



Infineon's TCPA-compliant security solution supports all PC security applications



By Thomas Rosteck,
Infineon Technologies AG

Communication over the Internet is growing continuously. Many applications, such as those intended for eCommerce, are based on trust in the communication partner and the reliability of the connection. You have to provide authenticity, integrity, and confidentiality/privacy.

With the development of TCPA (Trusted Computing Platform Alliance), a powerful business initiative was launched. Its objective is to increase confidence in the Internet. The TCPA founded by Compaq, Hewlett-Packard, IBM, Intel and Microsoft (now including more than 160 companies), has defined a device – known as the Trusted Platform Module (TPM) – which will assume responsibility for many important security functions. TPM is the root-of-trust in a given platform (e.g. a PC, notebook, and in the future, a mobile phone or PDA). It checks the system integrity – and authenticates third-party users who would like to access the platform – while remaining under complete control of its primary user. Thus, privacy and confidentiality are assured. With TPM-based platforms it will be possible for the first time to create the basis for a worldwide public key infrastructure (PKI). This in turn will ensure the security of many applications for private and corporate environments in particular – while making other types of applications possible for the first time. With an established reputation for cutting-edge and market-tested security technologies, Infineon is the first to market a security solution for all computing platforms. The activities of TCPA and the resulting security standard show the requirements for today's security technology. Infineon's Trusted Platform Module (TPM) architecture is designed to provide both highest security standards, based on proven security technology, and easy system integration by providing a complete solution. The TPM offers the same security features as Infineon's standard security controllers

including non-volatile memory, cryptographic implementations of RSA and Hash Algorithms (SHA-1 and MD-5) for highest possible performance, as well as a true random number generator. One of Infineon's goals is to fulfill the security requirements for all future computing platforms and therefore enables the growth of tomorrow's applications with certified security.

Infineon Technologies TPM offers:

- ▶ 16kByte Non Volatile Memory for the secure storage of keys and secrets
- ▶ HW-RSA-Accelerator (Signature Calculation, Signature Verification and Key Generation@2048bit key – using CRT)
- ▶ Hardware Hash-Accelerator (SHA-1, MD-5)
- ▶ True Random Number Generator (TRNG)
- ▶ The highest possible security levels against SPA and DPA
- ▶ Low power consumption
- ▶ 2 timers and 1 interrupt module
- ▶ LPC interface

Software Architecture:

- ▶ Embedded secure operating system
- ▶ Embedded application
- ▶ Reference implementation for PC-BIOS integration
- ▶ TSS software stack according to TCPA specification
- ▶ TPM Cryptographic service provider (CSP)

System Integration

To ease integration into virtually every known PC platform, the TPM uses the standardized LPC inter-

face (Low Pincount Interface) as defined by Intel. This has the advantage that a small package can be used.

Furthermore, the bandwidth of this bus is more than sufficient for the intended application (approximately 4Mbyte/s), thus enabling more sophisticated use of an Infineon TPM.

Finally, the necessary support for the LPC is already integrated in every system BIOS since the SuperIO is attached to this bus. This simplifies software integration of the TPM into the BIOS Boot Block.

