ST33TPM12SPI

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

Data brief

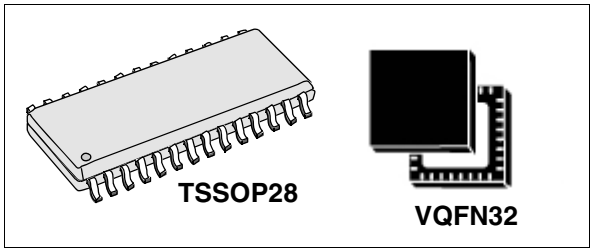
Features

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
- SPI support up to 10 MHz
- 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 ST33TPM12SPI 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 ST33TPM12SPI is based on a secure MCU hardware platform.

The ST33TPM12SPI 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 ST33TPM12SPI 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 ST33TPM12SPI offers a fast slave serial peripheral interface (SPI) supported by an embedded hardware communication engine.

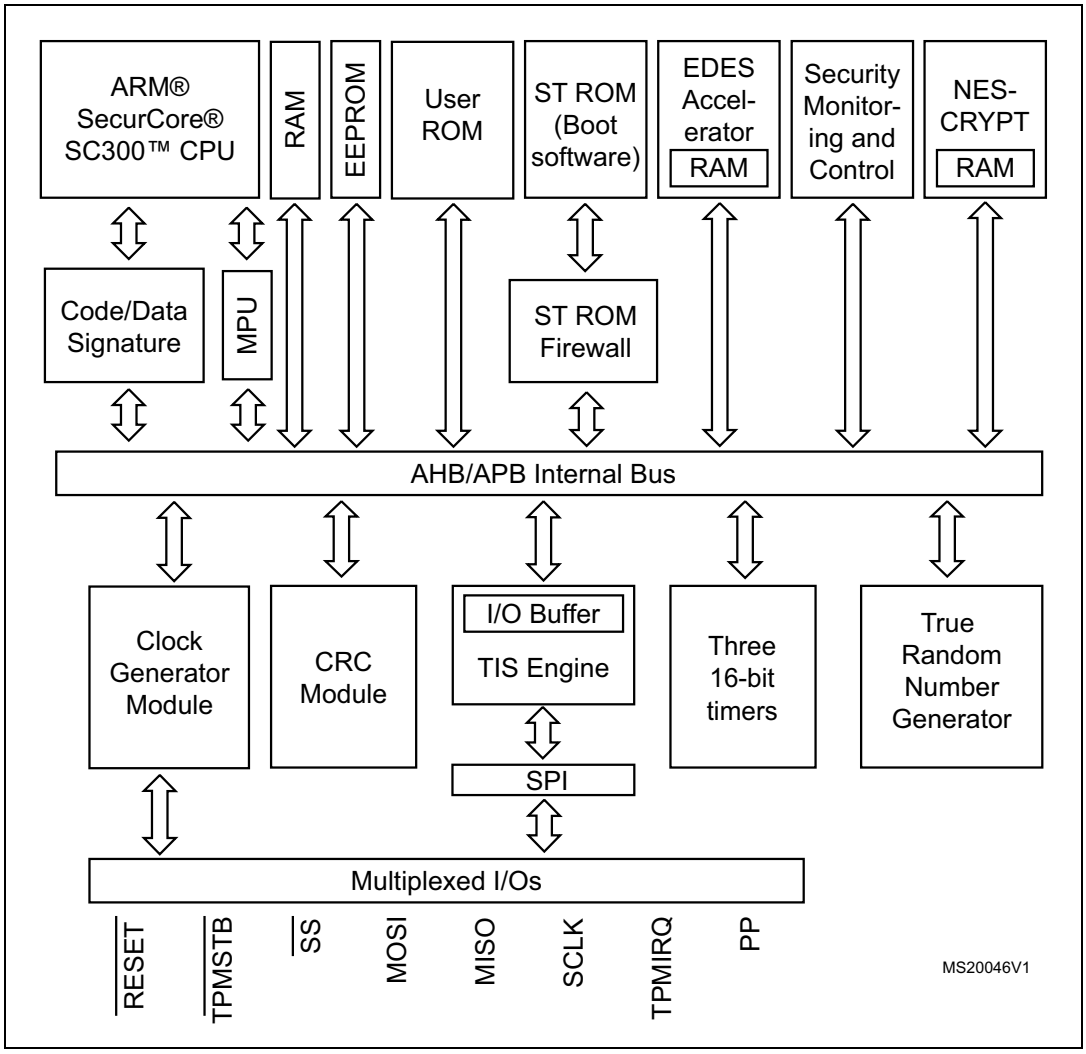
The ST33TPM12SPI features hardware accelerators for advanced cryptographic functions. The EDES peripheral provides a secure DES (Data Encryption Standard) algorithm implementation, while the NESCRYPT crypto-processor efficiently supports the public key algorithm.

