

Trusted Platform Module (TPM) with I²C interface

Data brief



Features

- Single-chip Trusted Platform Module (TPM)
- Embedded TPM 1.2 firmware
- I²C communication interface (Slave mode)
- Architecture based on ST19N Secure Smartcard IC platform:
 - 1088-bit Modular Arithmetic Processor providing full support for Asymmetric operations
 - Hardware-based SHA-1 accelerator enabling BIOS related fast hash operations
 - AIS-31 compliant True Random Number Generator
 - Active security sensors DocID022264
- EEPROM-based NVM including 128 Bytes of OTP area for production configuration
 - Highly reliable CMOS EEPROM submicron technology
 - 10 year data retention
 - 500,000 Erase/Write cycle endurance
- Available in recommended TCG PC client 1.2 compatible TSSOP28 ECOPACK[®] package (RoHS compliant)
- 3.3V ± 10% power supply voltage
- 0 to 70 °C operating temperature range
- ST19NP18 intrinsic cryptographic performance^(a)
 - RSA 1024-bit signature with CRT: 57 ms
 - RSA 1024-bit signature without CRT^(b): 189 ms
 - RSA 1024-bit verification (e='\$10001'): 3.7 ms
 - RSA 1024-bit key generation: 1.6 s
 - RSA 2048-bit signature with CRT^(b): 382 ms
 - RSA 2048-bit verification (e='\$10001'): 60 ms

a. Typical values, independent of external clock frequency and supply voltage.

b. CRT: Chinese Remainder Theorem.

1 Description

The ST19NP18-TPM-I2C is a cost-effective Trusted Platform Module (TPM) solution. The ST19NP18-TPM-I2C is designed to provide embedded platforms with enhanced security and integrity mechanisms as defined by Trusted Computing Group standards. The product provides full support of TCG v1.2 specifications.

The ST19NP18-TPM-I2C is based on the ST19NP18 silicon product and includes an I²C communication interface (Slave mode).

The ST19NP18 is driven from the Smartcard IC ST19N platform. It is manufactured using the advanced highly reliable STMicroelectronics CMOS EEPROM technology.

The ST19NP18 has an 8-bit CPU architecture and includes the following on-chip memories: User ROM, User RAM and EEPROM with state of the art security features. ROM, RAM and EEPROM memories can be configured into partitions with customized access rules.

The ST19NP18 also includes a Modular Arithmetic Processor (MAP). The 1088-bit architecture of this cryptographic engine allows processing of modular multiplication, squaring and additional calculations up to 2176 bit operands.

