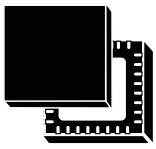
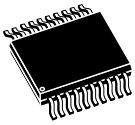
STSAFE-V100-TPM Trusted Platform Module for automotive applications



UFQFPN32 WF (5 × 5 × 0.55 mm)



TSSOP20 (6.4 × 4.4 mm)

Product status link
STSAFE-V100-TPM

Features

Automotive feature

- AEC-Q100 grade 2 qualified

TPM features

- Flash-memory-based trusted platform module (*TPM*)
- Compliant with trusted computing group (*TCG*) trusted platform module (*TPM*) library specifications 2.0, revision 1.59 errata version 1.4 and *TCG* PC client platform *TPM* profile (PTP) for *TPM* 2.0 version 1.05
- 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:
  - Common Criteria compliance with the *TPM* 2.0 protection profile (EAL4+ augmented with AVA_VAN.5, highest CC level of attack resistance)
  - FIPS 140-3
  - *TCG* certification
- *SPI* support at up to 48 MHz
- *I²C* support at up to 1 MHz

Hardware features

- Highly reliable flash memory with error correction code
- Extended temperature range: −40 °C to 105 °C
- 20 years flash data retention
- Electrostatic discharge (ESD) protection up to 4 kV (HBM)
- 1.8 V or 3.3 V supply voltage range

Security features

- Active shield
- Monitoring of environmental parameters
- Hardware and software protection against fault injection and side channel attacks
- *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, 3072 and 4096 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
  - *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 targeted compliance

- Compliant with Microsoft® Windows® 10 and 11
- 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, automotive, PC, mobile, 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 target all Common Criteria (EAL4+) and FIPS certifications.

The STSAFE-V100-TPM is also referenced as ST33KTPM2A in CC and FIPS certification documents.

The STSAFE-V100-TPM, by default, offer two exclusive configurations:

- a slave serial peripheral interface (*SPI*)
- a slave I²C interface.

Both of these configurations are 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 STSAFE-V100-TPM operates in the –40 °C to 105 °C extended temperature range.

The STSAFE-V100-TPM devices are offered in Ecopack2 packages.

The STSAFE-V100-TPM devices are qualified AEC-Q100 grade 2 for automotive applications and are offered in TCG standardized UFQFPN32 wettable flanks and TSSOP20 packages.

2 Pin and signal description

2.1 TCG standard package

2.1.1 UFQFPN32 pin and signal description

The figure below gives the pinout of the UFQFPN32 package in which the devices are delivered. Table 1 describes the associated signals.

Figure 1. UFQFPN32 pinout

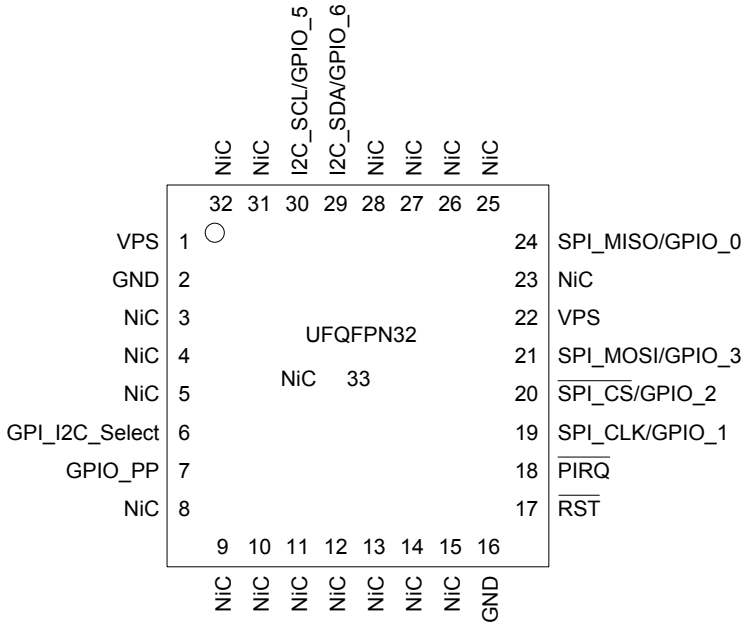


Table 1. UFQFPN32 descriptions

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	**Ground**, has to be connected to the main motherboard ground.
$\overline{\text{RST}}$	Input	**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/GPIO_0	Output	***SPI* master input, slave output** (output from slave) / General-purpose input/output if I^2C is activated
SPI_MOSI/GPIO_3	Input	***SPI* master output, slave input** (output from master) / General-purpose input/output if I^2C is activated
SPI_CLK/GPIO_1	Input	***SPI* serial clock** (output from master) / General-purpose input/output if I^2C is activated
$\overline{\text{SPI\_CS}}$/GPIO_2	Input	***SPI* chip (or slave) select**, internal pull-up (active low; output from master) / General-purpose input/output if I^2C is activated
$\overline{\text{PIRQ}}$	Output	**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*.
GPI_I2C_Select	Input	This pin must be connected to an external pull-down resistor to activate the *I²C* protocol during product boot time. It can remain unconnected for the *SPI* protocol. This pin is internal pull-up by default and becomes internal floating after *I²C* activation.
NiC	-	**Not internally connected**: not connected to the die. May be left unconnected but no impact on *TPM* if connected.
I2C_SDA/GPIO_6	Input/ output	**Bidirectional *I²C* serial data** (open drain without a weak pull-up resistor) / General-purpose input/output if *SPI* is activated
I2C_SCL/GPIO_5	Input	**Input *I²C* serial clock** (open drain without a weak pull-up resistor) / General-purpose input/ output if *SPI* is activated

1. *In GPIO configuration, this signal is Input/output.*

Note: The UFQFPN32 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.

