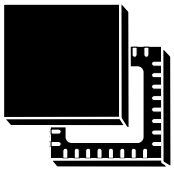
STSAFE-TPM ST33TPHF2XI2C: TPM 2.0 device with an I²C interface



VFQFPN32

5 × 5 mm

Product status link
ST33TPHF2XI2C

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 - errata 1.12 and TCG PC Client Specific TPM Platform Specifications 1.04 rev 37
- 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+ (augmented with AVA_VAN.5 and ALC_FLR.1)
  - FIPS 140-2 level 2 (physical security level 3)
  - TCG certification
- I²C support at up to 400 kHz
- Supports up to 4 GPIOs mapped with NV storage indices.

Hardware features

- Highly reliable Flash memory technology
- Extended temperature range: −40 °C to 105 °C
- ESD protection up to 4 kV (HBM) and 750 V (CDM)
- 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 SP800-90A and AIS20-compliant deterministic random-bit generator (DRBG)
- FIPS SP800-90B and AIS31-compliant true random-number generator (TRNG)
- Cryptographic algorithms:
  - RSA key generation (1024, 2048 or 3072 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 three 2048-bit RSA key pairs to reduce the TPM provisioning time

Product compliance

- Compliant with Microsoft® Windows® Internet of things (IoT) core
- Compliant with Linux® drivers
- Compliant with the TCG test suite for TPM 2.0

1 Description

The STSAFE-TPM (Trusted Platform Module) family offers a broad portfolio of standardized solutions for embedded, PC, mobile and computing applications.

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.

The STSAFE-TPM products are easy to integrate thanks to the variety of supported interfaces and the availability of TPM ecosystem software solutions.

These products are all Common Criteria (EAL4+) and FIPS certified.

The ST33TPHF2XI2C is based on a smartcard-class secure MCU.

The ST33TPHF2XI2C offers an I²C interface compliant with the TCG *PC Client TPM Profile* specifications.

The ST33TPHF2XI2C product offers resilience services during the TPM firmware upgrade process, and self-recovery of TPM firmware and critical data upon failure detection.

The ST33TPHF2XI2C 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 VFQFPN32 ECOPACK2 packages. ECOPACK is an ST trademark.

2 Pin and signal description

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

Figure 1. VQFN32 pinout

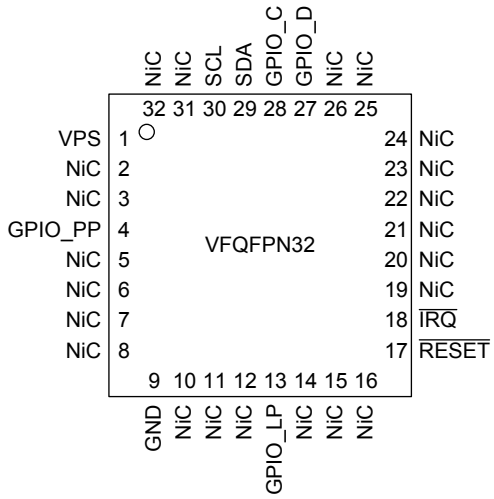


Table 1. Pin descriptions

Signal	Type	Description
VPS	Input	**Power supply**. This pin must be connected to the 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)
IRQ	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. GPIO Function could be modified by activating GPIO mapped with NV storage Indices feature.
GPIO_D	Input/output	General-purpose input/output. Defaults to low. GPIO Function could be modified by activating GPIO mapped with NV storage Indices 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 GPIO mapped with NV storage Indices 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 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.

Note: The VQFN32 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 I²C interface protocol

3.1 Compliance and features

The ST33TPHF2XI2C TPM device is compliant with [PTP 2.0 r1.04], with the following options:

- Bus speed must be in the range of 10 kbits to 400 kbits.
- 10-bit slave addressing is not supported.
- Slave address reconfiguration is supported in the range of 0x08 to 0x77.
- Clock stretching is not used.
- 1.8 V and 3.3 V are supported.
- Five localities are supported.
- The minimum guard time is 20 µs.
- Supported interrupts are “Locality Change” and “Data Available”.
- The burst count is dynamic, with a maximum burst of 1936 bytes.
- Data checksum is supported.

3.2 Register space addresses

The I²C TPM registers are used to map the FIFO TPM 2.0 interface to TPM 2.0 implementations where I²C is the host interface. The table below lists those registers.

Table 2. I²C TPM register overview

TPM-specific registers				
Address	**Name**	**Length**	**Description**	**Master access**
0x00	TPM_LOC_SEL	1	Selection of the locality of the current access.	Read/Write
0x01-0x03	Reserved	N/A	Read operations return 0xFF.	N/A
0x04	TPM_ACCESS	1	Used to gain ownership of the TPM for this particular locality.	Read/Write
0x05-0x07	Reserved	N/A	Read operations return 0xFF.	N/A
0x08-0XB	TPM_INT_ ENABLE	4	Enables specific interrupts and has the global enable feature.	Read/Write
0x0C-0x0F	Reserved	N/A	Read operations return 0xFF.	N/A
0x10-0x13	TPM_INT_ STATUS	4	Shows which interrupt has occurred.	Read/Write
0x14-0x17	TPM_INT_ CAPABILITY	4	Provides information about the interrupts supported by this particular TPM device.	Read-only
0x18-0x1B	TPM_STS	4	Contains general status details.	Read/Write
0x1C-0x1F	Reserved	N/A	Read operations return 0xFF.	N/A
0x20	TPM_HASH_END	1	This signals the end of the hash operation. Only available when locality 4 is selected.	Write-only
0x21-0x23	Reserved	N/A	Read operations return 0xFF.	N/A
0x24	TPM_DATA_FIFO	TPM_STS (burst-count)	Buffer to exchange the data for commands and responses with the host. For locality 4, this is also aliased to TPM_HASH_DATA.	Read/Write
0x25-0x27	Reserved	N/A	Read operations return 0xFF.	N/A
0x28	TPM_HASH_START	1	This signals the start of the hash operation. Only available when locality 4 is selected(1).	Write-only
0x29-0x2F	Reserved	N/A	Read operations return 0xFF.	N/A
0x30-0x33	TPM_I2C_ INTERFACE_ CAPABILITY	4	I²C Interface Capability register.	Read-only

