

# SLD 9630 TT 1.1

Trusted Platform Module

CONFIDENTIAL

Secure Mobile  
Solutions



Never stop thinking.

<b>CONFIDENTIAL SLD 9630 TT 1.1 Prel. Short Product Information</b>	
Details are subject to change without notice.	
Revision History: Current Version 2003-05-20	
Previous releases: V2.0	
<b>Page</b>	<b>Subjects (changed since last revision)</b>
	Changed page layout of 'Features' page Added TCPA version 1.1b where appropriate Changed operating temperature ranged according to Errata Sheet Added CLKRUN and powerdown features Changed software architecture description

<p><b>Important:</b> Further information is confidential and on request. Please contact          Infineon Technologies AG in Munich, Germany          Secure Mobile Solutions          Phone +49 89 234 80000, Fax +49 89 234-81000          E-Mail: security.chipcard.ics@infineon.com</p>
---

**Edition 2003-05-20**

**Published by Infineon Technologies AG,  
 St.-Martin-Strasse 53,  
 D-81541 München, Germany**

**© Infineon Technologies AG 2003.  
 All Rights Reserved.**

**Attention please!**

The information herein is given to describe certain components and shall not be considered as warranted characteristics.

Terms of delivery and rights to technical change reserved.

We hereby disclaim any and all warranties, including but not limited to warranties of non-infringement, regarding circuits, descriptions and charts stated herein.

Infineon Technologies is an approved CECC manufacturer.

**Information**

For further information on technology, delivery terms and conditions and prices please contact your nearest Infineon Technologies Office in Germany or our Infineon Technologies Representatives worldwide (see address list).

**Warnings**

Due to technical requirements components may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies Office.

Infineon Technologies Components may only be used in life-support devices or systems with the express written approval of Infineon Technologies, if a failure of such components can reasonably be expected to cause the failure of that life-support device or system, or to affect the safety or effectiveness of that device or system. Life support devices or systems are intended to be implanted in the human body, or to support and/or maintain and sustain and/or protect human life. If they fail, it is reasonable to assume that the health of the user or other persons may be endangered.

## **CONFIDENTIAL**

### **Features**

- TCPA-V1.1b compliant trusted platform module (TPM)
- Security architecture based on Infineon SLE66CxxxP security controller family
- 16-bit microcontroller in 0.25  $\mu\text{m}$  CMOS technology
- Firmware in on-chip ROM
- 16 kByte EEPROM
- 8 kByte XRAM
- Advanced crypto engine supporting RSA with up to 2048 bit key length
- Hardware accelerator for SHA-1 hash algorithm
- True random number generator (RNG)
- Power saving sleep mode
- 3.3 V power supply
- Operating temperature range: 0 °C to +70 °C

### **Interfaces**

- Low Pin Count (LPC) interface to allow easy system integration
- Operates from a single 33 MHz clock
- Support of power down signal to enter low-power standby mode
- Support of dynamic clock shutdown (CLKRUN)

### **EEPROM**

- Data retention for a minimum of 10 years

### **Package**

- Low profile TSSOP-28 package

### **Security Features**

- Over-/Undervoltage Detection
- Low frequency sensor
- High frequency filter
- Reset filter
- Memory Encryption (MED)
- Additional security features

