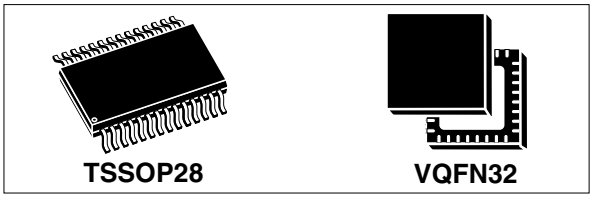
ST33TPM12I2C

Trusted Platform Module with I2C interface based on 32-bit ARM® SecurCore® SC300™ CPU

Data brief



Features

TPM features

- Single-chip Trusted Platform Module (TPM)
- Compliant with Trusted Computing Group (TCG) Trusted Platform Module (TPM) Main specifications 1.2, Level 2, Revision 116
- Based on TCG PC Client Specific TPM Interface Specifications 1.21
- Fully based on the common criteria (CC) EAL4+ certified LPC version ST33TPM12LPC
- I^2C support in Standard mode (100 kHz) and Fast mode (400 kHz), supporting clock stretching
- Provisioned with Endorsement key and Endorsement Key certificate
- Support of clock suspension for power saving mode
- Support of Field Upgrade and Dictionary Attack protection
- Monotonic counter endurance guaranteed for 7 years
- Support of software and hardware physical presence

Hardware features

- ARM® SecurCore® SC300™ 32-bit RISC core
- Highly reliable CMOS EEPROM submicron technology
  - 30-year data retention at 25 °C
  - 500 000 typical Erase/Write cycle endurance at 25 °C
- Temperature range: 0 °C to +70 °C
- ESD protection up to 4 kV (HBM)
- 3.3 V supply voltage range
- 28-lead thin shrink small outline and 32-lead very thin fine pitch quad flat pack ECOPACK® packages

Security features

- Active shield and environmental sensors
- Memory protection unit (MPU)
- Monitoring of environmental parameters (power and clock)
- Hardware and software protection against fault injection
- AIS-31 Class P2 compliant true random number generator (TRNG)
- Cryptographic algorithms:
  - RSA key generation from 512 to 2048 with a 2-byte step
  - RSA signature and encryption
  - SHA-1 and SHA-256
  - AES-128 in CTR mode

Performance and resource features

- SHA1 computation for 64-byte block: 155 µs[(a)]
- Signature with a 2048-bit key: 150 ms[(a)]
- Signature with a 1024-bit key: 30 ms[(a)]
- NV storage allocated space: 4 Kbytes (1.2 Kbytes used by EK certificate)
- Supported 2048-bit key slots:
  - up to 10 key slots (without EK and SRK)
  - 1 key slot in volatile memory for high-frequency loading use case

a. Typical value with clock configuration in secure mode without communication time.

Contents

1 Description

The ST33TPM12I2C is a cost-effective and high performance Trusted Platform Module (TPM) targeting embedded system applications.

This device implements the functions defined by the Trusted Computing Group (www.trustedcomputinggroup.org) in the TCG Trusted Platform Module Specifications version 1.2 Level 2 Revision 116 ([1][2][3]), and is also based on the TCG PC Client specific TPM interface specifications 1.21 [5] and the PC Client implementation specification for conventional BIOS [6] for what concerns the TPM internal register list and bit definitions.

The ST33TPM12I2C is based on a secure MCU hardware platform.

The ST33TPM12I2C is built on a 32-bit ARM® reduced instruction set computing (RISC) processor which provides high cryptographic and general performances. A crypto-processor NESCRYPT is also present to support efficiently all public key cryptographic algorithms.

1.1 Hardware features

The ST33TPM12I2C 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 attacks.

Cadenced at 30 MHz, the SC300™ core brings great performance and excellent code density thanks to the Thumb®-2 instruction set.