TPM-specific registers				
Address	Name	Length	Description	Master access
0x34-0x37	Reserved	N/A	Read operations return 0xFF.	N/A
0x38-0x39	TPM_I2C_DEVICE_ ADDRESS	2	This register is used to change the I²C device address.	Write-only
0x3A-0x3F	Reserved	N/A	Read operations return 0xFF.	N/A

1. *There are two ways to access TPM_HASH_START: the first is to write 0x04 to TPM_LOC_SEL followed by the write access to TPM_HASH_START; the second is to write 0x04 to TPM_LOC_SEL, then to write the requestUse bit in TPM_ACCESS followed by the write access to TPM_HASH_START.*

3.3 Integration recommendations

3.3.1 I²C bus access load

The I²C host driver should take both the I²C bus load and the TPM load into account. This means that TPM response availability checks have to be adapted to let enough time for the TPM to process the commands. ST recommend using the interrupt mode on “response availability” events when possible as defined in the [PTP 2.0 r1.04] specification (§7.1.8). If the interrupt mode is not possible, a polling mechanism with an incremental delay can also be used.

3.3.2 NACK on TPM I²C address

In §7.2.2.1.2 “*Register write with address NACK*”, the [PTP 2.0 r1.04] specification urges to repeat the current cycle using the correct I²C device address and not to stop after the first NACK. ST recommend that the I²C host driver repeats no less than eight times before considering the TPM I²C address NACK as true.

3.3.3 Hash locality 4 delay time to process command

After the HASH_DATA and HASH_END register commands, the TPM device makes specific cryptographic calculations. During this time, I²C communication is not available and a NACK is sent. The unavailability duration depends on the BYTE number and the HASH command type. The example below provides measurements for an I²C frequency of 400 kHz with the default PCR configuration (SHA-256 and SHA-384 banks allocated). It is possible to optimize the number of NACKs if only the SHA-256 bank is allocated with the TPM2_PCR_Allocate command).

Example

32 bytes:

Hash data: < 10 µs → 0 Nack

Hash end: 3.77 ms → 85 Nack

64 bytes:

Hash data: 334 µs → 8 Nack

Hash end: 3.74 → 85 Nack

128 bytes:

Hash data: 1.08 ms → 24 Nack

Hash end: 3.77 ms → 85 Nack

1936 bytes:

Hash data: 13.7 ms → 311 Nack

Hash end: 3.84 ms → 87 Nack

3.3.4 I2C Linux driver

Refer to application note AN5714 *Integrating the ST33TPHF2xSPI and ST33TPHF2xI2C trusted platform modules with Linux®* available at for information on how to integrate the TPM product over Linux.

The follow table indicates where the user can find the I2C Linux driver and the TCG I2C driver.

Table 3. Linux drivers location

Driver	Location
I2C Linux driver	https://github.com/STMicroelectronics/TCG-TPM-I2C-DRV/tree/5.10.y
TCG I2C driver for Linux Kernel 6.x[1]	

1. *ST recommends to deactivate the checksum feature.*

4 Electrical characteristics

This section summarizes the operating and measurement conditions, and the DC and AC characteristics of the device. The parameters in the DC and AC characteristic tables that follow are derived from tests performed under the measurement conditions summarized in the relevant tables. Users should check that the operating conditions in their circuit match the measurement conditions when relying on the quoted parameters.

4.1 Absolute maximum ratings

Table 4. Absolute maximum ratings

Symbol	Parameter	Value	Unit
V_{PS}	Supply voltage	–0.3 to 3.6	V
V_{IO}	Input or output voltage relative to ground	–0.3 to V_{PS} +0.3	V
T_A	Ambient operating temperature	–25 to +85	°C
		–40 to +105(1)	
T_{STG}	Storage temperature (refer to [AN2639])	–65 to +150	°C
V_{ESD}	Electrostatic discharge voltage according to JESD22-A114, human body model	4000	V
	Electrostatic discharge voltage according to ANSI ESD STM5.3.1, charged device model	750	V

1. *For the 3.3 V voltage range only.*

Note: Stresses listed above may cause permanent damage to the device. This is a stress rating only and functional operation of the device at these or any other conditions above those indicated in the operational sections of the specification is not implied.

Exposure to absolute maximum rating conditions for extended periods may affect device reliability.

4.2 DC and AC characteristics

T_A = −40 to 105 °C (for the 3.3 V voltage range only) and T_A = −25 to 85 °C (for the 1.8 V and 3.3 V voltage ranges).

The voltage (V_{PS}) on all inputs or outputs must not exceed one of the two authorized ranges: 1.8 V ±10% or 3.3 V ±10%.

