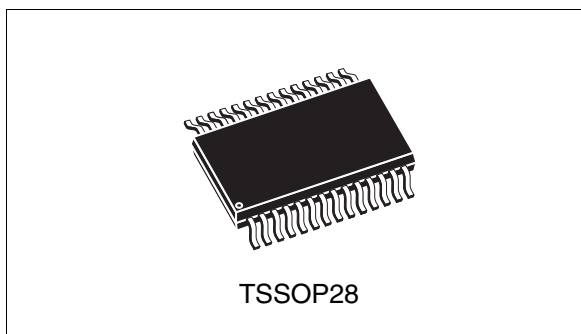# ST19NP18-TPM

Trusted Platform Module (TPM)

Features

■ Single-chip Trusted Platform Module (TPM)

■ Embedded TPM 1.2 firmware

■ 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

■ Compliant with Trusted Computing Group (TCG)[1] V1.1B / V1.2 specifications

■ 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
  – FIPS 140-2 and AIS-31 compliant Random Number Generators
  – Active security sensors

TSSOP28

■ 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 9 keys

■ 5 firmware-controlled General Purpose I/O (GPIO) pins

■ Power-saving mode

■ 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 performances[2]
  – RSA 1024-bit signature with CRT[3]:   57 ms
  – RSA 1024-bit signature without CRT[3]:   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[3]:   382 ms
  – RSA 2048-bit verification (e='$10001'):   60 ms

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

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

3. CRT: Chinese Remainder Theorem.

Contents

List of tables

List of figures

1   Description

The ST19NP18-TPM is a cost-effective Trusted Platform Module (TPM) solution. The ST19NP18-TPM 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 v1.2 specifications.

The ST19NP18-TPM is based on the ST19NP18 silicon product.

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.

The ST19NP18 is specially designed in line with TCG PC Client Specific TPM Implementation Specification (TIS) referring to Intel's LPC Specification revision 1.1.

Figure 1.   ST19NP18 block diagram
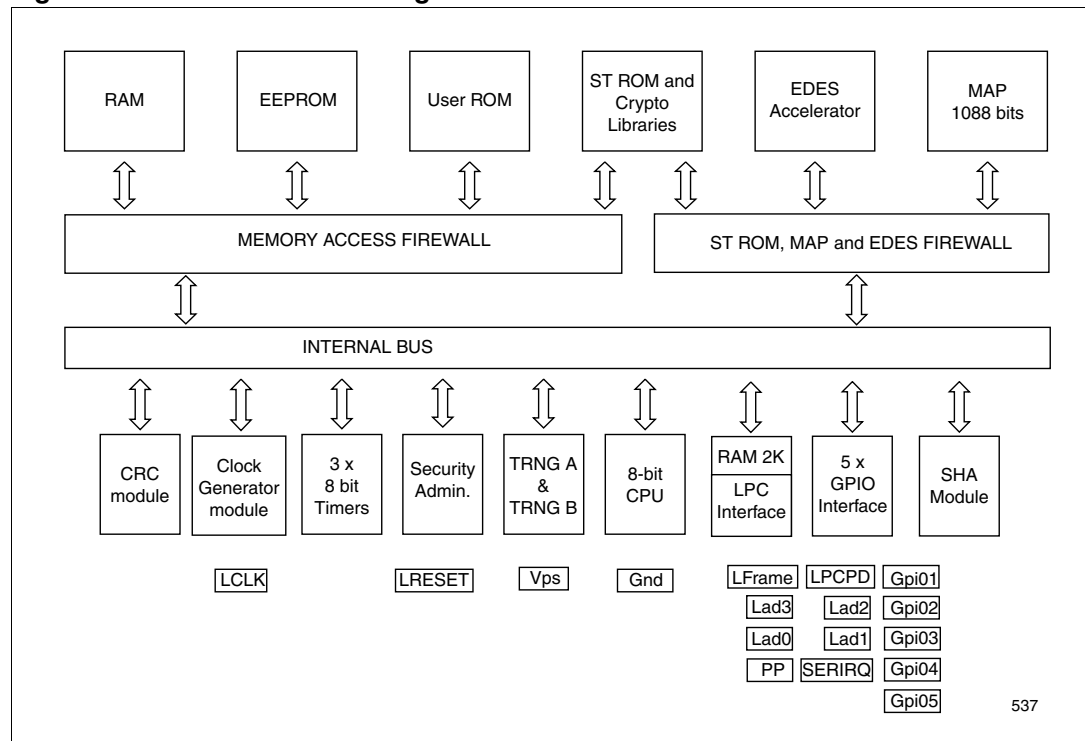
In order to meet environmental requirements, ST (also) offers these devices in ECOPACK® packages. ECOPACK® packages are Lead-free. The category of second Level Interconnect is marked on the package and on the inner box label, in compliance with JEDEC Standard JESD97. The maximum ratings related to soldering conditions are also marked on the inner box label.

ECOPACK is an ST trademark. ECOPACK specifications are available at: www.st.com.

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 provides OEMs with a cost-effective TPM solution for their PC platforms.

Figure 2.   ST19NP18-TPM overview
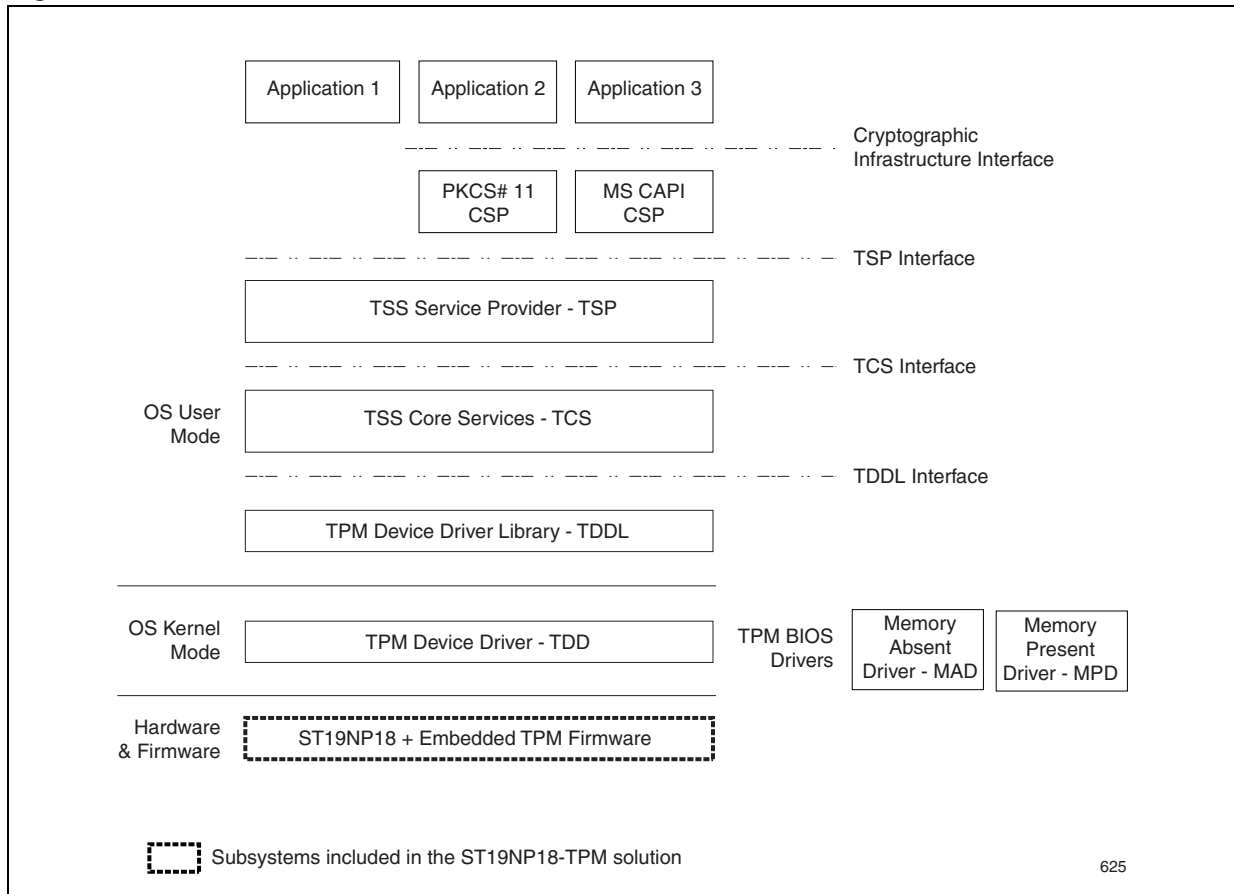
2   ST19NP18-TPM TCG solution