2.2 Optimized packages

2.2.1 TSSOP20 pin and signal description

The figure below shows the TSSOP20 pinout while Table 2 provides the pin description of this package.

Figure 2. **TSSOP20 pinout (top view through package)**

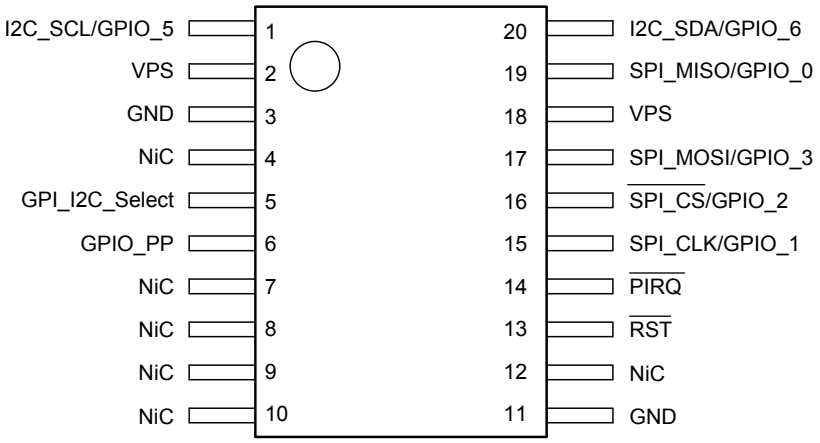


Table 2. TSSOP20 pin description

Pin number	Pin name	Description
1	I2C_SCL/GPIO_5(1)	**Input *I²C* serial clock** (open drain without a weak pull-up resistor) / General-purpose input/output if *SPI* is activated
2	VPS	**Power supply**. This pin must be connected to 1.8 V or 3.3 V DC power rail supplied by the motherboard.
3	GND	**Ground**, has to be connected to the main motherboard ground.
4	NiC	**Not internally connected**: not connected to the die. May be left unconnected but no impact on *TPM* if connected.
5	GPI_I2C_Select	This pin must be connected to an external pull-down resistor to activate the *I²C* protocol during product boot time. It can remain unconnected for the *SPI* protocol. This pin is internal pull-up by default and becomes internal floating after *I²C* activation.
6	GPIO_PP	**Physical presence**, active high, internal pull-down. Used to indicate physical presence to the *TPM*.
7	NiC	**Not internally connected**: not connected to the die. May be left unconnected but no impact on *TPM* if connected.
8	NiC	**Not internally connected**: not connected to the die. May be left unconnected but no impact on *TPM* if connected.
9	NiC	**Not internally connected**: not connected to the die. May be left unconnected but no impact on *TPM* if connected.
10	NiC	**Not internally connected**: not connected to the die. May be left unconnected but no impact on *TPM* if connected.
11	GND	**Ground**, has to be connected to the main motherboard ground.
12	NiC	**Not internally connected**: not connected to the die. May be left unconnected but no impact on *TPM* if connected.
13	$\overline{\text{RST}}$	**Reset**, active low, used to re-initialize the device. Must not be unconnected. External pull-up resistor required if it cannot be driven.
14	$\overline{\text{PIRQ}}$	**IRQ**, active low, open drain, used by the *TPM* to generate an interrupt
15	SPI_CLK/GPIO_1(1)	***SPI* serial clock** (output from master) / General-purpose input/output if I^2C is activated
16	$\overline{\text{SPI\_CS}}$/GPIO_2(1)	***SPI* chip (or slave) select**, internal pull-up (active low; output from master) / General-purpose input/output if I^2C is activated
17	SPI_MOSI/GPIO_3(1)	***SPI* master output, slave input** (output from master) / General-purpose input/output if I^2C is activated
18	VPS	**Power supply**. This pin must be connected to 1.8 V or 3.3 V DC power rail supplied by the motherboard.
19	SPI_MISO/GPIO_0(1)	***SPI* master input, slave output** (output from slave) / General-purpose input/output if I^2C is activated
20	I2C_SDA/GPIO_6(1)	**Bidirectional *I²C* serial data** (open drain without a weak pull-up resistor) / General-purpose input/output if *SPI* is activated

1. *In GPIO configuration, this signal is Input/output.*

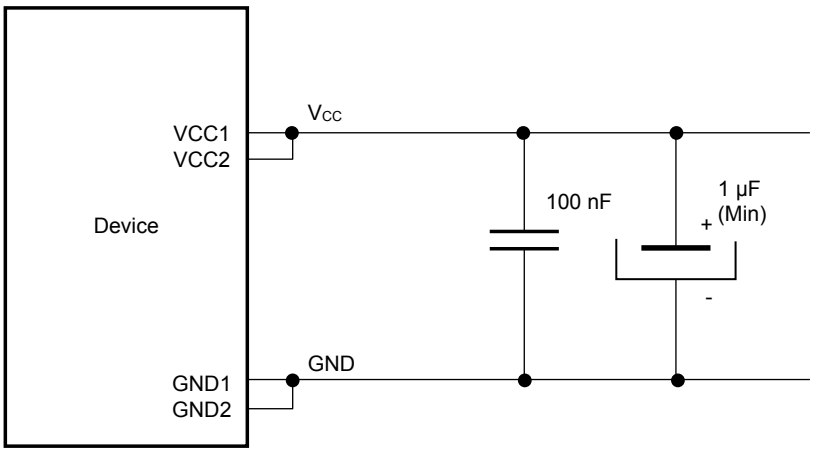
3 Electrical integration guidance

This section gives some guidance on how to integrate the STSAFE-V100-TPM device in an application.

3.1 Recommended power supply filtering

The power supply of the device should be filtered using the circuit shown in the figure below.

