Trusted Computing Group PC Client TPM Interface Specification (TIS)
FAQs, January 2006

Q. What is the relevance of this specification from TCG?
A. This new specification defines a set of standard interfaces and protocols to allow Family 1.2 TPMs to communicate with PC client components from different TPM vendors. This specification also specifies minimal resources and features of various types that a Family 1.2 TPM must have to function on a PC client platform. The new specification builds on the existing TPM Specification Family 1.2, Parts 1 through 3, which defines TPM functionality for use on any class of platform, from servers to cell phones.

Q. What is the TPM family that you refer to?
A. The TPM is a set of building blocks for implementing security under a set of criteria. Some implementations include the TPM 1.2, which is a silicon chip for use on in a PC client. In other cases, the implementation of the TPM might be different depending on the application requirements.

Q. Who does this specification affect and how do they implement this?
A. The primary audience for this specification is TPM manufacturers, but there are also requirements in this specification that must be met by PC client platform manufacturers, such as OEMs and ODMs, and suppliers of software components that communicate with a Family 1.2 TPM.

Q. Why is this new specification necessary?
A. It provides a standardized interface for building blocks that provide security.

Q. How do I know if the system purchased with a Family 1.2 TPM meets this requirement?
A. You will have to rely on documentation provided by either the TPM manufacturer or the PC client platform manufacturer that uses a particular vendor's Family 1.2 TPM. These manufacturers may publish such documentation regarding the use of the TCG specifications or you may have to ask these manufacturers for this documentation.

Q. Is there a significant feature value a machine or user perceives when using a machine that has implemented this specification
A. Yes, users will gain the advantage of a consistent set of resources and features.

Q. How do I know a PC client platform vendor is using a Family 1.2 TPM that has implemented this specification?

A. You can get that information from the system vendor.

Q. Can you name vendors that have implemented this specification?
A. Currently, the following TCG member companies offer proof of concept or engineering samples of Family 1.2 TPMs that implement this specification: Atmel, Broadcom, Infineon, Lenovo, SinoSun, STMicro, and Winbond. All of these companies participated, in some degree, to the development of the specification.

Q. What is the downside in performance or value if a PC maker does not follow this specification?
A. If a PC maker chooses to use a Family 1.2 TPM on its platform that does not follow this specification, the components on that platform will have to use proprietary interfaces and protocols, and the TPM may not provide the minimal resources (such as protected non-volatile storage capacity) and features that software components from other vendors expect.