The STMicroelectronics ST19NP18-TPM Trusted Computing Group V1.2 Solution is based on ST19NP18 silicon device and its embedded firmware compatible with TCG TPM specifications. This solution includes also the following software components providing a cost-effective TPM solution for PC OEMs.

2.1   ST19NP18 hardware device

Based on the STMicroelectronics ST19N product family, it is the silicon part of the ST19NP18-TPM TCG solution. it provides all TPM hardware capabilities and hosts the TCG TPM V1.2 firmware.

2.2   Embedded TCG TPM firmware

This firmware implements latest TCG specification functions and complies with TCG V1.2 specifications. Upon request, STMicroelectronics can configure the device to operate in TCG V1.1b operational mode. This embedded firmware takes full advantage of the state-of-the-art Cryptographic and Security functions of the ST19NP18 hardware device.

Note: *The ST19NP18 hardware device with its embedded TCG firmware represents STMicroelectronics' Trusted Platform Module (TPM) hardware.*

ST19NP18 is also validated under Windows® Vista® using the native Microsoft TPM driver.

3   ST19NP18 hardware description

3.1   ST19NP18 chip functions

The basis of the ST19NP18-TPM Trusted Computing Group V1.2 Solution is the ST19NP18 hardware product, a cost-effective circuit based on an 8 bit CPU core and driven from Secure Smartcard IC ST19N platform. The CPU of the ST19NP18 includes the ALU, the control logic and registers. The CPU interfaces with the on-chip memories RAM, ROM and EEPROM via the internal bus through two Firewalls.

The first Firewall is aimed to protect the on chip memories and controls access from any memory area to another memory area. The second Firewall protects against unauthorized jumps to sensitive chip resources.

A specific security block is added to the microcontroller to achieve an extremely high level of protection against software and hardware attacks.

The ST19NP18 device also includes two Random Number Generators, three 8-bit fully programmable Timers, a CRC module, a Modular Arithmetic Processor (MAP) and a SHA-1 Secure Hash Accelerator.

The product allows communication with the host using the Low-Pin Count (LPC) interface recommended by the TCG for PC Client TPM Specific implementation.

A set of five General Purpose Input/Output (GPIO) signals are provided for dedicated communication or control; those are fully configurable by firmware.

4   ST19NP18 cryptography overview

The MAP (Modular Arithmetic Processor) is a standalone 1088-bit crypto-processor that performs very efficiently basic operations. These operations, are driven by the cryptographic library of the ST19NP18 hardware device.

MAP along with its highly secured library allows following operations: additions, multiplications and squares, divisions, modular additions, Montgomery multiplications and squares, and computation of Montgomery constants.

The cryptographic library also includes higher level functions:

● RSA signature, verification and key generation with an RSA modulo up to 2176 bits

● Prime numbers generation up to 1088 bits for internal RSA key generation by the TPM

● DSA signatures and verifications with parameters of any length from 512 to 1088 bits

● SHA-1 hash function

5   Low Pin Count (LPC) interface

5.1   Introduction

The Low Pin Count (LPC) Interface implemented here complies with the Intel Low Pin Count Interface specification (Revision 1.1, August 2002). Please make reference to this specification if additional detail is needed. The LPC interface operates as an I/O slave peripheral. It supports I/O read or write cycles as well as the LPC special cycles as defined by the TCG TCG PC Client Specific TPM Interface Specification revision 1.2. All others cycles type such as DMA Read/write are ignored.

It has a read/write RAM buffer size of 2048 bytes. The LPC bus interface signals LCLK, $\overline{\text{LRESET}}$, $\overline{\text{LPCPD}}$, $\overline{\text{LFRAME}}$ and LAD[3:0] are connected to the device CLK, $\overline{\text{LRESET}}$, LPCPD, $\overline{\text{LFRAME}}$ and LAD[3:0] pins

The LPC macro holds a specific Base Address register that is used to define which LPC access cycles the ST19NP18 hardware device will have reply to. The value of this register is set by default (300h in I/O space) but can be changed at any time by the user. This can be easily done though ST TPM Windows Driver configuration settings.

5.2   Cycles overview

Data transfers on the LPC bus are serialized over a 4-bit Bus, LAD[3:0]. $\overline{\text{LFRAME}}$ is a control line used by the host to start or stop transfer. The LAD[3:0] bus communicates information serially and conveys the cycle type, cycle direction, chip selection, address, data and wait states. The general flow of a cycle is as follows:

   a)   A cycle is started by the host when it drives $\overline{\text{LFRAME}}$ low and puts appropriate information on the LAD[3:0] signal lines.

   b)   The host drives information relative to the cycle, such as I/O cycle type, read/write, direction and address.

   c)   The host optionally drives data, and turns the bus around (TAR) to monitor the peripheral for completion of the cycle.

   d)   The peripheral indicates completion of the cycle by driving appropriate values on the LAD[3:0] signal lines and potentially drives data.

   e)   The ST19NP18 turns the bus around (TAR) to the host, ending the cycle.

Figure 3 shows a typical timing for $\overline{\text{LFRAME}}$ and LAD[3:0].