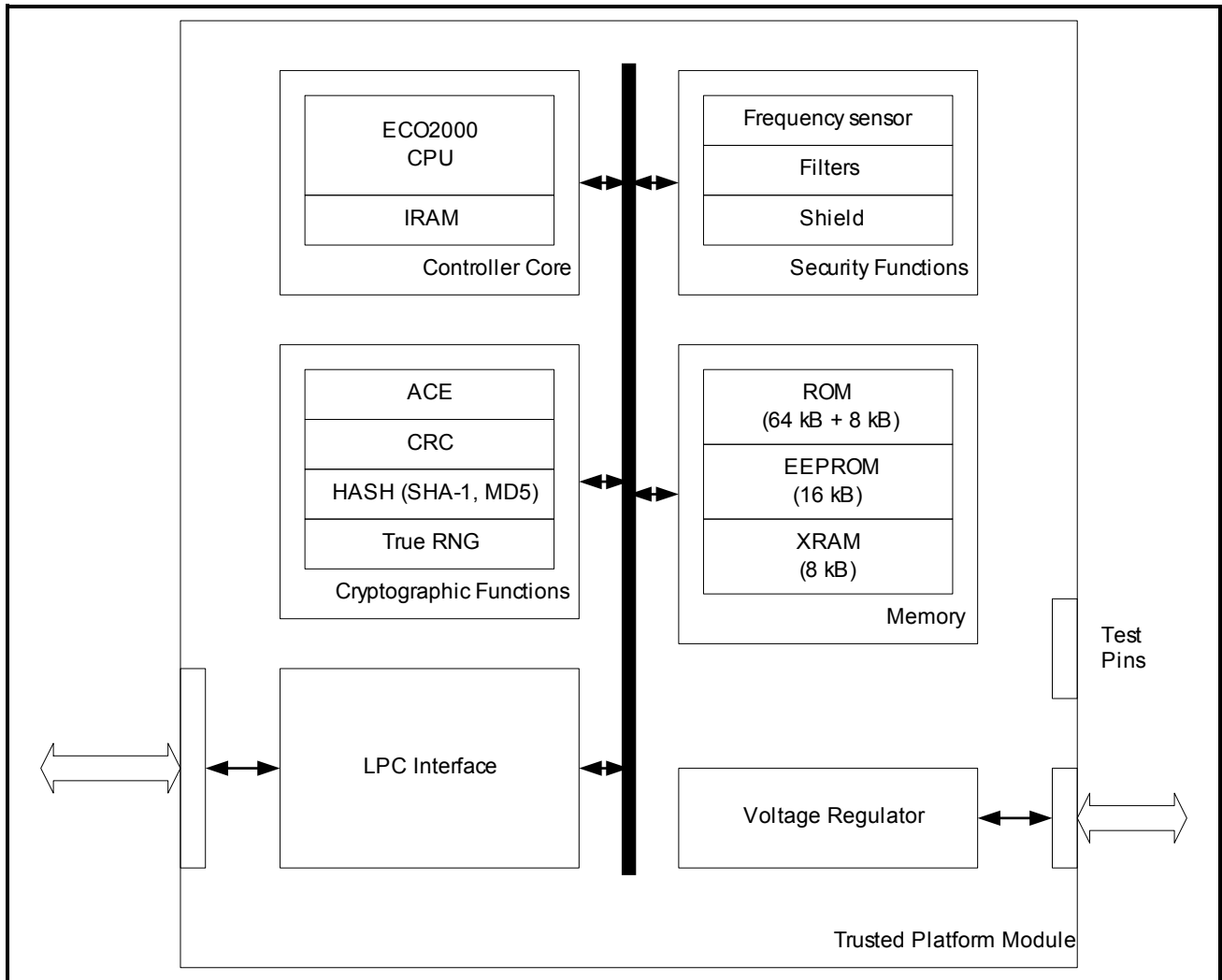
### **Support**

- Data book
- Application Notes

**CONFIDENTIAL**

**General Description**

The SLD 9630 TT 1.1 is a Trusted Computing Platform Alliance (TCPA<sup>1</sup>) compliant trusted platform module (TPM) for use in PC platforms. It is based on Infineon's high-secure 66P-core which is opcode compatible with the well-known 8051 core but provides enhanced performance, memory size and security features. Additional powerful instructions have been added to support secure systems.



**Figure 1 Block Diagram of Trusted Platform Module**

To simplify system integration into existing PC mainboards, the SLD 9630 TT 1.1 uses the LPC interface (Low Pin Count) as defined by Intel. This standardized interface is available on every mainboard and provides enough bandwidth.

The TPM supports secure key storage in non-volatile memory, an RSA hardware accelerator, an accelerator for the SHA-1 and MD5 hash algorithms and a true random number generator. All security modules are automatically tested after each reset.

<sup>1</sup>) Note that the TCPA has been renamed to Trusted Computing Group (TCG) as of March 2003.

