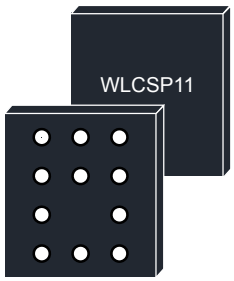
ST33GTPMII2C

Data brief

Flash-memory-based TPM2.0 device for industrial applications with an I²C interface



WLCSP11

Product status link
ST33GTPMII2C

Features

TPM features

- Flash-memory-based trusted platform module (TPM)
- Compliant with Trusted Computing Group (TCG) Trusted Platform Module (TPM) Library specifications 2.0, Level 0, Revision 138 and TCG PC Client Specific TPM Platform Specifications 1.03
- 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:
  - CC according to TPM 2.0 PP at EAL4+
  - FIPS 140-2 level 2 (physical security level 3)
- TCG certification
- I²C support at up to 200 kHz
- Supports up to 4 GPIOs mapped with NV storage indices

Hardware features

- Arm® SecurCore® SC300™ 32-bit RISC core
- Highly reliable Flash memory technology:
  - 500 000 cycles on the full temperature range
  - Data retention: 17 years at 85 °C and 10 years at 105 °C
- ESD (electrostatic discharge) protection against voltages greater than 4 kV (HBM)
- 1.8 V, 3.3 V or 5 V supply voltage range
- Industrial qualification (JEDEC)
- Wafer-level chip-scale package (WLCSP) JEDEC J-STD-020D-compliant MSL1 package

Security features

- Active shield and environmental sensors
- Monitoring of environmental parameters (power and clock)
- Hardware and software protection against fault injection
- FIPS compliant RNG built on an SP800-90A compliant SHA256 DRBG and an AIS-31 Class PTG2 compliant true random number generator (TRNG)

- Cryptographic algorithms:
  - RSA key generation (1024 or 2048 bits)
  - RSA signature (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
  - TDES 192 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 3 RSA key pairs to reduce the TPM provisioning time

Product compliance

- Compliant with TCG test suite for TPM 2.0
- Common Criteria certifications:
  - EAL 4+ on TCG TPM2.0 protection profile
  - EAL 5+ on hardware
- Targets FIPS 140-2 level 2 certification (physical security level 3)

1 Description

The ST33GTPMII2C is a cost-effective and high-performance trusted platform module (TPM) targeting industrial embedded systems.

The product implements the functions defined by the Trusted Computing Group (www.trustedcomputinggroup.org) in the TCG Trusted Platform Module Library Specifications version 2.0 Level 0 Revision 138 ([TPM 2.0 P1 r138], [TPM 2.0 P2 r138], [TPM 2.0 P3 r138], [TPM 2.0 P4 r138]) and errata version 1.4 [TPM 2.0 rev138 Err 1.4]. It is also based on the TCG PC client-specific TPM Platform specifications rev1.03 [PTP 2.0 r1.03]. The applicable protection profile is *TCG Protection Profile for PC Client Specific TPM 2.0* ([TPM 2.0 PP]).

The product also supports the ability to upgrade the TPM firmware thanks to a persistent Flash memory loader application to support new standard evolutions.

1.1 Security certifications

This product targets CC certification according to TPM 2.0 PP at EAL4+.

1.2 Hardware features

The ST33GTPMII2C is based on a smartcard-class secure MCU that incorporates the most recent generation of Arm® processors for embedded secure systems. Its SecurCore® SC300™ 32-bit RISC core is built on the Cortex®-M3 core with additional security features to help to protect against advanced forms of attack.

The ST33GTPMII2C offers an I²C interface supported by an embedded communication engine compliant with TCG PC client TPM Profile 1.03 [PTP 2.0 r1.03].

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

The ST33GTPMII2C comes in the WLCSP11 ECOPACK-compliant package. ECOPACK is an ST trademark.

Note: Arm is a registered trademark of Arm Limited (or its subsidiaries) in the US and/or elsewhere.

2 Pin and signal descriptions

The figure below gives the pinout of the wafer-level chip-scale (WLCSP11) package in which the devices are delivered. Table 1 describes the associated signals.

