ST19WP18-TPM-C

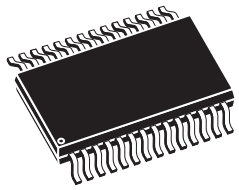
Trusted Platform Module (TPM)
With complete TCG Software Solution

DATA BRIEF

PRODUCT FEATURES

- SINGLE-CHIP TRUSTED PLATFORM MODULE (TPM)
- EMBEDDED TPM 1.2 FIRMWARE
- TPM DRIVER FOR BIOS AND WINDOWS™ 2000/XP
- TCG SOFTWARE STACK (TSS)(1)
- TPM ADMINSTRATION TOOL PROVIDING OWNER/USERS MANAGEMENT AS WELL AS KEY ARCHIVES POLICIES(1)
- 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)(2) 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



TSSOP28

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. Solution bundles an integrated Core TCG Software Stack from NTRU Cryptosystems along with the Embassy Security Center and Cryptographic Services Provider from Wave Systems. Any marks and brands contained herein are the property of their respective owners.
2. TCG website: http://www.trustedcomputinggroup.org

GENERAL DESCRIPTION

The ST19WP18-TPM-C is a cost effective Trusted Platform Module (TPM) solution. The ST19WP18-TPM-C 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.

ST19WP18-TPM-C is based on the ST19WP18 silicon product.

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.

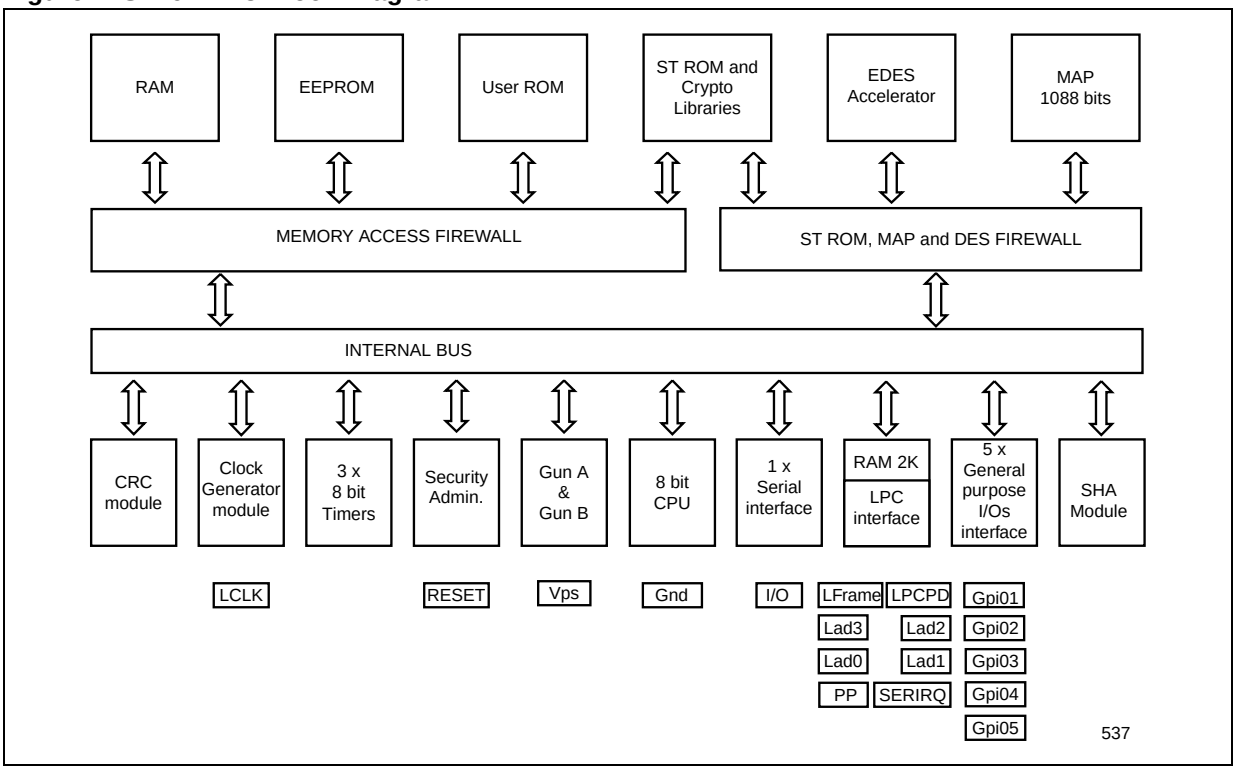
The ST19WP18 also includes a Modular Arithmetic Processor (MAP). The 1088 bits architecture of this cryptographic engine allows processing of modular multiplication, squaring and additional calculations up to 2176 bit operands.