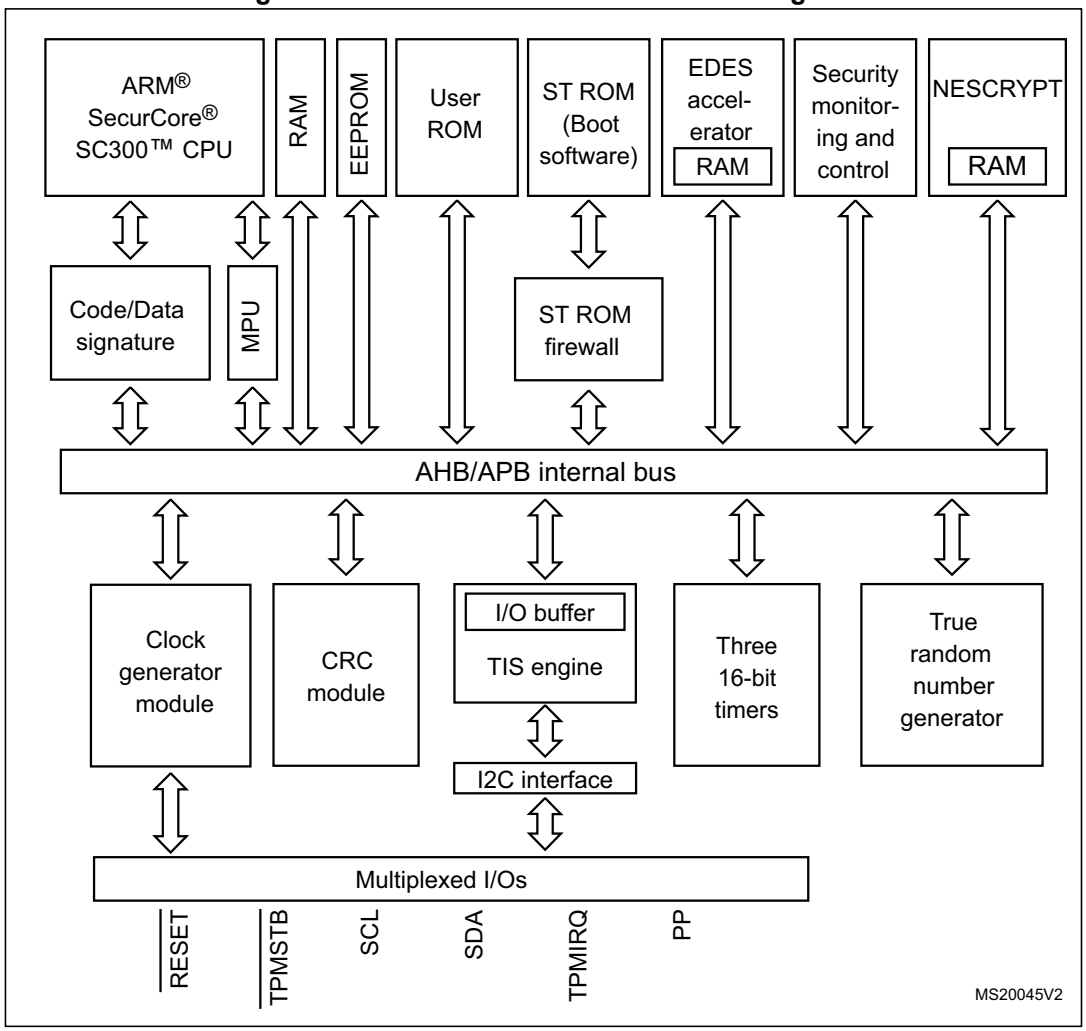
The ST33TPM12I2C offers a fast slave I²C interface supported by an embedded hardware communication engine.

The ST33TPM12I2C features hardware accelerators for advanced cryptographic functions. The EDES peripheral provides a secure DES (Data Encryption Standard) algorithm implementation, while the NESCRYPT crypto-processor efficiently supports the public key algorithm.

The ST33TPM12I2C operates in the 0 to +70°C temperature and 3.3V supply voltage ranges.

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.