The ST33TPM12SPI 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. ST33TPM12SPI hardware block diagram



2 Pin and signal description

2.1 Pinout descriptions

Figure 2. TSSOP28 pinout

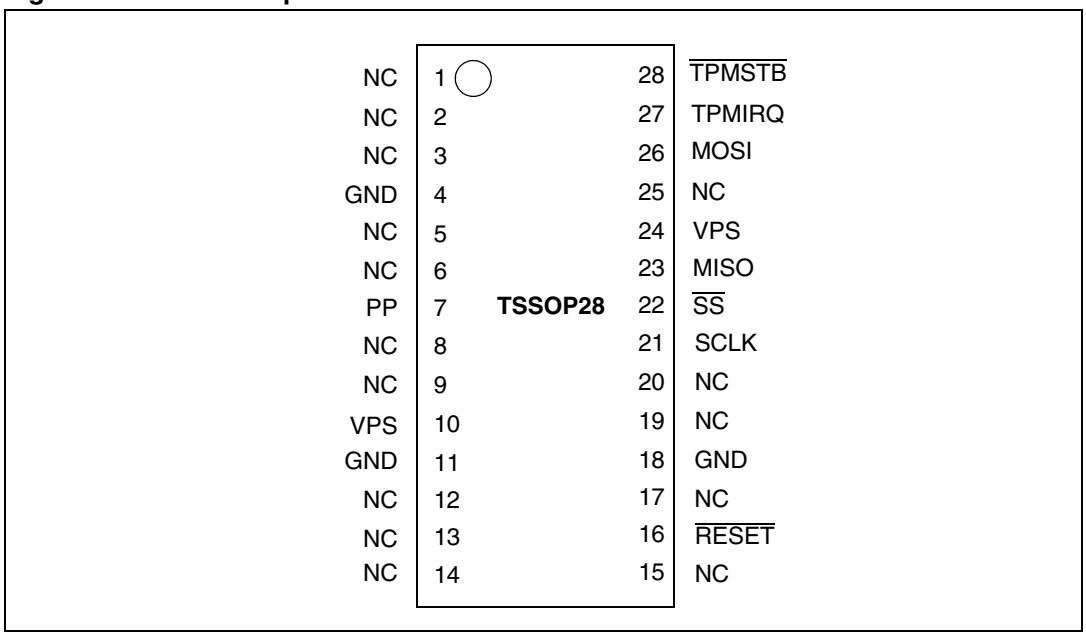


Figure 3. VQFN32 pinout

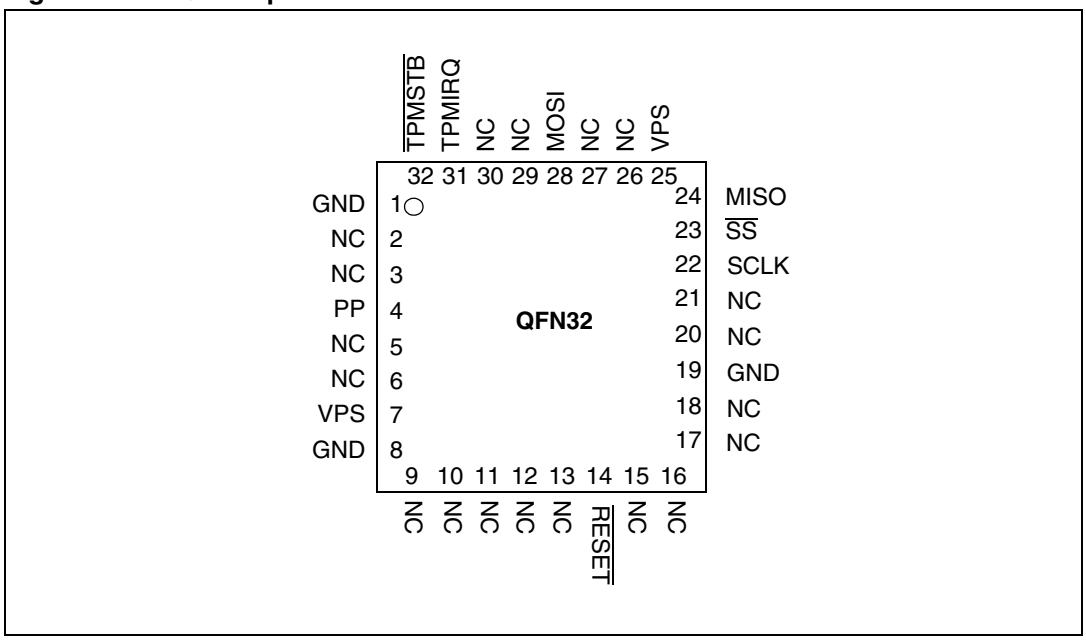


Table 1. Pin descriptions

Signal	Type	Description
VPS	Input	**3.3V 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.
$\overline{\text{TPMSTB}}$	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
MISO		**SPI** Master Input, Slave Output (output from slave)
MOSI		**SPI** Master Output, Slave Input (output from master)
SLCK		**SPI** Serial Clock (output from master)
$\overline{\text{SS}}$		**SPI** Slave Select (active low; output from master)
PP	Input	**Physical Presence**, active high, internal pull-down. Used to indicate Physical Presence to the TPM.
TPMIRQ	Output	**TPM IRQ** is used by TPM to handle interrupt support.

