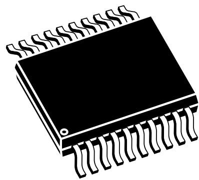
life.augmented

ST33GTPMASPI

Data brief

Flash-memory-based TPM 2.0 device for automotive applications with an SPI interface



TSSOP20
(6.5 × 4.4 mm)

Product status link
ST33GTPMASPI

Features

- AEC-Q100 qualified

TPM features

- Flash-memory-based Trusted Platform Module (TPM)
- TPM 2.0 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+
  - FIPS 140-2 level 2
  - (physical security level 3)
- SPI support at up to 18 MHz
- Support for hardware physical presence

Hardware features

- Arm® SecurCore® SC300™ 32-bit RISC core
- Highly reliable Flash memory technology:
  - 500 000 cycles on the full temperature range
  - 25 years' lifetime at 85 °C
  - 20 years' lifetime at 105 °C
- Automotive grade 2: −40 °C to 105 °C
- ESD (electrostatic discharge) protection against voltages greater than 4 kV (HBM)
- 1.8 V or 3.3 V supply voltage range
- 20-lead thin shrink small outline ECOPACK MSL1 package

Security features

- Active shield and environmental sensors
- Monitoring of environmental parameters (power and clock)
- Hardware and software protection against fault injection
- SP800-90A-compliant deterministic random bit generator (DRBG) built with an AIS-31 class PTG2-compliant true random 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 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 TCG test suite for TPM 2.0
- Common Criteria certifications:
  - EAL 4+ on TCG TPM2.0 protection profile
  - EAL 5+ on hardware
- Targets FIPS 140-2 level 2 certification (physical security level 3)

1 Description

The ST33GTPMASPI is a cost-effective and high-performance trusted platform module (TPM) targeting automotive and embedded systems.

The product implements the functions defined by the Trusted Computing Group (www.trustedcomputinggroup.org) in the TCG Trusted Platform Module Library Specifications version 2.0 Level 0 Revision 138 ([TPM 2.0 P1 r138], [TPM 2.0 P2 r138], [TPM 2.0 P3 r138], [TPM 2.0 P4 r138]) and errata version 1.4 [TPM 2.0 rev138 Err 1.4]. It is also based on the TCG PC client-specific TPM Platform specifications rev1.03 [PTP 2.0 r1.03]. The applicable protection profile is *TCG Protection Profile for PC Client Specific TPM 2.0* ([TPM 2.0 PP]).

The product also supports the ability to upgrade the TPM firmware thanks to a persistent Flash memory loader application to support new standard evolutions.

1.1 Security certifications

This product is CC certified according to TPM 2.0 PP at EAL4+.

1.2 Hardware features

The ST33GTPMASPI 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 attack.

The ST33GTPMASPI offers a fast slave serial peripheral interface (SPI) supported by an embedded communication engine compliant with TCG PC client TPM Profile 1.03 [PTP 2.0 r1.03].

The product features hardware accelerators for advanced cryptographic functions. The AES peripheral provides a secure AES (Advanced Encryption Standard) algorithm implementation, while the NESCRYPT cryptoprocessor efficiently supports public-key algorithms.

The ST33GTPMASPI comes in the TSSOP20 ECOPACK-compliant package. ECOPACK is an ST trademark.

Note: Arm is a registered trademark of Arm Limited (or its subsidiaries) in the US and/or elsewhere.

arm

2 Pin and signal descriptions

The figure below gives the pinout of the TSSOP20 package in which the devices are delivered. The table describes the associated signals.

