “2.0”, Level 00, Revision 01.83, Part3: Commands
[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
[Vendor Registry]	TCG TPM Vendor ID Registry Version 1.02 Revision 1.00
[FIPS PUB 140-3]	Security requirements for cryptographic modules – March 22, 2019

Revision history

Table 17. **Document revision history**

Date	Revision	Changes
15-Dec-2022	1	Initial release.
24-Jun-2024	2	Added: • Section 6.2: WLCSP24 tape and reel packing Updated: • Section Cover image • Section Features • Section 1: Description • Section 3.1.1: UFQFPN32 pin and signal description • Section 3.2.1: WLCSP24 ballout and signal description • Appendix A: Referenced documents
02-Jun-2025	3	Added: • Section 2: Firmware description • Section 5.1.1: UFQFPN32 thermal characteristics of packages • Appendix A: Referenced documents Updated: • Section Features • Section 1: Description • Table 3. UFQFPN32 pin descriptions • Figure 2. WLCSP 24 ballout - bottom view (balls side) title • Table 4. WLCSP24 ball description • Figure 6. UFQFPN32 - Outline • Table 11. UFQFPN32 - Packages on tape and reel • Section 5.2.1: PCB design and reflow recommendations • Table 14. WLCSP24 on tape and reel • Figure 15. WLCSP24 carrier tape • Figure 16. UFQFPN32 - Standard marking example • Section 8: Ordering information • Section 9: Support and information

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

I^{2}C 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

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.