**CONFIDENTIAL**

The secure EEPROM is mainly used to store RSA keys. The on-chip firmware supports five key slots (assuming 2,048-bit keys). It should be noted that the key manager of the TCPA Core Service (see software architecture, also refer to the TCPA specification) expands this to a (virtually) unlimited number.

The Advanced Crypto Engine (ACE) supports all of today known public-key algorithms based on large integer modular arithmetics. It allows fast and efficient calculation of RSA operations with key lengths of up to 2048 bit (using CRT).

The hash accelerator supports the SHA-1 and MD5 hash algorithms. Its bandwidth is more than 1 MByte per second. This allows for a complete hash of a standard PC BIOS (256 kByte) in less than 250 ms.

The random number generator (RNG) is able to supply the CPU with true random numbers under all conditions.

As an important measure, the chip provides a new and enhanced level of on-chip security features. This includes spike detectors for the power supply, filters for the clock and an active shield which covers the complete die area.

The chip operates from a single 33 MHz clock (LPC clock). It supports a low-power standby mode and dynamic clock shutdown (according to the CLKRUN protocol of the PCI Mobile Design Guide).

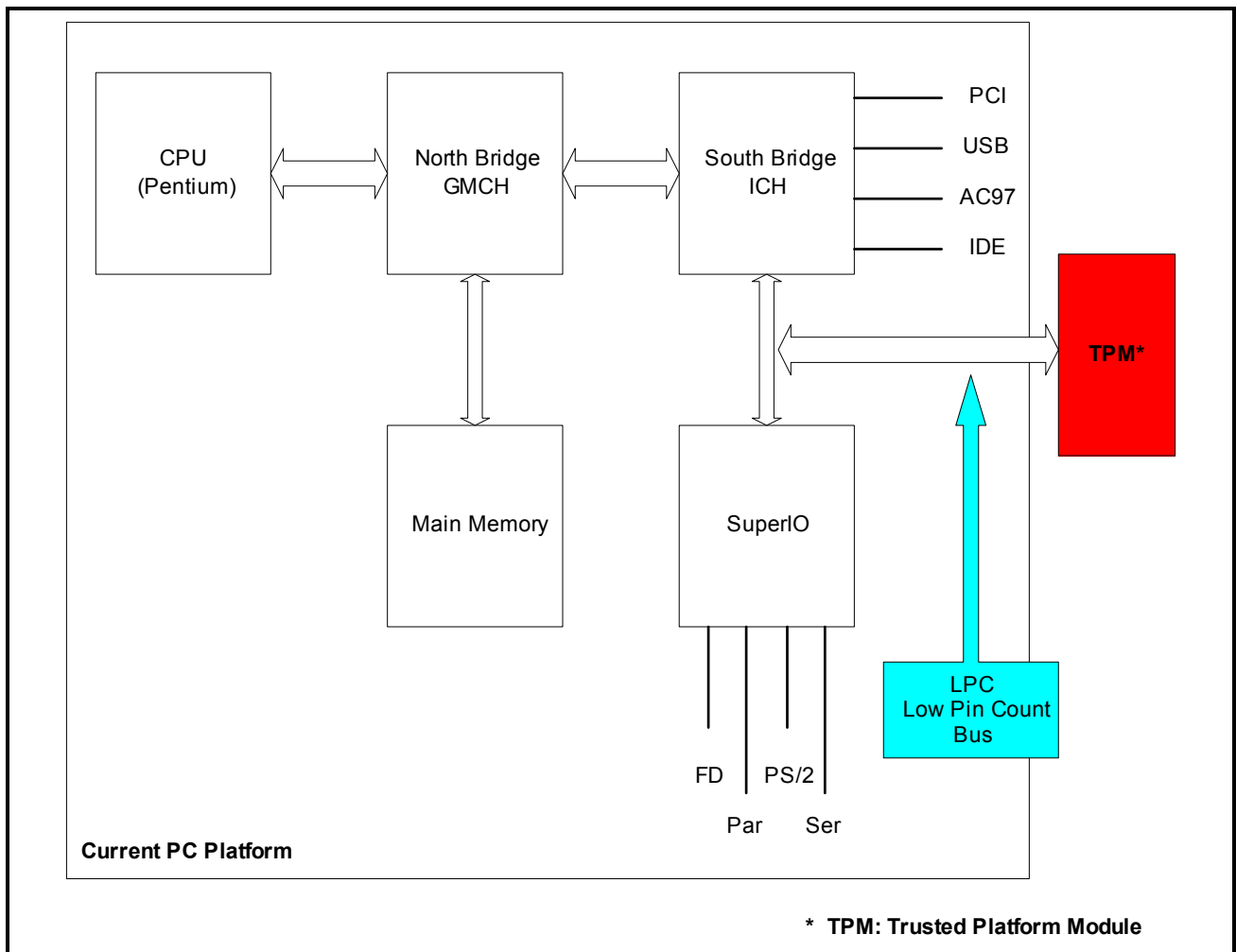
In conclusion, the SLD 9630 TT 1.1 fulfills all requirements of a TCPA-V1.1b compliant TPM for use in PC platforms. It integrates outstanding memory sizes, additional peripherals in combination with enhanced performance and optimized power consumption on a minimized die size.