Figure 1. ST33TPM12I2C hardware block diagram



2 Pin and signal description

2.1 Pinout descriptions

Figure 2. TSSOP28 pinout

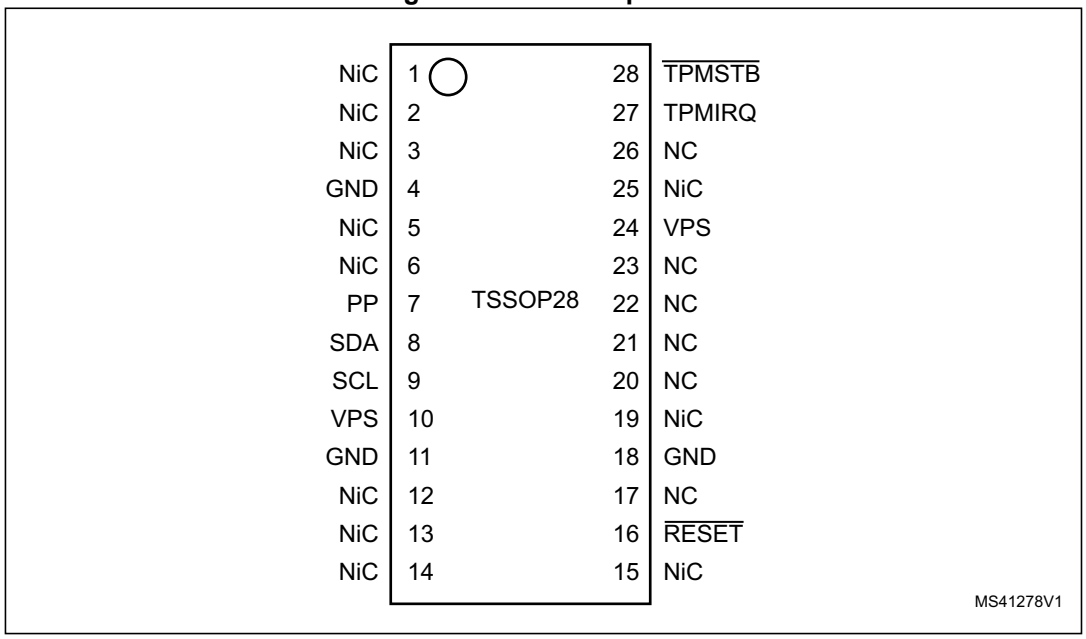


Figure 3. VQFN32 pinout

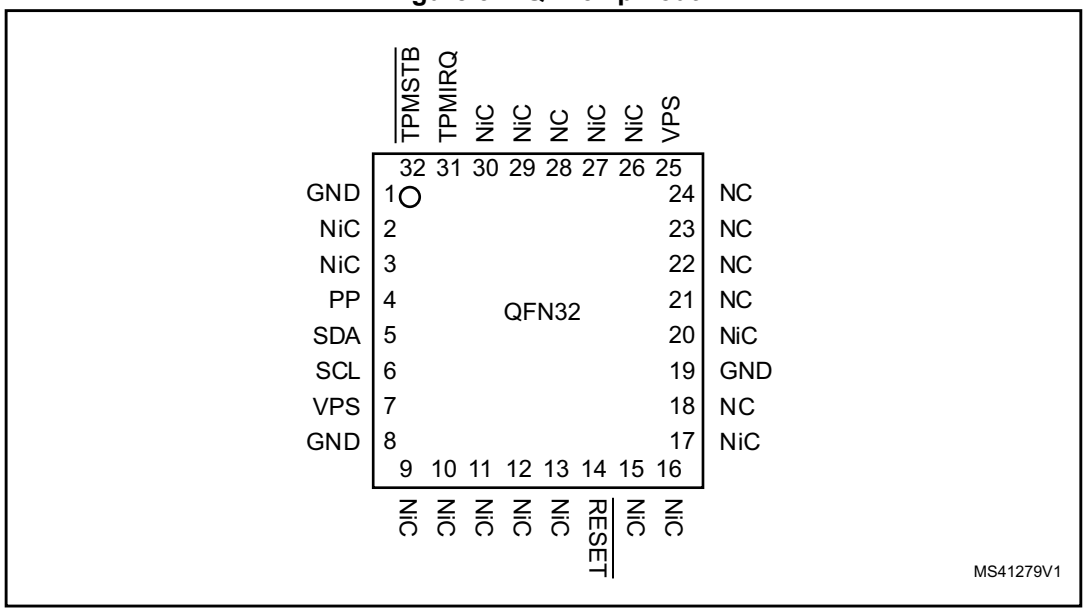


Table 1. Pin descriptions

Signal	Type	Description
VPS	Input	**3.3 V Power supply**. This pin must be connected to 3.3V DC power rail supplied by the motherboard.
GND	Input	GND has to be connected to the main motherboard ground.
$\overline{\text{TPMSTB}}$	Input	**Power Down** indicates that the peripheral should prepare for power to be removed from the interface devices. Actual power removal is system dependent.
$\overline{\text{RESET}}$	Input	**Reset** used to re-initialize the device
PP	Input	**Physical Presence**, active high, internal pull-down. Used to indicate Physical Presence to the TPM.
SCL	Input	**I²C serial clock** (Open drain with no weak pull-up resistor)
SDA	Bidirectional	**I²C serial data** (Open drain with no weak pull-up resistor)
TPMIRQ	Output	**TPM IRQ** is used by TPM to handle interrupt support.
NiC	-	Not internally connected: not connected to the die. May be left unconnected, but if it is connected there is no impact on the TPM device.
NC	-	Not connected: connected to the die but not usable. May be left unconnected.

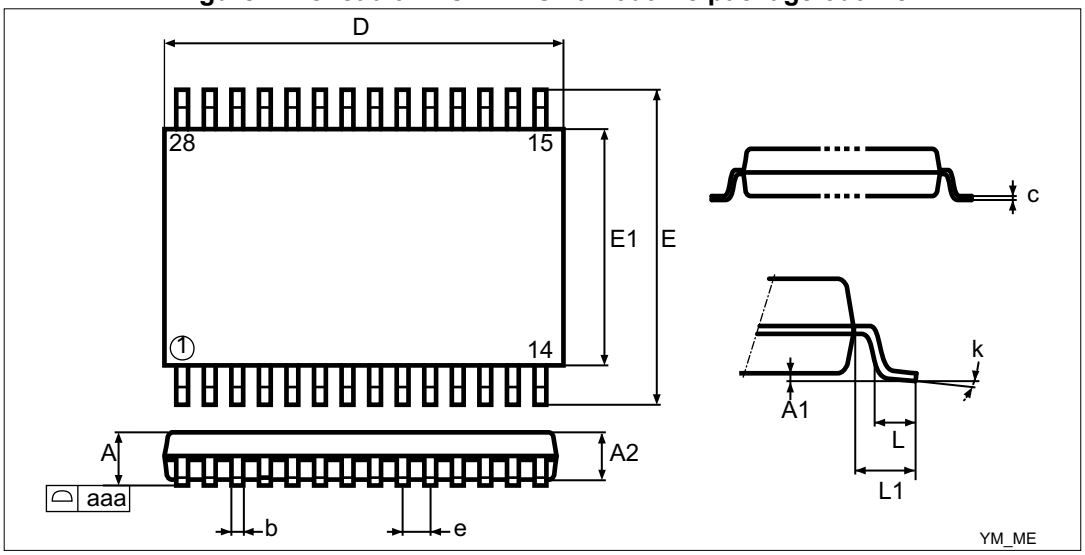
3 Package information

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.

3.1 28-pin thin shrink small outline package information

Dimensional features of the TSSOP28 package: 4.4 mm body width and 0.65 mm pitch. Unless otherwise specified, general tolerance is ± 0.1 mm.

