PC Client Physical Presence Interface Specification FAQ
March 2007

Q. What is this new PC Client Physical Presence specification?
A. Trusted Platform Modules (TPM) may support several methods for indicating that an operator is physically at the platform. One common method is using a BIOS screen that interacts directly with the user while they are at the platform's keyboard and monitor. The commands used for this method may only be executed during the platforms early startup time (i.e., when the BIOS has control of the platform.) However, since the BIOS setup screens are awkward for users to understand interact with, this specification provides a way for the OS to directly interact with the user providing a more sophisticated user interface. The OS sets flags in the BIOS to indicate what action the BIOS should take on the next boot cycle. The only interaction the user needs to have with BIOS is a single key press at an automated query screen requesting authorization to perform the OS requested operation.

Q. How does this specification relate to the existing PC Client and TPM specifications?
A. This specification augments the PC Client specification. The specification creates a relationship between a set of flags and the requested next TPM state. It is not a requirement to implement this specification to be compliant with the PC Client BIOS or UEFI specifications. However, this implementation may be required by other entities outside of the TCG.

Q. What does it enable OEMs to do?
A. It allows the OEM to provide a simple predefined set of prompts and resulting actions from the user.

Q. How will end users benefit from implementation of this specification?
A. The prompts provided will enable a simple and consistent set of user interfaces across all platform manufacturers. It also allows easier TPM management through higher level software.

Q. What is necessary to use this spec (TPM, PC Client specs, etc.)?
A. OS and BIOS developers will use this, the PC Client BIOS specification, and the TPM specification to change the state of the TPM.