Figure 1. **TSSOP20 pinout (top view)**

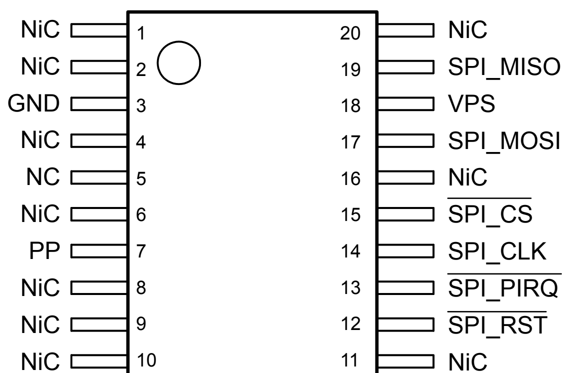


Table 1. **Pin descriptions**

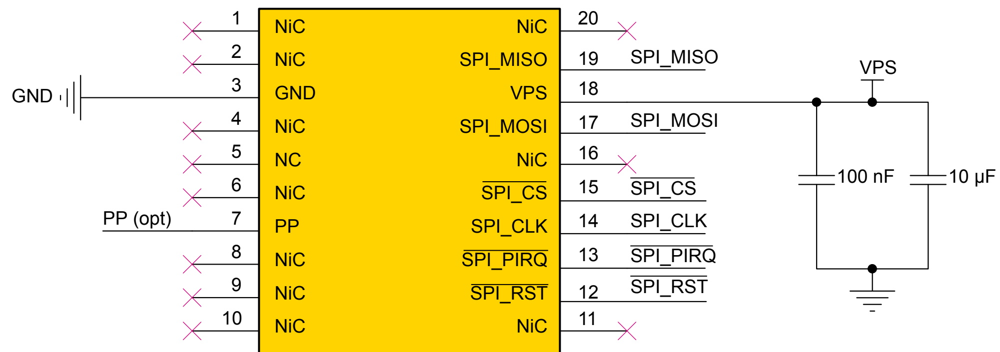
Signal	Type	Description
PP	Input	**Physical Presence**, active high, internal pull-down. Used to indicate Physical presence.
VPS	Input	**Power supply**. This pin must be connected to 1.8 V or 3.3 V DC power rail supplied by the motherboard.
GND	Input	GND has to be connected to the main motherboard ground.
SPI_RST	Input	**SPI Reset** active low, used to re-initialize the device. Must not be unconnected. External pull-up required if the pin cannot be driven.
MISO	Output	**SPI** Master Input, Slave Output (output from slave)
MOSI	Input	**SPI** Master Output, Slave Input (output from master)
SPI_CLK	Input	**SPI** Serial Clock (output from master)
SPI_CS	Input	**SPI** Chip (or Slave) Select, internal pull-up (active low; output from master)
SPI_PIRQ	Output	**SPI IRQ** active low, open drain, used by the TPM to generate an interrupt.
NiC	-	**Not internally connected**: not connected to the die. May be left unconnected but no impact on TPM if connected.
NC	-	**Not Connected**: connected to the die but not usable. Shall be left unconnected.

3 Integration guidance

3.1 Typical hardware implementation

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

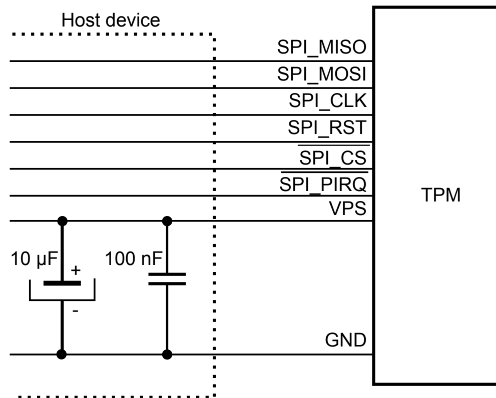
Figure 2. **Typical hardware implementation (TSSOP20 package)**



3.2 Power supply filtering

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

Figure 3. 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 2. Maximum V_{PS} rising slope