Figure 4. 28-lead thin shrink small outline package outline



1. Drawing is not to scale.

Table 2. 28-lead thin shrink small outline package mechanical data

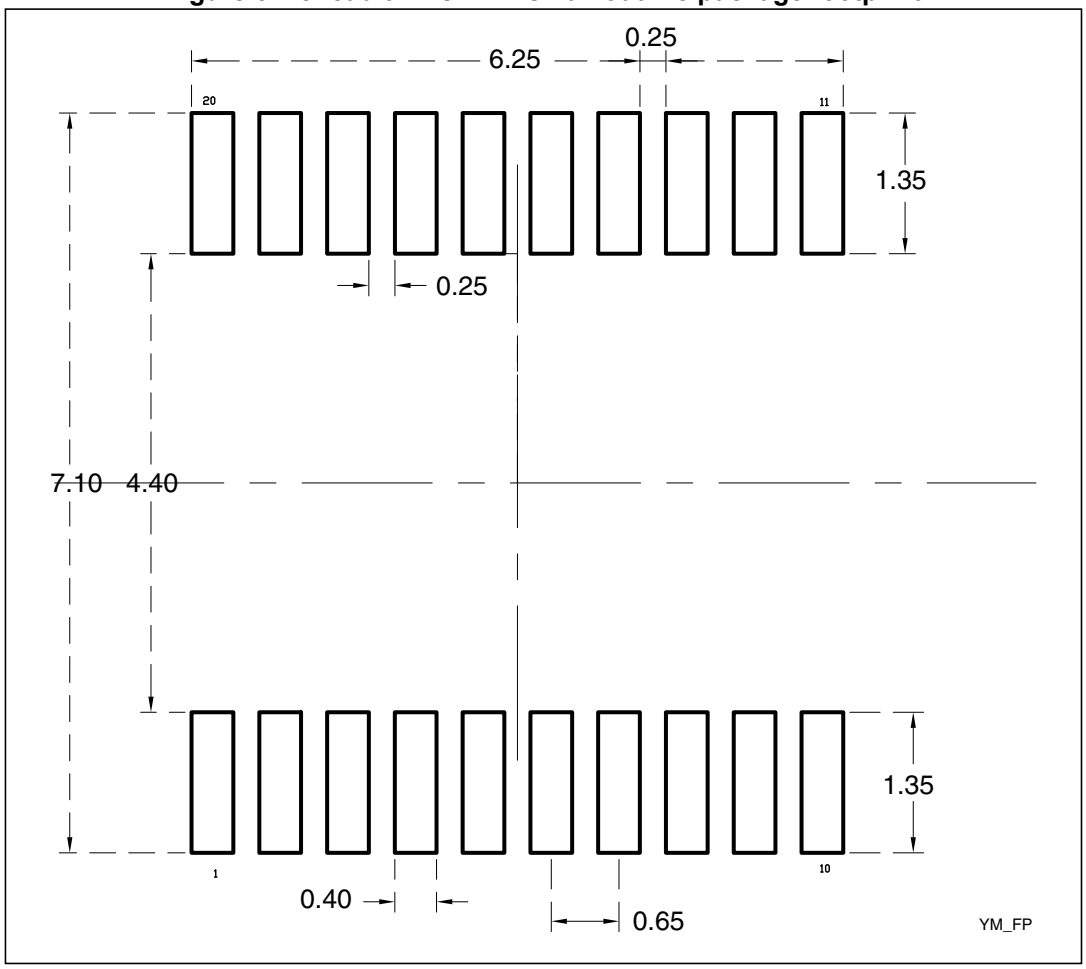
Symbol	millimeters			inches(1)		
	Min.	Typ.	Max.	Min.	Typ.	Max.
A	-	-	1.200	-	-	0.0472
A1	0.050	-	0.150	0.0020	-	0.0059
A2	0.800	1.000	1.050	0.0315	0.0394	0.0413
b	0.190	-	0.300	0.0075	-	0.0118
c	0.090	-	0.200	0.0035	-	0.0079
D	9.600	9.700	9.800	0.3780	0.3819	0.3858
E	6.200	6.400	6.600	0.2441	0.2520	0.2598
E1	4.300	4.400	4.500	0.1693	0.1732	0.1772
e	-	0.650	-	-	0.0256	-
L	0.450	0.600	0.750	0.0177	0.0236	0.0295
L1	-	1.000	-	-	0.0394	-

Table 2. 28-lead thin shrink small outline package mechanical data (continued)

Symbol	millimeters			inches[1]		
	Min.	Typ.	Max.	Min.	Typ.	Max.
k	0°	-	8°	0°	-	8°
aaa	-	-	0.100	-	-	0.0039

1. Values in inches are converted from mm and rounded to 4 decimal digits.

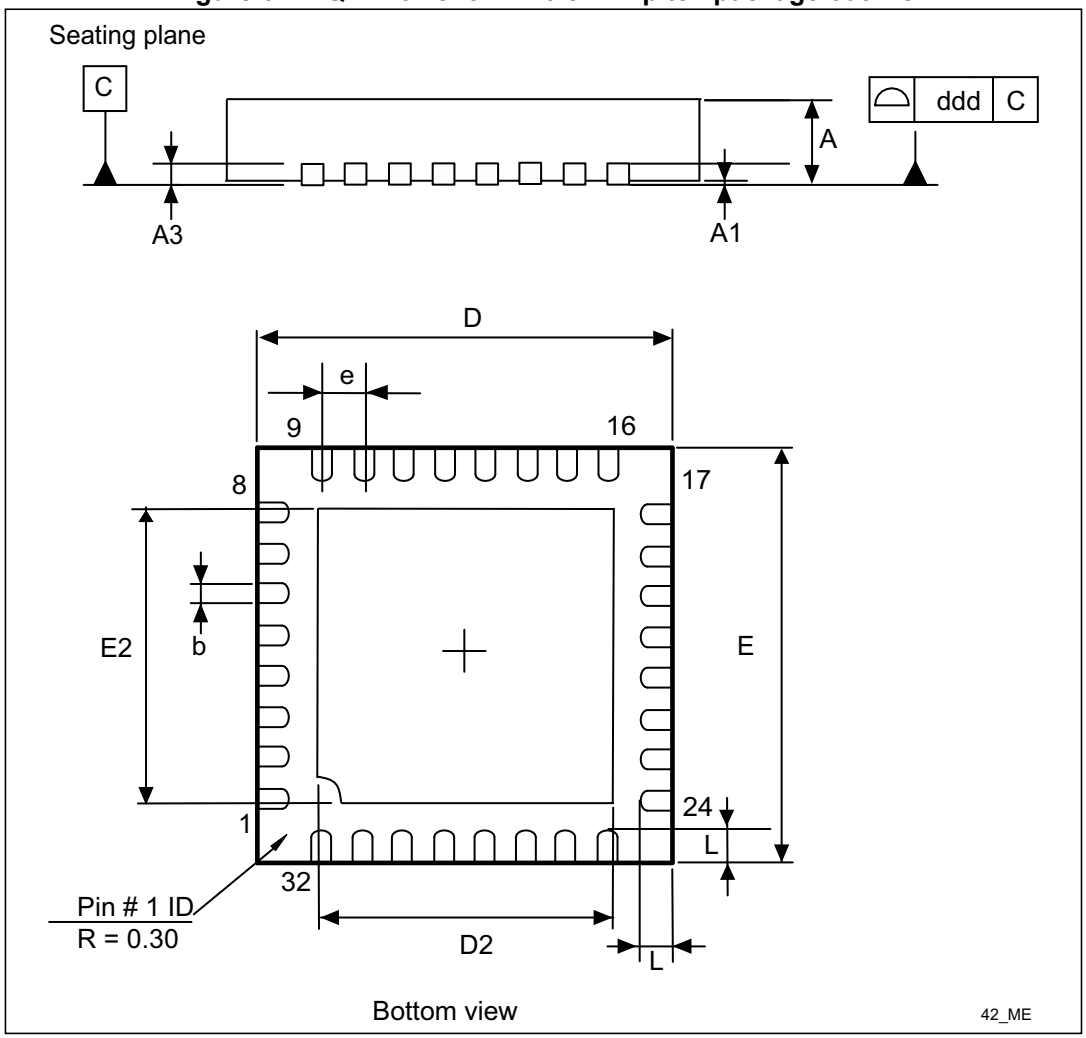
Figure 5. 28-lead thin shrink small outline package footprint



