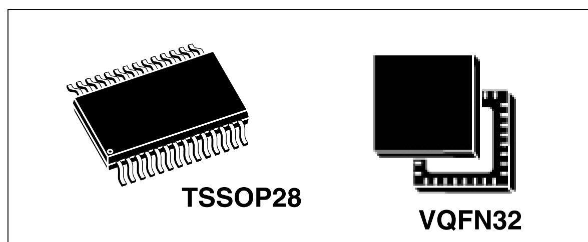
ST33TPM12LPC

life.augmented

Trusted Platform Module with LPC 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
- Common criteria (CC) certification based on the certified TPM Protection Profile (Revision 116) with Evaluation Assurance Level (EAL) 4+
- Up to 33-MHz Low Pin Count (LPC) interface V1.1
- 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 Erase/Write cycles endurance typical 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.

1 Description

The ST33TPM12LPC 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 ST33TPM12LPC is based on a secure MCU hardware platform.

The ST33TPM12LPC 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 ST33TPM12LPC 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 ST33TPM12LPC offers an LPC (Low Pin Count) communication interface compatible with Low Pin Count interface specification v1.1.

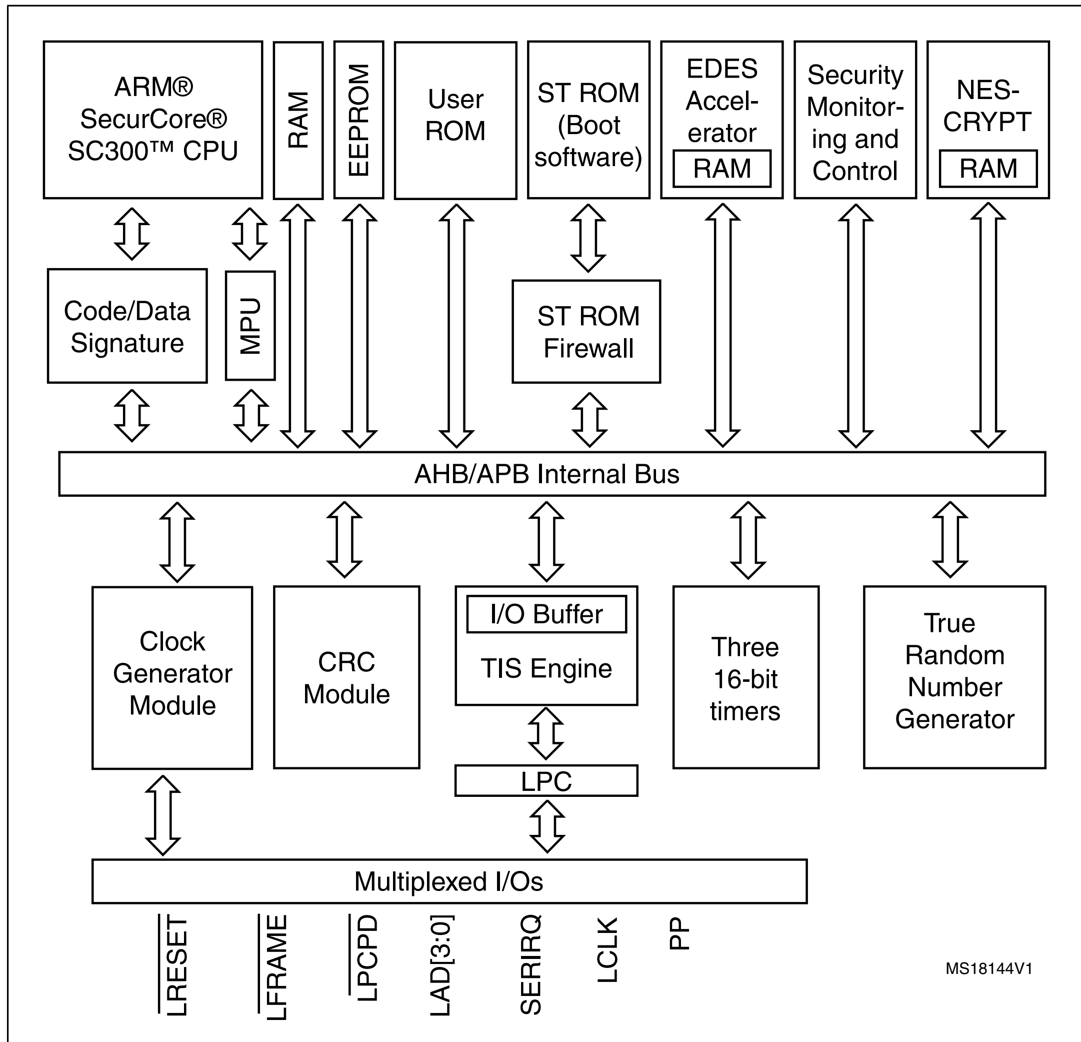
The ST33TPM12LPC features hardware accelerators for advanced cryptographic functions. The EDES peripheral provides a secure DES (Data Encryption Standard) algorithm implementation, while the NESCRYPT crypto-processor efficiently supports the public key algorithm.

