



Trusted Platform Module (TPM)

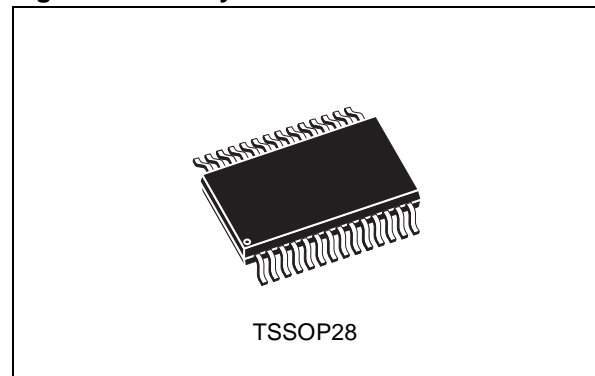
DATA BRIEF

PRODUCT FEATURES

- SINGLE-CHIP TRUSTED PLATFORM MODULE (TPM)
- EMBEDDED TPM 1.2 FIRMWARE
- FULL TPM SOLUTION WITH COMPLETE TCG COMPLIANT SOFTWARE STACK LAYERS
- 33-MHz LOW PIN COUNT (LPC) INTERFACE V1.1
- COMPLIANT WITH TCG PC CLIENT SPECIFIC TPM IMPLEMENTATION SPECIFICATION (TIS) V1.2
- DEDICATED LPC COMMUNICATION BUFFER FOR TPM COMMANDS HANDLING OPTIMIZATION
- TRUSTED COMPUTING GROUP (TCG)⁽¹⁾ V1.1B / V1.2 CONFIGURABLE MODE OF OPERATIONS
- ARCHITECTURE BASED ON ST19W 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
 - FIPS 140-2 compliant Random Number Generator
 - Active security sensors
- 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
 - Storage for up to 30 keys
- 5 SOFTWARE-CONTROLLED GENERAL PURPOSE I/O (GPIO) PINS

- POWER SAVING MODE
- AVAILABLE IN RECOMMENDED TCG PC CLIENT 1.2 COMPATIBLE TSSOP28
- 3.3V ± 10% POWER SUPPLY VOLTAGE
- 0-70°C OPERATING TEMPERATURE RANGE

Figure 1. Delivery Form



Function	Speed ⁽¹⁾
RSA 1024 bits signature with CRT ⁽¹⁾	62 ms
RSA 1024 bits signature without CRT ⁽²⁾	206 ms
RSA 1024 bits verification (e='\$10001')	4 ms
RSA 1024 bits key generation	1.8 s
RSA 2048 bits signature with CRT ⁽²⁾	416 ms
RSA 2048 bits verification (e='\$10001')	66 ms

1. Typical values, independent of external clock frequency and supply voltage.
2. CRT: Chinese Remainder Theorem.

1. TCG website: <http://www.trustedcomputinggroup.org>

GENERAL DESCRIPTION

The ST19WP18 is a cost effective Trusted Platform Module (TPM) solution. The ST19WP18 is designed to provide PC platforms with enhanced security and integrity mechanisms as defined by Trusted Computing Group standards. The product provides full support of TCG v1.1b as well as TCG v1.2 specifications

The ST19WP18 is driven from the Smartcard IC ST19W platform. It is manufactured using the advanced highly reliable STMicroelectronics CMOS EEPROM technology.

The ST19WP18 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.