1. All dimensions are in millimeters.

3.2 32-lead very thin fine pitch quad flat pack no-lead (VFQFPN) package information

Figure 6. VFQFPN32 5×5 mm 0.5 mm pitch package outline



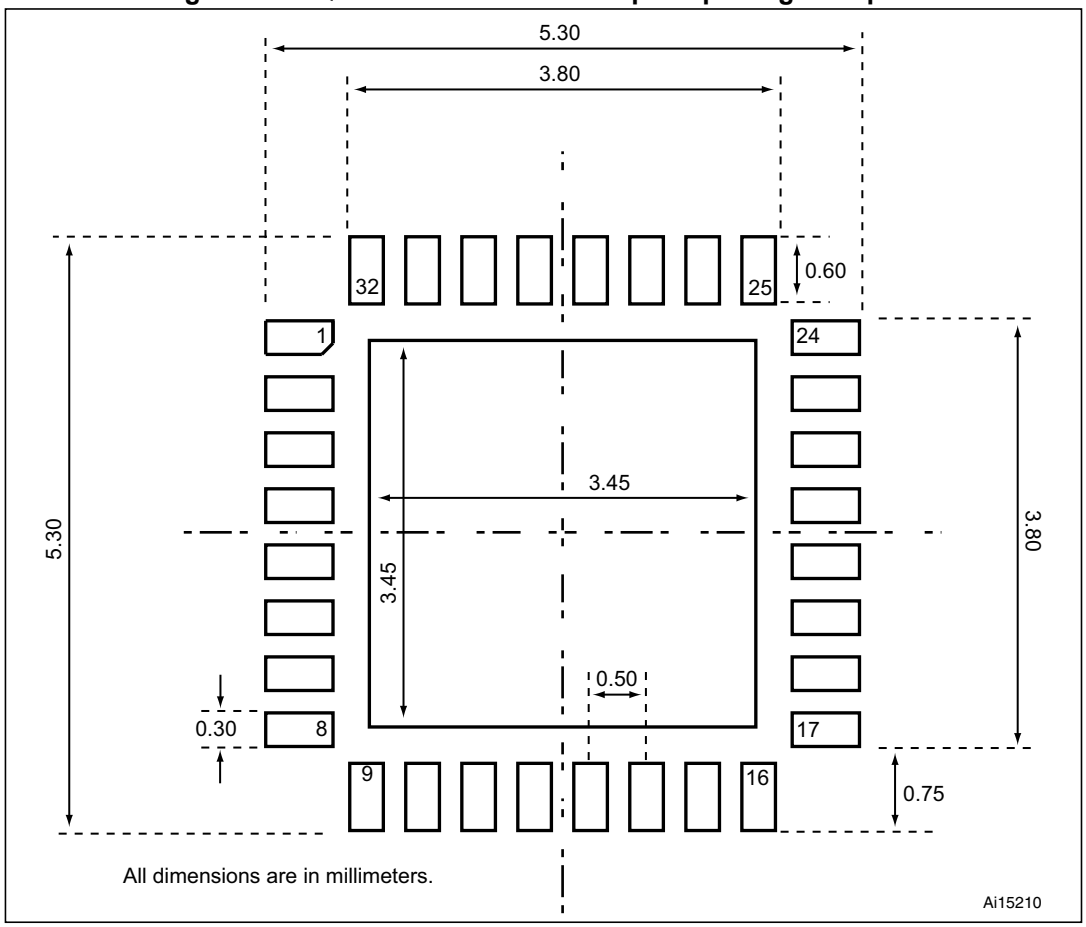
1. Drawing is not to scale.