Symbol	Parameter	Value	Unit
S_{VPS}	Maximum V_{PS} rising slope	5	V/µs

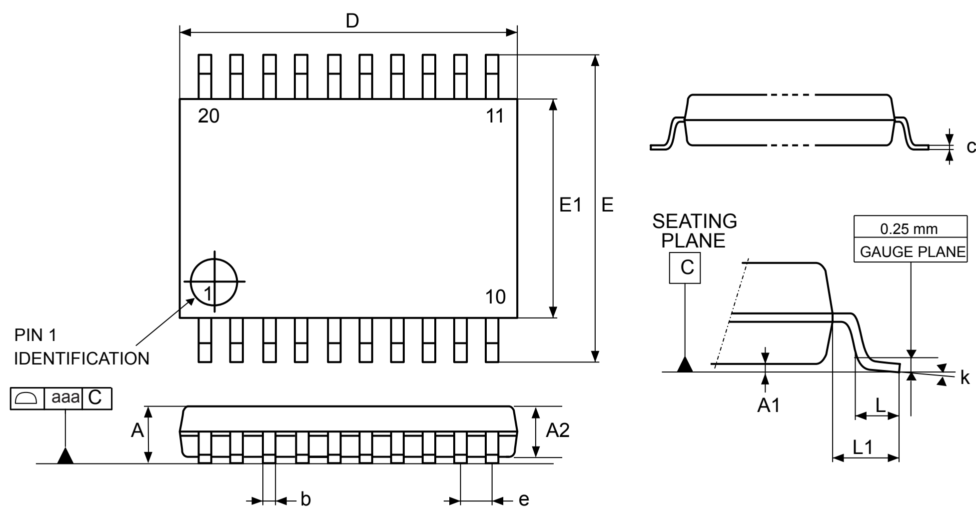
4 Package information

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 TSSOP20 package information

TSSOP20 is a 20-lead thin shrink small outline, 6.5 × 4.4 mm, 0.65 mm pitch package.

Figure 4. TSSOP20 – package outline



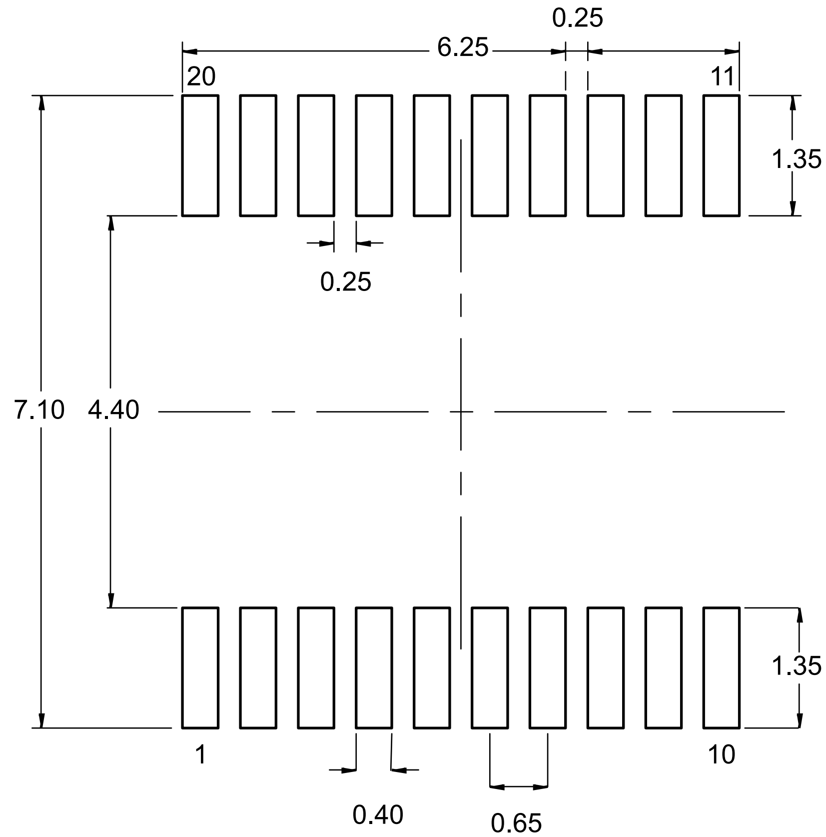
1. *Drawing is not to scale.*

Table 3. TSSOP20 – package mechanical data

Symbol	millimeters			inches [1]		
	Min.	Typ.	Max.	Min.	Typ.	Max.
A	-	-	1.200	-	-	0.0472
A1	0.050	-	0.150	0.0020	-	0.0059
A2	0.800	1.000	1.050	0.0315	0.0394	0.0413
b	0.190	-	0.300	0.0075	-	0.0118
c	0.090	-	0.200	0.0035	-	0.0079
D [2]	6.400	6.500	6.600	0.2520	0.2559	0.2598
E	6.200	6.400	6.600	0.2441	0.2520	0.2598
E1 [3]	4.300	4.400	4.500	0.1693	0.1732	0.1772
e	-	0.650	-	-	0.0256	-
L	0.450	0.600	0.750	0.0177	0.0236	0.0295
L1	-	1.000	-	-	0.0394	-
k	0°	-	8°	0°	-	8°
aaa	-	-	0.100	-	-	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 0.15mm per side.*
3. *Dimension “E1” does not include interlead flash or protrusions. Interlead flash or protrusions shall not exceed 0.25 mm per side.*

