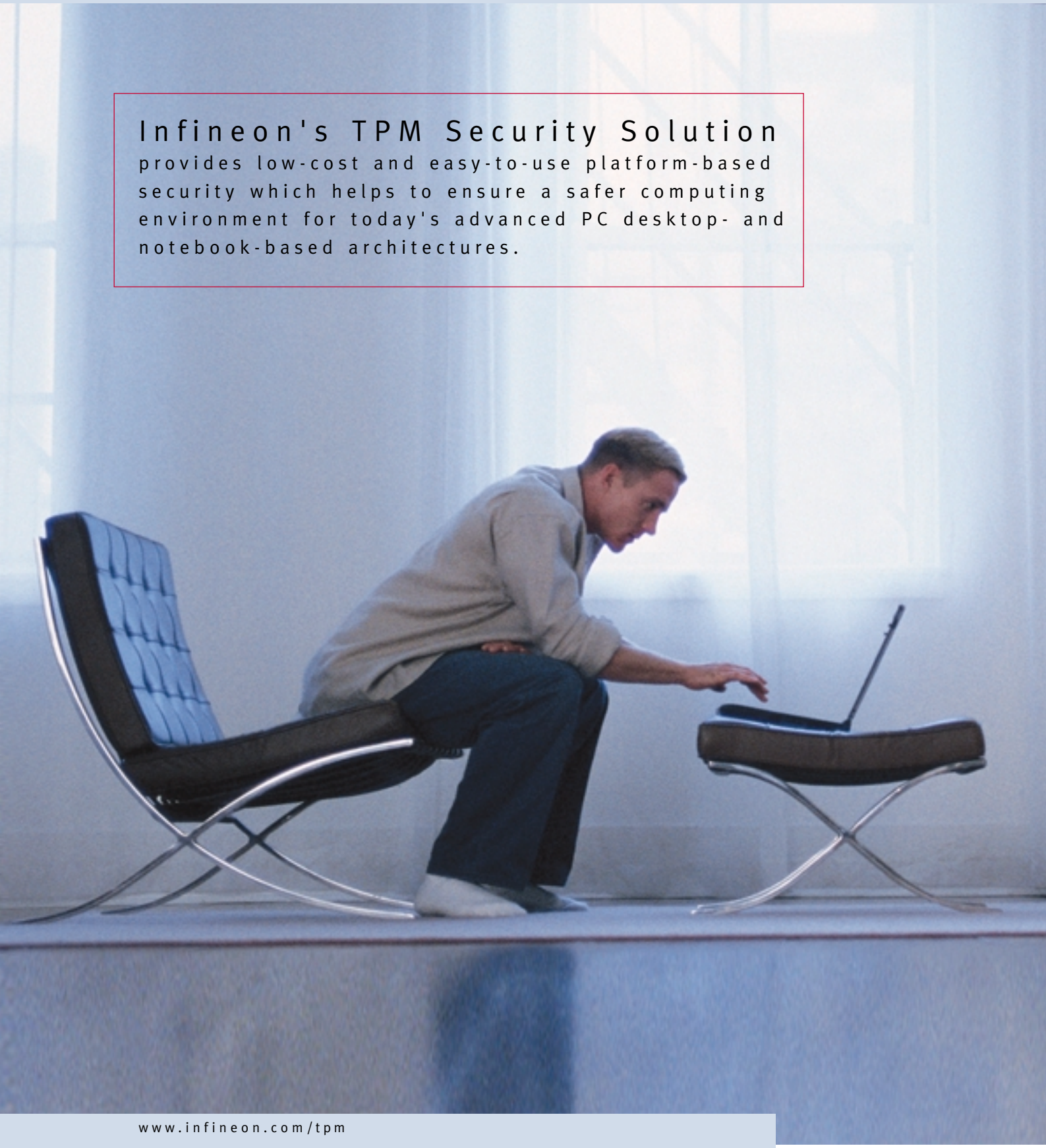
Infineon's TPM Security Solution

provides low-cost and easy-to-use platform-based security which helps to ensure a safer computing environment for today's advanced PC desktop- and notebook-based architectures.



www.infineon.com/tpm

Infineon technologies

Never stop thinking.

Infineon's TCPA-compliant security solution provides world-class platform security in conjunction with safer application software

As internet-based communication and commerce has rapidly developed in the past few years, the need for enhanced platform-based system security has grown as well. With the emergence of e-commerce and an increased reliance on the internet for all forms of communication, businesses and consumers alike are in greater need of assurance that their communication is trustworthy. The Infineon TPM solution provides for authenticity validation, platform integrity metrics checking, user confidentiality, and privacy. These attributes help to ensure that this safer communication environment is available and address today's business and consumer computing needs. The Trusted Computing Platform Alliance (TCPA) was founded by Intel, Hewlett-Packard, Compaq, IBM, and Microsoft in 1999 to address these issues and to allow for the continued growth of internet- and computing-based communications and commerce models. Today, the TCPA has more than 200 member companies and has developed both hardware and software security standards to address today's need for strong platform computing-based security and management.