Table 3. VFQFPN32 5×5 mm package mechanical data

Symbol	millimeters			inches [1]		
	Min.	Typ.	Max.	Min.	Typ.	Max.
A	0.800	0.900	1.000	0.0315	0.0354	0.0394
A1	0.000	0.020	0.050	0.0000	0.0008	0.0020
A3	-	0.200	-	-	0.0079	-
b	0.180	0.250	0.300	0.0071	0.0098	0.0118
D	4.850	5.000	5.150	0.1909	0.1969	0.2028
D2	3.500	3.600	3.700	0.1378	0.1417	0.1457
E	4.850	5.000	5.150	0.1909	0.1969	0.2028
E2	3.500	3.600	3.700	0.1378	0.1417	0.1457
e	-	0.500	-	-	0.0197	-
L	0.300	0.400	0.500	0.0118	0.0157	0.0197
ddd	-	-	0.050	-	-	0.0020

1. Values in inches are converted from mm and rounded to 4 decimal digits.

Figure 7. VFQFPN32 5×5 mm 0.5 mm pitch package footprint



4 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 & Reel specifications are compliant to the EIA 481-A standard specification.

Table 4. Packages on tape and reel

Package	Description	Tape width	Tape pitch	Reel diameter	Quantity per reel
TSSOP 28	Thin shrink small outline package	16 mm	8 mm	13 in.	2500
VFQFPN 32	Very thin fine pitch quad flat pack no-lead package	12 mm	8 mm	13 in.	3000

Figure 8. Reel diagram

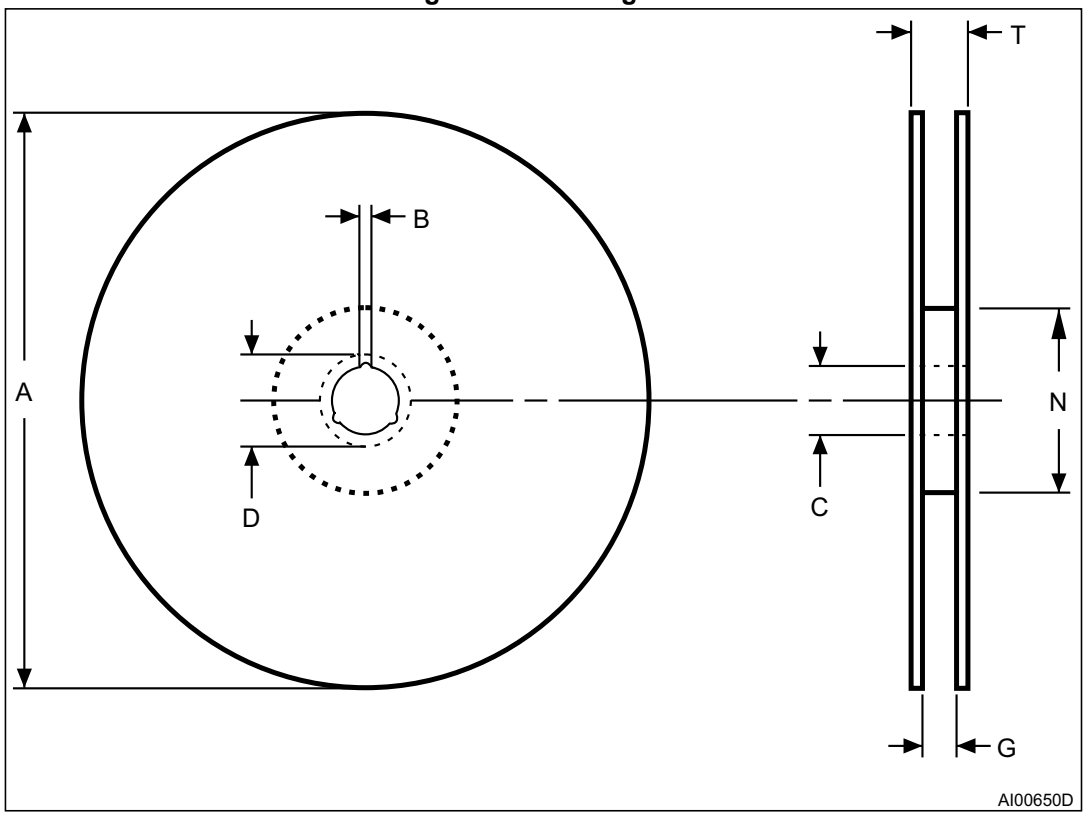
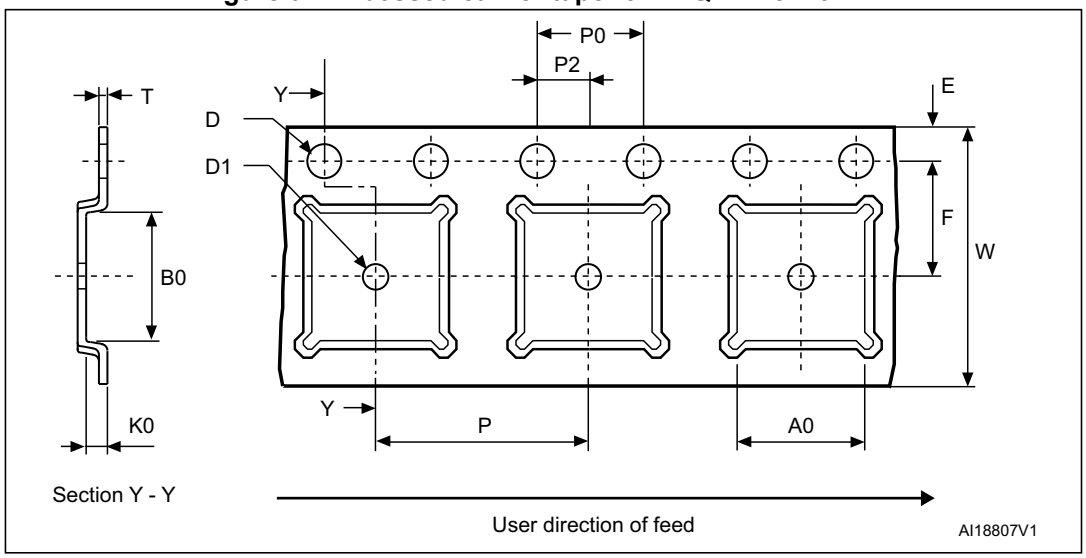