Figure 3. **LPC Bus timing**
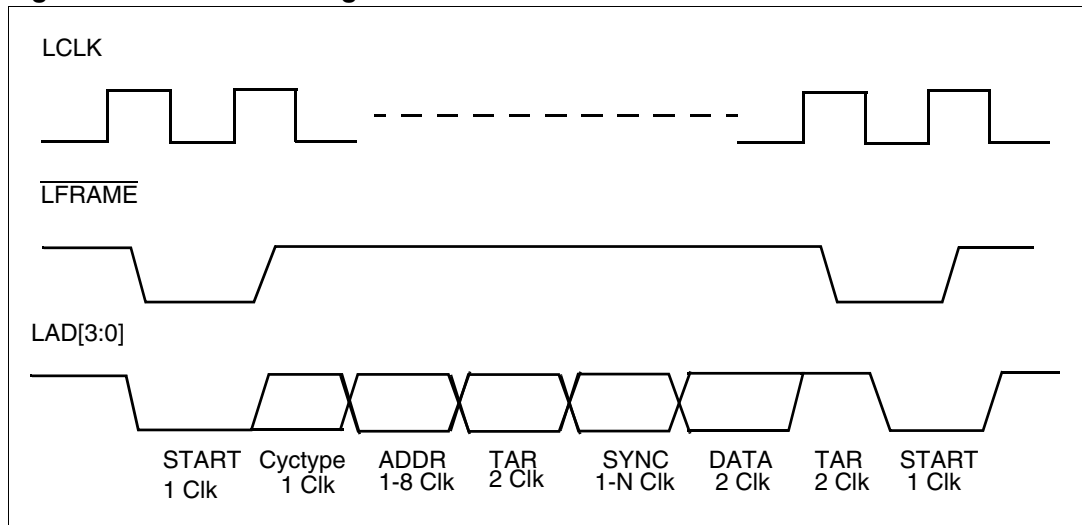
5.3 $\overline{\text{LRESET}}$, $\overline{\text{LPCPD}}$ and power down or standby management

When $\overline{\text{LRESET}}$ goes low, the device is reset and the internal LPC RAM contents is destroyed. When the Host drive the $\overline{\text{LPCPD}}$ signal low, it indicates that system power is going to be removed from the device. If auxiliary power is provided to the device, the device goes into standby and the contents of LPC RAM is preserved. The rising edge of $\overline{\text{LRESET}}$ signal is then used to generate an interrupt that wakes up the CPU as described in the following timing diagram.

The Host can also send a Power-down/Standby command to put the device into Standby mode and persevere the contents of LPC RAM as shown in the following timing diagram. The falling edge of the subsequent $\overline{\text{LFRAME}}$ signal is then used to generate an interrupt to the CPU and wakes up the device.

Figure 4.   LPC Power Down/Standby Timings
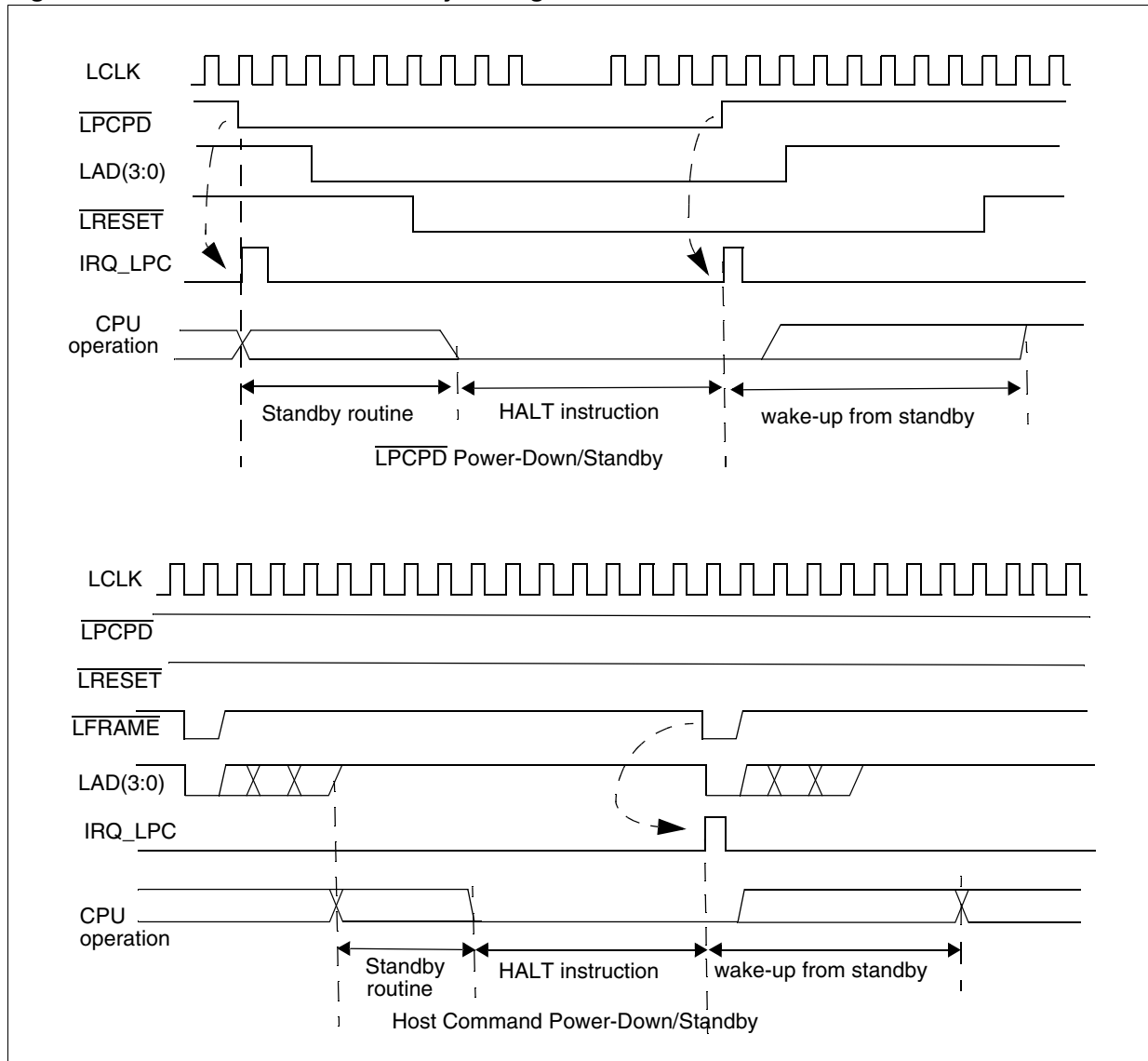
6 Secure Hash Accelerator (SHA-1)

The Secure Hash Accelerator is included to speed up the computation of the Secure Hash Algorithm (SHA), as defined by the FIPS- 180-1 document. The SHA-1 accelerator can hash a 64-KByte message in less than 0.3s. In addition, the accelerator proposes a set of elementary operations to accelerate most hashing algorithms based on 32-bit arithmetic.

7 Security

The high level security of the ST19NP18 hardware device is the result of the combination of:

● Technology
● Circuit architecture and design
● Firmware
● Manufacturing environment

At each level the concern is to achieve the maximum performance in terms of confidentiality, integrity and availability when referring to CC (Common criteria).

7.1 Technology

The integrity of the data stored into the EEPROM strongly relies on the technology used to manufacture the component.

The CMOS technology used for production allows 500,000 erase and program operations on each byte. This feature is important for applications where bytes are updated a large number of times. The data retention covers a minimum of 10 years.

7.2 Circuit architecture and design

In order to prevent unauthorized use of the chip or fraudulent access to data, a set of hardware security mechanisms has been implemented:

● Physical protection against micro-probing
● Non-observability of memory content
● Reset and power management
● EEPROM content destruction capability
● RAM destruction after POR and Reset
● True Random Number Generators
● Firewall against unauthorized access to memories or unauthorized execution
● Environment sensors managed by security administrator
● Built-in protection against power analysis attacks

7.3 Security at manufacturing level

A set of security procedures at every step of manufacturing process has been implemented in order to ensure the confidentiality of the development of the TPM as well as of its related credentials information.

Only those authorized are allowed to perform sensitive operations such as an electrical test, material handling from one location to another and to have access to the storage data.

Full traceability of all operations is kept for 10 years.