Figure 5. TSSOP20 – package footprint



1. *Dimensions are expressed in millimeters.*

4.2 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 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
TSSOP20 4.4 mm body	Thin shrink small outline package	16 mm	12 mm	13 in.	2500

Figure 6. Reel diagram

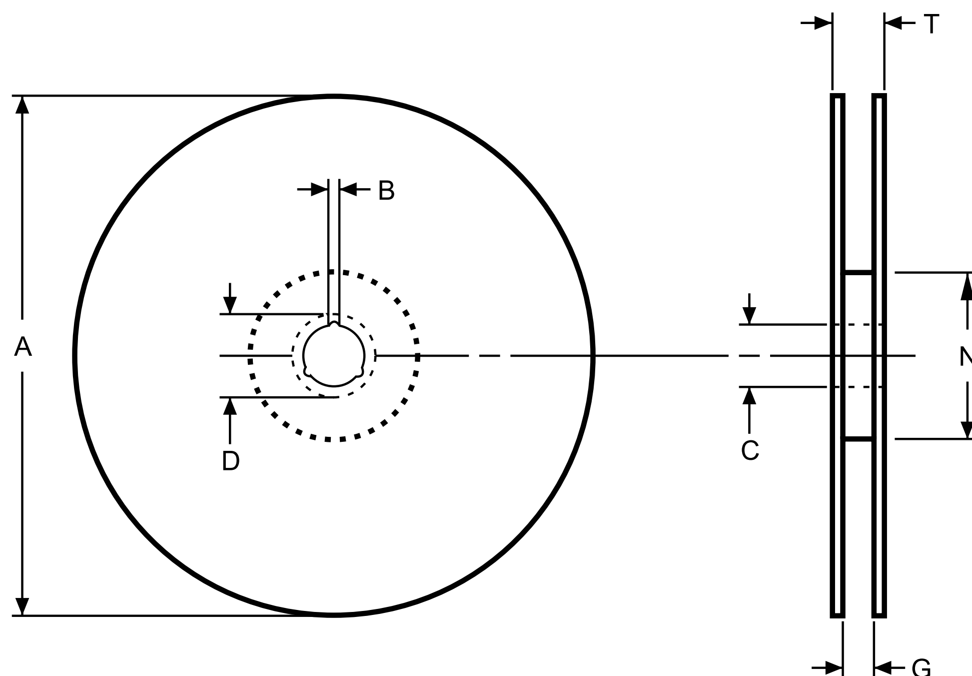


Table 5. Reel dimensions

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

Figure 7. Leader and trailer

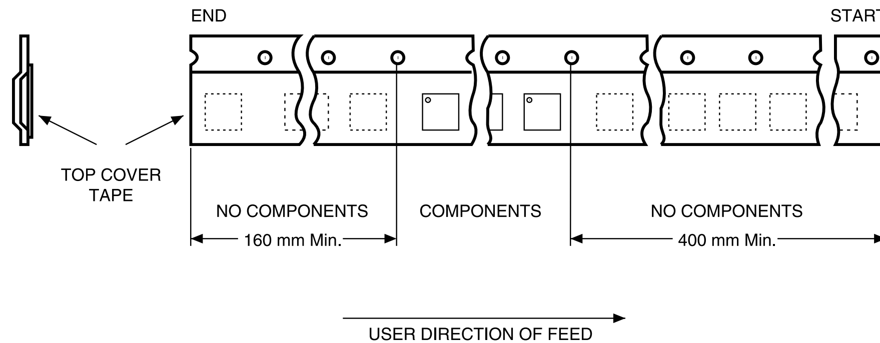
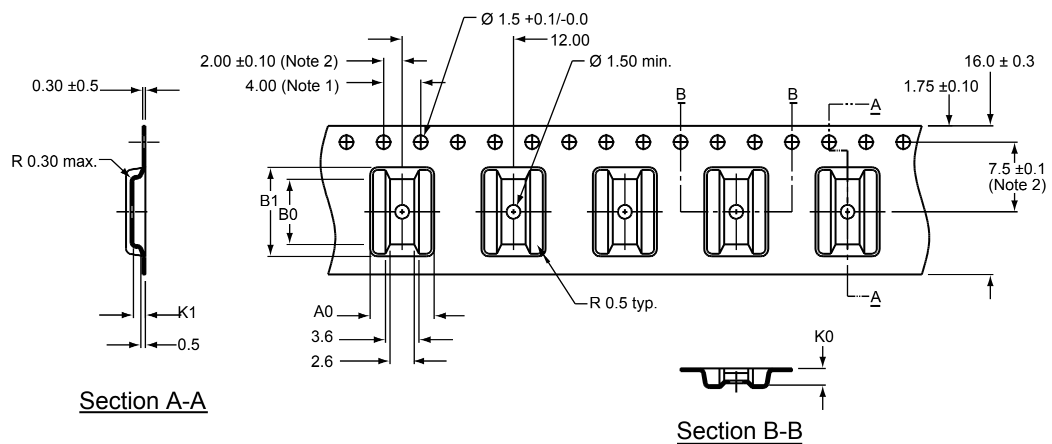


Figure 8. Embossed carrier tape for the TSSOP20 package



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.*

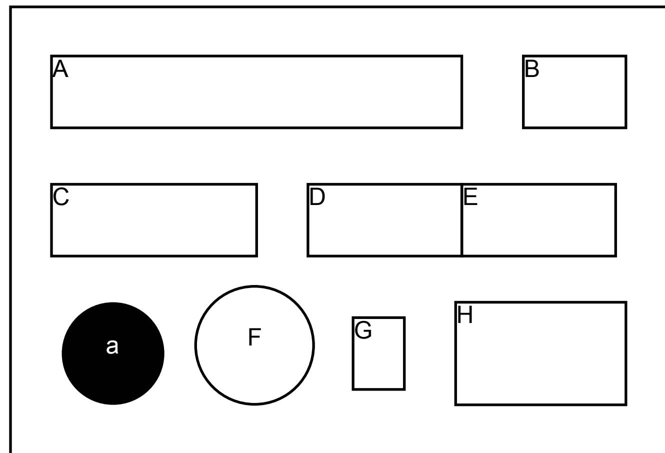
Table 6. Carrier tape dimensions for TSSOP20 package

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

5 Package marking information

The figure below illustrates the typical markings of the device's TSSOP20 package.

Figure 9. **TSSOP20 package standard marking example**



Caption:

a: Pin 1 reference

A: Marking area: GTPMASPI

B: Assembly week (ww)

C: Marking area: AE5

D: Backend sequence (LLL)

E: Country of origin (3 characters)

F: ECOPACK level

G: Assembly year (Y)

H: Standard ST logo

6 Ordering information

Table 7. Ordering information for products supporting firmware 0x00.0x03.0x01.0x00 (0x0003.0x0100) (3.256) preloaded in factory

Ordering code	Firmware version	Operating temperature range	Maximum SPI clock frequency	Package	Marking (area A)
ST33GTPMA020FAE5	0x00 0x03 0x01 0x00 (0x0003 0x0100) (3.256)	−40 °C to +105 °C	18 MHz	TSSOP20	AE5

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*.

