FOR IMMEDIATE RELEASE

CONTACT: Anne Price
+ 602-840-6495
press@trustedcomputinggroup.org

TRUSTED COMPUTING GROUP RELEASES TRUSTED PLATFORM MODULE SPECIFICATION v1.2 TO ENABLE ENHANCED COMPUTING SECURITY

Trusted Platform Modules for Computing Devices to Include Additional Privacy Protections, More User Control, Better Defense Against Attacks

RSA Conference, Amsterdam, November 5, 2003 – The Trusted Computing Group -- an open industry standards organization whose specifications help vendors build products that let users protect critical data and information -- today released a new specification for a Trusted Platform Module component for computing devices.

The specification builds on an existing version that is implemented in millions of desktop and notebook PCs. The new specification, v1.2, has been anticipated for several months, and vendors are expected to begin development of new Trusted Platform Modules for shipment in the second half of 2004. Users will realize benefits from the specification enhancements as Trusted Platform Modules and supporting software become available. In the meantime, users can get substantial security benefits from systems using today's Trusted Platform Modules, available from a number of vendors.

"With the proliferation of viruses and other types of attacks, the need for vendor-independent open security standards has never been greater," noted Rob Enderle, principle analyst for the Enderle Group. "The availability of the new Trusted Platform Module specification v1.2 will enable the computer industry to showcase its cooperation and provide the critical trusted platforms necessary to protect users' privacy and confidential data."

Specification Details

The new specification includes support for trusted software processes as well as modifications resulting from extensive review and feedback from developers, users and industry experts.

Enhancements to the specification include:

- *Direct anonymous attestation* reliably communicates information about the static or dynamic capabilities of a computer with a Trusted Platform Module. This capability does not require the disclosure of personally identifiable information and is under the control of the platform owner, who can be an individual user or an IT department.

  Users can generate multiple keys for interaction with different parties to maintain anonymity. DAA complements and is in addition to the existing Trusted Platform Module specification, v1.1B. However, direct anonymous attestation has the advantage that it can be implemented with or without a trusted third party.

- *Locality* allows owners of the Trusted Platform Module to assign permissions to external software processes, such as a trusted operating system. Locality assumes that there are hardware- or software-based processes outside the Trusted Platform Module that have different levels of trustworthiness.

-- more --

- *Delegation* allows platform owners to delegate software, an object or other entity to use specific, owner-authorized commands, without allowing access of other commands in the Trusted Platform Module. For example, owners can withhold their password from untrusted entities or software for sensitive functions, while allowing access to non-sensitive functions. Together with locality, delegation is anticipated to simplify platform management and allow management to remain under the owner's control.

- *Non-volatile storage* can be used by system software or firmware to store information on the Trusted Platform Module. This storage is user defined and has controlled access. It could be used, for example, to ease technology deployment with certificates stored on the Trusted Platform Module.

Other new features of the specification include transport protection for commands sent to the Trusted Platform Module, helping ensure the confidentiality of data exchanged between the module and remote software; monotonic counters to help prevent "replay" attacks in which stored data is compared to current values; and a tick counter that allows the Trusted Platform Module to do time-related sequencing of transactions.

More information and the specification are available at the Trusted Computing Group's website, www.trustedcomputinggroup.org.

- 30 –

Nov. 5, 2003

Vendors Comment on Trusted Computing Group Trusted Platform Module Specification

"Atmel is committed to bring a v1.2 TPM to market to support the needs of our customers while we continue with the production and promotion of the V1.1 TPM," commented Kerry Maletsky, Atmel's business unit director.

Contact: Vicki McCann
(719) 540-1724
vmccann@cso.atmel.com

"With information and data being available at any time and any place, security plays a decisive role in terms of the reliability of the data source and the data's confidentiality, integrity and availability. The cooperation of various market parties succeeded in the TPM v1.2 specification as a sound basis on which to build secure solutions to recognize and prevent unauthorized access to stored data on computers and networks. Infineon is committed to further promote TCG and to contribute its best-in-class security expertise to make PC and laptop computers trustworthy platforms for communication."

Thomas Rosteck, senior director, Secure Mobile Solutions, Infineon Technologies

Contact: Monika Sonntag
Monika.Sonntag@infineon.com

“National Semiconductor fully supports and applauds the efforts of the TCG TPM v1.2 specification. As a supplier of TPMs, we at National have worked together with the rest of the industry to formalize the next-generation secure computing base. We will aggressively pursue this security technology roadmap while, at the same time, making these implementations integrated and affordable to spur adoption across all market segments. Certainly, security and trust will become the next touchstone in the PC marketplace.”

Jonathan Levy, general manager, Advanced PC Division, National Semiconductor

Contact: Megan Carter
(408) 721-6929
megan.carter@nsc.com