7.4   Security implemented by TCG TPM firmware

The security of the STMicroelectronics TPM not only relies on the security mechanisms implemented on the ST19NP18 hardware device, but it is also strongly related to the embedded TCG TPM firmware.

The development of this firmware takes advantage of ST security rules.

7.5   True Random Number Generators (TRNG)

Random numbers are necessary for advanced authentication, signature and encryption techniques.

The hardware TRNG implemented in ST19N family is AIS-31 compliant.

8 TPM configurations

This sections provides information concerning the default STMicroelectronics ST19NP18 TPM Configuration. For further information or specific configuration requests, please contact your local ST sales representative.

8.1 TPM default configuration

- TIS Mode LPC Addressing (TPM mapped in FED4xxxxh memory range)
- Firmware supporting TPM specifications Version 1.2 Rev. 103
- firmware_version (See *Section 10: Ordering information on page 22*)
- Number of PCRs   : 24
- Number of DIRs   : 1
- Revision ID (TPM_RID_x)   : 4Eh
- Vendor & Device ID (TPM_DID_VID_x)   : 0000104Ah
- Manufacturer information   : 53544D20h ('STM ')
  (TPM_CAP_VERSION_INFO.tpmVendorID,
  TPM_CAP_PROP_MANUFACTURER):

8.2 PCR configuration

Table 1 provides the PCR attribute value. Bit 0 stands for Locality 0, Bit 1 refers to Locality 1 and so on. A bit set means that the rights are granted.

Table 1.   PCR values

PCR number	Resetable	Extendable	PCR number	Resetable	Extendable
0	00h	1Fh	12	00h	1Fh
1	00h	1Fh	13	00h	1Fh
2	00h	1Fh	14	00h	1Fh
3	00h	1Fh	15	00h	1Fh
4	00h	1Fh	16	1Fh	1Fh
5	00h	1Fh	17	10h	1Ch
6	00h	1Fh	18	10h	1Ch
7	00h	1Fh	19	10h	0Ch
8	00h	1Fh	20	14h	0Eh
9	00h	1Fh	21	04h	04h
10	00h	1Fh	22	04h	04h
11	00h	1Fh	23	1Fh	1Fh

8.3 TPM addressing and register mapping

Early versions of the TCG specifications, e.g. v1.1, did not specify neither the Trusted Platform Module logical interface in terms of register mapping nor the TPM access protocol. As a consequence, Version 1.1 TPMs were designed to operate using a different hardware interface although most were logically mapped to be accessed through the I/O space of the system.

Upon release of Version 1.2 of the TPM specifications, TCG has defined a standardized TPM interface used to access the TPM in a more standardized way. The TCG PC Client Specific TPM Interface Specification V1.2 (or TIS) describes this interface.

8.3.1 Legacy addressing

In order to ensure backward compatibility or to ease integration of the TPM within a specific platform environment, the ST19NP18-TPM can be configured during the production phase to operate in Legacy mode.

In Legacy mode, the ST19NP18-TPM is mapped in the I/O space and responds to LPC I/O read and write access cycles. These access cycles are characterized by a START field set to 0000h in compliance with LPC specifications.

Table 2 and *Table 3* list the mapping of the ST19NP18-TPM registers in Legacy mode. Two I/O ports are used and internal TPM registers are accessed in an indexed manner. Port 0 is used to point the internal TPM register to access and Port 1 is used to read/write from the internal TPM register indicated in Port 0. In Legacy mode, the base address of the ST19NP18-TPM is the I/O address of Port 0. By default, this address is set to 300h.

Table 2.   Legacy I/O addresses

I/O address	Default value	Description
Port 0	300h	Index register
Port 1	301h	Data register

Table 3.   ST19NP18-TPM Legacy (I/O) registers mapping

Index register value	Description
00h	TPM_ACCESS_0
01h	TPM_ACCESS_1
02h	TPM_ACCESS_2
03h	TPM_ACCESS_3
04h	TPM_ACCESS_4
07h to 05h	Reserved for future use
08h	TPM_INT_ENABLE[7:0]
09h	TPM_INT_ENABLE[15:8]
0Ah	TPM_INT_ENABLE[23:16]
0Bh	TPM_INT_ENABLE[31:24]
0Ch	TPM_INT_VECTOR
12h to 0Dh	Reserved for future use

Table 3.   ST19NP18-TPM Legacy (I/O) registers mapping (continued)

Index register value	Description
0Ch	TPM_INT_STATUS[7:0]
13h	Reserved for future use
15h to 14h	Reserved for future use
16h	TPM_INTF_CAPABILITY[7:0]
17h	TPM_INTF_CAPABILITY[15:8]
18h	TPM_STATUS[7:0]
19h	TPM_STATUS[15:8]
1Ah	TPM_STATUS[23:16]
1Fh to 1Ch	Reserved for future use
20h	TPM_HASH_END
23h to 21h	Reserved for future use
27h to 24h	TPM_DATAFIFO
28h	TPM_HASH_START
29h	TPM_DID-VID[7:0]
2Ah	TPM_DID-VID[15:8]
2Bh	TPM_DID-VID[23:16]
2Ch	TPM_DID-VID[31:24]

8.3.2   TIS addressing (ST19NP18-TPM)

This is the standardized way of accessing the TPM on a PC Client environment. The TIS mode is fully defined by the TCG PC Client Specific TPM Interface Specification v1.2 (TIS). To take into account new TCG version 1.2 concepts such as locality, TIS specifies that the TPM is mapped in a memory space in the address range FED4-0000h to FED4-4FFFh.

In TIS mode, the ST19NP18-TPM responds to new LPC Memory read and write access cycles. These access cycles are characterized by a START field set to 0101h in compliance with TIS specifications.

Table 4 and *Table 5* list the mapping of the ST19NP18-TPM registers in TIS mode. All internal TPM registers are accessed in a direct manner.

Table 4.   TIS Memory addresses

Memory segment	index Tange	Description
FED4h	0nnnh	Locality 0
FED4h	1nnnh	Locality 1
FED4h	2nnnh	Locality 2
FED4h	3nnnh	Locality 3
FED4h	4nnnh	Locality 4

Note: *nnn refers to the offset in* Table 5.