Appendix A Terms and abbreviations

Table 8. List of abbreviations

Term	Meaning
AES	Advanced Encryption Standard
CA	Certificate authority
CC	Common Criteria
DRBG	Deterministic random-bit generator
DAM	Dictionary attack mitigation mechanism
Data byte	Byte from the TPM command or answer or register value.
DES	Data Encryption Standard
EC	Elliptic curve
ECDAA	Elliptic curve direct anonymous attestation (algorithm)
ECDH	Elliptic curve Diffie–Hellman
EK	Endorsement key
FIPS	Federal Information Processing Standard
GPIO	General-purpose I/O
HMAC	Keyed-Hashing for message authentication
HSM	Hardware security module
NIST	National Institute of Standards and Technology
NV	Non-volatile (memory)
OEM	Original equipment manufacturer
OIAP	Object-independent authorization protocol
OSAP	Object-specific authorization protocol
PCR	Platform Configuration Register
RSA	Rivest Shamir Adelman
RTM	Root of trust for measurement
RTR	Root of trust for reporting
SHA	Secure Hash algorithm
SPI	Serial Peripheral Interface
SRK	Storage root key
TCG	Trusted Computed Group
TIS	TPM interface specification
TPM	Trusted Platform Module
TRNG	True random-number generator
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 this document, or are referenced in it.

[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 1.4]	TPM Library, Family 2.0, rev 1.38, Errata 1.4, January 8, 2018, TCG.
[PTP 2.0 r1.03]	TCG PC Client Specific Platform TPM Specification (PTP) - Version 2.0 Revision 1.03
[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
[TPM 20 PP]	Protection Profile PC Client Specific TPM, Family 2.0 Level 0 revision 1.38 (1.1), TCG.

Revision history

Table 9. **Document revision history**

Date	Version	Changes
17-Sep-2019	1	Initial release.
19-Dec-2019	2	Document confidentiality changed to public. Updated Features. Replaced *Engineering sample information* section by Section 5 Package marking information. Small text changes.

Contents

1 Description 3
1.1 Security certifications 3
1.2 Hardware features 3
2 Pin and signal description 4
3 Integration guidance 5
3.1 Typical hardware implementation 5
3.2 Power supply filtering 6
4 Package information 7
4.1 28-pin thin shrink small outline package information 7
4.2 Thermal characteristics of packages 10
5 Package marking information 12
6 Ordering information 13
7 Support and information 14
Appendix A Terms and abbreviations 15
Appendix B Referenced documents 16
Revision history 17
Contents 18
List of tables 19
List of figures 20

List of tables

Table 1. Pin descriptions . . . 4
Table 2. Maximum V_{PS} rising slope . . . 6
Table 3. TSSOP20 – package mechanical data . . . 8
Table 4. Packages on tape and reel . . . 10
Table 5. Reel dimensions . . . 10
Table 6. Carrier tape dimensions for TSSOP20 package . . . 11
Table 7. Ordering information for products supporting firmware 0x00.0x03.0x01.0x00 (0x0003.0x0100) (3.256) preloaded in factory . . . 13
Table 8. List of abbreviations . . . 15
Table 9. Document revision history . . . 17

List of figures

Figure 1. TSSOP20 pinout (top view) 4
Figure 2. Typical hardware implementation (TSSOP20 package) 5
Figure 3. Mandatory filtering capacitors on V_{PS} 6
Figure 4. TSSOP20 – package outline 7
Figure 5. TSSOP20 – package footprint 9
Figure 6. Reel diagram 10
Figure 7. Leader and trailer 11
Figure 8. Embossed carrier tape for the TSSOP20 package. 11
Figure 9. TSSOP20 package standard marking example 12

IMPORTANT NOTICE – PLEASE READ CAREFULLY

STMicroelectronics NV and its subsidiaries (“ST”) reserve the right to make changes, corrections, enhancements, modifications, and improvements to ST products and/or to this document at any time without notice. Purchasers should obtain the latest relevant information on ST products before placing orders. ST products are sold pursuant to ST’s terms and conditions of sale in place at the time of order acknowledgement.

Purchasers are solely responsible for the choice, selection, and use of ST products and ST assumes no liability for application assistance or the design of Purchasers’ products.

No license, express or implied, to any intellectual property right is granted by ST herein.

Resale of ST products with provisions different from the information set forth herein shall void any warranty granted by ST for such product.

ST and the ST logo are trademarks of ST. For additional information about ST trademarks, please refer to www.st.com/trademarks. All other product or service names are the property of their respective owners.

Information in this document supersedes and replaces information previously supplied in any prior versions of this document.

© 2019 STMicroelectronics – All rights reserved