The TPM-based system forms a Root of Trust for every computer and a basis for "safer computing" among these more trusted PC clients. In the near future, TPMs will be present in additional devices such as PDAs and mobile phones to increase the network of trusted communication for consumers and businesses. In addition to the ability of a TPM-based system to authenticate remote users and systems via policy and permission, the system can help to ensure that both users are operating within their authorized system configuration profiles. Thus, both user privacy and confidentiality are assured for computing-based transactions and communication. One of the most important secured features of a TPM-based system is its ability to support a Public Key Infrastructure (PKI).

The ability to support a public key hierachy provides the first managed security system architecture to develop a globally assured mutual trust network for commerce and communications on PCs, PDAs, and mobile phones. The PKI environment helps to ensure that applications are more secure, and extends the trusted computing model to numerous device types that could not safely communicate in the past.

Infineon Technologies has a well-established reputation for developing innovative and certified security solutions for numerous device types. We have sold almost 3 billion security controllers. The TCPA and the standards it has developed for the computing market continue to demonstrate the need for innovation in the field of platform security. Infineon Technologies is committed to providing certified world-class security solutions that comply with TCPA standards in order to address the complexities of today's full-time network environments. Infineon has developed the only complete end-to-end TCPA solution that includes all required hardware, software, and management utilities to design a complete platform security solution from one source. The Infineon TPM Solution offers numerous security features including non-volatile memory, multiple algorithm support, secure hashing, true random number generation, key generation, numerous security controller sensors to prevent physical attacks, and a secure operating system. In conjunction with an on-going committment to providing complete security solutions, Infineon Technologies will continue to provide complete solutions that will guarantee the adoption of tomorrow's technologies today.

Infineon Technologies Platform Module Solution Provides the Following Features

Infineon Technologies TPM Hardware Overview:

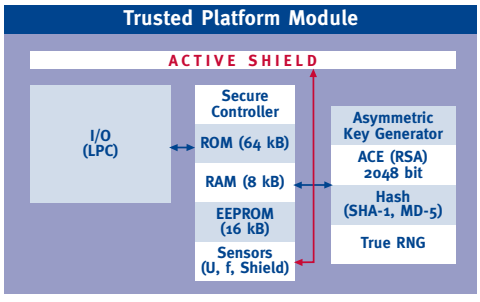
- 64 kBytes of ROM & 8 kBytes of RAM
- 16 kBytes of EEPROM with 500 write-erase cycles
- 48 kBytes of EEPROM for firmware secure updates
- RSA hardware accelerator for signature calcution and verification as well as 2048 bit key generation when using CRT
- World-leading security protection against SPA and DPA
- Low Pin Count (LPC) bus optimized
- Low power consumption

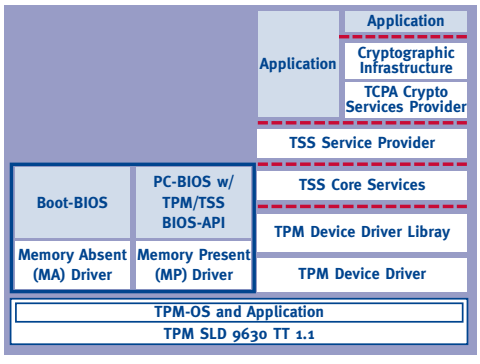
Software Architecture Overview:

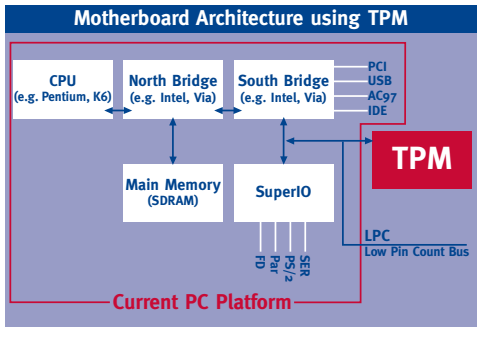
- Embedded Secure Operating System
- Embedded Secure Application Support
- TCPA Software Stack (TSS) compliant to current and released specifications
- TCPA PC BIOS support available with design guide
- TPM cryptographic service providers for MS-CAPI 2.0 and PKCS#11

System Integration:

In order to ensure easy integration into almost every platform type PC desktop and notebook, the Infineon TPM solution utilizes the Low Pin Count (LPC) bus interface as defined by Intel Corporation. Utilizing the bus together with the low-cost TPM package provides cost savings and power efficiency. Due to the available bandwidth of the LPC bus (approximately 4 mBytes), the Infineon TPM can perform numerous sophisticated platform security functions to enhance the safety of today's PC architecture.
In conclusion, the LPC bus offers an optimized way of easily integrating Infineon's TPM solution into both notebook and desktop PC BIOS images for initiation of safer computing.







Published by Infineon Technologies AG

Ordering No. B116-H7956-G3-X-7600
Printed in Germany
WS 04033.

Z&P 2002705