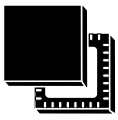
ST33TPHF2XSPI

Data brief

Long-term evolution Flash-memory-based TPM 2.0 device with an SPI interface



VFQFPN32
(5 × 5 mm)

Product status link
ST33TPHF2XSPI

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+ (AVA_VAN.5, resistant to high-potential attacks)
  - FIPS 140-2 level 2 (physical security level 3)
  - TCG certification
- SPI support at up to 33 MHz

Hardware features

- Arm® SecurCore® SC300™ 32-bit RISC core
- Highly reliable Flash memory technology
- Extended temperature range: −40 °C to 105 °C
- ESD (electrostatic discharge) protection up to 4 kV (HBM)
- 1.8 V or 3.3 V supply voltage range

Security features

- Active shield and environmental sensors
- Monitoring of environmental parameters (power)
- 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
- 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 Microsoft® Windows® 10
- 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.

These devices are easy to integrate thanks to the variety of supported interfaces and the availability of TPM ecosystem software solutions.

The STSAFE-TPM devices are all Common Criteria (EAL4+) and FIPS certified.

They embed an Arm® SecurCore® SC300™ processor with additional security features to help protect against advanced forms of attack.

The ST33TPHF2XSPI offers a slave serial peripheral interface (SPI) 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 ST33TPHF2XSPI operates in the –25 to +85 °C commercial temperature range at 1.8 V, or in the –40 °C to 105 °C extended temperature range at 3.3 V.

The device is offered in the VFQFPN32 ECOPACK2 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 description

The figure below gives the pinout of the VFQFPN32 package in which the devices are delivered. The table describes the associated signals.

Figure 1. VFQFPN32 pinout

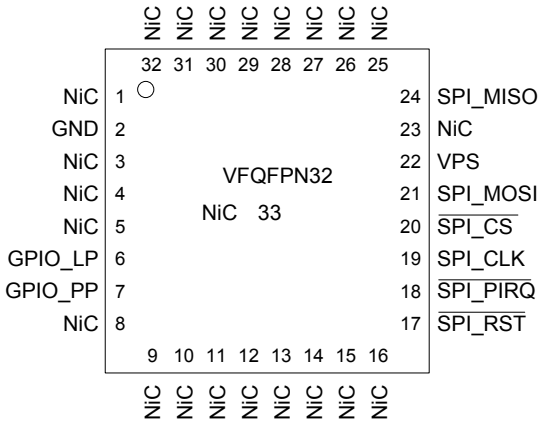


Table 1. Pin descriptions

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.
$\overline{\text{SPI\_RST}}$	Input	**SPI 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	Output	**SPI Master Input, Slave Output** (output from slave)
SPI_MOSI	Input	**SPI Master Output, Slave Input** (output from master)
SPI_CLK	Input	**SPI Serial Clock** (output from master)
$\overline{\text{SPI\_CS}}$	Input	**SPI Chip (or Slave) Select**, internal pull-up (active low; output from master)
$\overline{\text{SPI\_PIRQ}}$	Output	**SPI IRQ**, active low, open drain, used by the TPM to generate an interrupt
GPIO_PP	Input	**Physical Presence**, active high, internal pull-down. Used to indicate Physical Presence to the TPM. The 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 (`TPMLowPowerByGpio`). The GPIO function could be modified by activating the GPIOs mapped with the NV storage index feature.
NiC	-	**Not internally connected**: not connected to the die. May be left unconnected but no impact on TPM if connected.

Note: The VFQFPN32 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.