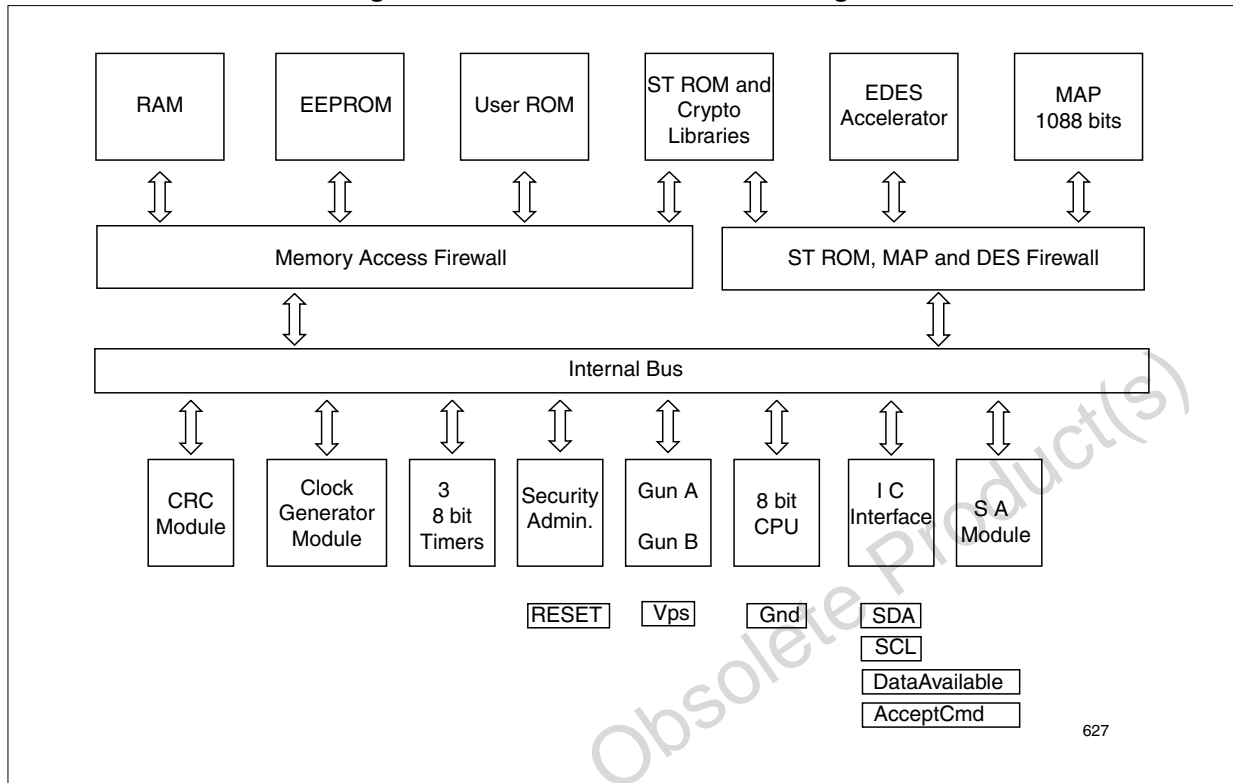
The Modular Arithmetic Processor (MAP) is designed to speed up cryptographic calculations using Public Key Algorithms.

The Secure Hash Accelerator allows fast SHA-1 computation especially well suited for BIOS hash operations during early boot stages.

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.



Figure 1. ST19NP18-TPM-I2C block diagram



2 Embedded TCG TPM firmware

The ST19NP18 includes TPM firmware compatible with TPM V1.2 specifications.

This firmware supports features such as Cryptographic Key Generation, Integrity Metrics and Secure Storage, as well as Locality, Delegation and Transport Session functions.

This TCG TPM firmware uses an optimized and flexible software architecture that easily integrates Trusted Computing Framework enhancements or dedicated functions.

The ST19NP18-TPM-I2C provides OEMs with a cost-effective TPM solution for their embedded platforms.

3 ST19NP18 pins and signals

Figure 2. Pinout description

SDA	1	TSSOP28	28	VPS ⁽¹⁾
SCL	2		27	VPS ⁽¹⁾
VNC	3		26	VPS ⁽¹⁾
GND1	4		25	NC
NC	5		24	VPS
DataAvailable	6		23	VPS ⁽¹⁾
PP	7		22	VPS ⁽¹⁾
NC	8		21	NC
AcceptCmd	9		20	VPS ⁽¹⁾
VPS	10		19	NC
GND2	11		18	GND3
NC	12		17	VPS ⁽¹⁾
NC	13		16	LRESET
NC	14		15	NC

1. These pins must be connected to V_{PS} through a 10-kOhm pull-up resistor.

Note: The CLKRUN signal is not listed on Pin 15 as it is not supported on ST TPM devices. However, ST TPM devices natively support Clock Stop mode (LCLK stopped). See GPIO5 pin description in table below.