Table 5. DC characteristics (V_{PS} = 1.8 V or 3.3 V ± 10%)

Symbol	Parameter	Condition	Min.	Typ.	Max.	Unit
V_{IL}	Input low voltage	-	–0.3	-	0.2 × V_{PS}	V
V_{IH}	Input high voltage	-	0.7 × V_{PS}	-	V_{PS} + 0.3	V
I_{IL}	Input low current in high Impedance mode	0 V < V_{IL} < 0.2 × V_{PS}	–10	-	10	µA
	Input low current in Weak Pull-up mode (V_{PS} = 1.8 V±10%)	0 V < V_{IL} < 0.2 × V_{PS}	–500	-	1000	
	Input low current in Weak Pull-up mode (V_{PS} = 3.3 V±10%)	0 V < V_{IL} < 0.2 × V_{PS}	–500	-	-	
I_{IH}	Input high current in high Impedance mode	0.7 × V_{PS} < V_{IH} < V_{PS}	–10	-	10	µA
	Input high current in Weak Pull-down mode (V_{PS} = 1.8 V±10%)	0.7 × V_{PS} < V_{IH} < V_{PS}	–20	-	20	
	Input high current in Weak Pull-down mode (V_{PS} = 3.3 V±10%)	0.7 × V_{PS} < V_{IH} < V_{PS}	–30	-	30	

Symbol	Parameter	Condition	Min.	Typ.	Max.	Unit
V_{OH}	Output high voltage	I_{OH} = −1 mA	0.75 × V_{PS}	-	V_{PS}	V
V_{OL}	Output low voltage (V_{PS} = 1.8 V±10%)	I_{OL} = 500 µA	0	-	0.15 × V_{PS}	V
	Output low voltage (V_{PS} = 3.3 V±10%)	I_{OL} = 1 mA	0	-	0.15 × V_{PS}	
POR	Power on reset voltage(1)	-	-	1.45	1.61	V
PD_R	Pull-down resistor	-	-	10	-	kΩ
PU_R	Pull-up resistor	-	-	100	-	kΩ

1. *V_{PS} voltage from which the device starts to run or V_{PS} voltage below which the device starts to switch off during a shutdown.*

4.3 Overshoot

The TPM has been tested in accordance with JEDEC standard JESD78D.

- Tolerated overshoot: 1.5 ×V_{PS}
- Maximum time during overshoot: 10 ms.

4.4 Performance and power consumption characteristics

The values provided in the table below were measured at T_A = −40 to 105 °C (for the 3.3 V voltage range only) and T_A = −25 to 85 °C (for the 1.8 V and 3.3 V voltage ranges).

Table 6. Power-on and warm reset timing characteristics

Symbol	Parameter	Condition	Min.	Typ.	Max.	Unit
t_{WL}	$\overline{\text{RESET}}$ pin low state pulse width for reset	-	1	-	-	ms
t_{INIT}	Minimum time for TPM_ACCESS_x registers to contain valid data from TPM reset	-	-	-	25	ms
t_{CMD}	Time required before sending first TPM command from TPM reset	-	-	-	30	ms
t_{POR_RST}	POR to reset time	C_{LOAD} = 30 pF	-	200	-	µs
t_{Init_stb}	Wakeup time from Standby	-	-	-	150	µs

Table 7. Power consumption characteristics

The values provided in the table below were measured at T_A = 25 °C.

Symbol	Parameter	Typ.	Max.	Unit
I_{CC} Run	Normal TPM operation	-	17.5	mA
I_{CC} Idle	Supply current when not processing any commands.	4	-	mA
I_{CC} Standby	Supply current when the device is in Deep Sleep mode(1).	60	-	µA