Figure 3. Recommended filtering capacitors on V_{CC}



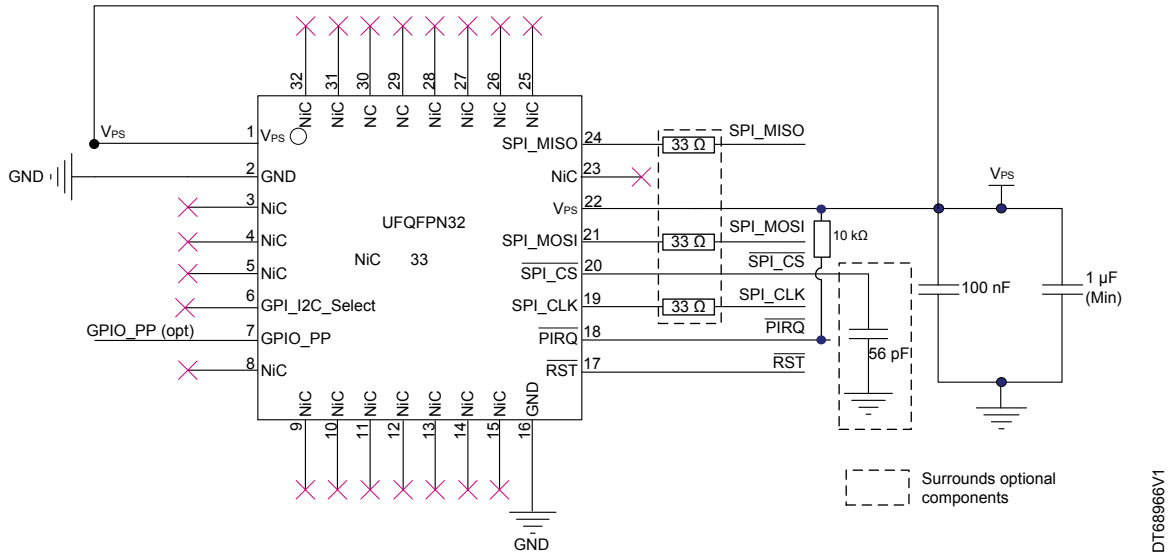
3.2 $\overline{\text{SPI\_CS}}$ optional filtering

Recommendation for SPI_CS integration: It is mandatory that SPI_CLK is at the low logic level when the falling edge occurs on the SPI_CS signal. An external capacitance of 56 pF is recommended on SPI_CS for that purpose. This capacitor might not be required depending on the intrinsic line capacitance, the SPI bus frequency, or both.

3.3 Device integration for SPI communication

The figure below shows the typical hardware implementation of the STSAFE-V100-TPM device for *SPI* communication.

Figure 4. Typical hardware implementation for SPI communication (UFQFPN32 package)



Note: The use of a low-value resistor (typically 33 Ω) on SPI_MISO, SPI_MOSI and SPI_CLK can be recommended for line adaptation when the signals are affected by parasite spikes. Its use is mandatory to avoid disturbance of the ramp-up and ramp-down signals.

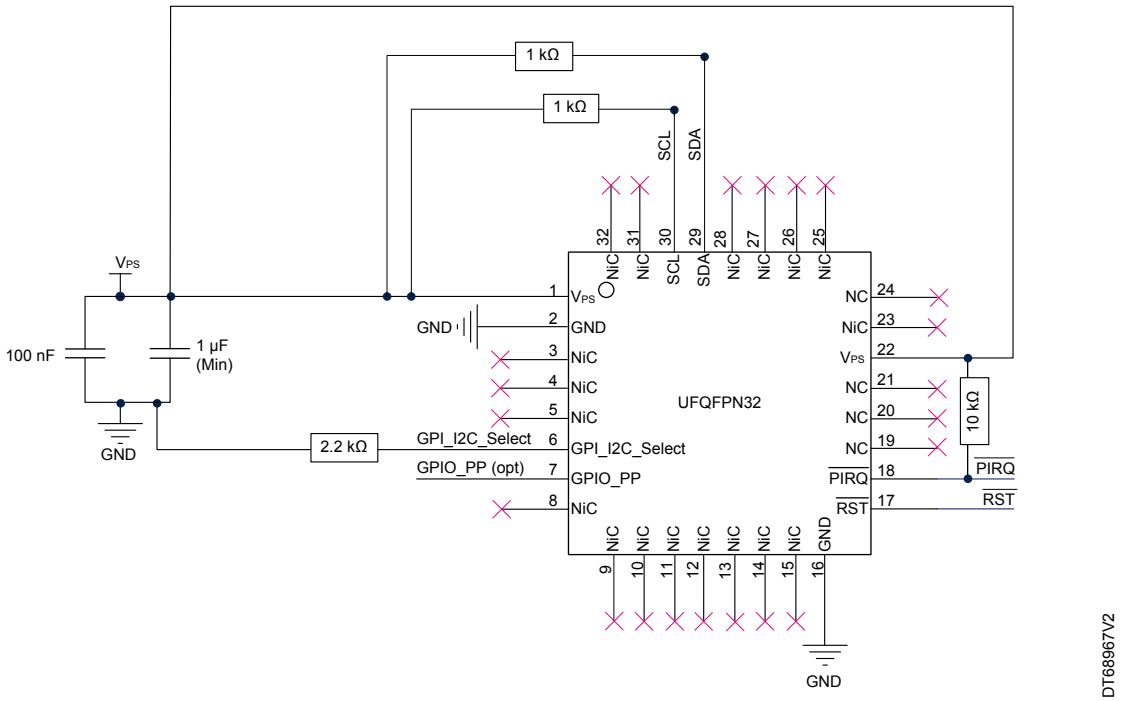
Note: The capacitor on $\overline{SPI\_CS}$ is optional (see Section 3.2 $\overline{SPI\_CS}$ optional filtering or Recommendations).

Note: The pull-up resistor on the PIRQ line is mandatory to optimize the power consumption in standby mode.