Table 1. Signal descriptions

Signal	Type	Description
LRESET	Input	Reset used to re-initialize the device
GPIO5/ CLKRUN	Bidir	General-purpose IO , fully configurable by Firmware. CLKRUN same as PCI <u>CLKRUN</u> . Only needed by peripherals that need DMA or bus mastering in a system that can stop the PCI bus (generally in mobile systems).
PP	Input	Physical Presence , active high, internal pull-down. Used to indicate Physical Presence to the TPM
VPS	Input	3.3V Power supply . VPS has to be connected to 3.3v DC power rail supplied by the motherboard
GND	Input	Zero volts ground reference. GND has to be connected to the main motherboard ground.
VNC	-	Vendor-controlled No Connect : internal pull-up implemented. Can be left unconnected. Must not be tied to GND.
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)
DataAvailable	Output	Data Available (push-pull)
AcceptCmd	Output	Accept Command (push-pull)

4 Package description

28-pin Thin Shrink Small Outline Package (TSSOP) with 4.4-mm body width

Dimensional features of the TSSOP28 package: Body width 4.4 mm. Pitch 0.65 mm. Unless otherwise specified, general tolerance is ± 0.1 mm.

Figure 3. Mechanical drawing

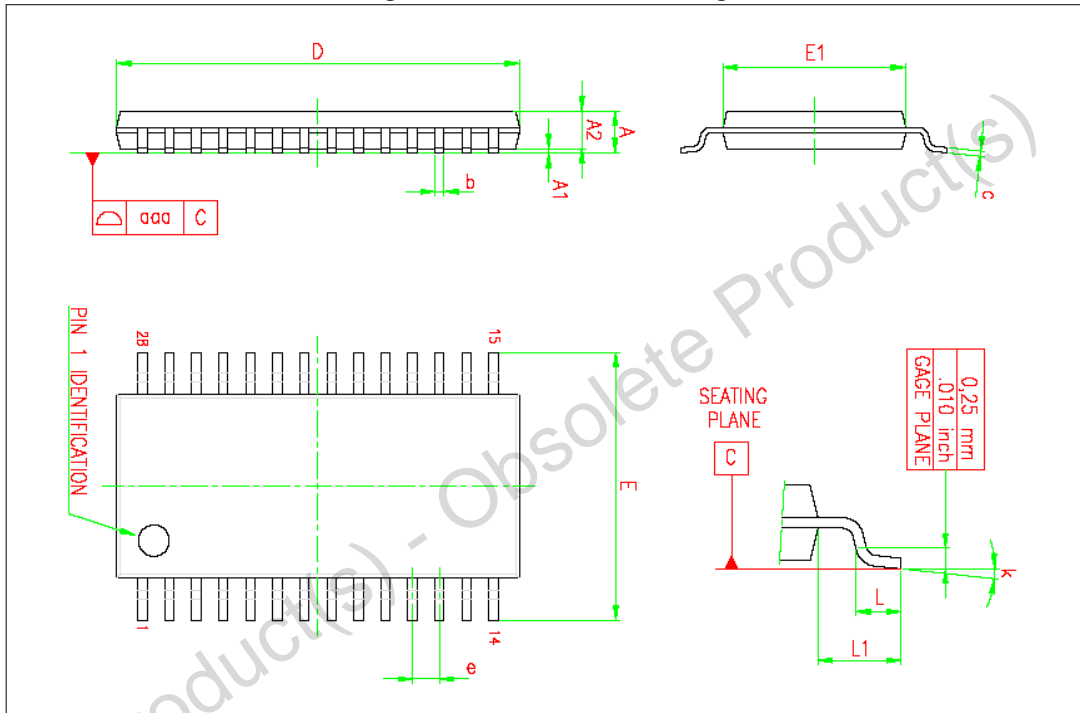


Table 2. Package dimensions

Symbol	millimeters			inches		
	Min.	Typ.	Max.	Min.	Typ.	Max.
A			1.20			0.047
A1	0.05		0.15	0.002		0.006
A2	0.80	1.00	1.05	0.031	0.040	0.041
b	0.19		0.30	0.007		0.012
c	0.09		0.20	0.004		0.008
D	9.60	9.70	9.80	0.378	0.382	0.386
E	6.20	6.40	6.60	0.244	0.252	0.260
E1	4.30	4.40	4.50	0.170	0.173	0.177
e		0.65			0.026	
L	0.45	0.60	0.75	0.018	0.024	0.0230
L1		1.00			0.040	
k	0°		8°	0°		8°
aaa			0.10			0.004

5 Revision history

Table 3. Document revision history

Date	Revision	Changes
01-Aug-2004	1	Initial release.
07-Nov-2013	2	Updated logo information on page 2.