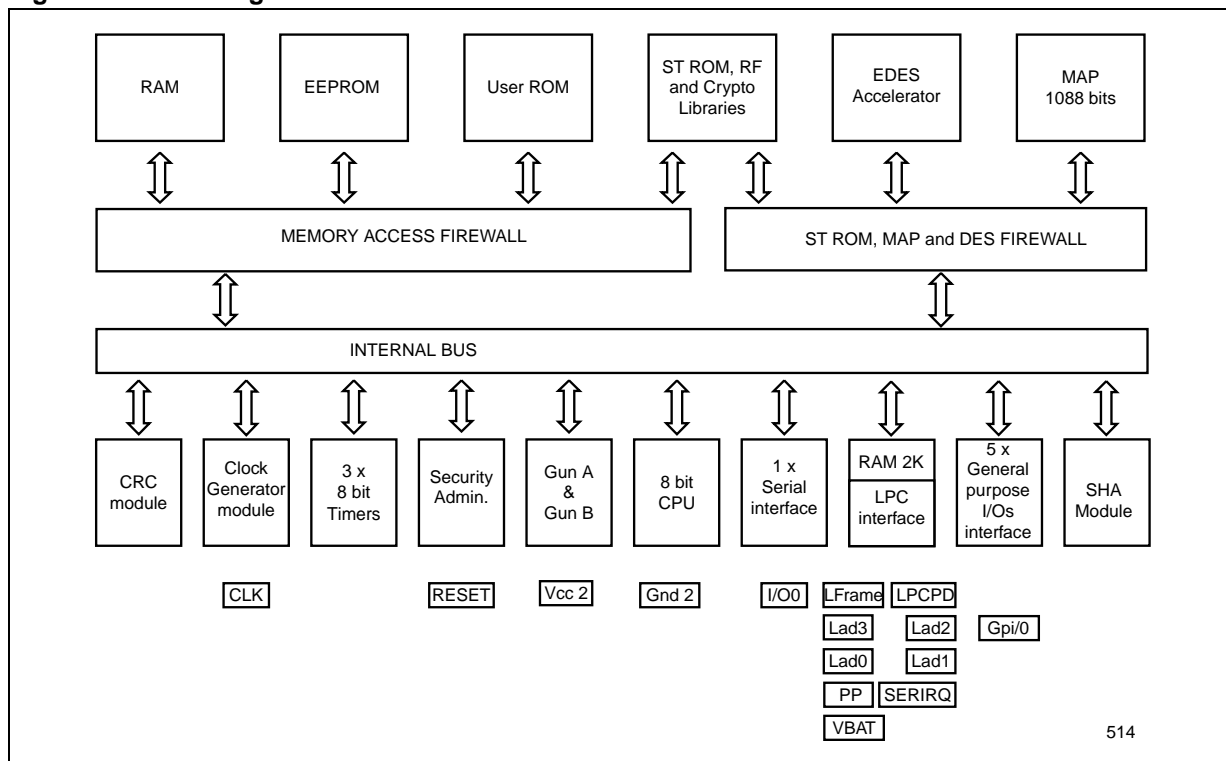
The ST19WP18 also includes a Modular Arithmetic Processor (MAP). The 1088 bits architecture of this cryptographic engine allows processing of modular multiplication, squaring and additional calculations up to 2176 bit operands.

The Modular Arithmetic Processor 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.

The ST19WP18 has been specially designed in line with TCG PC Client Specific TPM Implementation Specification (TIS) referring to Intel's LPC Specification revision 1.0.

Figure 2. Block Diagram



SOFTWARE DESCRIPTION

Embedded firmware

The ST19WP18 includes fully compliant TCG v1.1b firmware which supports features like cryptographic key generation, integrity metrics and secure storage. In addition, the product is TCG v1.2 ready and provides support for functions such as Delegation, Transport session and Locality.

This TCG v1.1b / v1.2 compliant firmware uses an optimized and flexible software architecture allowing the integration of Trusted Computing Framework enhancements or implementation of dedicated functions.

TCG Software Stack

The ST19WP18 provides complete system software layers, fully compliant with TCG Trusted Software Stack specification.

Microsoft Windows™ 2000/XP operating systems are supported. Please contact ST for a complete list of supported operating systems. The embedded firmware plus additional modules bring OEMs a complete TPM solution for their PC platforms.

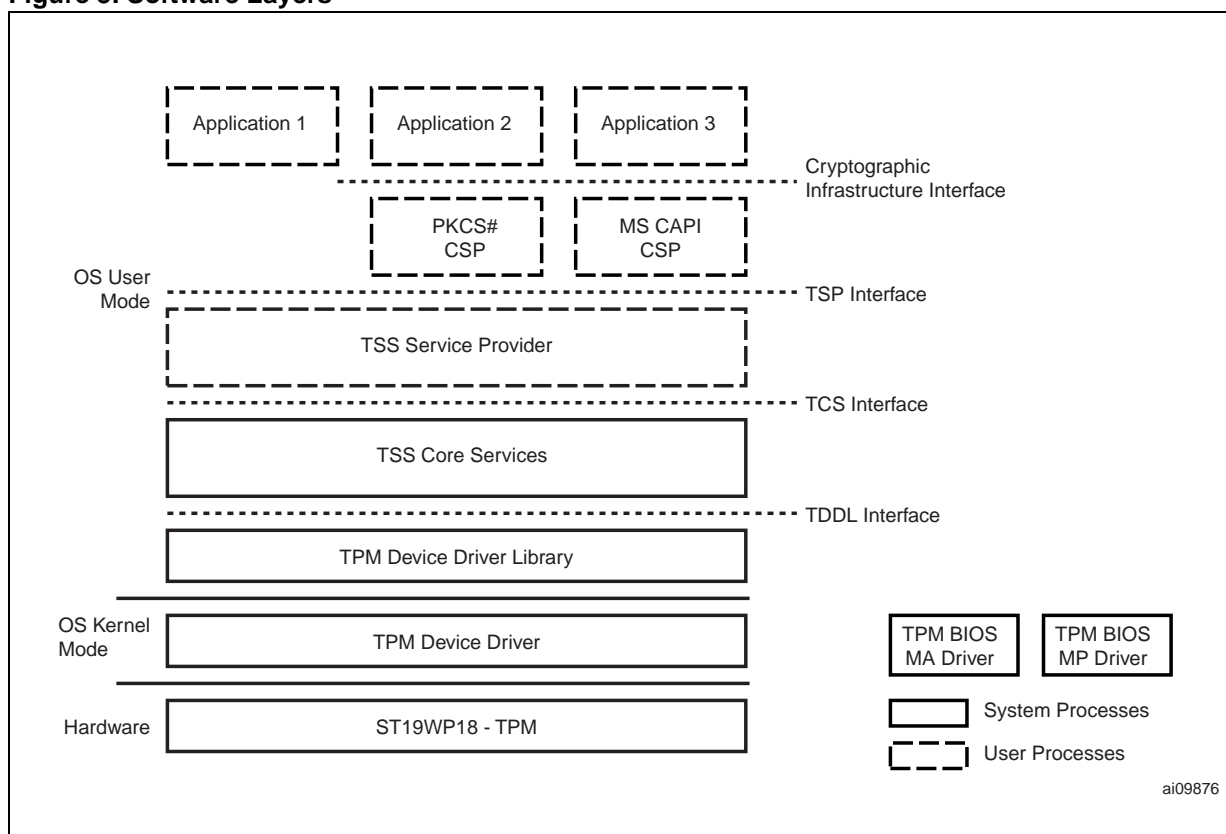
The software stack comprises the following modules:

