Infineon Announces Trusted Platform Module to Enhance PC Security

May 31 2005

In an effort to ensure safer computing, Infineon Technologies AG announced availability of its latest Trusted Platform Module (TPM) security microcontroller supporting the main specification 1.2 of the Trusted Computing Group (TCG) at the "Computex 2005" show in Taipei. Infineon is the worldâ€™s only supplier to offer an own comprehensive hardware and software solution compliant with the TCGâ€™s 1.2 specification. Its TPM security solution features a secure chip hardware, a complete suite of embedded security and TPM system management utilities as well as application software, which simplify data protection through e. g. file and folder encryption protected with hardware-based key generation and storage. PC manufacturers benefit from Infineonâ€™s TPM offering since it secures all core components of a security subsystem used for authenticity, integrity and confidentiality of data stored.

Integrated on to the motherboard of a stationary or mobile PC, the TPM helps to shield against unauthorized access to the data stored and improves the system integrity. Thus, it enables more secure data storage, online secure business information exchange and online commerce transactions while protecting privacy. As TPM comes in the industryâ€™s smallest package, it is also suitable for integration on mainboards of mobile devices, such as handheld computers and PDAs.

â€œThe TPM 1.2 specification is a sound hardware basis on which to build secure solutions to recognize and prevent unauthorized access to stored data on computers and networks,â€? said Thomas Rosteck,

Senior Director and Product Line Manager Trusted Computing, Chip Card and Security ICs business unit at Infineon Technologies. â€œPure software solutions are far from offering the security level of hardware. Infineonâ€™s secure microcontrollers meet the toughest international requirements for security. Combined with its easy-to-use management and application software we are able to offer a secure solution to PC manufacturers and PC users. The company is committed to further contribute its best-in-class hardware security expertise to make PC and laptop computers trustworthy platforms for communication.â€?

Complete Hardware and Software Solution for Safer Computing; Technical details on Infineonâ€™s TPM (SLB 9635 TT 1.2)

Infineon provides the highest possible performance for TPM systems comprising secure hardware and complete system software and application software. Infineonâ€™s TPM solution is based on the companyâ€™s proven family of 16-bit security controllers which was developed for use in high-security chip card applications. To securely and reliably store keys and passwords, Infineonâ€™s TPM offers state-of-the-art security features, such as an active shielding that sends a continuous stream of random data over the surface of the chip. Apart from active shielding, the chip features the true random number generator (RNG), hardware accelerated RSA crypto algorithms (named after its developers Rivest, Shamir, Adleman) with key lengths of up to 2,048 bit and hash algorithms (where a document, file or computer drive is assigned a unique, cryptographically protected checksum which can be used to recognize manipulation) required by the Trusted Computing Group specification.

Infineonâ€™s new TPM compliant with TCGâ€™s 1.2 specification offers 16K bytes of non-volatile memory capacity for user data. It

contains also 50 percent more internal working memory, supporting the next-generation operating systems, such as Microsoft Longhorn.

Infineonâ€™s TPM is expected to be compliant with one of the worldâ€™s strictest security evaluations conducted according to internationally accepted standards: the Common Criteria EAL 4+ (evaluation assurance level four plus).

In addition to the security controller hardware, Infineon provides computer manufacturers with a proven secure operating system inside the TPM and embedded applications to implement the subsystem. This includes host software API to integrate the TPM into the PC software environment and a TPM management application. In contrast to software solutions, keys and passwords are almost as safe as ones own thoughts once stored into the secure hardware environment of the TPM, where they can be controlled only by its primary user and system administrator. The TPM provides protected storage for secretes, automatically checks system integrity, and can authenticate the platform to third parties if authorized by the primary user.

Major computer manufacturers, such as HP Compaq with its business notebooks and desktops, are already using Infineonâ€™s TPM management software which is also an integral part of the TPM v1.2 solution. It allows easy management of the TPM, provides integrated security applications like Personal Secure Drive encryption and supports secure e-mail correspondence, Wireless LAN security, Virtual Private Networks (VPN), and other use for security issues.

Starting July 2005, Infineonâ€™s TPM compliant with TCGâ€™s 1.2 specification will be available in sample quantities for integration into with desktop systems and notebooks. The TPM will be delivered in a green (lead-free) small low-profile TSSOP-28 package.

More information on Infineonâ€™s TPM solution is available at: www.infineon.com/tpm

Infineon presents its Trusted Platform Module solution at the Computex 2005 show (May 31, to June 4, 2005, Taipei, Taiwan) at booth 722 in hall 1 at Taipei World Trade Center.