



Date: 7 December 2009

CESG and Infineon in Partnership Deliver Assured Trusted Platform Module

7 December, 2009 - Infineon Technologies AG and CESG today announced that, in addition, to completing Common Criteria and TCG certification, the Infineon Trusted Platform Module (TPM) has successfully completed a CESG Assessment of its suitability to protect security critical data in UK Government systems.

To strongly authenticate authorized notebook and desktop PC platforms and to securely store keys and passwords, the Infineon TPM, the SLB9535 T 1.2, offers hardware-based security features. Integrated onto the motherboard of a mobile or stationary PC, Infineon's TPM helps shield the stored data against unauthorised access.

The Trusted Computing Group (TCG), an impartial not-for-profit organization, confirmed that Infineon's TPM is "TCG Certified". This TCG certification is based on the international security standard Common Criteria and on TCG's own compliance tests.

"In order to foster compliant and secure product implementations, the TCG recently launched its 'TPM Certification Program'. The program demonstrates compliance and security evaluation of products and identifies those that have successfully passed all its requirements," said Scott Rotondo, President and Chairman of the Trusted Computing Group. "That Infineon is the world's first semiconductor provider that has successfully passed our TPM Certification Program underlines Infineon's leading role in hardware-based security."

Further to the Infineon TPM's successful CC and TCG certification, the company has worked closely with CESG to ensure that the product meets strict UK Government requirements for protecting security critical data. CESG is the UK National Technical Authority for Information Assurance.

The close working relationship between CESG and Infineon has enabled the first in depth, fully impartial assessment of a TPM's security from development through deployment. CESG has assessed that the Infineon TPM is suitable to protect security critical data at Business Impact Level 3 (i.e. RESTRICTED classified data). This makes Infineon the first provider of TPMs that have been assessed as fully compliant with the strict UK-specific requirements.

NOT PROTECTIVELY MARKED

"Partnering with industry is critical for CESH, which has a key role in aggregating the UK Government's Information Assurance (IA) requirements, to gain assurance in commercial IA products and reduce reliance on expensive bespoke systems," said Nick Hopkinson, CESH's Director General for Information Security and Assurance. "The cooperation with Infineon is a significant first step in enabling the use of Trusted Computing technology in UK government networks."

"Infineon's commitment to security standards can be seen by our speed in bringing fully compliant products to market so quickly after completion of the TCG Certification Program to accelerate market penetration of security technologies," said Thomas Rosteck, Vice President and General Manager, Chip Card & Security Division at Infineon Technologies. "Infineon will continue innovation focusing on security. Our aim is to develop state-of-the-art chips that will support tailored security for the data later stored on them and offer the right level of certified security that the respective application needs."

More information on the Trusted Computing Group (TCG) and the organization's specifications are available at www.trustedcomputinggroup.org.

Further information is available at www.infineon.com/press/