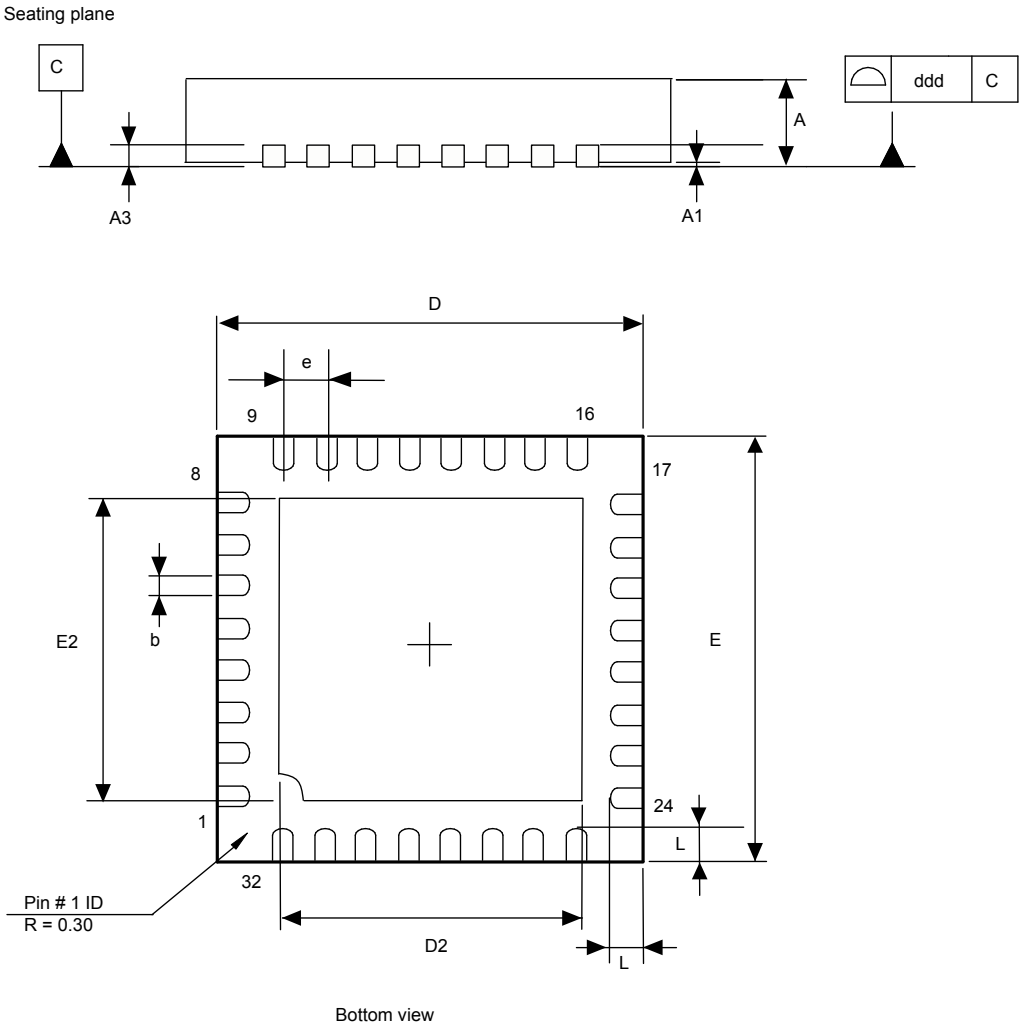
3 Package information

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 VFQFPN32 package information

VFQFPN32 is a 32-lead, 5 × 5 mm, 0.5 mm pitch, very thin fine pitch quad flat pack no-lead package.

Figure 2. VFQFPN32 - outline



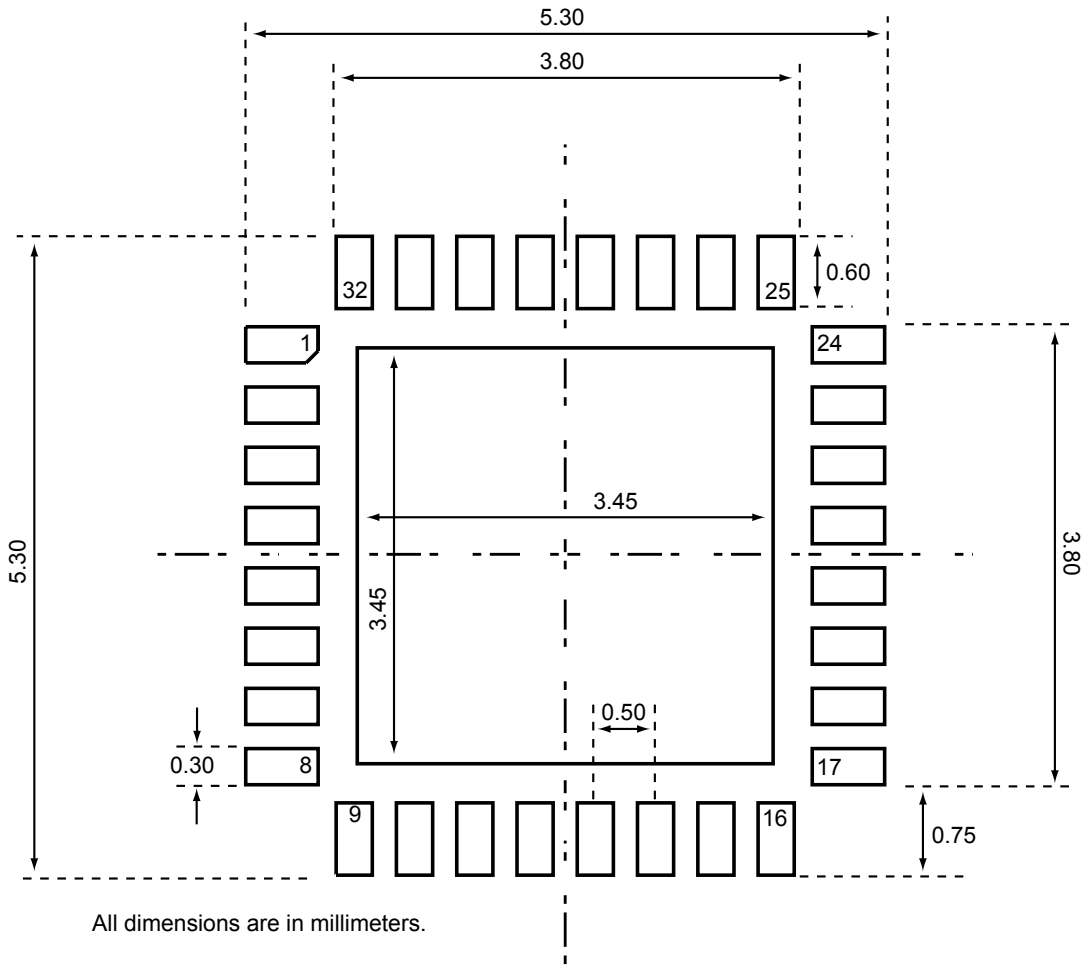
1. Drawing is not to scale.