Figure 1. WLCSP11 pinout (top view)

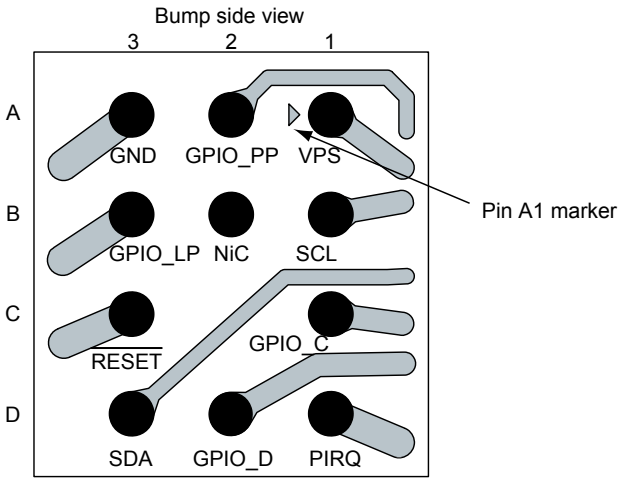


Table 1. Pin descriptions

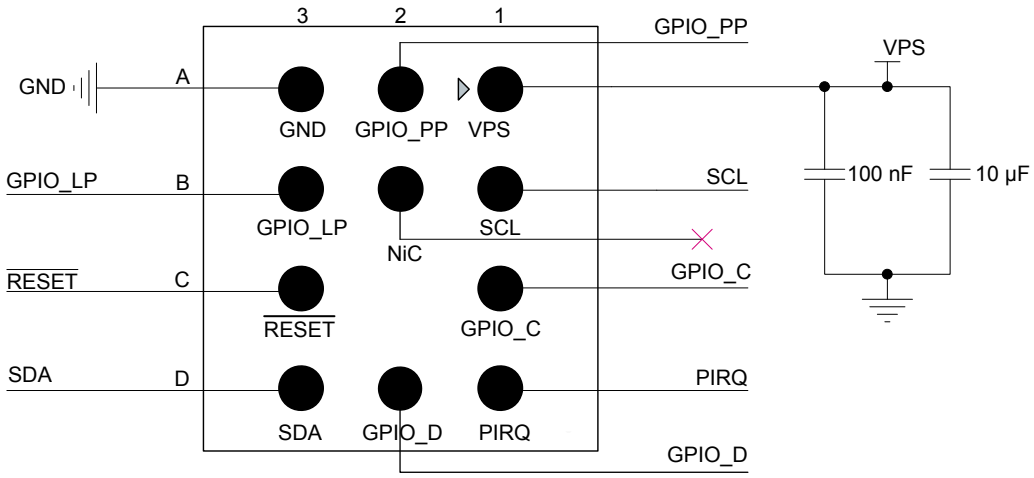
Signal	Type	Description
VPS	Input	**Power supply**. This pin must be connected to 1.8 V or 3.3 V DC power rail supplied by the motherboard.
GND	Input	GND has to be connected to the main motherboard ground.
SDA	Bidir	I²C serial data (open drain with no weak pull-up resistor)
SCL	Input	I²C serial clock (open drain with no weak pull-up resistor)
PIRQ	Output	IRQ used by the TPM to generate an interrupt
$\overline{\text{RESET}}$	Input	Reset used to re-initialize the device
GPIO_C	Input/output	General-purpose input/output. Defaults to low. The GPIO function could be modified by activating the GPIOs mapped with the NV storage index feature.
GPIO_D	Input/output	General-purpose input/output. Defaults to low. The GPIO function could be modified by activating the GPIOs mapped with the NV storage index feature.
GPIO_PP	Input	**Physical Presence**, active high, internal pull-down. Used to indicate Physical Presence to the TPM. GPIO Function could be modified by activating the GPIOs mapped with the NV storage index feature.
GPIO_LP	Input	By default: Used for activation and deactivation of the TPM Standby mode (not found). The GPIO function could be modified by activating GPIOs mapped on the NV storage index feature.
NiC	-	**Not internally connected**: not connected to the die. May be left unconnected, but has no impact on the TPM if connected.

3 Integration guidance

3.1 Typical hardware implementation

The Physical Presence (PP) pin should be connected if platform implementation (at boot level) uses a hardware physical presence function.