3.4 Device integration for I²C communication

The figure below shows the typical hardware implementation of the STSAFE-V100-TPM device for *I²C* communication.

Figure 5. Typical hardware implementation for *I²C* communication (UFQFPN32 package)



Note: The pull-up resistor on the $\overline{PIRQ}$ line is mandatory to optimize the power consumption in standby mode.

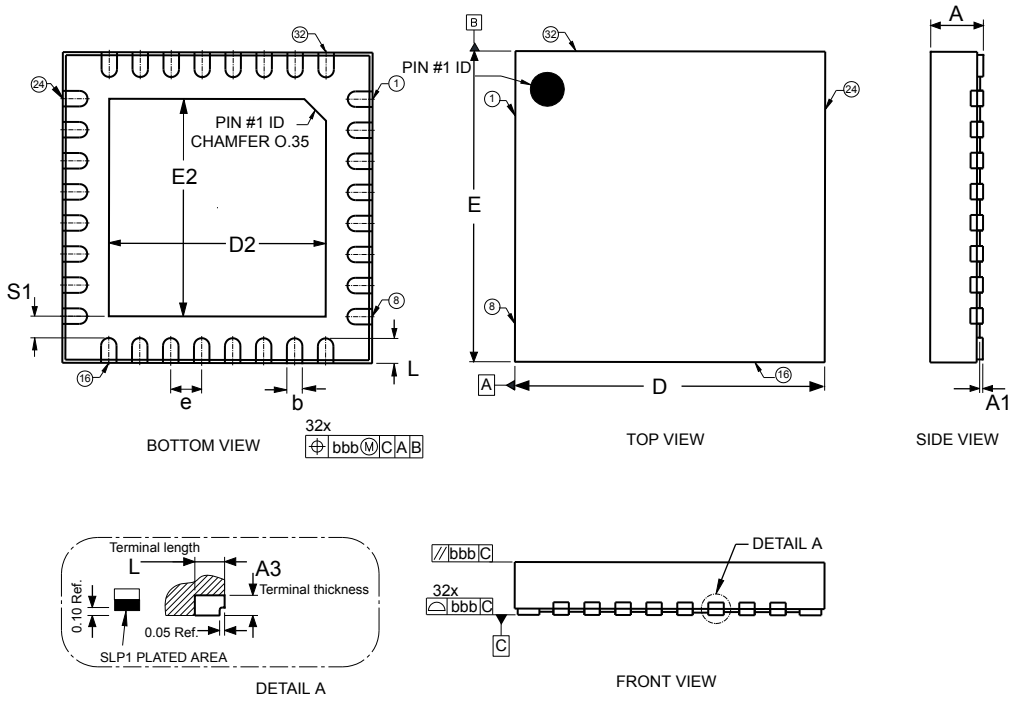
4 Package information

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.

4.1 UFQFPN32 package information (B0EY)

This UFQFPN is a 32 lead wettable flank, 5x5 mm, 0.5 mm pitch ultra thin fine pitch quad flat package.

Figure 6. UFQFPN32 - Outline



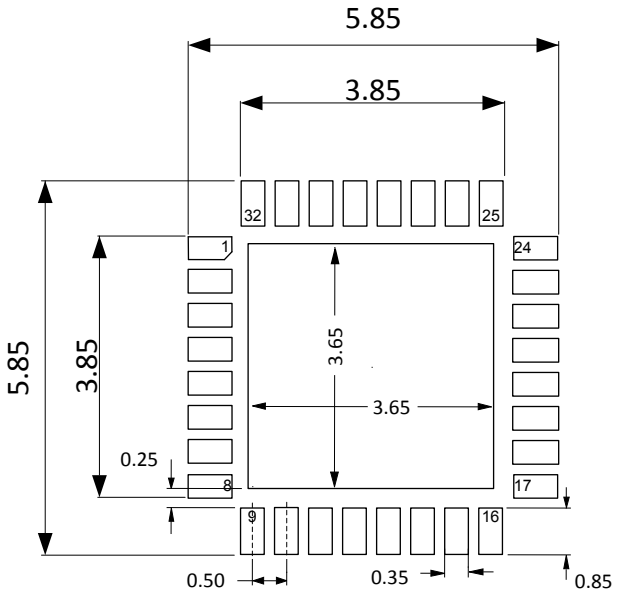
1. *Drawing is not to scale.*
2. *Coplanarity applies to the exposed pad as well as the terminal.*

Table 3. UFQFPN32 - Mechanical data

Symbol	millimeters			inches[1]		
	Min	Typ	Max	Min	Typ	Max
A	0.50	0.55	0.65	0.0197	0.0217	0.0256
A1	-	0.05	-	-	0.0020	-
A3		0.152 ref.			0.0060 ref.	
L	0.30	0.40	0.50	0.0118	0.0157	0.0196
b	0.18	0.25	0.30	0.0071	0.0098	0.0118
D		5.00 BSC			0.1968 BSC	
E		5.00 BSC			0.1968 BSC	
e		0.50 BSC			0.0197 BSC	
D2	3.50	3.65	3.80	0.1377	0.1437	0.1496
E2	3.50	3.65	3.80	0.1377	0.1437	0.1496
S1		0.30 ref.			0.0118 ref.	
N[2]			32			
bbb	-	0.10	-	-	0.0039	-
ccc	-	0.10	-	-	0.0039	-
eee	-	0.08	-	-	0.0031	-

1. *Values in inches are converted from mm and rounded to 4 decimal digits.*
2. *Total number of terminals.*