Table 2. VFQFPN32 - 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 3. VFQFPN32 - recommended footprint



3.2 Thermal characteristics of packages

The table below provides the thermal characteristics of the VFQFPN32 package.

Table 3. 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	−43 to 108 °C
Absolute maximum junction temperature		-	125 °C
Maximum power dissipation		-	63 mW
Theta-JA, -JB and -JC	Junction to ambient thermal resistance	θ_{JA}	35.8 at 0 lfpm (1)
	Junction to case thermal resistance	θ_{JC}	1.48 at 0 lfpm(1)
	Junction to board thermal resistance	θ_{JB}	13.9 at 0 lfpm(1)

1. *Linear feet per minute.*

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 and reel specifications are compliant with the EIA 481-A standard specification.

Table 4. Packages on tape and reel

Package	Description	Tape width	Tape pitch	Reel diameter	Quantity per reel
VFQFPN32	Very thin fine pitch quad flat pack no-lead package	12 mm	8 mm	13 in.	3000

Figure 4. Reel diagram

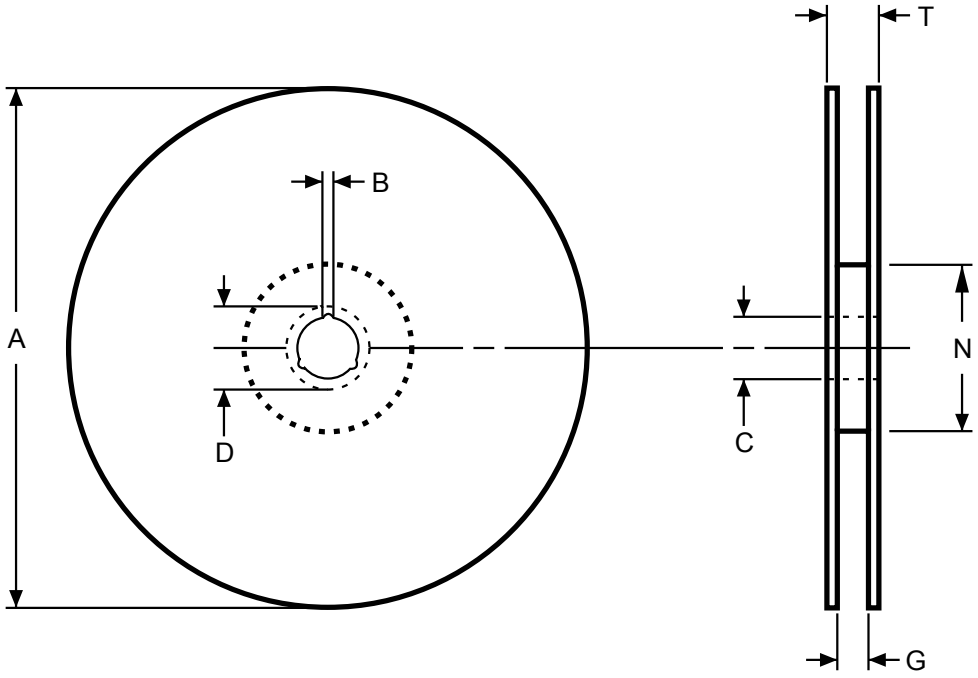
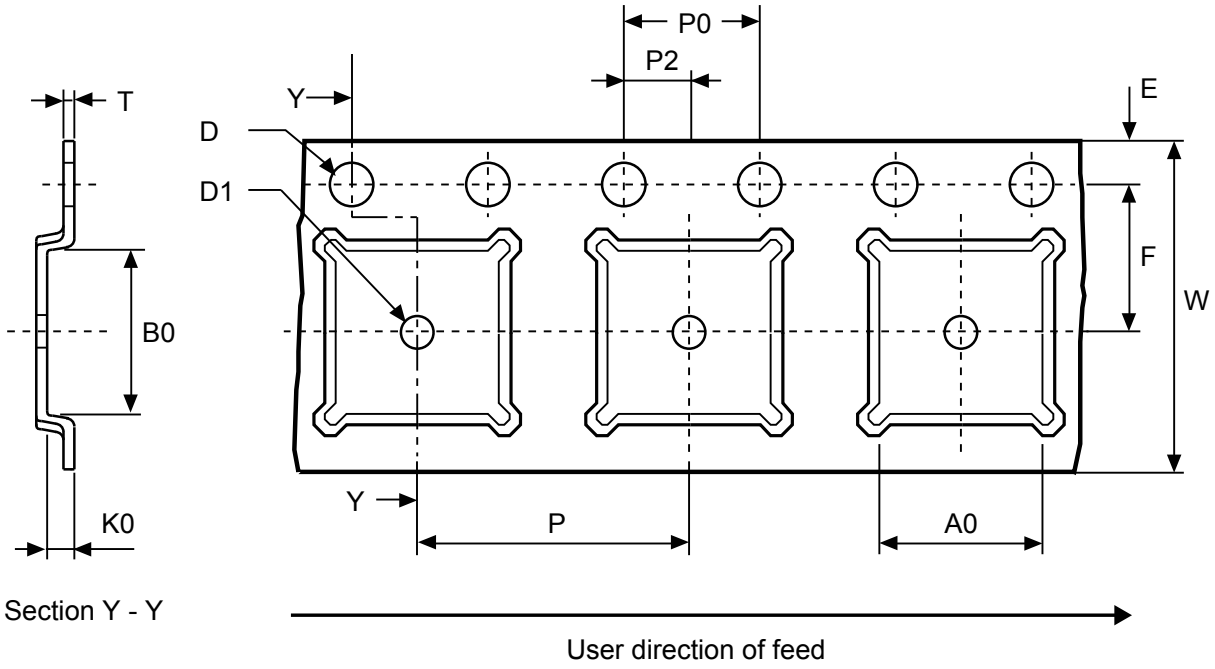


Table 5. Reel dimensions

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 5. **Embossed carrier tape for VFQFPN32 5 × 5 mm**



1. Drawing is not to scale.

Figure 6. **Chip orientation in the embossed carrier tape for VFQFPN32 5 × 5 mm**

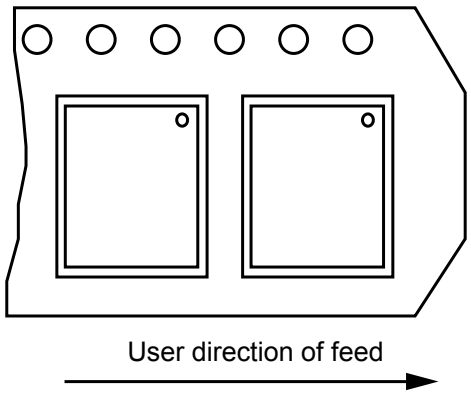


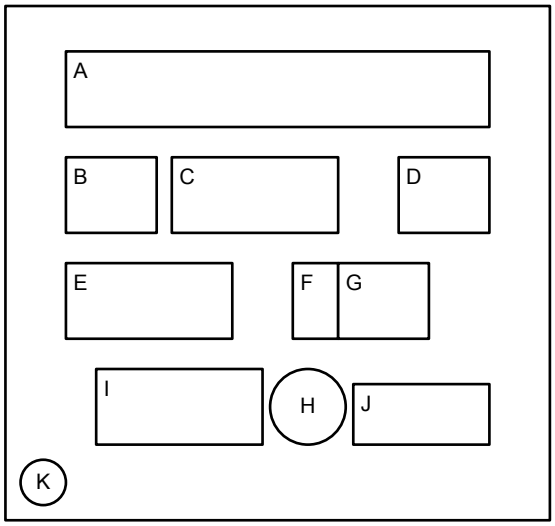
Table 6. **Carrier tape dimensions for VFQFPN32 5 × 5 mm**