The ST33TPM12LPC 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 device status are available at: www.st.com.

ECOPACK® is an ST trademark.

Figure 1. ST33TPM12LPC hardware block diagram



2 Pin and signal description

2.1 Pinout descriptions

Figure 2. TSSOP28 pinout

Signal	Pin	Pin	Signal
NC	1	28	LPCPD (active low)
NC	2	27	SERIRQ
NC	3	26	LAD0
GND	4	25	NC
NC	5	24	VPS
NC	6	23	LAD1
PP	7	22	LFRAME (active low)
VNC	8	21	LCLK
VNC	9	20	LAD2
VPS	10	19	NC
GND	11	18	GND
NC	12	17	LAD3
NC	13	16	LRESET (active low)
NC	14	15	NC

Figure 3. VQFN32 pinout

Pin	Signal	Pin	Signal
1	GND	17	NC
2	NC	18	LAD3
3	NC	19	GND
4	PP	20	NC
5	VNC	21	LAD2
6	VNC	22	LCLK
7	VPS	23	LFRAME (active low)
8	GND	24	LAD1
9	NC	25	VPS
10	NC	26	NC
11	NC	27	NC
12	NC	28	LAD0
13	NC	29	NC
14	LRESET (active low)	30	NC
15	NC	31	SERIRQ
16	NC	32	LPCPD (active low)

Table 1. Pin descriptions

Signal	Type	Description
VPS	Input	**3.3V 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.
LAD[3:0]	Bidir	**LPC Multiplexed Command, Address and Data** (see LPC Spec)
LCLK	Input	**Clock** Same clock as PCI clock on the host (typically 33 MHz, but may be as low as 10 MHz). Same clock phase with typical PCI skew. (see LPC Spec)
$\overline{\text{LFRAME}}$	Input	**Frame** indicates start of a new cycle, termination of broken cycle (see LPC Spec)
$\overline{\text{LPCPD}}$	Input	**Power Down** indicates that the peripheral should prepare for power to be removed from the LPC i/F devices. Actual power removal is system dependent (see LPC Spec)
$\overline{\text{LRESET}}$	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.
SERIRQ	Bidir	**Serialized IRQ** is used by TPM to handle interrupt support (see LPC Spec)
VNC	-	**Vendor-controlled No Connect**: internal pull-up implemented. Can be left unconnected. Must not be tied to GND.

3 Package mechanical data

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 (TSSOP) with 4.4-mm body width