Figure 7. UFQFPN32 - PCB footprint example

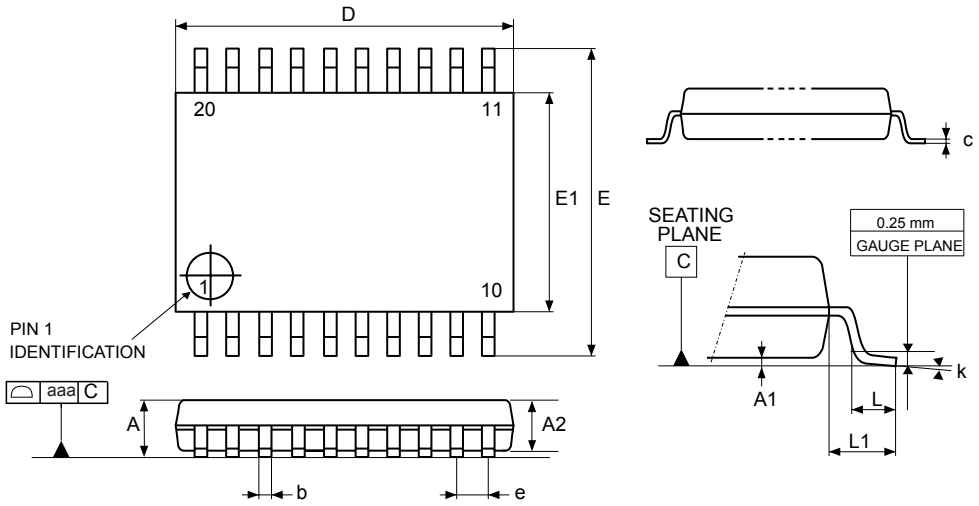


1. *Dimensions are expressed in millimetres.*
2. *Pin 1 is identified in the PCB footprint example. The location of this pin must be identified using the customer manufacturing process.*

4.2 TSSOP20 package information

This TSSOP20 is a 20-lead, 6.5 × 4.4 mm, 0.65 mm pitch, thin shrink small outline package (TSSOP). The physical dimensions and specification are given in Figure 8 and Table 4

Figure 8. TSSOP20 – Outline



1. *Drawing is not to scale.*

Table 4. TSSOP20 – Mechanical data

Symbol	millimeters			inches[1]		
	Min.	Typ.	Max.	Min.	Typ.	Max.
A	-	-	1.20	-	-	0.0472
A1	0.05	-	0.15	0.0020	-	0.0059
A2	0.80	1.00	1.05	0.0315	0.0394	0.0413
b	0.19	-	0.30	0.0075	-	0.0118
c	0.09	-	0.20	0.0035	-	0.0079
D[2]	6.40	6.50	6.60	0.2520	0.2559	0.2598
E	6.20	6.40	6.60	0.2441	0.2520	0.2598
E1[3]	4.30	4.40	4.50	0.1693	0.1732	0.1772
e	-	0.65	-	-	0.0256	-
L	0.45	0.60	0.75	0.0177	0.0236	0.0295
L1	-	1.00	-	-	0.0394	-
k	0°	-	8°	0°	-	8°
aaa	-	-	0.10	-	-	0.0039

1. *Values in inches are converted from mm and rounded to four decimal digits.*
2. *Dimension “D” does not include mold flash, protrusions or gate burrs. Mold flash, protrusions or gate burrs shall not exceed 0.15 mm per side.*
3. *Dimension “E1” does not include interlead flash or protrusions. Interlead flash or protrusions shall not exceed 0.25 mm per side.*

5 Delivery packing

5.1 UFQFPN32 - tape and reel 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 5. UFQFPN32 - Packages on tape and reel

Package	Description	Tape width	Tape pitch	Reel diameter	Quantity per reel
UFQFPN32	Very thin fine pitch quad flat pack no-lead package	12 mm	8 mm	13 in.	3000

Figure 9. UFQFPN32 - Reel diagram

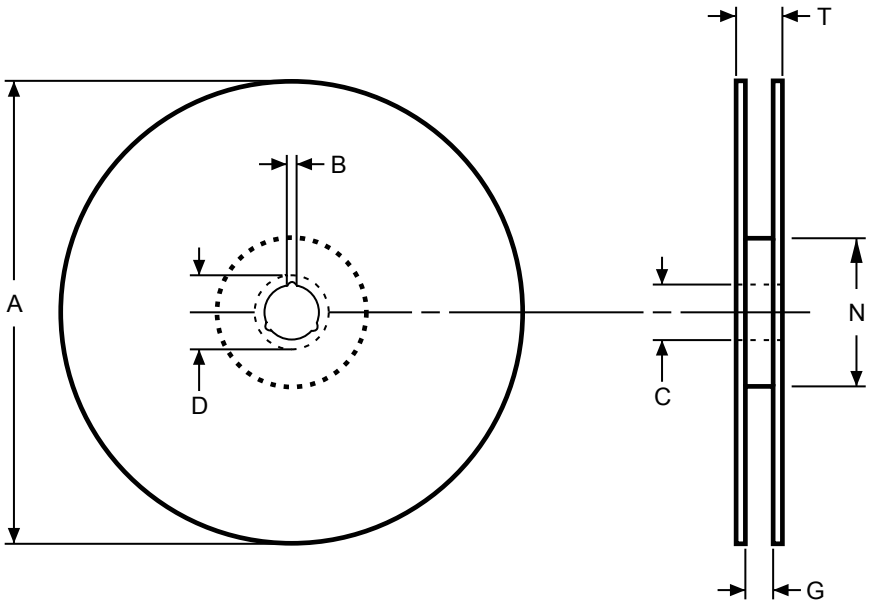
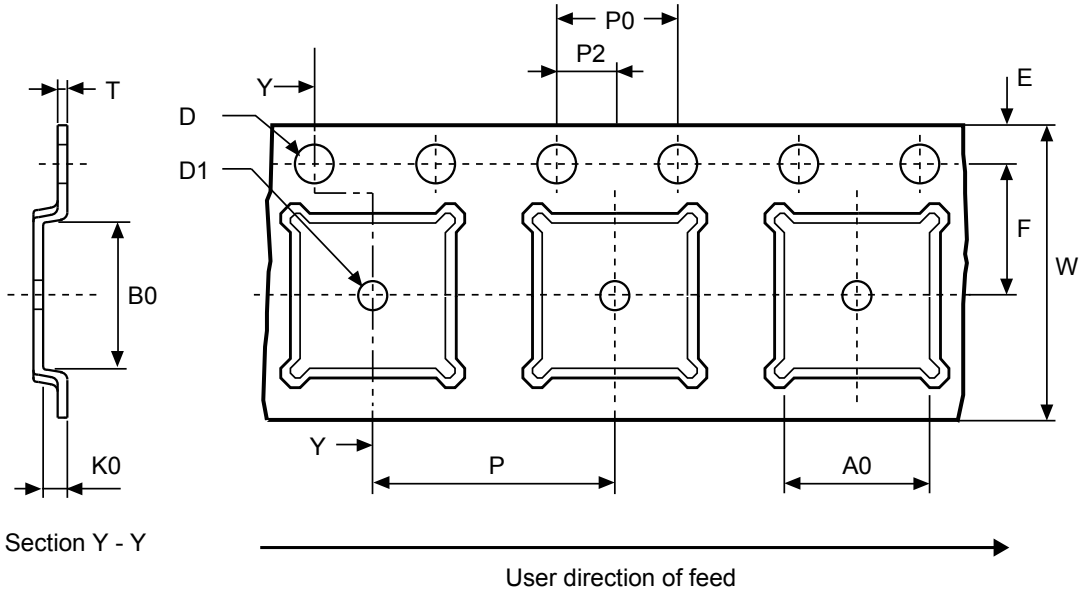