Package	A0	B0	K0	D1 Min.	P	P2	D	P0	E	F	W	T Max.	Unit
VFQFPN 5×5	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

5 Package marking information

The figure below illustrates the typical marking of the VFQFPN32 device package.

Figure 7. VFQFPN32 device package marking area



A: Marking area

B: Assembly plant

C: BE sequence

D: Diffusion plant

E: Country of origin

F: Assembly year

G: Assembly week

H: ECOPACK

I: ST logo

J: Marking area - 2 digits

K: Dot

For both packages, the 6-digit ‘A’ marking area is equal to "PXYZZZ", with:

- Y = Hardware revision
- ZZZ = Product identifier

6 Ordering information

Table 7. **Ordering information for ST33TPHF2XSPI products**

Ordering code	Firmware version	Operating temperature range	Maximum SPI clock frequency	Package	Marking (area A)	Product status
ST33HTPH2X32AHC4	0x00.01.01.00 (1.256)	−40 °C to +105 °C	33 MHz	VFQFPN32	PXAHC4	NRND (Not recommended for new design)
ST33HTPH2X32AHD4	0x00.01.01.01 (1.257)				PXAHD4	Active
ST33HTPH2X32AHD8	0x00.01.01.02 (1.258)				PXAHD8	Active

Note: A technical note describing the evolutions between the different firmware versions is available through e-mail support or the sales channels.

7 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 Terms and abbreviations

Table 8. List of abbreviations

Term	Meaning
AES	Advanced Encryption Standard
CA	Certificate authority
CC	Common Criteria
DES	Data Encryption Standard
DRBG	Deterministic random bit generator
EC	Elliptic curve
ECC	Elliptic curve cryptography
ECDA	Elliptic curve direct anonymous attestation
ECDH	Elliptic curve Diffie–Hellman
ECDSA	Elliptic curve digital signature algorithm
EK	Endorsement key
ESD	Electrostatic discharge
FIPS	Federal Information Processing Standard
GPIO	General-purpose I/O
HBM	Human body model
HMAC	Keyed-Hashing for Message Authentication
NIST	National Institute of Standards and Technology
NV	Non-volatile (memory)
PKCS	Public key cryptographic standards
PSS	Probabilistic signature scheme
RNG	Random number generator
RSA	Rivest Shamir Adelman
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 Computed Group
TDES	Triple Data Encryption Standard
TPM	Trusted Platform Module
TRNG	True random number generator
TSS	TPM software stack

Revision history

Table 9. Document revision history

Date	Revision	Changes
10-Oct-2017	1	Initial release.
21-Jun-2019	2	Removed UFQFPN20 package. Updated *Features* and *Section 1: Description*. Added STSAFE-TPM logo. Updated *Figure 4: TSSOP28 - recommended footprint*. Added *Section 3.3: Thermal characteristics of packages*. Added description of marking to *Section 5: Package marking information*. Added *Section 6: Ordering information*. Removed *Reference documents* section.
06-Nov-2019	3	Updated document publication scope. Cover page: changed title of the document and updated *Product compliance*. Updated *Section 2: Pin and signal descriptions*. First page and *Section 3: Package information*: changed package presentation (no dimension changes). Added values for θ_{JC} and θ_{JB} in *Section 3.3: Thermal characteristics of packages*. Updated *Section 6: Ordering information*.
26-Jun-2020	4	Replaced STSAFE-TPM logo by STSECURE logo on cover page. Updated *TPM features* and *Product compliance*. Updated *Section 6 Ordering information*. Updated *Terms and abbreviations*. Small text changes.
19-Mar-2021	5	Removed TSSOP28 package: • Removed TSSOP28 silhouette from cover page. • Updated Section 1 Description. • Updated Section 2 Pin and signal description. • *Removed TSSOP28 package information* section. • Updated Section 3.2 Thermal characteristics of packages. • Updated Section 4 Delivery packing. • Updated Section 5 Package marking information • Updated Section 6 Ordering information. Updated Section 7 Support and information. Small text changes throughout.

Contents

List of tables

List of figures