Table 5. Reel dimensions

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 9. Embossed carrier tape for VFQFPN 5 × 5 mm



1. Drawing is not to scale.

Figure 10. Chip orientation in the embossed carrier tape for VFQFPN 5 × 5 mm

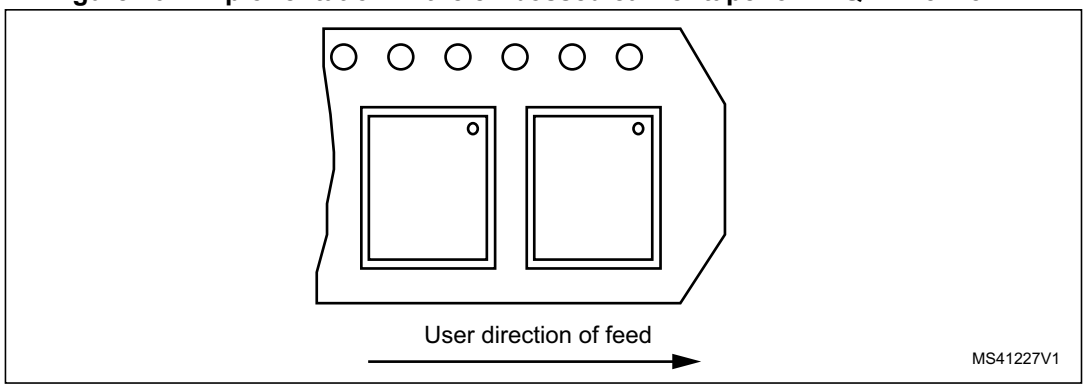
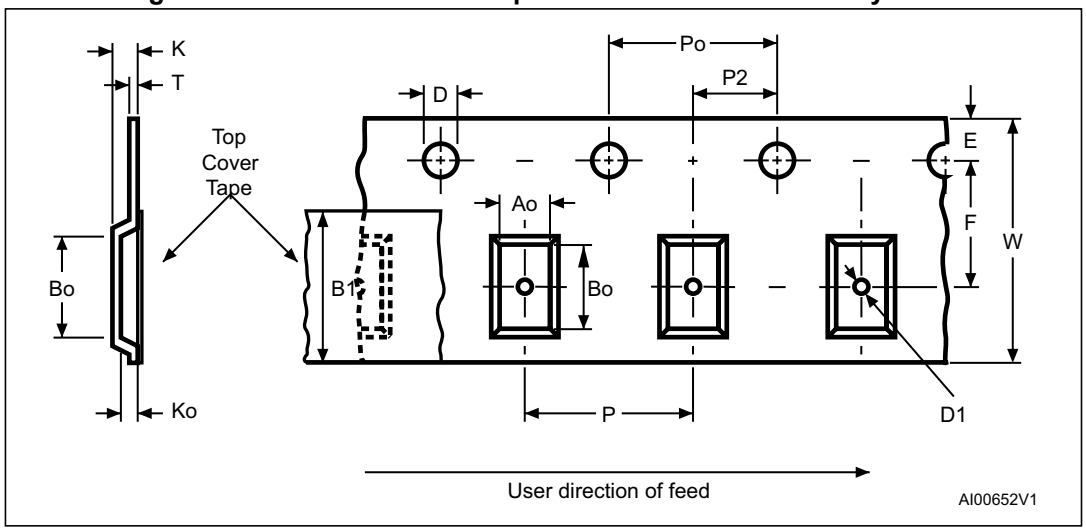


Table 6. Carrier tape dimensions for VFQFPN 5 × 5 mm

Package	A0	B0	K0	D1 Min.	P	P2	D	P0	E	F	W	T Max.	Unit
FPN 5x5	5.25 ±0.1	5.25 ±0.1	1.1 ±0.1	1.5	8 ±0.1	2 ±0.1	1.55 ±0.05	4 ±0.1	1.75 ±0.1	5.5 ±0.1	12 ±0.3	0.3 ±0.05	mm

Figure 11. Embossed carrier tape for TSSOP28 4.4 mm body width



1. Drawing is not to scale.

Figure 12. Chip orientation in the embossed carrier tape for TSSOP28 4.4 mm body width

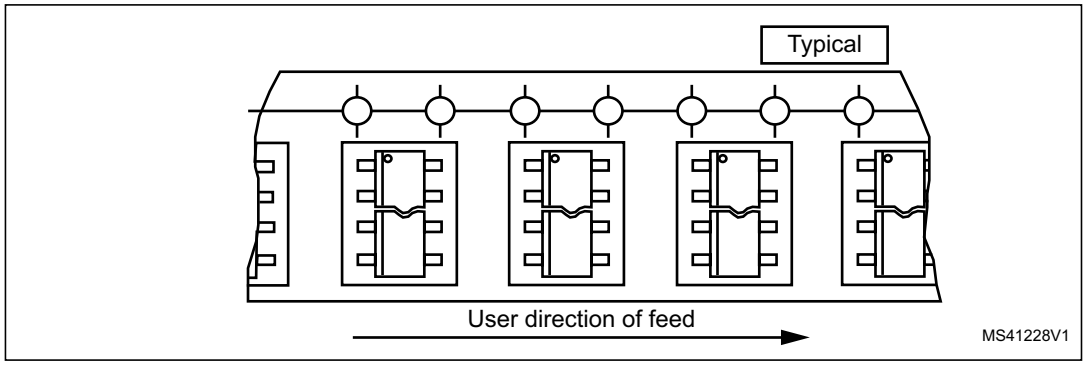


Table 7. Carrier tape constant dimensions for TSSOP 4.4 mm body width

Tape size	Ao, Bo, Ko(1)	D	E	Po	T Max.	Unit
16 mm	See note.	1.5 +0.1 / -0	1.75 ±0.1	4 ±0.1	0.4	mm