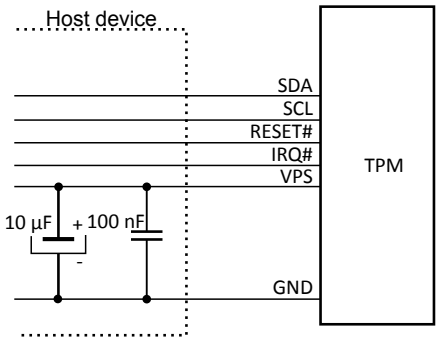
Figure 2. Typical hardware implementation (WLCSP11 package)



3.2 Power supply filtering

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

Figure 3. Mandatory filtering capacitors on V_{PS}



1. 10 µF and 100 nF are recommended values. The minimum required capacitor value is 2.1 µF (2 µF in parallel with 100 nF).

Table 2. Maximum V_{PS} rising slope

Symbol	Parameter	Value	Unit
S_{VPS}	Maximum V_{PS} rising slope	5	V/µs

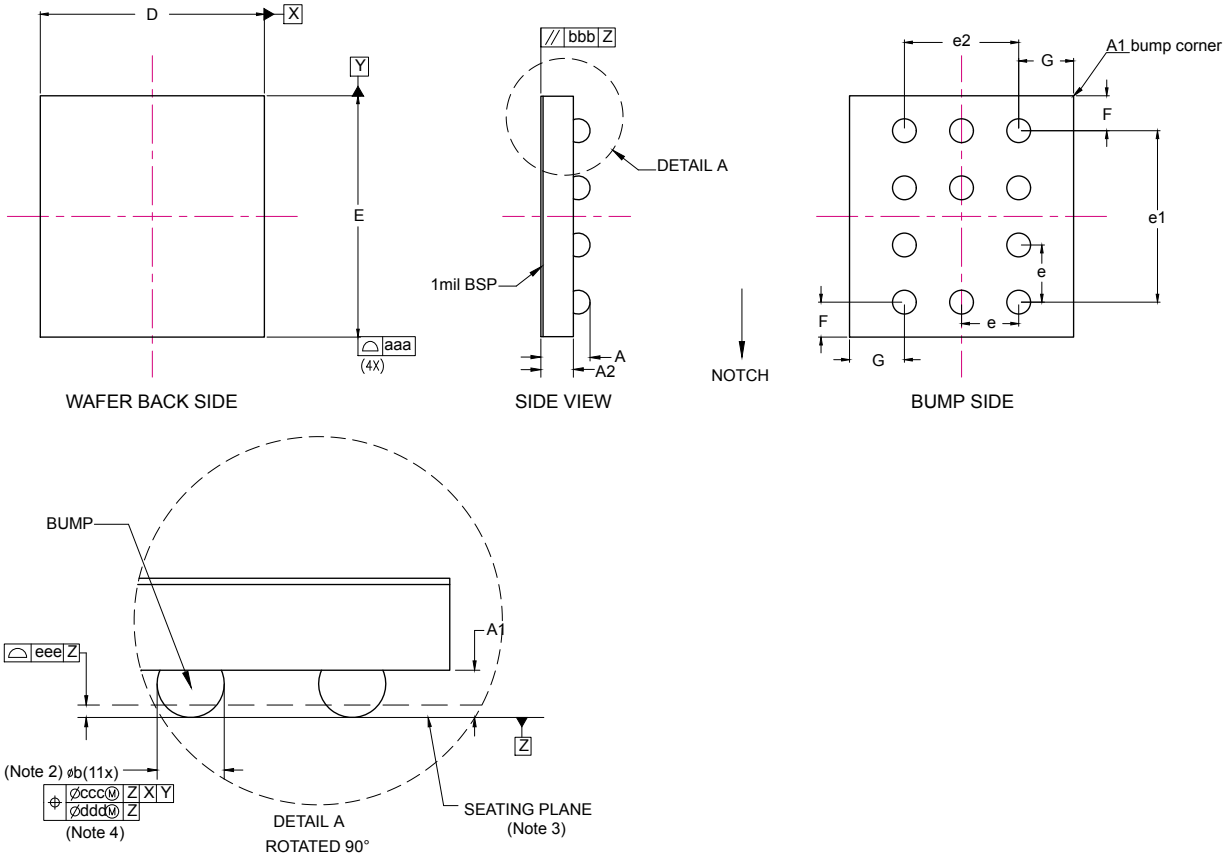
4 Package information

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 WLCSP11 package information

WLCSP11 stands for 2.549 × 2.745 mm 11-bump wafer-level chip-scale package.