**CONFIDENTIAL**

**System Integration**

As outlined before, the TPM will be connected to the so-called LPC interface. This interface has been defined by Intel and is available on virtually every PC mainboard. In standard configurations, only the SuperIO chip is connected to that interface.

Using this interface has the advantage that necessary code to handle it is already integrated in the BIOS boot block (this is necessary since the floppy disk and the standard keyboard are accessed via the SuperIO). This saves some integration effort and also some space in the boot block.



**Figure 2 System Integration of TPM**

The LPC is a synchronous interface running with the clock of the PCI bus (33 MHz typ). The available bandwidth is dependent on other devices occupying the bus.

**CONFIDENTIAL**

**Software Architecture**

The software provided for the SLD 9630 TT 1.1 consists of the embedded operating system and application, a reference implementation for the PC-BIOS integration, the software stack as defined by the TCPA specification and a Cryptographic Service Provider (CSP).

The TPM operating system is designed to provide a robust and highly secure basis for systems like the TPM which are based on the controller core of the SLD 9630 TT 1.1.

To reduce the efforts for the integration of the TCPA functionality into the PC-BIOS, a reference implementation (currently based on a PHOENIX BIOS) for the communication with the TPM is provided as well.

The TPM service provider exposes the functionality as specified by the TCPA. Dependent on the protection profiles, it implements functions by itself or uses the TPM as a provider of the function. In conjunction with the related service provider dynamic link library (DLL) it allows synchronized access to the trusted platform functionality for multiple applications at the same time.

The TPM Cryptographic Service Provider (CSP) delivered with the TPM software provides instant value for users working with a system which includes the SLD 9630 TT 1.1. It utilizes the Protected Storage functionality as defined by the TCPA to protect the user's key material. The TPM-CSP exposes its functionality to the Microsoft Cryptographic API (MS-CAPI). Therefore, applications like Microsoft Outlook (Express) and Internet Explorer can be used for secure mail (S/MIME) and with SSL client authentication.

Please refer to the figure on the next page for an overview of the software architecture.