1. Ao, Bo, Ko, are determined by components sizes. The clearance between the component and the cavity must be within 0.05 mm (Min.) to 0.90 mm (Max.)

5 Package marking information

Figure 13 and *Figure 14* illustrate the typical markings of the TSSOP28 and the VQFN32 device packages, respectively.

Figure 13. TSSOP28 device package marking area

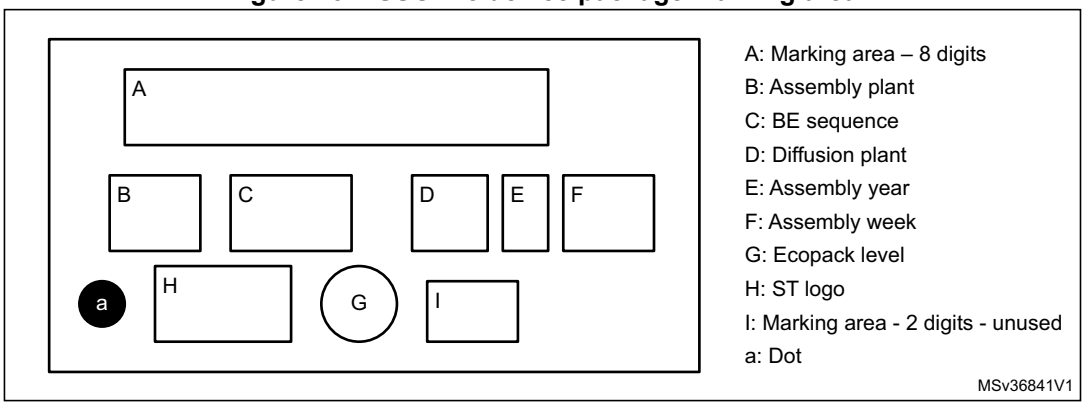
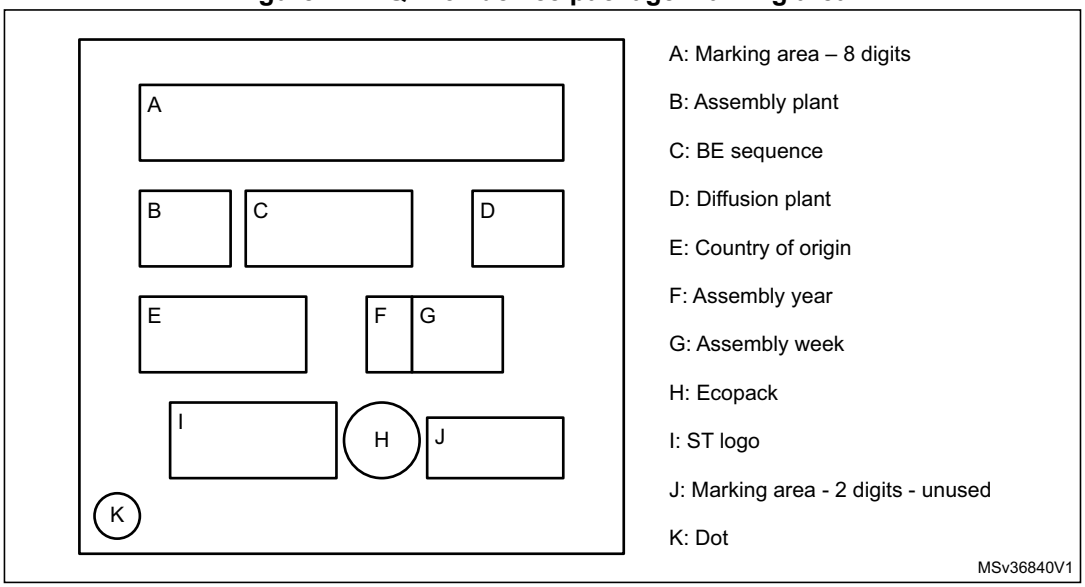


Figure 14. VQFN32 device package marking area



For both packages, the 8-digit ‘A’ marking area is equal to “P24XYYYY” with:

- X = Hardware revision
- YYYY = Firmware revision

6 Ordering information

Table 8. Ordering information

Ordering code	Firmware version	Description
ST33ZP24AR28PVSK	0x01 0x02 0x0D 0x0A	TSSOP28-packaged ST33TPM12I2C
ST33ZP24AQFNPVSK	0x01 0x02 0x0D 0x0A	VQFN32-packaged ST33TPM12I2C

7 Revision history

Table 9. Document revision history

Date	Revision	Changes
07-Mar-2012	1	Initial release.
07-Nov-2013	2	Updated logo information on page 2.
02-May-2016	3	Updated Common Criteria information on cover page. Updated *Section 3: Package information*. Added *Section 5: Package marking information* and *Section 6: Ordering information*. Small text changes.