Obsolete Product(s) - Obsolete Product(s)

Please Read Carefully:

Information in this document is provided solely in connection with ST products. STMicroelectronics NV and its subsidiaries ("ST") reserve the right to make changes, corrections, modifications or improvements, to this document, and the products and services described herein at any time, without notice.

All ST products are sold pursuant to ST's terms and conditions of sale.

Purchasers are solely responsible for the choice, selection and use of the ST products and services described herein, and ST assumes no liability whatsoever relating to the choice, selection or use of the ST products and services described herein.

No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted under this document. If any part of this document refers to any third party products or services it shall not be deemed a license grant by ST for the use of such third party products or services, or any intellectual property contained therein or considered as a warranty covering the use in any manner whatsoever of such third party products or services or any intellectual property contained therein.

UNLESS OTHERWISE SET FORTH IN ST'S TERMS AND CONDITIONS OF SALE ST DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY WITH RESPECT TO THE USE AND/OR SALE OF ST PRODUCTS INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE (AND THEIR EQUIVALENTS UNDER THE LAWS OF ANY JURISDICTION), OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

ST PRODUCTS ARE NOT DESIGNED OR AUTHORIZED FOR USE IN: (A) SAFETY CRITICAL APPLICATIONS SUCH AS LIFE SUPPORTING, ACTIVE IMPLANTED DEVICES OR SYSTEMS WITH PRODUCT FUNCTIONAL SAFETY REQUIREMENTS; (B) AERONAUTIC APPLICATIONS; (C) AUTOMOTIVE APPLICATIONS OR ENVIRONMENTS, AND/OR (D) AEROSPACE APPLICATIONS OR ENVIRONMENTS. WHERE ST PRODUCTS ARE NOT DESIGNED FOR SUCH USE, THE PURCHASER SHALL USE PRODUCTS AT PURCHASER'S SOLE RISK, EVEN IF ST HAS BEEN INFORMED IN WRITING OF SUCH USAGE, UNLESS A PRODUCT IS EXPRESSLY DESIGNATED BY ST AS BEING INTENDED FOR "AUTOMOTIVE, AUTOMOTIVE SAFETY OR MEDICAL" INDUSTRY DOMAINS ACCORDING TO ST PRODUCT DESIGN SPECIFICATIONS. PRODUCTS FORMALLY ESCC, QML OR JAN QUALIFIED ARE DEEMED SUITABLE FOR USE IN AEROSPACE BY THE CORRESPONDING GOVERNMENTAL AGENCY.

Resale of ST products with provisions different from the statements and/or technical features set forth in this document shall immediately void any warranty granted by ST for the ST product or service described herein and shall not create or extend in any manner whatsoever, any liability of ST.

ST and the ST logo are trademarks or registered trademarks of ST in various countries.

Information in this document supersedes and replaces all information previously supplied.

The ST logo is a registered trademark of STMicroelectronics. All other names are the property of their respective owners.

© 2013 STMicroelectronics - All rights reserved

STMicroelectronics group of companies

Australia - Belgium - Brazil - Canada - China - Czech Republic - Finland - France - Germany - Hong Kong - India - Israel - Italy - Japan - Malaysia - Malta - Morocco - Philippines - Singapore - Spain - Sweden - Switzerland - United Kingdom - United States of America

www.st.com