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

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

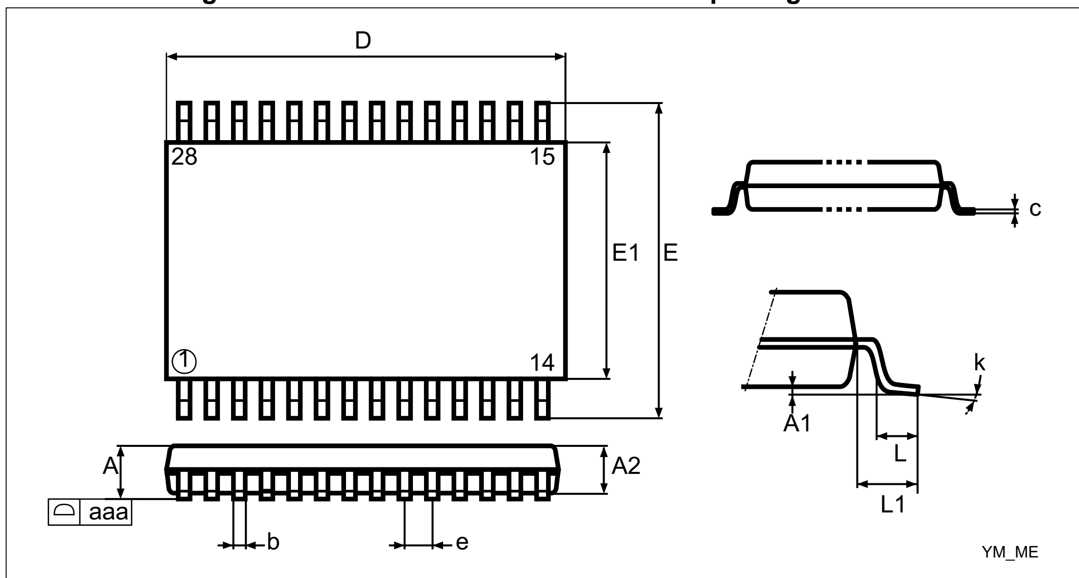


Table 2. 28-lead thin shrink small outline package mechanical data

Symbol	millimeters			inches		
	Min.	Typ.	Max.	Min.	Typ.	Max.
A			1.20			0.047
A1	0.05		0.15	0.002		0.006
A2	0.80	1.00	1.05	0.031	0.040	0.041
b	0.19		0.30	0.007		0.012
c	0.09		0.20	0.004		0.008
D	9.60	9.70	9.80	0.378	0.382	0.386
E	6.20	6.40	6.60	0.244	0.252	0.260
E1	4.30	4.40	4.50	0.170	0.173	0.177

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

Symbol	millimeters			inches		
	Min.	Typ.	Max.	Min.	Typ.	Max.
e		0.65			0.026	
L	0.45	0.60	0.75	0.018	0.024	0.0230
L1		1.00			0.040	
k	0°		8°	0°		8°
aaa			0.10			0.004