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

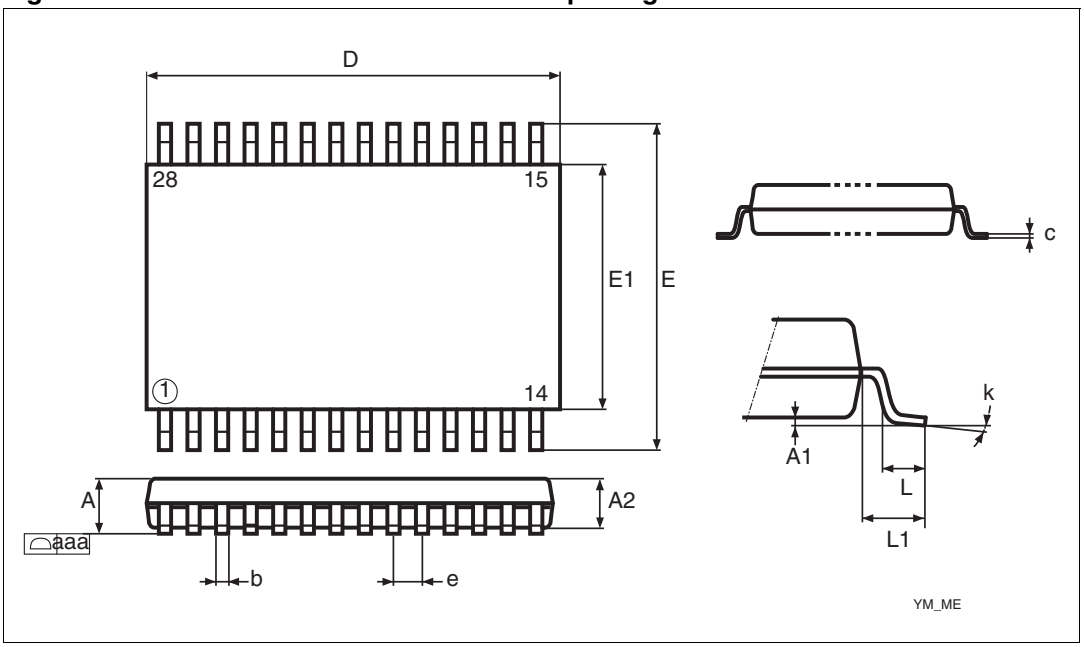


Table 2. 28-lead thin shrink small outline package mechanical data

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

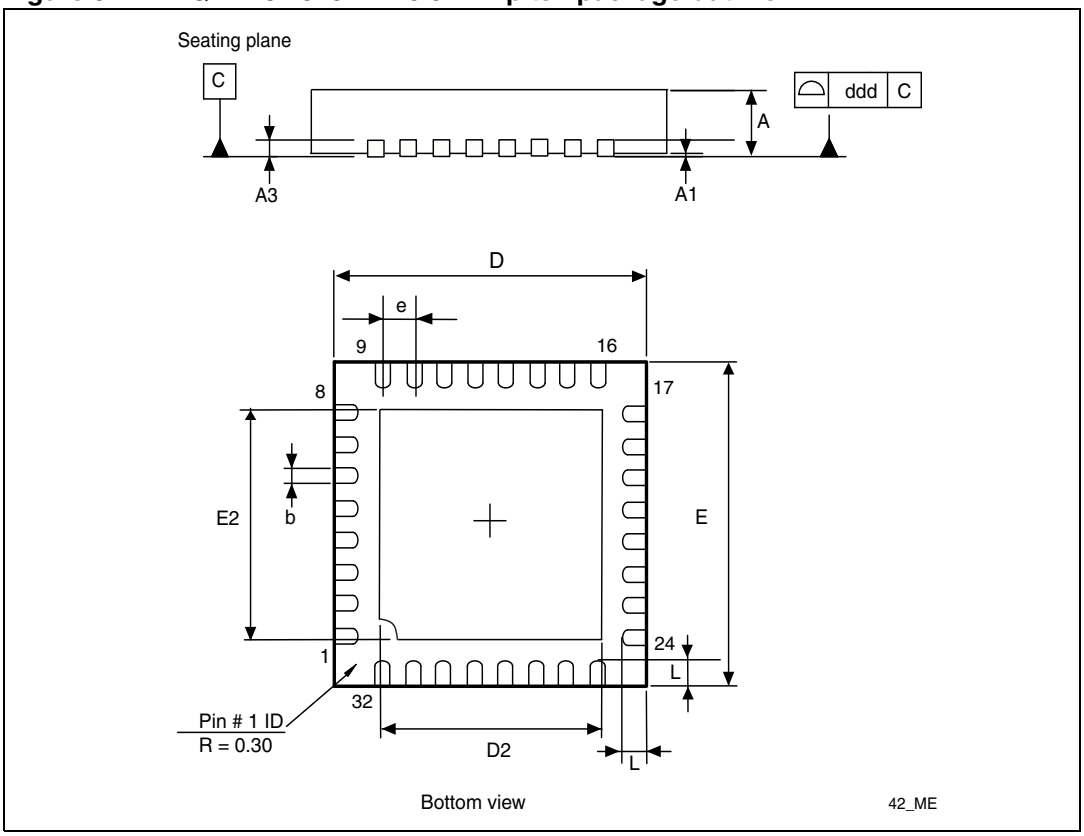


Table 3. VFQFPN32 5x5 mm package mechanical data

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
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. They contain 2500 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 & 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

Figure 6. Reel diagram

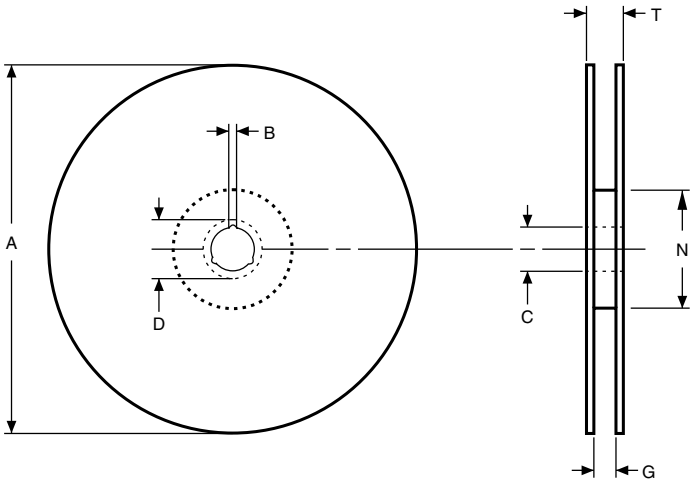


Table 5. Reel dimensions

Reel size	Tape size	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	60	22.4	mm

Revision history

Table 6. Document revision history

Date	Revision	Changes
23-Apr-2012	1	Initial release.

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.

UNLESS EXPRESSLY APPROVED IN WRITING BY TWO AUTHORIZED ST REPRESENTATIVES, ST PRODUCTS ARE NOT RECOMMENDED, AUTHORIZED OR WARRANTED FOR USE IN MILITARY, AIR CRAFT, SPACE, LIFE SAVING, OR LIFE SUSTAINING APPLICATIONS, NOR IN PRODUCTS OR SYSTEMS WHERE FAILURE OR MALFUNCTION MAY RESULT IN PERSONAL INJURY, DEATH, OR SEVERE PROPERTY OR ENVIRONMENTAL DAMAGE. ST PRODUCTS WHICH ARE NOT SPECIFIED AS "AUTOMOTIVE GRADE" MAY ONLY BE USED IN AUTOMOTIVE APPLICATIONS AT USER’S OWN RISK.

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.

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