Table 5.   ST19NP18-TPM TIS (Memory) registers mapping

Index Value	Description
x000h	TPM_ACCESS_x (alias of TPM_ACCESS_0)
x008h	TPM_INT_ENABLE_x (alias of TPM_INT_ENABLE_0)
x009h	TPM_INT_ENABLE_x (alias of TPM_INT_ENABLE_0)
x00Ah	TPM_INT_ENABLE_x (alias of TPM_INT_ENABLE_0)
x00Bh	TPM_INT_ENABLE_x (alias of TPM_INT_ENABLE_0)
x00Ch	TPM_INT_VECTOR_x (alias of TPM_INT_VECTOR_0)
x010h	TPM_INT_STATUS_x (alias of TPM_INT_STATUS_0)
x011h	TPM_INT_STATUS_x (alias of TPM_INT_STATUS_0)
x012h	TPM_INT_STATUS_x (alias of TPM_INT_STATUS_0)
x013h	TPM_INT_STATUS_x (alias of TPM_INT_STATUS_0)
x014h	TPM_INTF_CAPABILITY_x (alias of TPM_INTF_CAPABILITY_0)
x015h	TPM_INTF_CAPABILITY_x (alias of TPM_INTF_CAPABILITY_0)
x016h	TPM_INTF_CAPABILITY_x (alias of TPM_INTF_CAPABILITY_0)
x017h	TPM_INTF_CAPABILITY_x (alias of TPM_INTF_CAPABILITY_0)
x018h	TPM_STS_x (alias of TPM_STS_0)
x019h	TPM_STS_x (alias of TPM_STS_0)
x01Ah	TPM_STS_x (alias of TPM_STS_0)
x020h	TPM_HASH_END. Valid only for x=4, e.g. locality 4
x024h	TPM_HASH_DATA (for x=4) TPM_DATA_FIFO_x (for x≠4)
x025h	TPM_HASH_DATA (for x=4) TPM_DATA_FIFO_x (for x≠4)
x026h	TPM_HASH_DATA (for x=4) TPM_DATA_FIFO_x (for x≠4)
x027h	TPM_HASH_DATA (for x=4) TPM_DATA_FIFO_x (for x≠4)
x028h	TPM_HASH_START. Valid only for x=4, e.g. Locality 4
xF00h	TPM_DID_VID_x (alias of TPM_DID_VID_0)
xF01h	TPM_DID_VID_x (alias of TPM_DID_VID_0)
xF02h	TPM_DID_VID_x (alias of TPM_DID_VID_0)
xF03h	TPM_DID_VID_x (alias of TPM_DID_VID_0)
xF04h	TPM_RID_x (alias of TPM_RID_0)

Note: *1   x refers to the locality number.*

2   All read accessed to addresses not defined in Table 5 will return FFh; write accesses will be discarded.

8.3.3   Register description

For a detailed description of the TPM internal registers listed above, please refer to the TCG PC Client Specific TPM Interface Specification version 1.2.

9   ST19NP18-TPM firmware

The firmware embedded in the ST19NP18 is compatible with the TCG TPM Specification Version 1.2 (revision 103). *Table 6* lists the supported commands. Please contact your local STMicroelectronics support person for further information about the latest information regarding ST19NP18-TPM TCG compatibility.

Table 6.   TCG TPM Version 1.2 commands

TPM_ActivateIdentity	TPM_Delegate_VerifyDelegation	TPM_LoadKey2	TPM_ReleaseTransportSigned
TPM_AuthorizeMigrationKey	TPM_DirRead[2]	TPM_LoadKeyContext [2]	TPM_Reset [2]
TPM_CertifyKey	TPM_DirWriteAuth[2]	TPM_LoadMaintenanceArchive[1]	TPM_ResetLockValue
TPM_CertifyKey2	TPM_DisableForceClear	TPM_LoadManuMaintPub [1]	TPM_RevokeTrust [1]
TPM_ChangeAuth	TPM_DisableOwnerClear	TPM_MakeIdentity	TPM_SaveAuthContext [2]
TPM_ChangeAuthAsymFinish[2]	TPM_DisablePubekRead [2]	TPM_MigrateKey	TPM_SaveContext
TPM_ChangeAuthAsymStart [2]	TPM_DSAP	TPM_NV_DefineSpace	TPM_SaveKeyContext [2]
TPM_ChangeAuthOwner	TPM_EstablishTransport	TPM_NV_ReadValue	TPM_SaveState
TPM_CMK_ApproveMA	TPM_EvictKey [2]	TPM_NV_ReadValueAuth	TPM_Seal
TPM_CMK_ConvertMigration	TPM_ExecuteTransport	TPM_NV_WriteValue	TPM_Sealx [1]
TPM_CMK_CreateBlob	TPM_Extend	TPM_NV_WriteValueAuth	TPM_SelfTestFull
TPM_CMK_CreateKey	TPM_FieldUpgrade	TPM_OIAP	TPM_SetCapability
TPM_CMK_CreateTicket	TPM_FlushSpecific	TPM_OSAP	TPM_SetOperatorAuth
TPM_CMK_SetRestrictions	TPM_ForceClear	TPM_OwnerClear	TPM_SetOrdinalAuditStatus [1]
TPM_ContinueSelfTest	TPM_GetAuditDigest [1]	TPM_OwnerReadInternalPub	TPM_SetOwnerInstall
TPM_ConvertMigrationBlob	TPM_GetAuditDigestSigned [1]	TPM_OwnerReadPubek [2]	TPM_SetOwnerPointer
TPM_CreateCounter	TPM_GetCapability	TPM_OwnerSetDisable	TPM_SetRedirection [1]
TPM_CreateEndorsementKeyPair	TPM_GetCapabilityOwner	TPM_PCR_Reset	TPM_SetTempDeactivated
TPM_CreateMaintenanceArchive [1]	TPM_GetPubKey	TPM_PcrRead	TPM_SHA1Complete
TPM_CreateMigrationBlob	TPM_GetRandom	TPM_PhysicalDisable	TPM_SHA1CompleteExtend
TPM_CreateRevocableEK [1]	TPM_GetTestResult	TPM_PhysicalEnable	TPM_SHA1Start
TPM_CreateWrapKey	TPM_GetTicks	TPM_PhysicalSetDeactivated	TPM_SHA1Update
TPM_DAA_JOIN	TPM_IncrementCounter	TPM_Quote	TPM_Sign
TPM_DAA_SIGN	TPM_Init	TPM_Quote2	TPM_Startup
TPM_Delegate_CreateKeyDelegation	TPM_KeyControlOwner	TPM_ReadCounter	TPM_StirRandom
TPM_Delegate_CreateOwnerDelegation	TPM_KillMaintenanceFeature [1]	TPM_ReadManuMaintPub [1]	TPM_TakeOwnership
TPM_Delegate_LoadOwnerDelegation	TPM_LoadAuthContext [2]	TPM_ReadPubek	TPM_Terminate_Handle [2]
TPM_Delegate_Manage	TPM_LoadContext	TPM_ReleaseCounter	TPM_TickStampBlob
TPM_Delegate_ReadTable	TPM_LoadKey	TPM_ReleaseCounterOwner	TPM_UnBind
TPM_Delegate_UpdateVerification			TPM_Unseal

1. Functions currently under development, not supported by default.

2. Functions deprecated from earlier TCG TPM standards. Still supported for backward compatibility reasons. Please contact your local ST Sales Office for most recent update.

10   Ordering information

Table 7.   Ordering Information

Ordering Code	Firmware Version	Description
ST19NP18ER28PVLR	0x01020700	TSSOP28-packaged ST19NP18-TPM (Tape & Reel delivery)

11   ST19NP18 pins and signals

Pinout description

GPIO1	1 ○		28	$\overline{\text{LPCPD}}$
GPIO2	2		27	SERIRQ
VNC	3		26	LAD0
GND1	4		25	NC
NC	5		24	VPS
GPIO3	6		23	LAD1
PP	7	**TSSOP28**	22	$\overline{\text{LFRAME}}$
NC	8		21	LCLK
GPIO4	9		20	LAD2
VPS	10		19	NC
GND2	11		18	GND3
NC	12		17	LAD3
NC	13		16	$\overline{\text{LRESET}}$
NC	14		15	GPIO5