1. *Activated by default. See Proprietary commands and Technical features.*

Figure 2. Power on and warm reset sequence

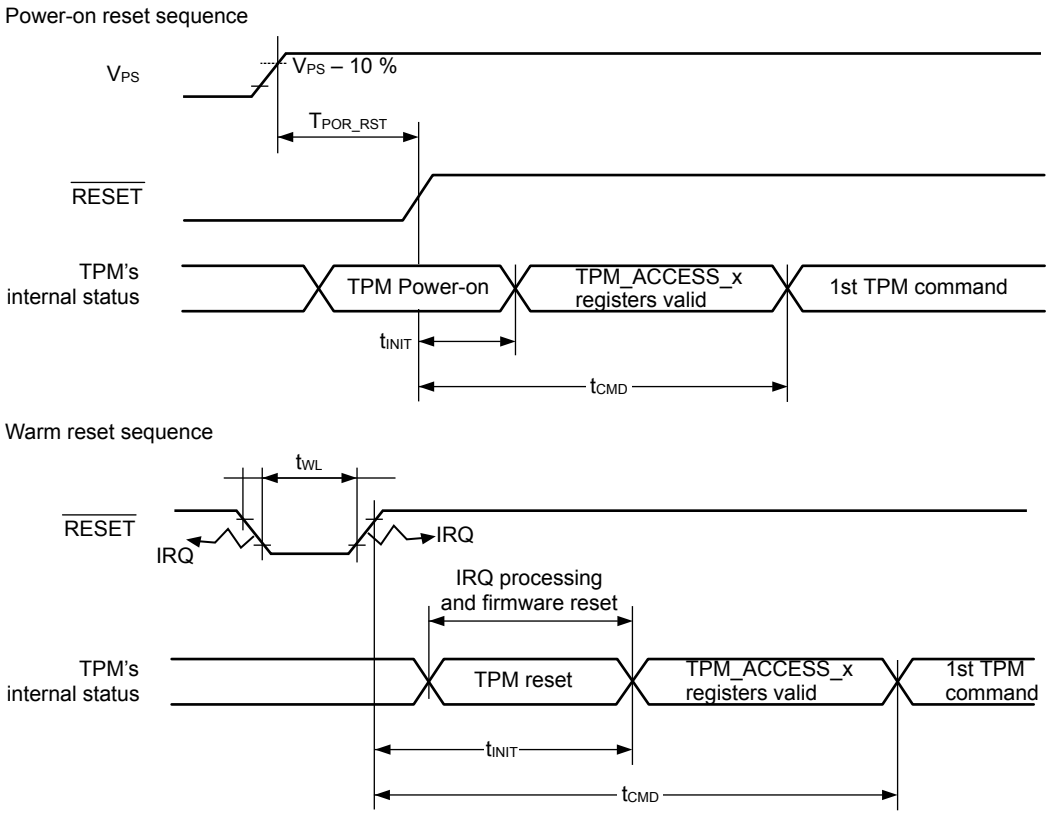
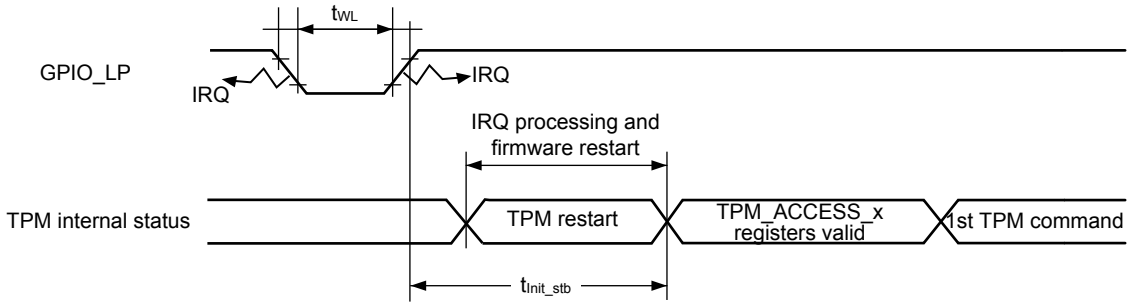


Figure 3. Standby sequence



4.5 I²C characteristics

Table 8. I²C characteristics

Symbol	Parameter	Min.	Max.	Unit
f_{SCL}	SCL clock frequency	10	400	kHz
t_{LOW}	Low period of the SCL clock	1.3	-	µs
t_{HIGH}	High period of the SCL clock	0.6	-	µs
$t_{SU;STA}$	Setup time for a repeated Start condition	0.6	-	µs
t_r	Rise time of the SDA or SCL signal	20	300	ns
t_f	Fall time of the SDA or SCL signal (VPS = 3.3 V)	12	300	ns
	Fall time of SCL (VPS = 1.8 V)	6	300	
$t_{VD;DAT}$	Data valid time	-	0.9	µs
$t_{VD;ACK}$	Data valid acknowledge time	-	0.9	µs
$t_{SU;STO}$	Setup time for a Stop condition	0.6	-	µs
$t_{SU;DAT}$	Data setup time	100	-	ns
$t_{HD;DATA}$	Data hold time	0	-	ns
$t_{HD;STA}$	Hold time for a (repeated) Start condition	0.6	-	µs
t_{Start}	$t_{HD;STA} + t_{LOW}$	1.9	-	µs

Figure 4. I²C bus protocol

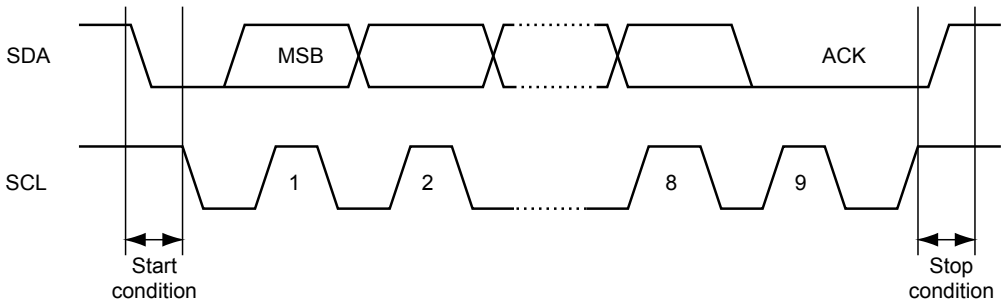
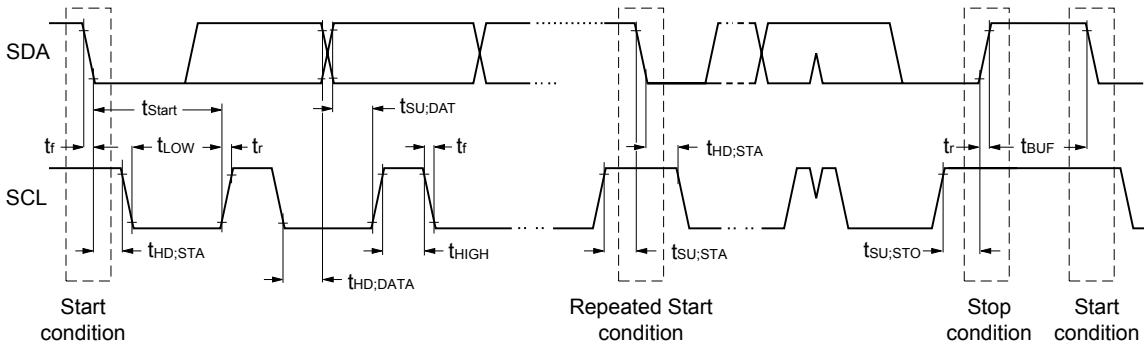


Figure 5. Typical application with I²C bus and timing diagram



4.6 AC measurement conditions

Table 9. AC measurement conditions

T_A = −40 to 105 °C (for the 3.3 V voltage range only) and T_A = −25 to 85 °C (for the 1.8 V and 3.3 V voltage ranges).
f = 1 MHz, unless otherwise specified.