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

Figure 5. VFQFPN32 5x5 mm 0.5 mm pitch package outline

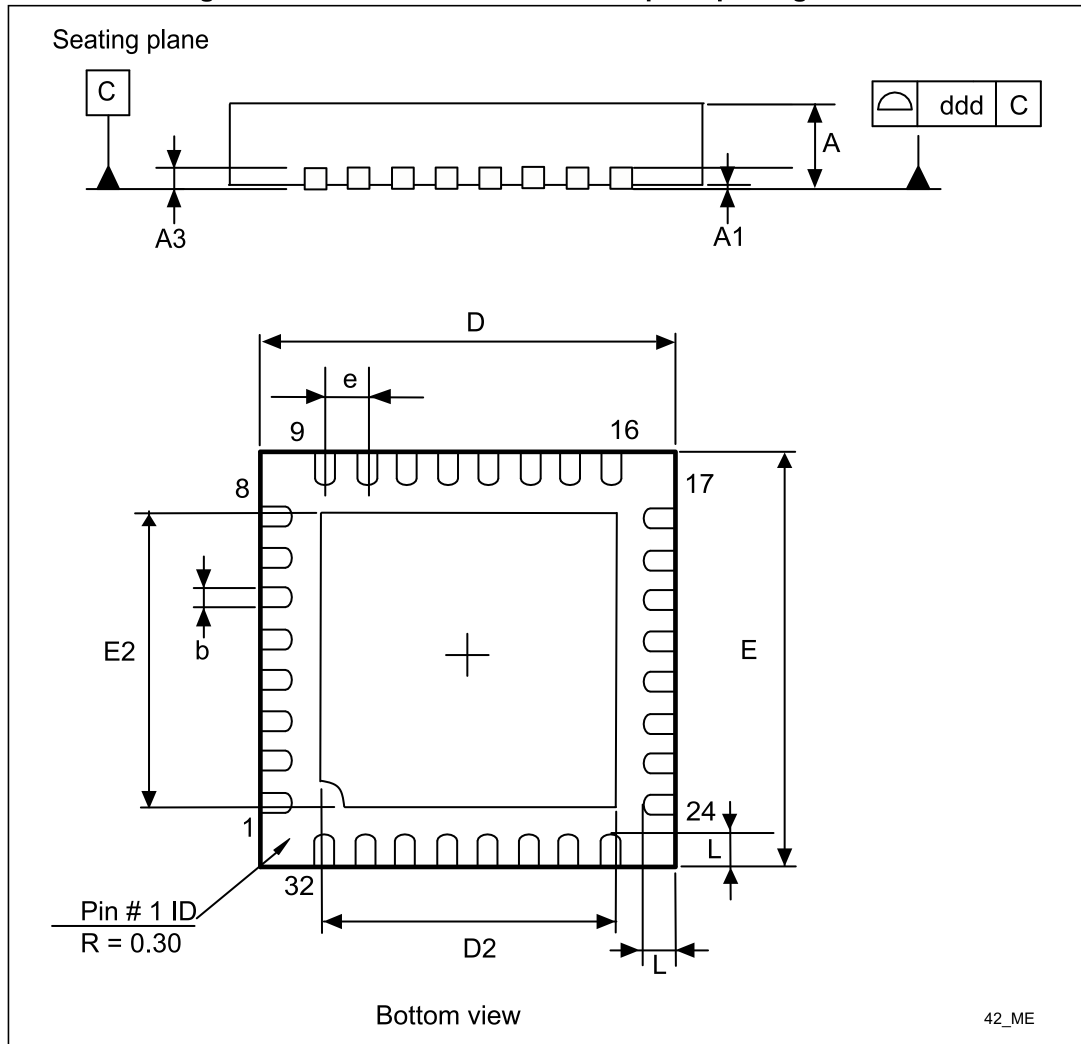


Table 3. VFQFPN32 5x5 mm package mechanical data

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

Table 3. VFQFPN32 5x5 mm package mechanical data

Symbol	millimeters			inches (1)		
	Min.	Typ.	Max.	Min.	Typ.	Max.
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.

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 6. Reel diagram

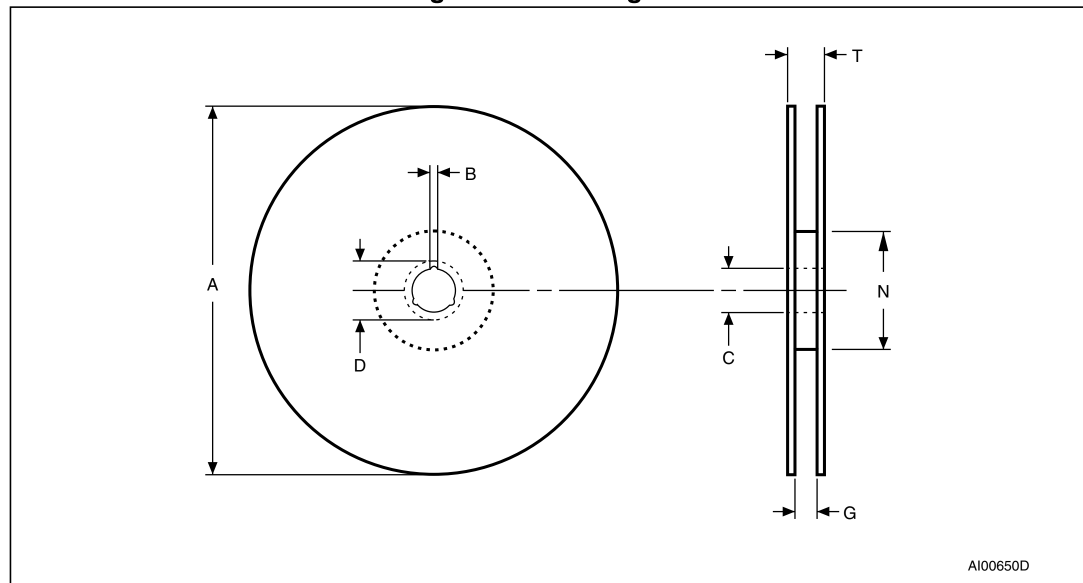
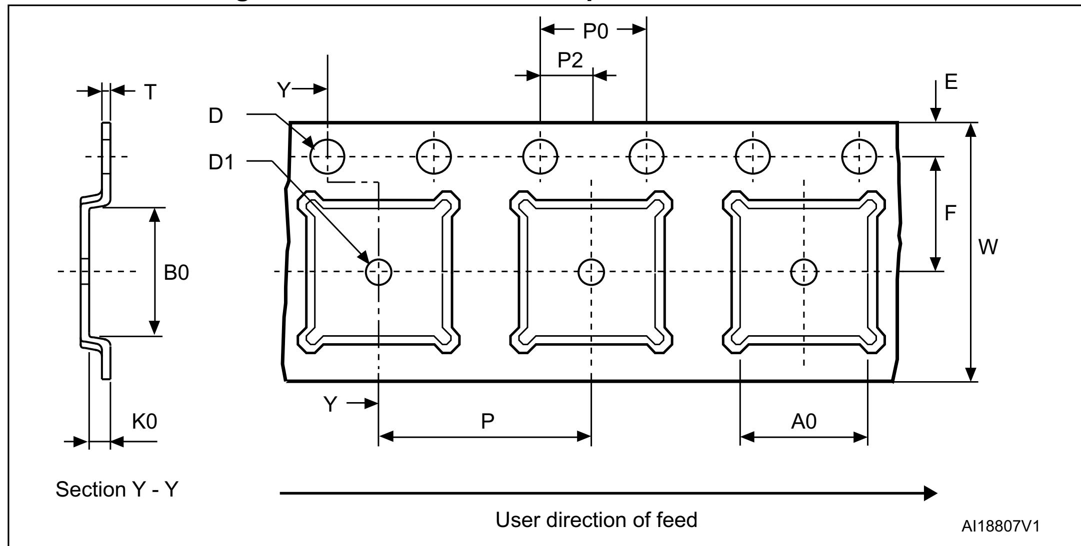