Table 8.   Signal descriptions

Signal	Type	Description
LAD[3:0]	Bidir	**Multiplexed Command, Address and Data** (see LPC Spec)
$\overline{\text{LPCPD}}$	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 Spec)
LCLK	Input	**Clock** Same 33MHz clock as PCI clock on the host. Same clock phase with typical PCI skew. (see LPC Spec)
$\overline{\text{LFRAME}}$	Input	**Frame** indicates start of a new cycle, termination of broken cycle (see LPC Spec)
$\overline{\text{LRESET}}$	Input	**Reset** (used to re-initialize the device) same as PCI Reset on the host (see LPC Spec)
SERIRQ	Bidir	**Serialized IRQ** is used by TPM to handle interrupt support (see LPC Spec)
GPIO5/$\overline{\text{CLKRUN}}$	Bidir	**General Purpose IO**, fully configurable by Firmware **$\overline{\text{CLKRUN}}$** same as PCI $\overline{\text{CLKRUN}}$. 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
GPIO4	Bidir	**General Purpose IOs** fully configurable by Firmware
GPIO3	Bidir	**General Purpose IOs** fully configurable by Firmware
GPIO2	Bidir	**General Purpose IOs** fully configurable by Firmware
GPIO1	Bidir	**General Purpose IOs** fully configurable by Firmware
VPS	Input	**3.3V Power supply**. VPS has to be connected to 3.3v DC power rail supplied by the motherboard

Table 8.   Signal descriptions (continued)

Signal	Type	Description
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.

# 12 Electrical characteristics

12.1 Absolute maximum ratings

Table 9. **Absolute maximum ratings**

Symbol	Parameter	Value	Unit
V_{PS}	Supply voltage	-0.3 to 7.0	V
V_{IO}	Input or output voltage relative to ground	-0.3 to V_{PS}+0.3	V
T_A	Ambient operating temperature	-25 to +85	°C
T_{STG}	Storage temperature (Please also refer to package specification)	-65 to +150	°C
V_{ESD}	Electrostatic discharge voltage according to MIL STD 883C Method 3015, Human Body Model	2000	V

12.2 Recommended power supply filtering

The power supply of the circuit must be filtered with the following circuit:

Figure 5. Recommended filtering capacitors on power supply signals
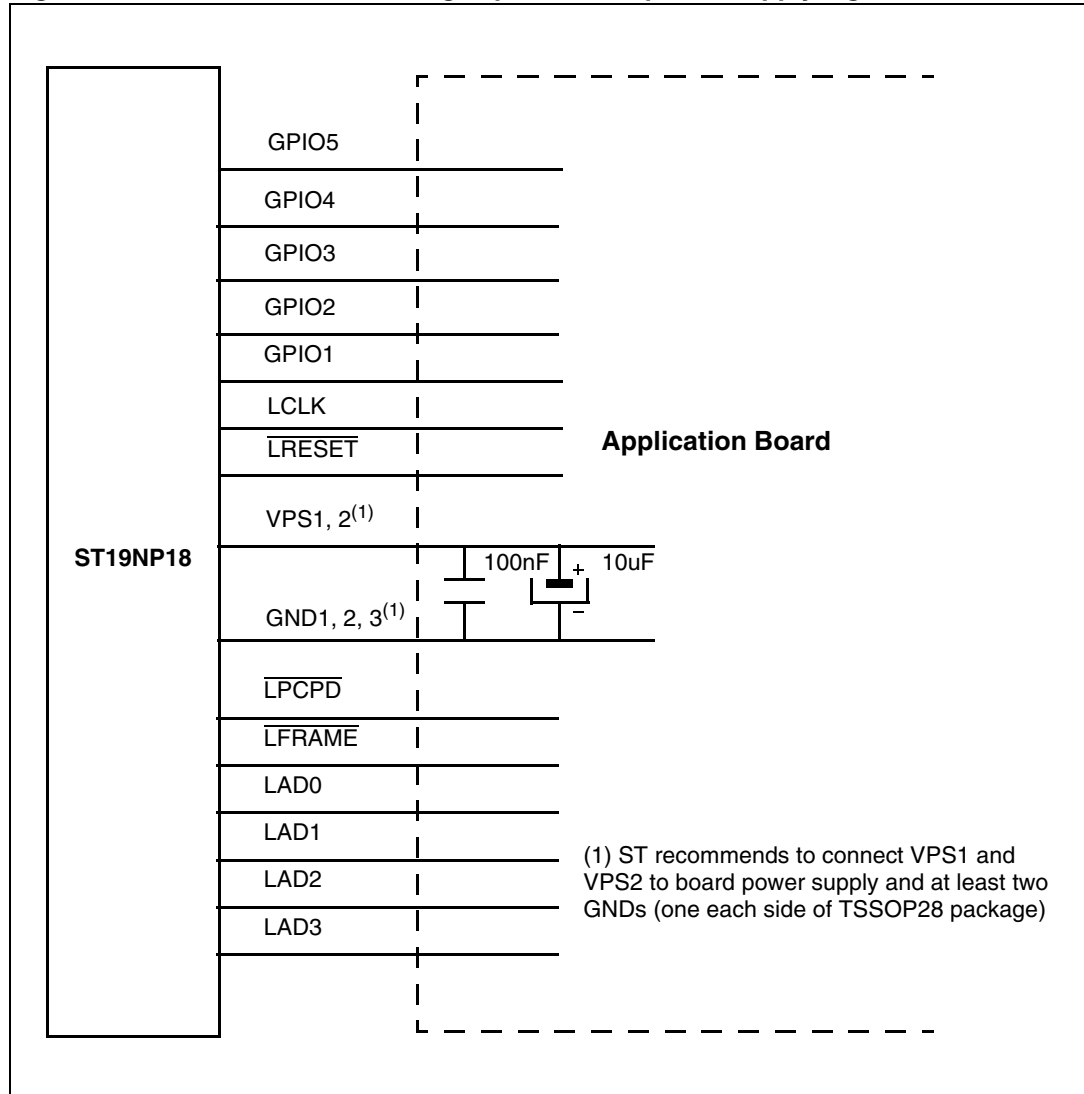
Table 10. Maximum VPS rising slope, T_A = 0 to 70°C

Symbol	Parameter	Value	Unit
S_{VPS}	Maximum VPS rising slope[1]	5	V/µs

1. To avoid more than 60mA current peak through VPS

Sampled only, not 100% tested.

12.3   DC and AC characteristics

V_{PS} = 3.3V ±10% and T_A = 0 to 70°C, unless otherwise specified.

The voltage on all inputs or outputs must not exceed Vcc +0.3V or be less than -0.3V.