Table 6. UFQFPN32 - Reel dimensions

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 10. **UFQFPN32 - Embossed carrier tape**



1. *Drawing is not to scale.*

Figure 11. **UFQFPN32 - Chip orientation in the embossed carrier tape**

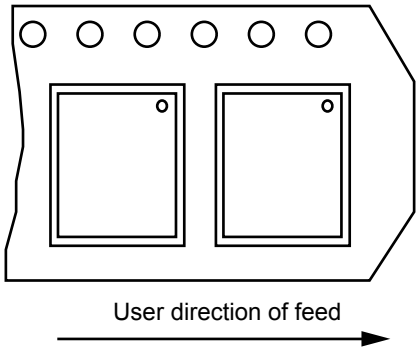


Table 7. **UFQFPN32 - Carrier tape dimensions**

Package	A0	B0	K0	D1 Min.	P	P2	D	P0	E	F	W	T Max.	Unit
UFQFPN 5×5	5.3 ±0.1	5.3 ±0.1	0.75 ±0.1	1.5	8 ±0.1	2 ±0.05	1.55 ±0.05	4 ±0.1	1.75 ±0.1	5.5 ±0.1	12 ±0.3	0.3 ±0.05	mm

5.2 TSSOP20 tape and reel packing

Surface-mount packages can be supplied with Tape and Reel packing. The reels have a 13" typical diameter. They contain 2500 devices each. The detailed dimensions are illustrated in Figure 12 and the stated in Table 8

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

Table 8. TSSOP20 packages on tape and reel

Package	Description	Tape width	Tape pitch	Reel diameter	Quantity per reel
TSSOP20 4.4 mm body	Thin shrink small outline package	16 mm	12 mm	13 in.	2500

Figure 12. TSSOP20 reel diagram

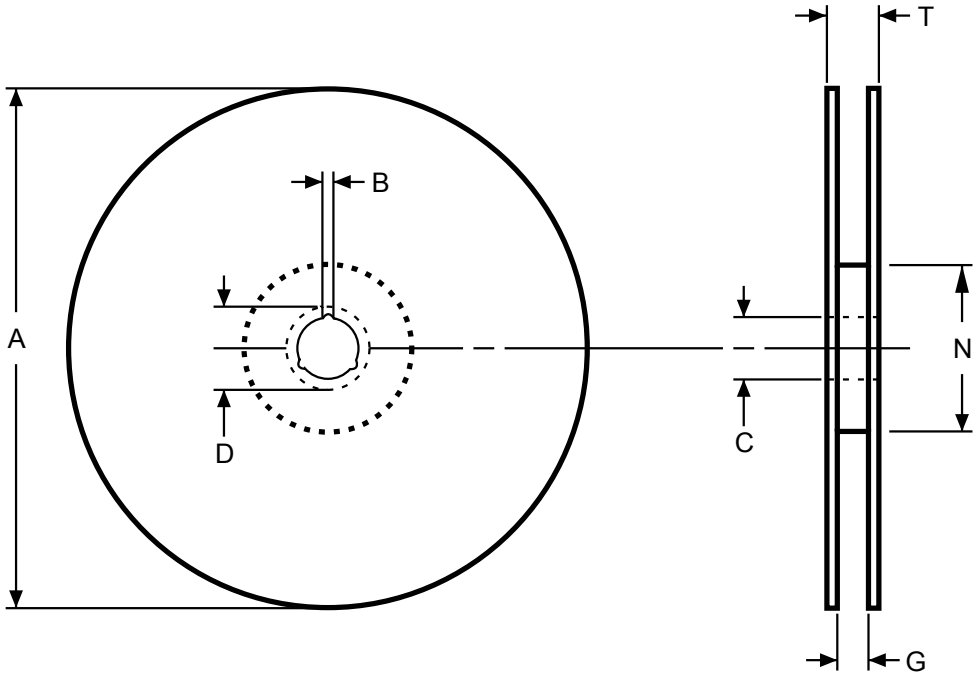


Table 9. TSSOP20 - Reel dimensions

Reel size	Tape size	A Max.	B Min.	C	D Min.	G Max.	N Min.	T Max.	Unit
13”	16 mm	330	0.9	13 ±0.25	21.5	17 ±0.3	100	19.4 ±1	mm