Parameter	Value (1)
Input rise and fall times	10 ns max
Input pulse voltage	V_{IL} to V_{IH}
Input timing reference voltage	0.5 × V_{PS}
Output timing reference voltage	V_{OL} to V_{OH}

1. *Measurement points are at CMOS levels: 0.3 × V_{PS} and 0.7 × V_{PS}.*

Figure 6. AC testing input/output waveforms

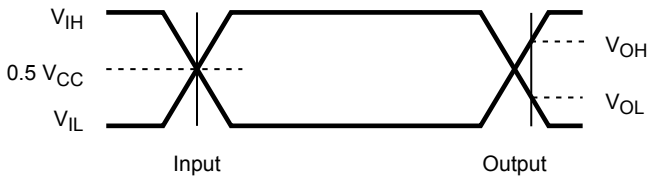
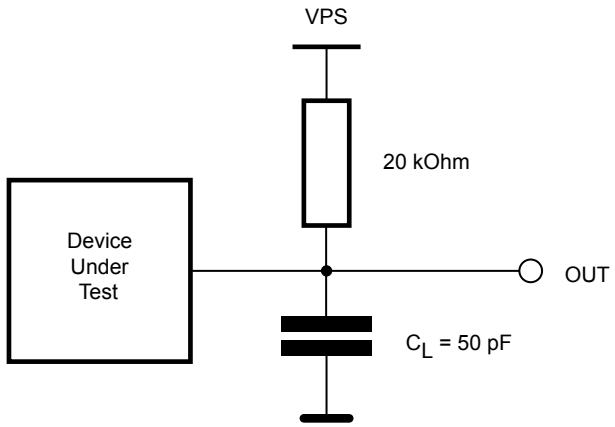


Figure 7. AC testing load circuit



C_L includes JIG capacitance

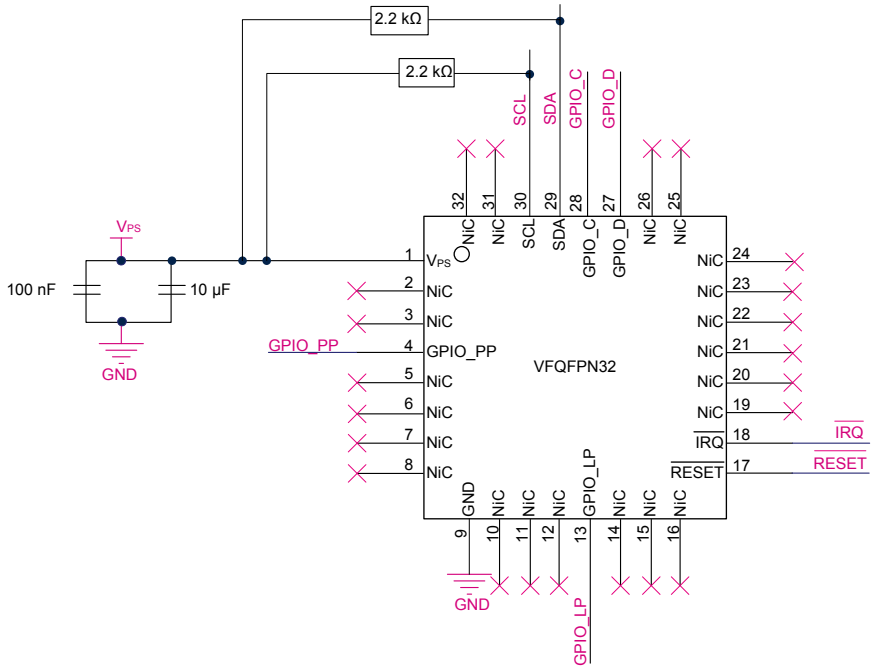
5 Integration guidance

5.1 Typical hardware implementation

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

The figure below shows the hardware implementation for the VFQFPN32 package.

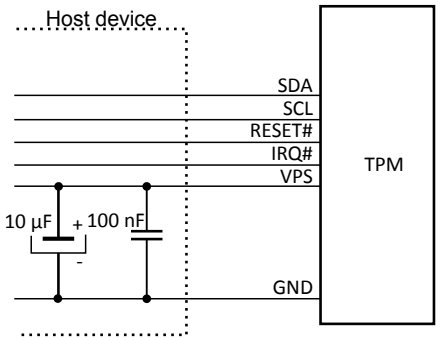
Figure 8. Typical hardware implementation (VFQFPN32 package)



5.2 Power supply filtering

As mentioned in Section 2 Pin and signal description, the power supply of the circuit must be filtered using the circuit shown in the figure below.