Figure 4. WLCSP11 – package outline



1. Dimensions and tolerance as per ASME Y 14.5M - 1994.
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 bump.
4. Bump position designation per JESD 95-1, SPP-010.

Table 3. WLCSP11 - package mechanical data

Symbol	Millimeters			Inches [1]		
	Min	Typ	Max	Min	Typ	Max
A	-	-	0.600	-	-	0.0236
A1	-	0.190	-	-	0.0075	-
A2	-	-	0.395	-	-	0.0156
b	-	0.270	-	-	0.0106	-
D	-	2.549	2.579	-	0.1004	0.1015
E	-	2.745	2.775	-	0.1081	0.1092
e	-	0.650	-	-	0.0256	-
e1	-	1.950	-	-	0.0768	-
e2	-	1.300	-	-	0.0512	-
F	-	0.398	-	-	0.0157	-
G	-	0.625	-	-	0.02446	-
N[2]	-	11	-	-	11	-
aaa	-	0.110	-	-	0.0043	-
bbb	-	0.110	-	-	0.0043	-
ccc	-	0.110	-	-	0.0043	-
ddd	-	0.060	-	-	0.0024	-
eee	-	0.060	-	-	0.0024	-

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

4.2 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 5. PCB landing pattern

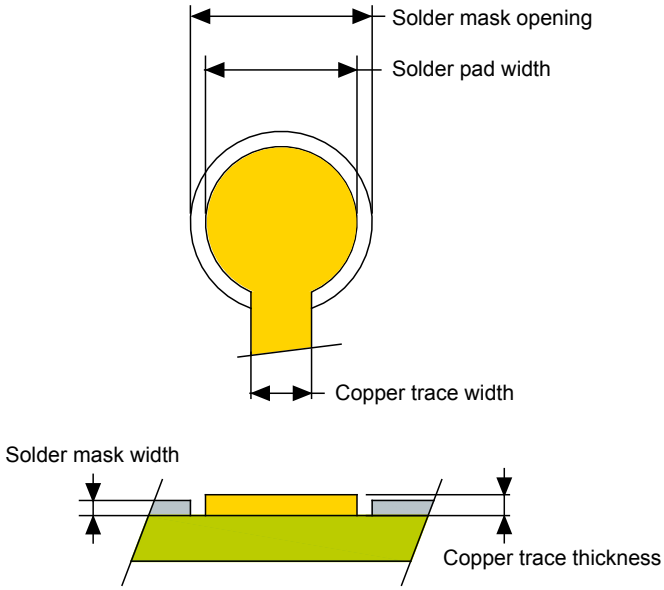


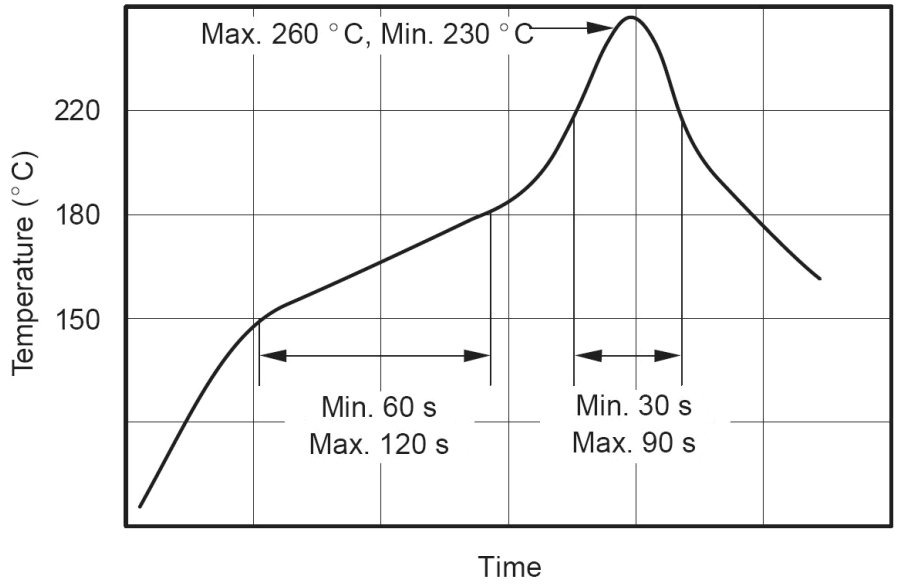
Table 4. PCB design parameters

Parameter	Value
Solder pad width	230 µm
Solder mask opening	345 µm
Solder mask thickness	25 µm
Copper trace thickness	30 µm