Table 11.   LPC Bus DC Characteristics $\overline{LPCPD}$, $\overline{LFRAME}$, LAD[3:0] and GPIOs

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
V_{IL}	Input Low voltage: LCLK, $\overline{LRESET}$, $\overline{LFRAME}$, $\overline{LPCPD}$, PP, LAD (0:3)		0		0.3VPS	V
	SERIRQ, GPIO (1;5)				0.8	V
V_{IH}	Input High voltage: LCLK, $\overline{LRESET}$, $\overline{LFRAME}$, $\overline{LPCPD}$, PP, LAD (0:3)		0.5*VPS		VPS	V
	SERIRQ, GPIO (1;5)		0.7*VPS			V
I_{IL}	Input Low current: LCLK, $\overline{LRESET}$, $\overline{LFRAME}$, $\overline{LPCPD}$, PP, LAD (0:3)	0 < V_{IL} < 0.8	-10		10	µA
	Input Low current: SERIRQ, GPIO (1;5)	0 < V_{IL} < 0.8 Open drain / No weak pull up	-10		10	µA
		0 < V_{IL} < 0.8 Open drain / Weak pull up			500	µA
I_{IH}	Input High current: SERIRQ, GPIO (1;5)	0.7*VPS < V_{IH} < VPS Open drain / No weak pull up	-10		10	µA
		0.7 * VPS < V_{IH} < VPS Open drain / Weak pull up			250	
	Input High current: LCLK, $\overline{LRESET}$, $\overline{LFRAME}$, $\overline{LPCPD}$, PP, LAD (0:3)	0.5*VPS < V_{IH} < VPS	-10		10	
V_{OH}	Output High voltage: SERIRQ, GPIO (1;5)	I_{OHMAX} = -20 µA Open drain / Weak pull up	0.7*VPS		VPS	V
		I_{OHMAX} = -1 mA				
	Output High voltage: LAD (0:3)	I_{OHMAX} = -500 µA	0.9*VPS			
VOL	Output Low voltage: SERIRQ, GPIO (1:5)	I_{OLMAX} = 3 mA	0		0.4	V
	Output Low voltage: LAD (0:3)	I_{OLMAX} = 1.5 mA			0.1*VPS	
C_{IN}	Input Pin Capacitance: LCLK, $\overline{LRESET}$, $\overline{LFRAME}$, $\overline{LPCPD}$, PP, LAD (0:3), SERIRQ, GPIO (1:5)	10 MHz < f_{CLOCK} < 33 MHz See *Figure 9*. RP/CP model.			16	pF

Table 12.   AC characteristics

Symbol	Parameter	Min.	Typ.	Max.	Unit
f_{CLOCK}	LPC Clock Frequency			33	MHz
t_{WL}	$\overline{LRESET}$ pin pulse width for reset	1			µs
t_{HL}	$\overline{LRESET}$ active minimum time after VPS stable	1			ms

Table 13.   LPC Bus AC Characteristics $\overline{LFRAME}$ and LAD[3:0]

Symbol	Parameter	Min.	Typ.	Max.	Unit
t_{VAL}	LCLK to DataOut	2		11	ns
t_{ON}	LCLK to Active (Float to Active delay)	2			ns
t_{OFF}	LCLK to Inactive (Active to Float delay)	28			ns
t_{SU}	Input Set-up Time	7			ns
t_{H}	Input Hold Time	0			ns

Table 14.   Power Consumption characteristics

Symbol	Parameter	Conditions	Min.	Typ.	Max.	Unit
I_{CC}	Supply current				30	mA
$I_{CC}STB$	Supply current in Standby	LCLK signal stopped, $T_A = 25°C$		60	150	µA

Note: 1   Stresses listed under 'absolute maximum ratings' may cause permanent damage to the device. This is a stress rating only and functional operation of the device at these or any other conditions above those indicated in the operational sections of the specification is not implied.

2   Exposure to absolute maximum rating conditions for extended periods may affect device reliability.

12.4 Timings

Figure 6.   **LPC Bus waveforms**
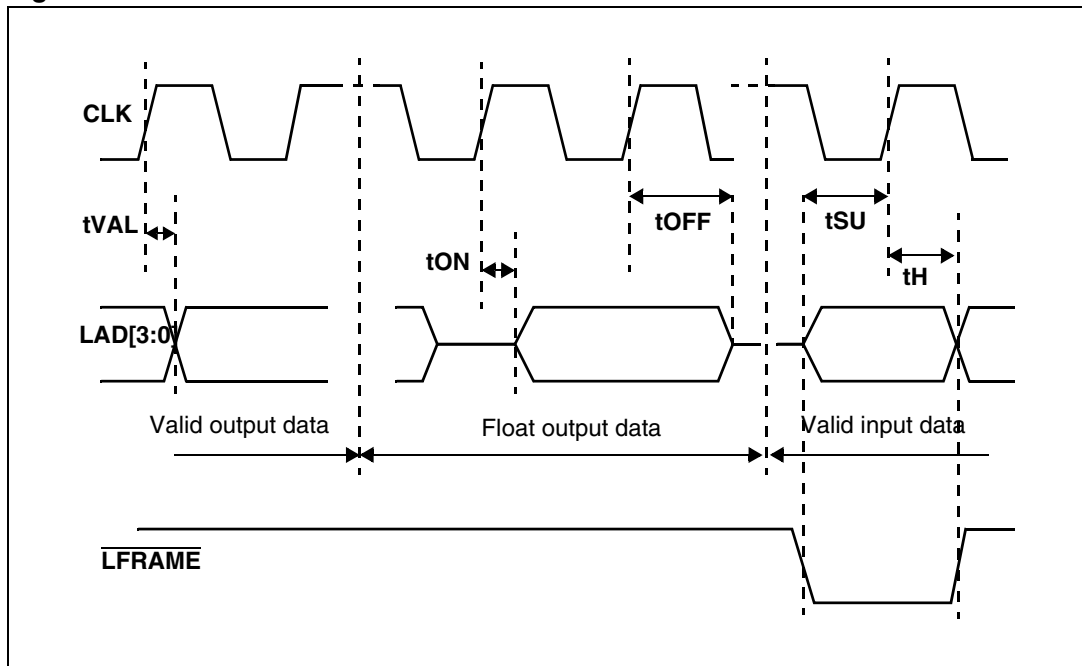
12.5 AC measurement conditions

Input Rise and Fall Times	10 ns max
Input Pulse Voltage	V_{IL} to V_{IH}
Input Timing Reference Voltage	$(V_{IL} + V_{IH})/2$
Output Timing Reference Voltage	Vt_{rise} to Vt_{fall}

Figure 7.   AC Testing Input Output Waveforms
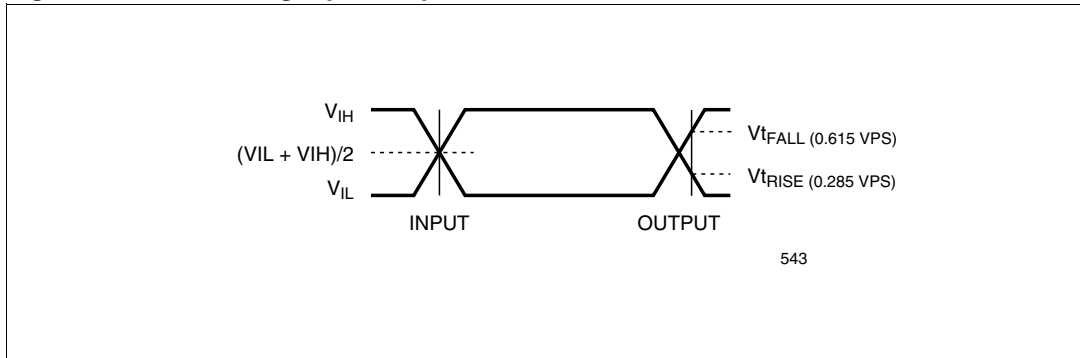