Figure 9. 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 10. Maximum V_{PS} rising slope

Symbol	Parameter	Value	Unit
S_{VPS}	Maximum VPS rising slope	3.3	V/µs

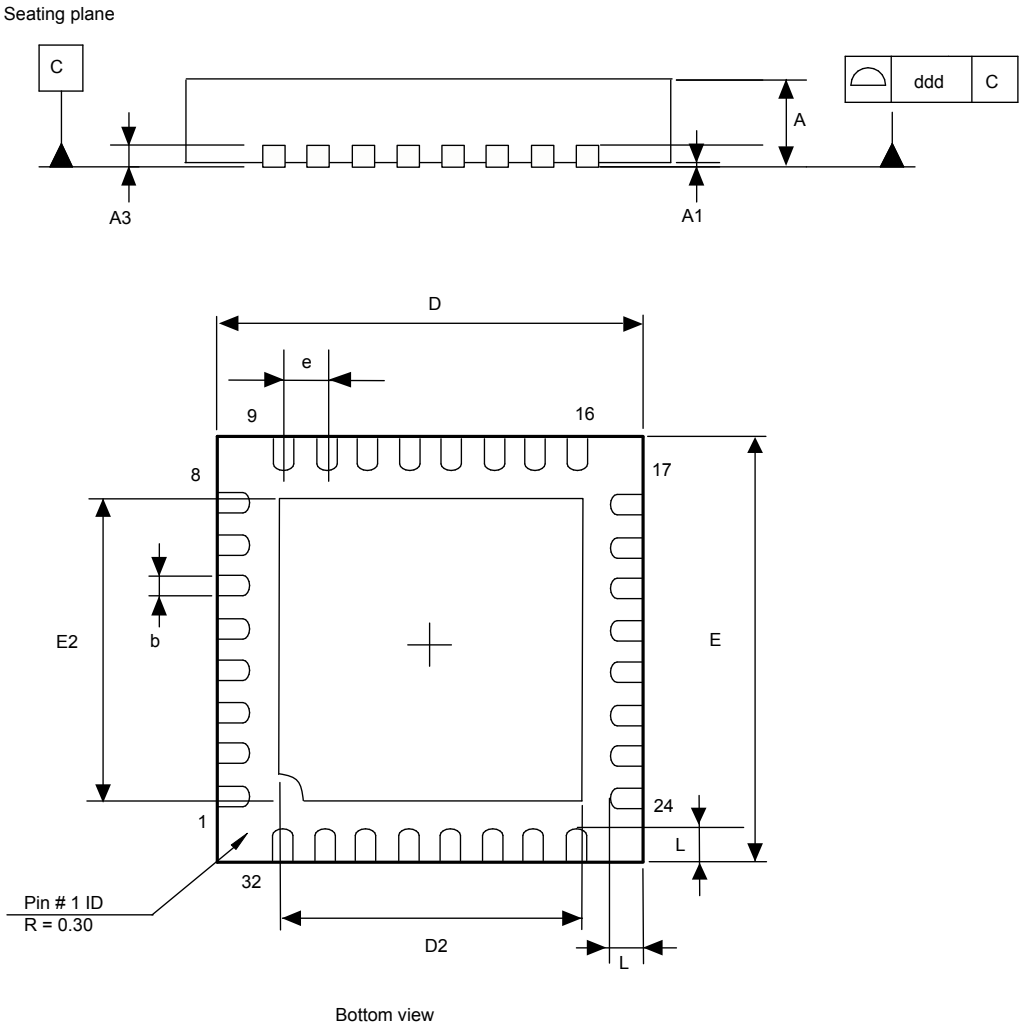
6 Package information

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.

6.1 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 10. VFQFPN32 - outline



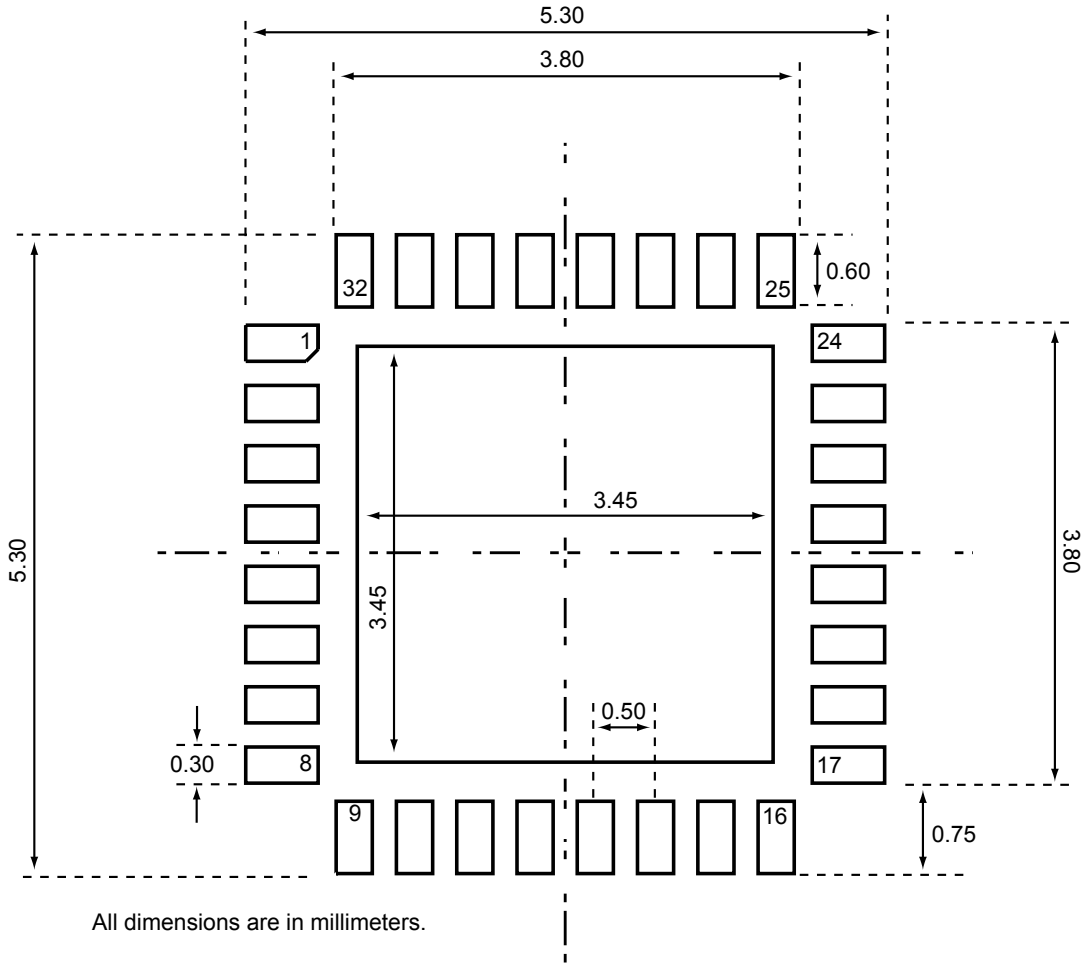
1. Drawing is not to scale.