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. ST19WP18 Block Diagram



SOFTWARE DESCRIPTION

Embedded TPM firmware

The ST19WP18 includes fully compliant TCG v1.1b TPM 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 TPM firmware uses an optimized and flexible software architecture allowing the integration of Trusted Computing Framework enhancements or implementation of dedicated functions.

Software Stack

To enable its integration on PC motherboards, ST19WP18-TPM-C provides BIOS and Microsoft Windows™ drivers.

Memory Absent (MA) and Memory Present (MP) BIOS drivers source codes are made available for easy integration into compound or integrated BIOSes. Both provide means for BIOS to access TPM resources in memory - less or post BIOS system environments.

In addition a Windows™ 2000/XP driver is also supplied in the form of a TPM Device Driver (TDD) running in Kernel mode and a TPM Device Driver Library (TDDL) running in User mode.

Please contact ST for a complete list of supported operating systems.

The ST19WP18-TPM-C also includes a TCG Trusted Software Stack (TSS) fully compliant with TCG Specification standard version 1.1 interface and security services for application that relies on ST TPM.

The stack, enhanced with strong, standards compliant cryptographic libraries, is composed of two dedicated components: the TCG Service Provider (TSP) and the TCG Core Services (TCS).

The overall software stack of the ST19WP18-TPM-C then 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)

TPM Administrative Tool

As a full part of the ST19WP18-TPM-C solution is the Embassy Security Center (ESC) from Wave Systems.

The ESC is a dedicated application providing TCG platform management functions, advanced user authentication functions and TPM keys archive and restore functionality.

Platform management functions provided by ESC is a key feature of TPM enabled PC. They allow a super user to take ownership of the TPM and as such getting TPM administrative privileges.

Once ownership taken, additional users can then make use of the TPM as well, thanks to a simple initialization process.

It is important that both owner and users can move their sensitive information (typically their respective keys) out from the TPM, for mobility or maintenance reasons. Key management feature of ESC also allows to migrate and restore keys in an easy and intuitive way.

Cryptographic infrastructure interface

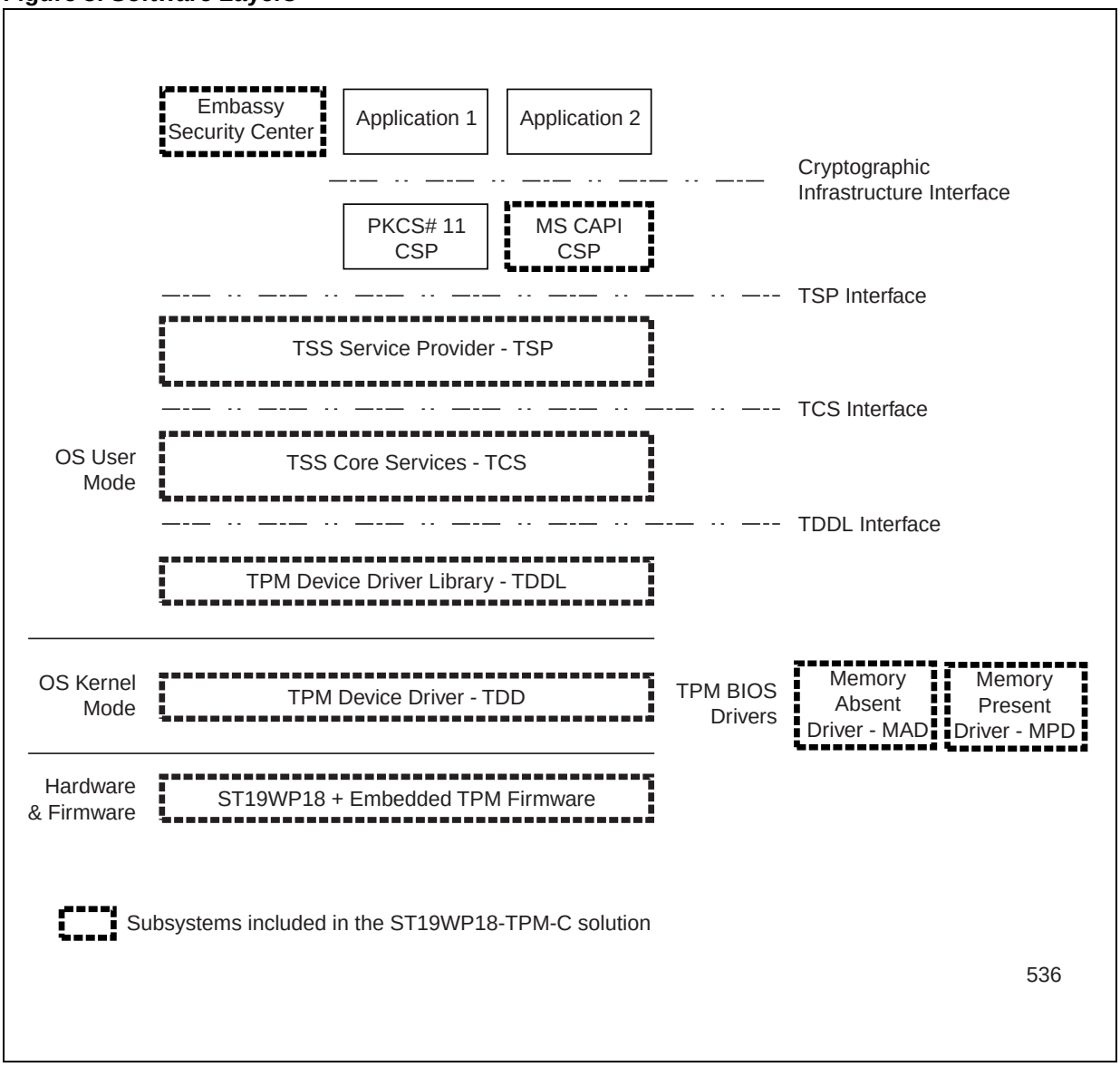
Secure and trustworthy functions of the ST19WP18 and its embedded TPM firmware module are made available to applications through cryptographic Application Programming Interfaces (APIs) compliant either to PKCS#11standard or to the MS CAPI specification. The ST19WP18-TPM-C solution includes an MS CAPI TCG enabled CSP fully supporting the TPM functions of the ST19WP18 and its embedded firmware.

