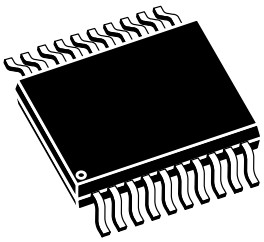
ST33GTPMAI2C

Data brief

Flash-memory-based TPM2.0 device for automotive applications with an I²C interface



TSSOP20

Product status link
ST33GTPMAI2C

Features

- AEC-Q100 qualified

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+
  - FIPS 140-2 level 2
  - (physical security level 3)
- TCG certification
- I2C support at up to 200 kHz
- Supports up to 4 GPIOs mapped with NV storage indices

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 protection against voltages greater than 4 kV (HBM)
- 1.8 V, 3.3 V or 5 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
- 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 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 ST33GTPMAI2C 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 targets CC certification according to TPM 2.0 PP at EAL4+.

1.2 Hardware features

The ST33GTPMAI2C 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 ST33GTPMAI2C offers an I²C interface 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 ST33GTPMAI2C 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.

2 Pin and signal descriptions

The figure below gives the pinout of the TSSOP20 package in which the devices are delivered. Table 1. Pin descriptions describes the associated signals.

Figure 1. TSSOP20 pinout (top view)

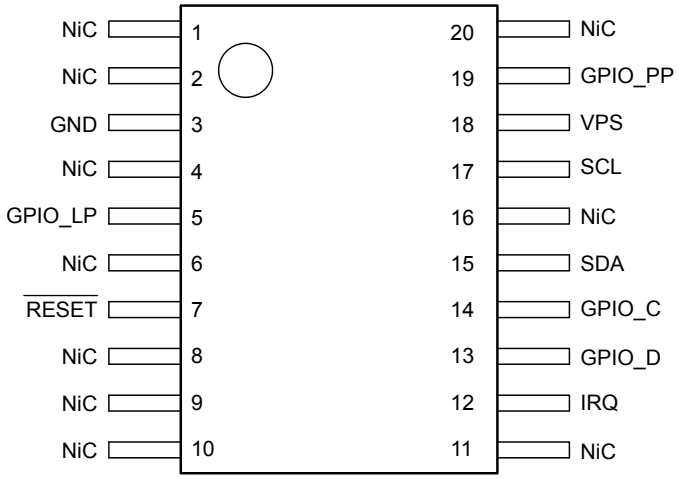


Table 1. Pin descriptions

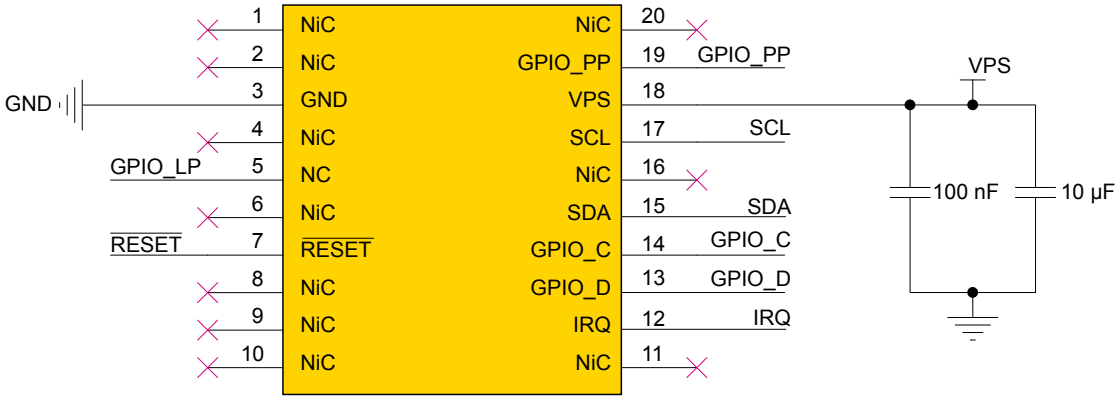
Signal	Type	Description
VPS	Input	**Power supply**. This pin must be connected to 1.8 V or 3.3 V DC power rail supplied by the motherboard.
GND	Input	GND has to be connected to the main motherboard ground.
SDA	Bidir	I2C serial data (open drain with no weak pull-up resistor)
SCL	Input	I2C serial clock (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 (not found). 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.