Table 11. 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 11. VFQFPN32 - recommended footprint



6.2 Thermal characteristics of packages

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

Table 12. 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} (1)	35.8 at 0 lfpm (2)
	Junction to case thermal resistance	θ_{JC}	1.48 at 0 lfpm (2)
	Junction to board thermal resistance	θ_{JB}	13.9 at 0 lfpm (2)

1. *According to JESD51-2 (still air condition).*
2. *Linear feet per minute.*

7 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 13. 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 12. Reel diagram

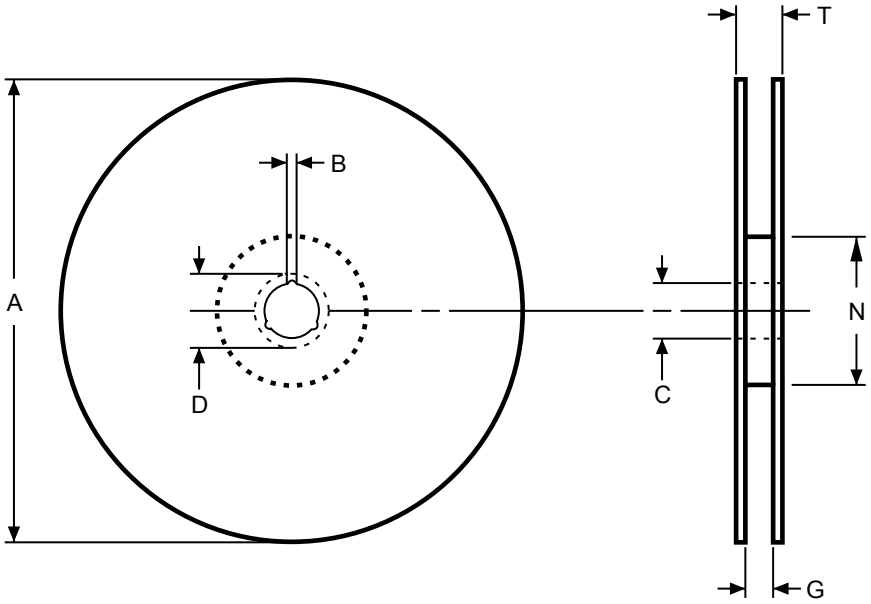
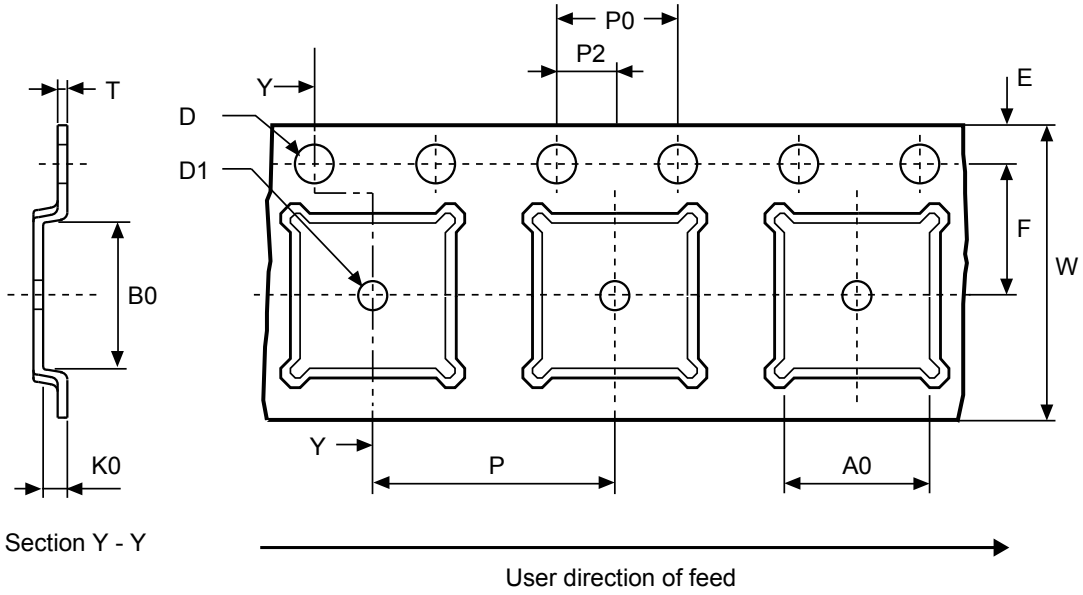