Figure 8.   AC Testing Load Circuit

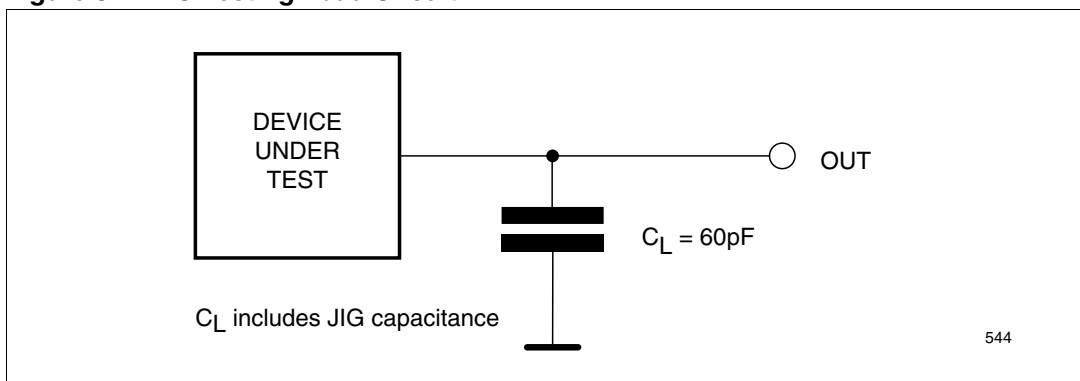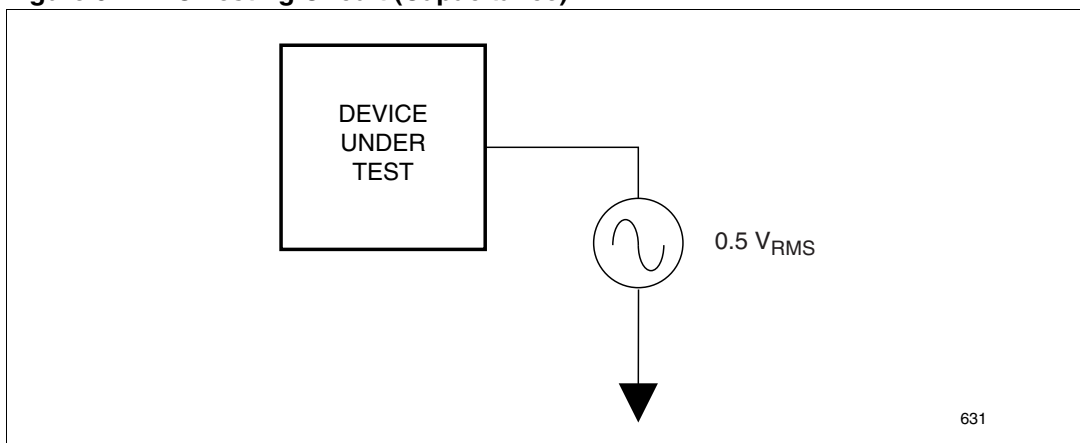**Figure 9.   AC Testing Circuit (Capacitance)**

Note: For more test details see PCI local bus specification revision 3.0.

13   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.
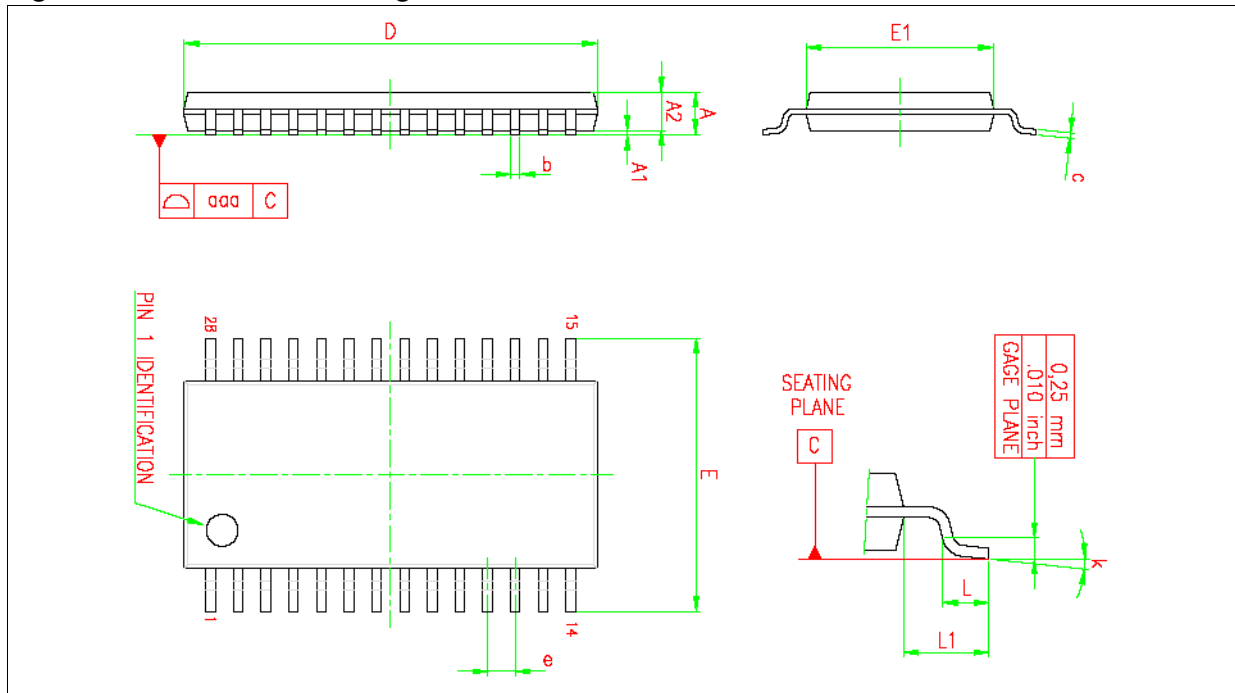
Figure 10.   Mechanical drawing

Table 15.   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

14 Revision history

Table 16. Document revision history

Date	Revision	Changes
18-Jan-2007	1	Initial release.
4-Apr-2007	2	Reformatted cover page. Added Windows® Vista® compatibility and ECOPACK® package information. Updated *Section 8.1: TPM default configuration on page 17*. Updated C_{IN} value in *Table 11: LPC Bus DC Characteristics LPCPD, LFRAME, LAD[3:0] and GPIOs on page 27*. Added *Figure 9: AC Testing Circuit (Capacitance) on page 30*.
10-Aug-2007	3	Added *Section 8.3.1: Legacy addressing on page 18*. Updated *Section 8.1: TPM default configuration on page 17* and *Section 10: Ordering information on page 22*.
14-Aug-2007	4	Upgraded document from Preliminary Data to Datasheet.
18-Jan-2008	5	Upgraded *Section 10: Ordering information on page 22*.
20-Mar-2008	6	Updated cover page and added number of key slots. Updated *Table 6: TCG TPM Version 1.2 commands on page 21*. Upgraded *Section 10: Ordering information on page 22*.

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.

UNLESS EXPRESSLY APPROVED IN WRITING BY AN AUTHORIZED ST REPRESENTATIVE, ST PRODUCTS ARE NOT RECOMMENDED, AUTHORIZED OR WARRANTED FOR USE IN MILITARY, AIR CRAFT, SPACE, LIFE SAVING, OR LIFE SUSTAINING APPLICATIONS, NOR IN PRODUCTS OR SYSTEMS WHERE FAILURE OR MALFUNCTION MAY RESULT IN PERSONAL INJURY, DEATH, OR SEVERE PROPERTY OR ENVIRONMENTAL DAMAGE. ST PRODUCTS WHICH ARE NOT SPECIFIED AS "AUTOMOTIVE GRADE" MAY ONLY BE USED IN AUTOMOTIVE APPLICATIONS AT USER'S OWN RISK.

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.