Copper trace width	80 µm

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 6. **Reflow soldering temperature profile**



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

Table 5. **Critical reflow parameters**

Parameter	Value (typical)
Process step Lead-free solder: Ramp rate	3 °C/s
Pre-heat	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

4.3 WLCSP tape and reel packing

Surface-mount packages can be supplied with tape and reel packing.

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 “A1”) on the same side as the sprocket holes in the tape.

The STMicroelectronics tape and reel specifications are compliant to the EIA 481-A standard specification.

Table 6. **WLCSPs on tape and reel**

Package	Quantity per reel
11-bump, wafer-level chip-scale package (WLCSP)	5000

Figure 7. **WLCSP11 reel diagram**

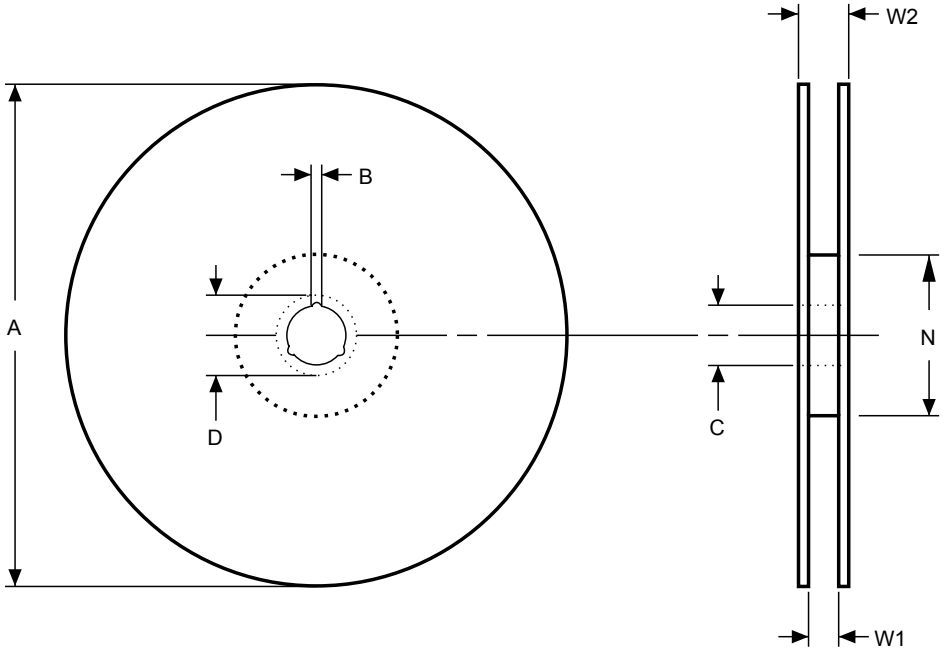


Table 7. **WLCSP11 reel dimensions**

All dimensions except for the reel diameter are in millimeters.

Reel diameter	A	B	C	D	N	W1(1)W1	W2W1
13 inches	330 (typ.)	2.2 (±0.5)	13 (±0.25)	20.2 (min.)	4 inches	12.4 (+2, −0)	18.4 (max.)