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.

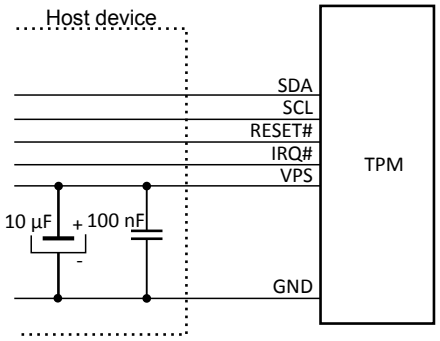
Figure 2. Typical hardware implementation (TSSOP20 package)



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

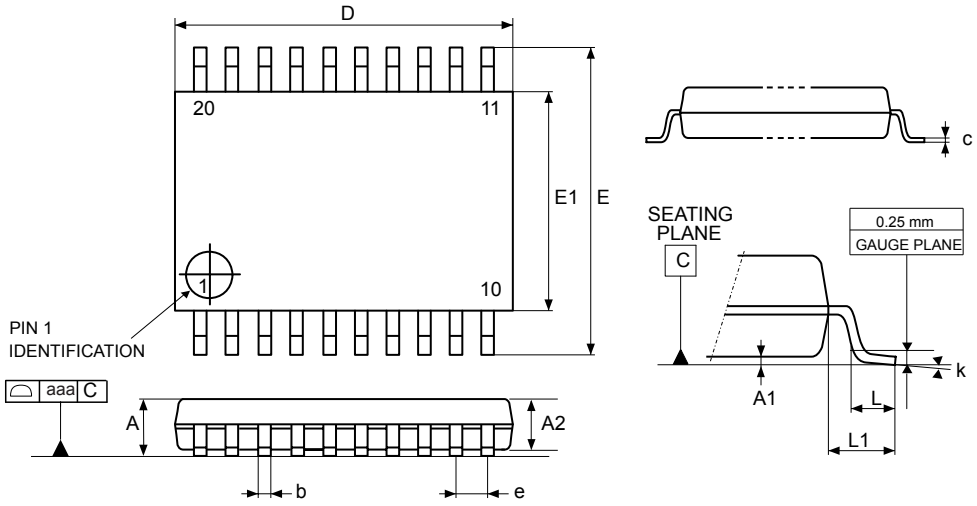
4 Package information

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



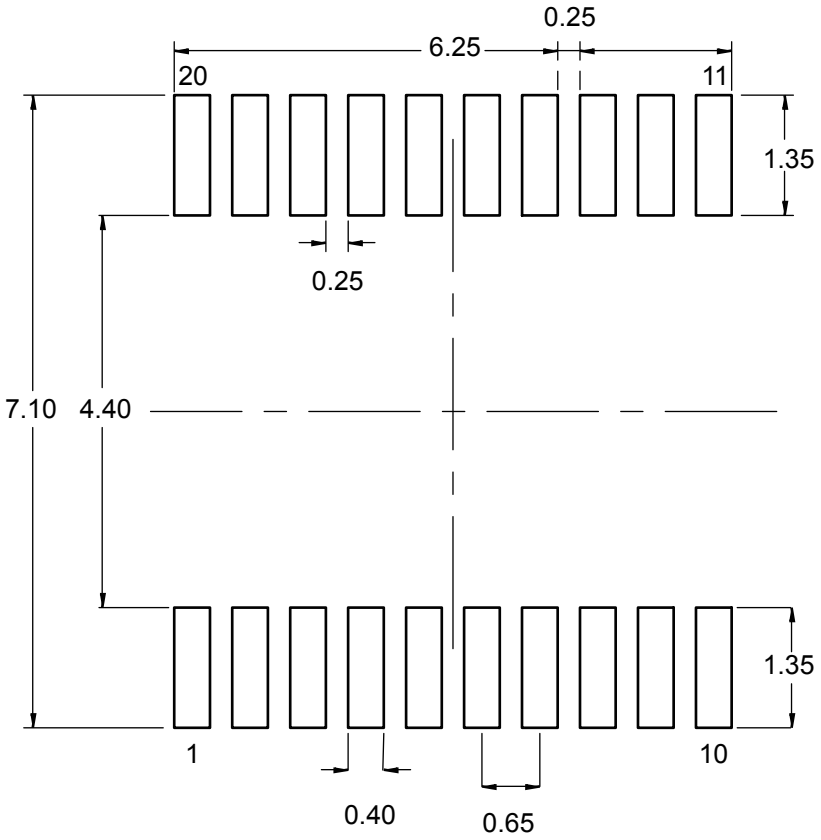
1. *Drawing is not to scale.*

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**

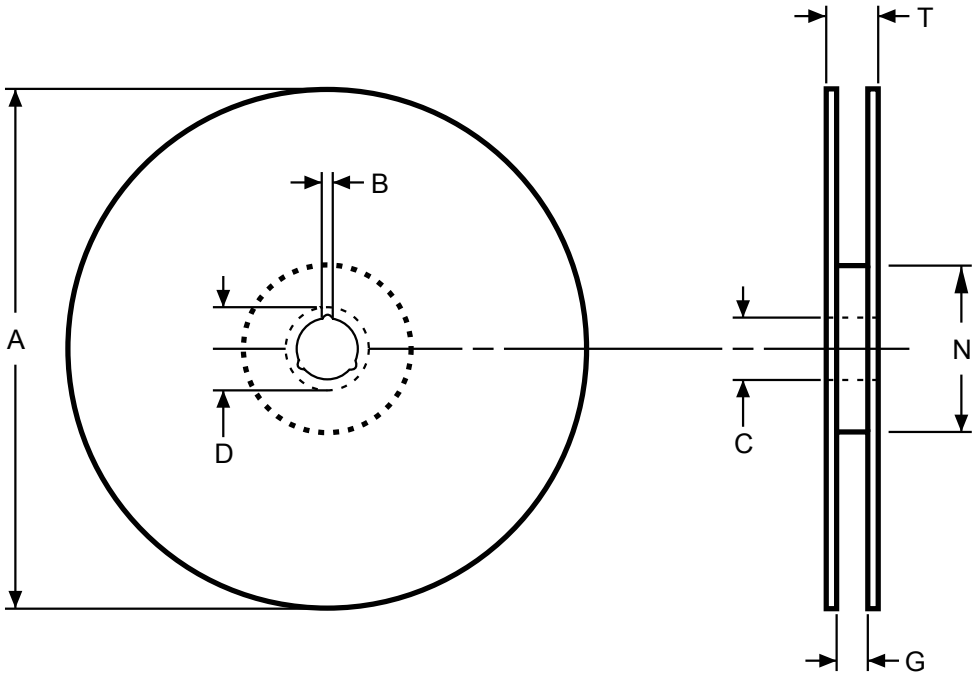


Table 5. **Reel dimensions**

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**

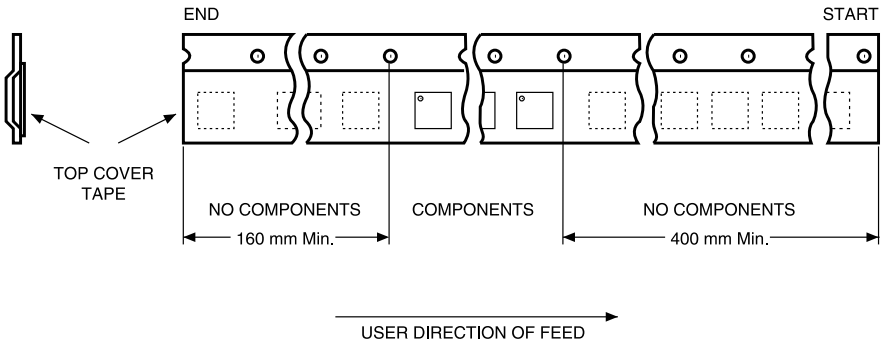
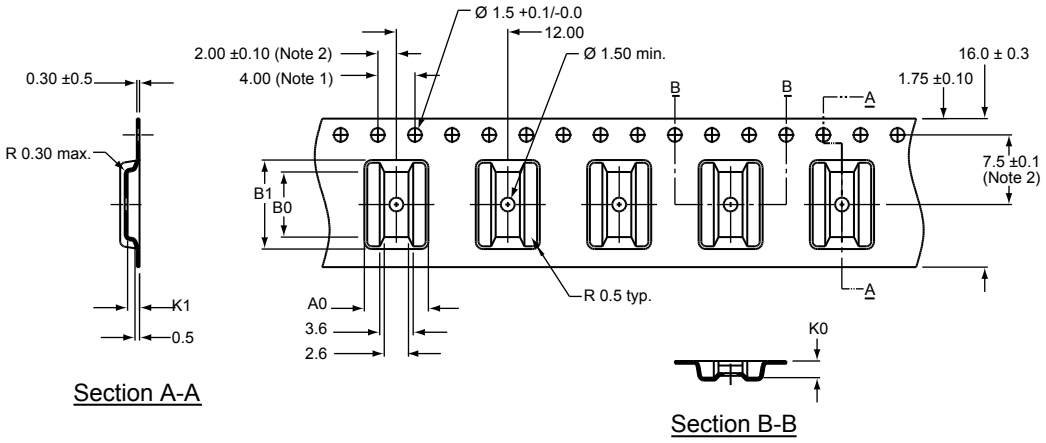


Figure 8. Embossed carrier tape for the TSSOP20 package