Figure 13. **TSSOP20 - Leader and trailer**

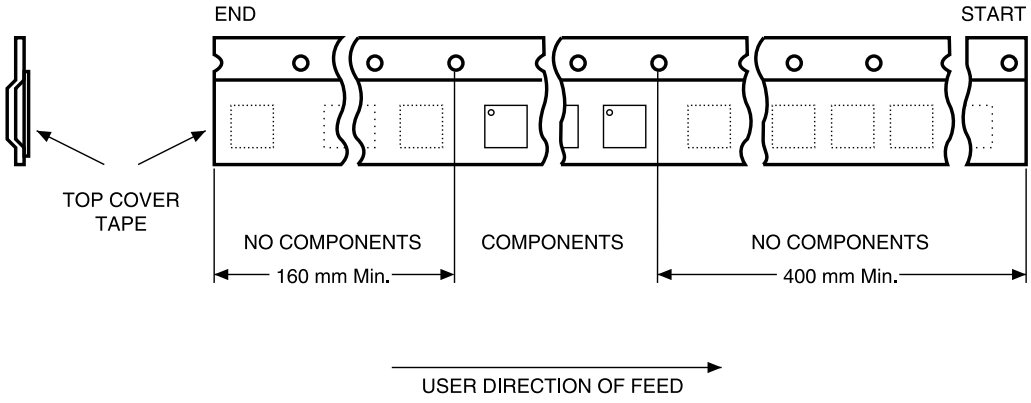
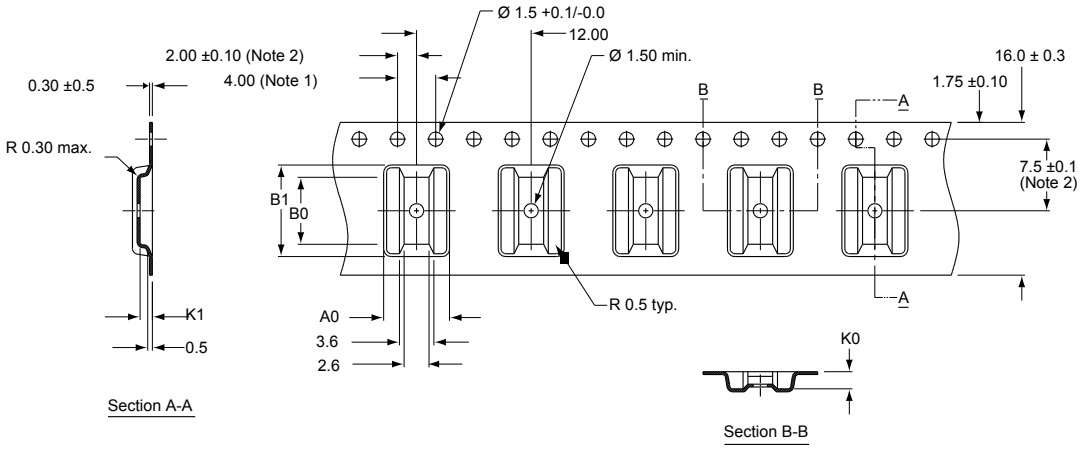


Figure 14. **TSSOP20 - Embossed carrier tape**



1. *Cumulative tolerance of the 10 sprocket hole pitches = ±0.2.*
2. *Pocket position relative to sprocket hole measured as true position of pocket, not pocket hole.*
3. *A0 and B0 are calculated on a plane at a distance “R” above the bottom of the pocket.*
4. *Drawing is not to scale.*
5. *Unless otherwise specified, dimensions are in millimeters and decimal values of the form x.x are with ±0.2 tolerance whereas values of the form x.xx are with ±0.10 tolerance.*

Table 10. **TSSOP20 - Carrier tape dimensions**

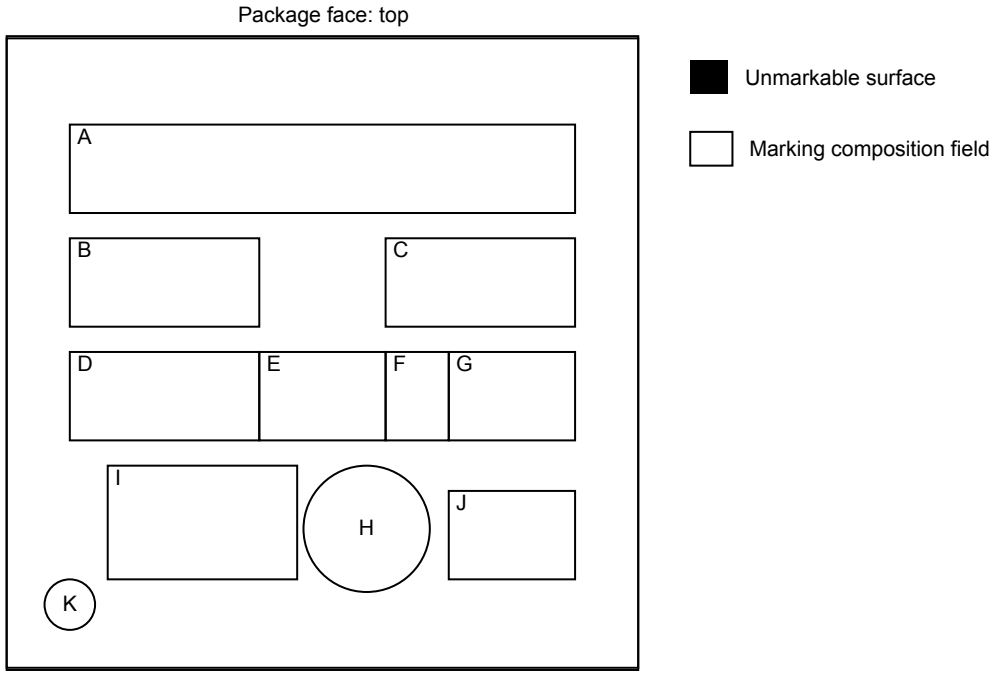
Package	A0	B0	B1	K0	K1	Unit
TSSOP20 4.4 mm body	6.90 ±0.10	7.00 ±0.10	9.60 ±0.10	1.80 ±0.10	1.30 ±0.10	mm