1. *Measured at hub.*

Figure 8. **WLCSP11 leader and trailer**

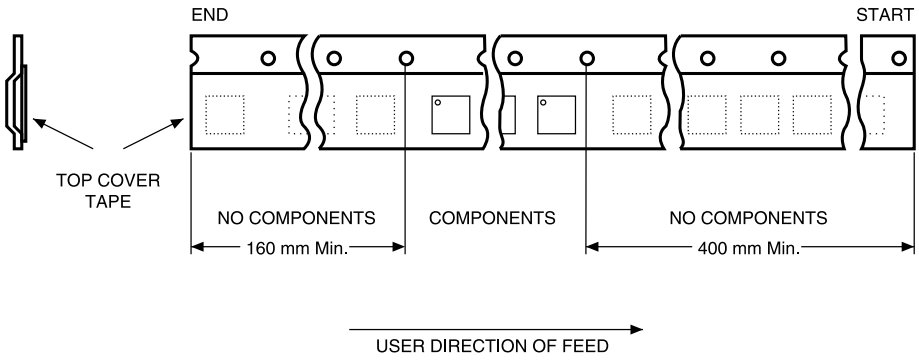
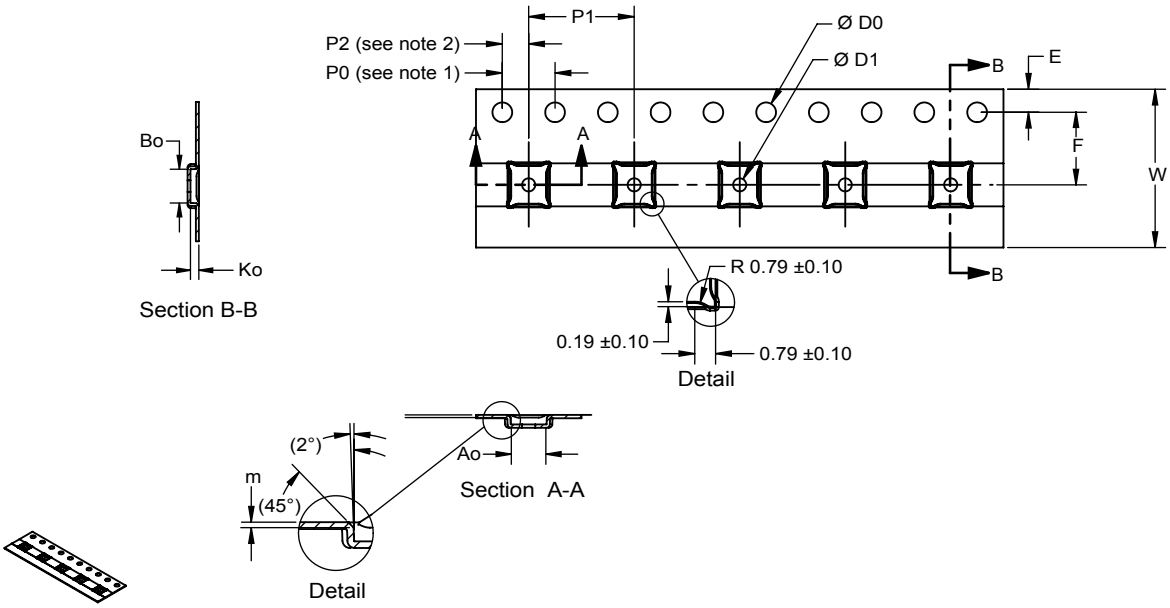


Figure 9. Embossed carrier tape for WLCSP11



1. Cumulative tolerance of the sprocket hole pitch is ±0.2.
2. Pocket position relative to sprocket hole measured as the true position of the pocket, not the pocket hole.
3. Ao and Bo are measured on a plane at a distance R above the bottom of the pocket.
4. Drawing is not to scale.
5. Dimensions are in millimeters.