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.*

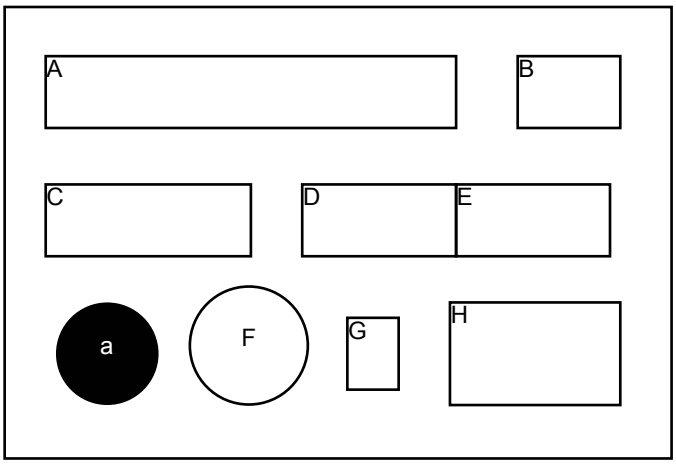
Table 6. Carrier tape dimensions for TSSOP20 package

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



Marking composition field

Unmarkable surface

Caption:

a: Pin 1 reference

A: Marking area: GTPMAI2C

B: Assembly week (ww)

C: Marking area: AE6

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 0x00.0x06.0x01.0x00 (0x0006.0x0100) (6.256) preloaded in factory

Ordering code	Firmware version	Operating temperature range	Maximum I²C clock frequency	Package	Marking (area C)
ST33GTPMA020FAE6	0x00.0x06.0x01.0x00 (0x0006.0x0100) (6.256)	-40 °C to +105 °C	200 kHz	TSSOP20	AE6

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
AFL	Applicative Flash memory loader
CA	Certificate authority
CC	Common Criteria
DRBG	Deterministic random-bit generator
EC	Elliptic curve
ECDAA	Elliptic curve direct anonymous attestation (algorithm)
ECDH	Elliptic curve Diffie–Hellman
FIPS	Federal Information Processing Standard
GPIO	General-purpose I/O
HMAC	Keyed-Hashing for Message Authentication
I²C	Inter-integrated circuit
NV	Non-volatile (memory)
RSA	Rivest Shamir Adelman
RTR	Root of trust for reporting
SHA	Secure Hash algorithm
TCG	Trusted Computed Group
TPM	Trusted Platform Module
TRNG	True random-number generator

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
04-Oct-2019	1	Initial release.
19-Dec-2019	2	Document confidentiality changed to public. Updated Product compliance. Small text changes.

Contents

List of tables

List of figures