- BIOS Memory Absent driver (MA)
- BIOS Memory Present driver (MP)
- TPM Device Driver (TDD)
- TPM Device Driver Library (TDDL)
- TSS Core Services (TCS)
- TSS Service Provider (TSP)

Cryptographic infrastructure interface

Secure and trustworthy functions of the ST19WP18 module are made available to applications through cryptographic Application Programming Interfaces (APIs) compliant either to PKCS#11 standard or to the MS CAPI specification. An ST19WP18 ready Cryptographic Service Provider (CSP) can then be used to enhance Operating System security policies or applications security plug-ins which take full advantage of the secure TPM functionalities such as sealed storage, key generation, signature and encryption.

Figure 3. Software Layers



PIN AND SIGNAL OVERVIEW

Figure 4. Pinout description

	TSSOP28		
GPIO1	1	28	LPCPD#
GPIO2	2	27	SERIRQ
IO	3	26	LAD0
GND	4	25	NC
NC	5	24	VPS
GPIO3	6	23	LAD1
PP	7	22	LFRAME#
NC	8	21	LCLK
GPIO4	9	20	LAD2
VPS	10	19	NC
GND	11	18	GND
NC	12	17	LAD3
NC	13	16	LRESET#
NC	14	15	GPIO5/CLKRUN#

Table 1. Signal description

Signal	Type	Description
LAD[3:0]	Bidir	Multiplexed Command, Address and Data (see LPC Interface Spec)
LPCPD#	Input	Power Down indicates that the peripheral should prepare for power to be removed from the LPC i/F devices. Actual power removal is system dependent (see LPC Interface Spec)
LCLK	Input	Clock Same 33Mhz clock as PCI clock on the host. Same clock phase with typical PCI skew. (see LPC Interface Spec)
LFRAME#	Input	Frame indicates start of a new cycle, termination of broken cycle (see LPC Interface Spec)
LRESET#	Input	Reset same as PCI Reset on the host (see LPC Interface Spec)
SERIRQ	Bidir	Serialized IRQ is used by TPM to handle interrupt support (see LPC Interface Spec)
GPIO5/CLKRUN#	Bidir	General Purpose IO , weak internal pull-up fully configurable by Software CLKRUN# same as PCI CLKRUN#. 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
GPIO[4:1]	Bidir	General Purpose IOs with weak internal pull-up fully configurable by Software
IO	Bidir	Bidirectional IO ISO 7816-2 compliant serial port
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

Information furnished is believed to be accurate and reliable. However, STMicroelectronics assumes no responsibility for the consequences of use of such information nor for any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of STMicroelectronics. Specifications mentioned in this publication are subject to change without notice. This publication supersedes and replaces all information previously supplied. STMicroelectronics products are not authorized for use as critical components in life support devices or systems without express written approval of STMicroelectronics.

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

© 2004 STMicroelectronics - All rights reserved
BULL CP8 Patents

STMicroelectronics GROUP OF COMPANIES
Australia - Belgium - Brazil - Canada - China - Czech Republic - Finland - France - Germany -
Hong Kong - India - Israel - Italy - Japan - Malaysia - Malta - Morocco - Singapore -
Spain - Sweden - Switzerland - United Kingdom - United States
www.st.com