Table 5. Reel dimensions

<table>
<tr><th>Reel size</th><th>Tape width</th><th>A Max.</th><th>B Min.</th><th>C</th><th>D Min.</th><th>G Max.</th><th>N Min.</th><th>T Max.</th><th>Unit</th></tr>
<tr><td rowspan="2">13”</td><td>16</td><td rowspan="2">330</td><td rowspan="2">1.5</td><td rowspan="2">13 ±0.2</td><td rowspan="2">20.2</td><td>16.4 +2/–0</td><td rowspan="2">100</td><td>22.4</td><td rowspan="2">mm</td></tr>
<tr><td>12</td><td>12.6</td><td>18.4</td></tr>
</table>

Figure 7. Embossed carrier tape for VFQFPN 5x5 mm

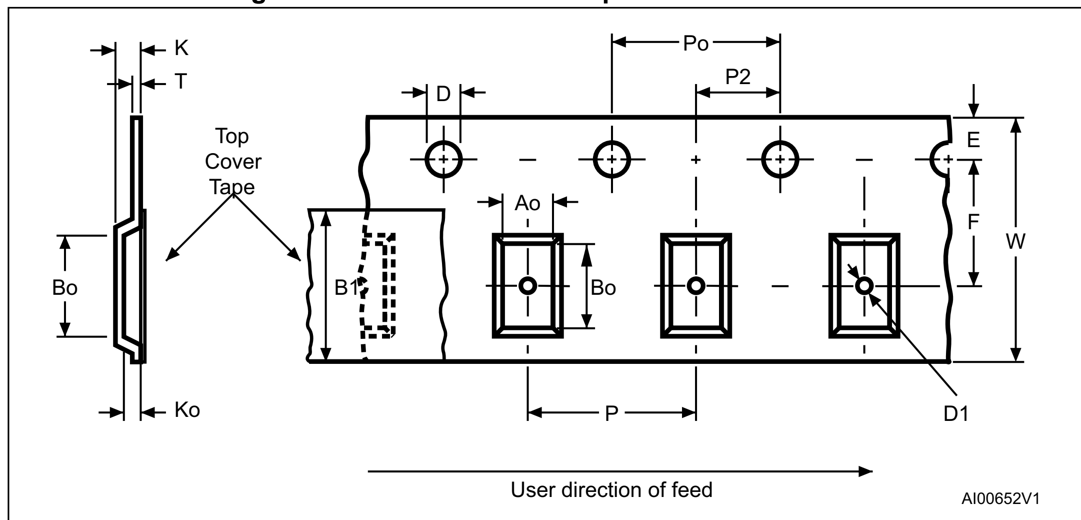


1. Drawing is not to scale.

Table 6. Carrier tape dimensions for VFQFPN 5x5 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 8. Embossed carrier tape for TSSOP 16 mm