CONFIDENTIAL

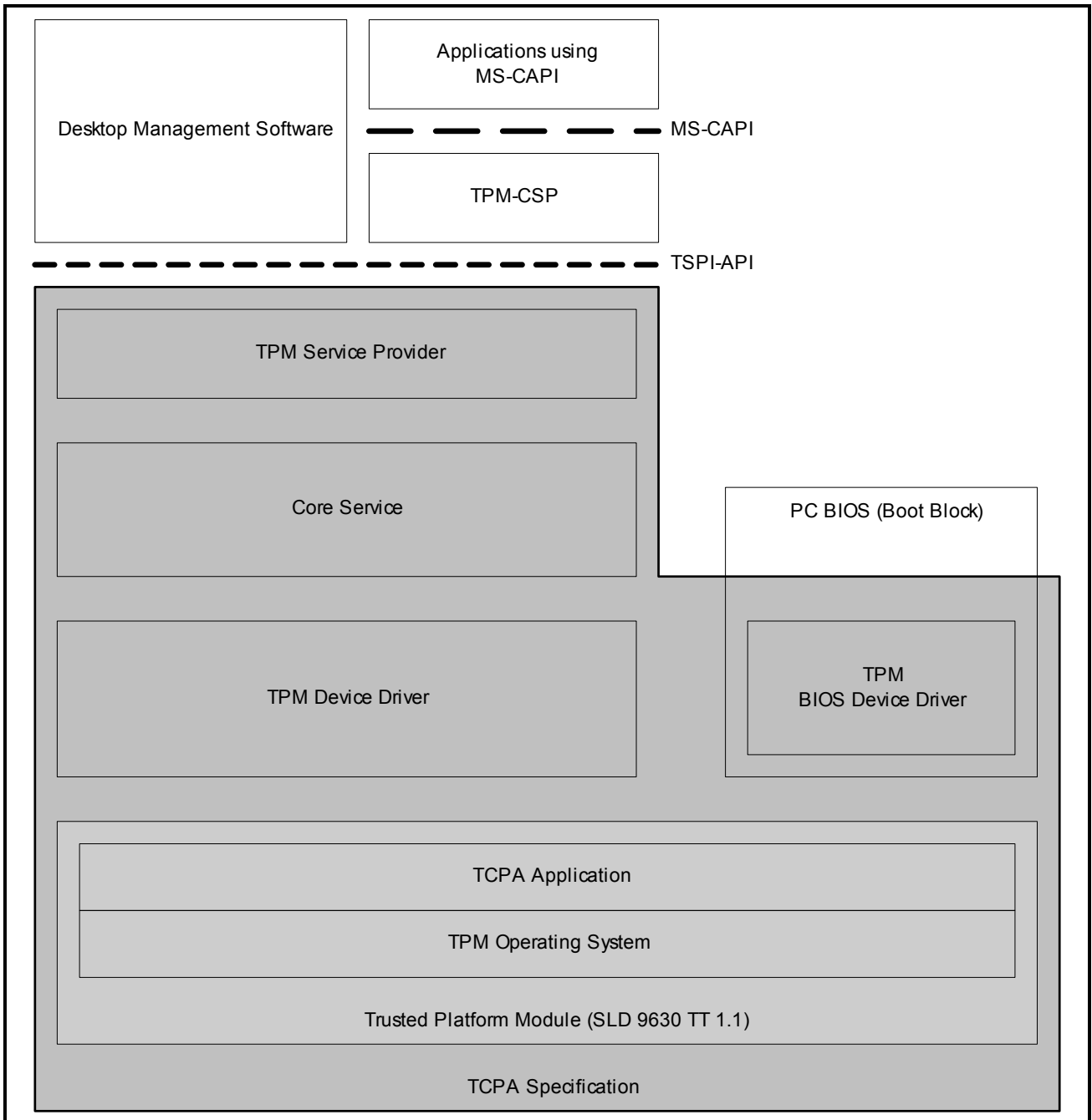


Figure 3 Software Architecture

**CONFIDENTIAL**

**Glossary**

ACE	Advanced Crypto Engine
CBC	Cipher Block Chaining
CLL	Contact-Less Logic
CFB	Cipher Feedback
CRC	Cyclic Redundancy Check
DES	Data Encryption Standard
EC2	Elliptic Curves
EPP	Enhanced Parallel Port
FIFO	First In First Out
GF	Galois Field
LPC	Low Pin Count Interface (Intel)
MED	Memory Encryption Device
MMU	Memory Management Unit
OCP	On Chip Processor
OFB	Output Feedback
OS	Operating System
PLL	Phase Locked Loop
RMS	Resource Management System
RNG	Random Number Generator
RSA	Rivest Shamir Adelman, Asymmetric crypto algorithm
TCG	Trusted Computing Group (formerly TCPA)
TCPA	Trusted Computing Platform Alliance
TPM	Trusted Platform Module