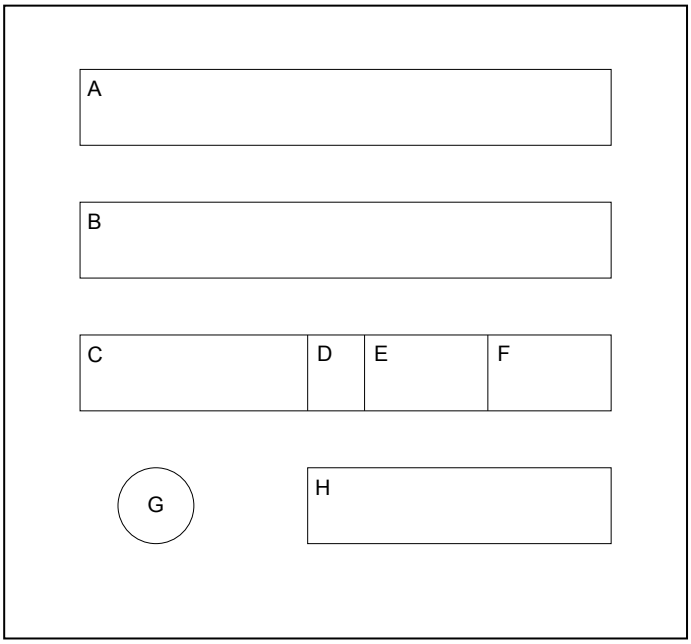
Table 8. Carrier tape dimensions for WLCSP11

D0	D1	E	F	m (max)	Ko	Ao	Bo	P0	P1	P2	W
1.50 +0.1/–0.0	1.00 +0.1/–0.0	1.75 ±0.10	5.50 ±0.05	≤ 0.25	0.72 ±0.05	2.71 ±0.05	2.91 ±0.05	4.00 ±0.1	8.00 ±0.1	2.00 ±0.05	12.00 +0.3/–0.1

5 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. WLCSP11 standard marking example



Legend:

A: Marking area – 8 digits

B: Marking area – 8 digits

C: BE sequence

D: Assembly year

E: Assembly week

F: Assembly plant

G: Dot(1)

H: Marking area – 5 digits

1. *The dot on the back side indicates the A1 ball location.*

6 Ordering information

Table 9. Ordering information for products supporting firmware 0x00.0x06.0x01.0x01 (0x0006.0x0101) (6.257) preloaded in factory

Ordering code	Firmware version	Operating temperature range	Maximum I²C clock frequency	Package	A marking area	B marking area
ST33GTPMIWLFZE5	0x00.0x06.0x01.0x01 (0x0006.0x0101) (6.257)	-40 °C to +105 °C	200 kHz	WLCSP11	GTPMII2C	FZE5

Appendix A Terms and abbreviations

Table 10. List of abbreviations

Term	Meaning
AES	Advanced Encryption Standard
AFL	Applicative Flash memory loader
CA	Certificate authority
CC	Common Criteria
DRBG	Deterministic random-bit generator
EC	Elliptic curve
ECDAA	Elliptic curve direct anonymous attestation (algorithm)
ECDH	Elliptic curve Diffie–Hellman
FIPS	Federal Information Processing Standard
GPIO	General-purpose I/O
HMAC	Keyed-Hashing for Message Authentication
I²C	Inter-integrated circuit
NV	Non-volatile (memory)
RSA	Rivest Shamir Adelman
RTR	Root of trust for reporting
SHA	Secure Hash algorithm
TCG	Trusted Computed Group
TPM	Trusted Platform Module
TRNG	True random-number generator

Appendix B Referenced documents

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

[TPM 2.0 P1 r138]	TPM Library, Part 1, Architecture, Family 2.0, rev 1.38, TCG
[TPM 2.0 P2 r138]	TPM Library, Part 2, Structures, Family 2.0, rev 1.38, TCG
[TPM 2.0 P3 r138]	TPM Library, Part 3, Commands, Family 2.0, rev 1.38, TCG
[TPM 2.0 P4 r138]	TPM Library, Part 4, Supporting routines, Family 2.0, rev 1.38, TCG
[TPM 2.0 rev138 Err 1.4]	TPM Library, Family 2.0, rev 1.38, Errata 1.4, January 8, 2018, TCG.
[PTP 2.0 r1.03]	TCG PC Client Specific Platform TPM Specification (PTP) - Version 2.0 Revision 1.03
[PKCS#1]	PKCS#1: v2.1 RSA Cryptography Standard, RSA Laboratories
[AN2639]	Application note, Soldering recommendations and package information for Lead-free ECOPACK® microcontrollers, STMicroelectronics
[TPM 20 PP]	Protection Profile PC Client Specific TPM, Family 2.0 Level 0 revision 1.38 (1.1), TCG.

Revision history

Table 11. **Document revision history**

Date	Version	Changes
07-Sep-2020	1	Initial release.

Contents

List of tables

List of figures