1. Drawing is not to scale.

Table 7. Carrier tape constant dimensions for TSSOP 16 mm tape

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.)

Revision history

Table 8. Document revision history

Date	Revision	Changes
16-Sept-2011	1	Initial release.
08-Dec-2011	2	Updated *Features*.
11-Jan-2013	3	Updated Common Criteria information on page 1.
07-Nov-2013	4	Updated logo information on page 2.

Please Read Carefully:

Information in this document is provided solely in connection with ST products. STMicroelectronics NV and its subsidiaries (“ST”) reserve the right to make changes, corrections, modifications or improvements, to this document, and the products and services described herein at any time, without notice.

All ST products are sold pursuant to ST’s terms and conditions of sale.

Purchasers are solely responsible for the choice, selection and use of the ST products and services described herein, and ST assumes no liability whatsoever relating to the choice, selection or use of the ST products and services described herein.

No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted under this document. If any part of this document refers to any third party products or services it shall not be deemed a license grant by ST for the use of such third party products or services, or any intellectual property contained therein or considered as a warranty covering the use in any manner whatsoever of such third party products or services or any intellectual property contained therein.

UNLESS OTHERWISE SET FORTH IN ST’S TERMS AND CONDITIONS OF SALE ST DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY WITH RESPECT TO THE USE AND/OR SALE OF ST PRODUCTS INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE (AND THEIR EQUIVALENTS UNDER THE LAWS OF ANY JURISDICTION), OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

ST PRODUCTS ARE NOT DESIGNED OR AUTHORIZED FOR USE IN: (A) SAFETY CRITICAL APPLICATIONS SUCH AS LIFE SUPPORTING, ACTIVE IMPLANTED DEVICES OR SYSTEMS WITH PRODUCT FUNCTIONAL SAFETY REQUIREMENTS; (B) AERONAUTIC APPLICATIONS; (C) AUTOMOTIVE APPLICATIONS OR ENVIRONMENTS, AND/OR (D) AEROSPACE APPLICATIONS OR ENVIRONMENTS. WHERE ST PRODUCTS ARE NOT DESIGNED FOR SUCH USE, THE PURCHASER SHALL USE PRODUCTS AT PURCHASER’S SOLE RISK, EVEN IF ST HAS BEEN INFORMED IN WRITING OF SUCH USAGE, UNLESS A PRODUCT IS EXPRESSLY DESIGNATED BY ST AS BEING INTENDED FOR “AUTOMOTIVE, AUTOMOTIVE SAFETY OR MEDICAL” INDUSTRY DOMAINS ACCORDING TO ST PRODUCT DESIGN SPECIFICATIONS. PRODUCTS FORMALLY ESCC, QML OR JAN QUALIFIED ARE DEEMED SUITABLE FOR USE IN AEROSPACE BY THE CORRESPONDING GOVERNMENTAL AGENCY.

Resale of ST products with provisions different from the statements and/or technical features set forth in this document shall immediately void any warranty granted by ST for the ST product or service described herein and shall not create or extend in any manner whatsoever, any liability of ST.

ST and the ST logo are trademarks or registered trademarks of ST in various countries.
Information in this document supersedes and replaces all information previously supplied.
The ST logo is a registered trademark of STMicroelectronics. All other names are the property of their respective owners.

© 2013 STMicroelectronics - All rights reserved

STMicroelectronics group of companies

Australia - Belgium - Brazil - Canada - China - Czech Republic - Finland - France - Germany - Hong Kong - India - Israel - Italy - Japan - Malaysia - Malta - Morocco - Philippines - Singapore - Spain - Sweden - Switzerland - United Kingdom - United States of America

www.st.com