This Cryptographic Service Provider (CSP) can 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.

Please contact ST for other CSP model support.

The ST19WP18-TPM-C bring OEMs a complete TPM solution for their PC platforms.

Figure 3. Software Layers



PIN AND SIGNAL OVERVIEW

Figure 4. Pinout description

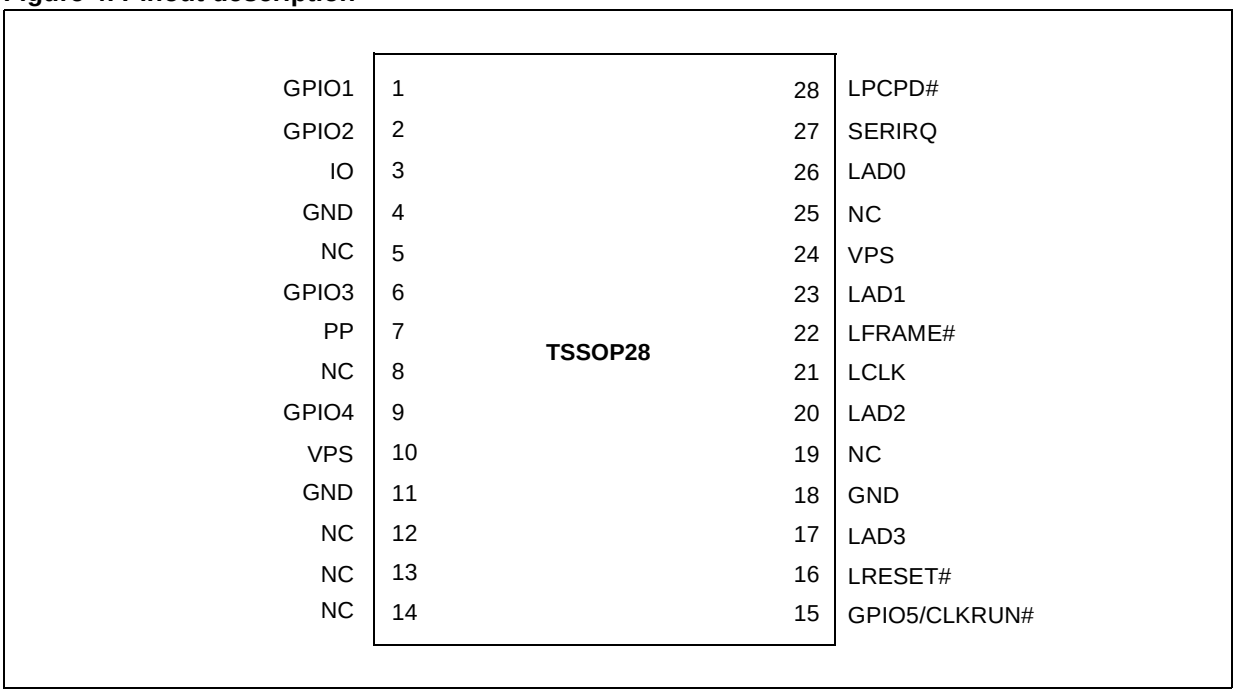


Table 1. Signal description

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 mother board ground