6 Package marking information

6.1 UFQFPN32 package marking information

Parts marked as E or ES (for engineering sample) are not yet qualified and therefore not approved for use in production. ST is not responsible for any consequences resulting from such use. In no event will ST be liable for the customer using any of these engineering samples in production. ST's Quality department must be contacted prior to any decision to use these engineering samples to run a qualification activity.

Figure 15. UFQFPN32 - Standard marking example



Legend:

A: Marking area – Up to 8 digits
B: Marking area – 3 digits
C: BE sequence (LLL)
D: Country of origin (3 characters allowed (max.))
E: Assembly plant (PP)
F: Assembly year (Y)
G: Assembly week (WW)
H: Second level interconnect
I: Standard STMicroelectronics logo
J: Diffusion traceability plant (WX)
K: Dot(1)

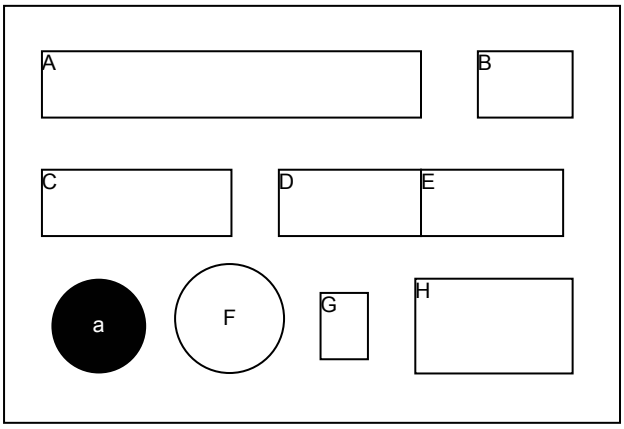
1. *The dot on the back side indicates the pin 1 location.*

6.2 TSSOP20 marking example

The package marking layout information is illustrated in Figure 16.

Parts marked as E or ES (for engineering sample) are not yet qualified and therefore not approved for use in production. STMicroelectronics is not responsible for any consequences resulting from such use. In no event will STMicroelectronics be liable for the customer using any of these engineering samples in production. STMicroelectronics Quality department must be contacted prior to any decision to use these engineering samples to run a qualification activity.

Figure 16. TSSOP20 package standard marking example



Caption:

A: Marking area
B: Assembly week (ww)
C: Marking area
D: Backend sequence (LLL)
E: Country of origin (3 characters)
F: ECOPACK level
G: Assembly year (Y)
H: Standard ST logo

7 Ordering information

Table 11. **Ordering information for STSAFE-V100-TPM production parts**

Ordering code	Package	Factory firmware version	Supported interfaces	Marking area A	Marking area
ST33KTPM2A3WBAC5	UFQFPN32 WF	10.257	I²C or SPI	KTPMA	area B: AC5
ST33KTPM2AT2BAC5	TSSOP20				area C: AC5

8 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@stmicroelectronics.onmicrosoft.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 Referenced documents

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

[TPM 2.0 P1 r159]	TPM Library, Part 1, Architecture, Family 2.0, rev 1.59, TCG
[TPM 2.0 P2 r159]	TPM Library, Part 2, Structures, Family 2.0, rev 1.59, TCG
[TPM 2.0 P3 r159]	TPM Library, Part 3, Commands, Family 2.0, rev 1.59, TCG
[TPM 2.0 P4 r159]	TPM Library, Part 4, Supporting routines, Family 2.0, rev 1., TCG
[TPM 2.0 rev1 Err 1.4]	Errata Version 1.4 for Trusted Platform Module Library Family 2.0 Revision 1.59, TCG
[PTP 2.0 r1.]	TCG PC Client Platform TPM Profile (PTP) for TPM 2.0 Version 1.05 Revision 14, 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]	TCG Protection Profile for PC Client Specific TPM 2.0 Library Revision 1.59; Version 1.3
[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 12. **Document revision history**

Date	Revision	Changes
29-Nov-2023	1	Initial release.

Glossary

3D Three-dimensional

AES Advanced encryption standard

CA Certification Authority

CC Common Criteria

CRT Chinese remainder theorem

DES Data encryption standard

DRBG Deterministic random bit generator

DXE Driver execution environment

EC Elliptic curve

ECC Elliptic curve cryptography

ECDA Elliptic curve direct anonymous attestation

ECDAA Elliptic curve direct anonymous attestation (algorithm)

ECDH Elliptic curve Diffie–Hellman

ECDSA Elliptic curve digital signature algorithm

EK Endorsement key

ESD Electrostatic discharge

FIPS Federal Information Processing Standards

GPIO General purpose input/output

HBM Human body model

HMAC Hash-based message authentication code or keyed-hash message authentication code

I²C Inter-integrated circuit

MCU Microcontroller unit

NIST National Institute of Standards and Technology

NV Nonvolatile

PKCS Public key cryptographic standards

PSS Probabilistic signature scheme

RNG Random number generator

RSA Public-key cryptosystem (created by Ron Rivest, Adi Shamir and Leonard Adleman)

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 Computing Group®

TDES Triple DES cryptographic algorithm

TPM Trusted platform module

TRNG True random number generator

TSS TPM software stack

Contents

List of tables

List of figures