Table 14. Reel dimensions

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



1. Drawing is not to scale.

Figure 14. **Chip orientation in the embossed carrier tape for VFQFPN32 5 × 5 mm**

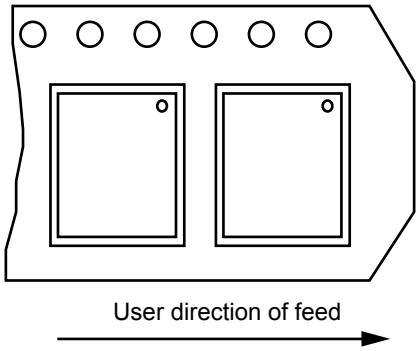


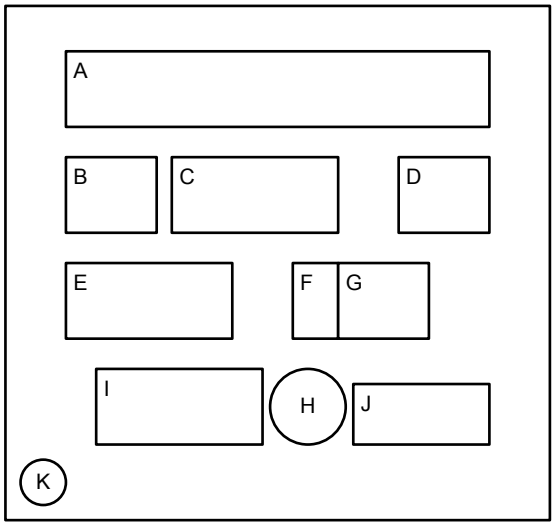
Table 15. **Carrier tape dimensions for VFQFPN32 5 × 5 mm**

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

8 Package marking information

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

Figure 15. 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: Second-level interconnect (JESD97)

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

9 Ordering information

Table 16. Ordering information

Ordering code	Firmware version	TPM Library	Package	Marking A	Product status
ST33HTPH2X32AHE1	0x00.02.02.00 (1.512)	1.38	VFQFPN32	PXAHE1	Active (recommended for new design)
ST33HTPH2X32AHD5	0x00.02.01.10 (1.272)	1.38		PXAHD5	Active

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

10 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 17. List of abbreviations

Term	Meaning
AES	Advanced Encryption Standard
CA	Certificate authority
CC	Common Criteria
DAM	Dictionary attack mitigation mechanism
Data byte	Byte from the TPM command or answer or register value.
DES	Data Encryption Standard
EC	Elliptic curve
ECC	Elliptic curve cryptography
ECDDA	Elliptic curve direct anonymous attestation
ECDH	Elliptic curve Diffie-Hellman
ECDSA	Elliptic curve digital signature algorithm
ECSchorr	Elliptic curve with Schnorr signature code
EK	Endorsement key
eps	Endorsement primary seed
FIPS	Federal Information Processing Standard
FU	Firmware update
GPIO	General-purpose I/O
HLK	Hardware Lab Kit (Windows®)
HMAC	Keyed-Hashing for Message Authentication
I²C	Inter-integrated circuit
lfpm	Linear feet per minute
HSM	Hardware security module
HWINTF	Hardware interface layer in the TPM's internal firmware; used to drive communication.
NIST	National Institute of Standards and Technology
NV	Non-volatile (memory)
OAEP	Optimal asymmetric encryption padding
OEM	Original equipment manufacturer
OIAP	Object-Independent Authorization Protocol
OSAP	Object Specific Authorization Protocol
PCR	Platform Configuration register
PKCS	Public-key cryptography standards
PKI	Public-key infrastructure
PSS	Probabilistic signature scheme
RSA	Rivest Shamir Adelman
RSAES	Rivest Shamir Adelman encryption/decryption scheme
RSASSA	Rivest Shamir Adelman signature scheme with appendix
RTM	Root of trust for measurement
RTR	Root of trust for reporting

Term	Meaning
SHA	Secure Hash algorithm
SRK	Storage root key
TCG	Trusted Computed Group
TDES	Triple data encryption standard
TIS	TPM interface specification
TPM	Trusted Platform Module
TPME	TPM manufacturer
Transaction bytes	All bytes from a TPM command or TPM answer.
TSS	TPM software stack

Appendix B Referenced documents

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

[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 1.12]	TPM Library, Family 2.0, rev 1.38, Errata 1.12, January 28 2021, TCG.
[PTP 2.0 r1.04]	TCG PC Client Specific Platform TPM Specification (PTP) - Version 2.0 Revision 37, February 3, 2020, TCG
[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
[TCG EK Cre Profile TPM 2.3]	TCG EK credential profile for TPM Family 2.0 Level 0. Specification Version 2.3 Revision 2, 23 July 2020, TCG.
[TPM 2.0 PP]	Protection Profile PC Client Specific TPM, Family 2.0 Level 0 revision 1.38 (1.2), TCG.
[SP800-90B]	Recommendation for the entropy sources used for random bit generation, January 2018, NIST
[SP800-90Ar1]	Recommendation for random number generation using deterministic random bit generators, June 2015, NIST

Revision history

Table 18. **Document revision history**

Date	Revision	Changes
20-Dec-2022	1	Initial release.

Contents

List of figures

List of tables