



Trusted Computing Group Work Group Charter Summary

Authentication Work Group

The Authentication Work Group will provide a standardized mechanism to allow authentication sources to authorize TPM actions. This will include the trustworthy transfer of authentication information from authentication sources, plus the mapping of authentication information to TPM authorization information. Authentication sources can include (but are not limited to) smartcards, biometric readers, keyboards, USB tokens, one-time-password tokens, remote authentication servers, etc. The goal is to define a profile for biometric readers and smartcards. This will include ensuring interoperability and consistency across functional classes of authentication sources. The AWG will use both existing and proposed TPM commands and interfaces to define the standards, including the Generalized Authorization (GA) extension, while maintaining TPM 1.2 Level 2 compatibility.

Compliance Work Group

The Compliance Work Group will provide all required mechanisms to enable evaluation and certification of TCG related products regarding functional correctness, completeness and interoperability (= compliance).

Conformance Work Group

The Conformance Work Group will develop appropriate specifications and documents as pertain to, and provide for, the definition of protection profiles and other evaluation criteria as required.

This may include specifying methods of evaluation for adherence, or "Conformance", to TCG components and specifications. The work group will also provide functional, as opposed to implementation specifications.

Hardcopy Working Group

The Hardcopy Working Group will define open and vendor neutral technical specifications for the components of hardcopy ecosystems that use TCG components to establish their root of trust. Included will be a minimum set of functional, interface, and privacy requirements for hardcopy components. It will further satisfy requirements of scalability, owner control, and interoperability, all qualified by HCWG defined use cases.

The HCWG will operate as an independent working group, rather than as a subgroup of the existing Peripheral Working Group. Hardcopy systems encompass a complex set of components, and are not limited to traditional "direct-connected" printing peripherals. The Hardcopy Working Group will define specifications for these components within the context of the complete system.



Infrastructure Work Group

The Infrastructure Work Group will work on the adoption and integration of TCG platform specific specifications into Internet and enterprise infrastructure technologies to enable various business models in a mixed environment of open platform architectures. Conventions for representing and exchanging information useful in making trust decisions will be established by leveraging existing Internet and related infrastructure standards. Considerations shall be made for representing platform roots of trust, trust chaining, key lifecycle services and the relationship these may have to owner policies.

The work group will define an architectural framework, interfaces and metadata necessary to bridge infrastructure gaps.

Marketing Work Group

The Marketing Work Group is responsible for creating the awareness of TCG, driving shows and events, and press and analyst engagements. The work group will develop a marketing strategy for promotion of the TCG organization's mission and specifications; develop TCG organization messaging and manage the use of both TCG messaging and technical content through various external communications vehicles; and define, create, and distribute marketing collateral, white papers, and presentations regarding TCG and TCG specifications.

Mobile Phone Work Group

The Mobile Phone Work Group will work on the adoption of TCG concept for mobile devices to enable different business models in market environment of open terminal platform. The work group will enhance TCG as needed to address specific features of mobile devices like their connectivity and limited capability as analyzed through various usage scenarios that may demonstrate added value of mobile devices in TCG.

PC Client Work Group

The PC Client Work Group will provide common functionality, interfaces, and a minimum set of security and privacy requirements for PC client that use TCG components to establish their root of trust.

This work group shall serve an advisory role by providing information to the TPM Work Group and other TCG Work Groups on possible architectural and design issues that may impact their work.

This work group's deliverables SHALL NOT address any functionality, interface (except those interfaces between the OS and the pre-OS environment), security or privacy issues for the Operating System(s) that are hosted by the platform.



Peripherals Work Group

The trustworthiness of a computing platform is clearly dependent in part on the trustworthiness of the peripheral devices connected to that platform. The purpose of the Peripherals Work Group is to identify the trust-related properties of peripherals and to explore the varied environments in which they operate, including usage scenarios and threat models, in order to better understand the role and impact of peripherals in an overall multi-component trusted platform. The work group will deal with the issues common to all peripheral devices, while individual aspects of particular classes of peripherals will be addressed in the subgroups of the Peripherals Work Group.

Server Specific Work Group

The purpose of the Server Work Group is to provide definitions, specifications, guidelines, and technical requirements as they pertain to the implementation of TCG technology in servers. The work group will endeavor to produce a spec that allows compatibility with currently specified API's and further enables current TCG infrastructures.

Storage System Work Group

The Storage System Work Group will build upon existing TCG technologies and philosophy, and focus on standards for security services on dedicated storage systems. One objective is to develop standards and practices for defining the same security services across dedicated storage controller interfaces, including but not limited to ATA, Serial ATA, SCSI, FibreChannel, USB Storage, IEEE 1394, Network Attached Storage (TCP/IP), and iSCSI. Storage systems include disk drives, removable media drives, flash storage, and multiple storage device systems. Act as TCG liaison to other storage industry standards groups that have jurisdiction over the interface standards to promote adoption of TCG technology. Interaction with other standards groups will be with the approval of the Technical Committee.

Technical Committee

The Technical Committee shall work with and under the auspices of the Board. The Technical Committee serves an advisory role to the board by monitoring all technical work groups for consistency and interoperability of technical specifications and initiatives. The Technical Committee follows scope guidance from the Board, develops ongoing technical agenda/vision/architecture for organization encompassing charters of each technical work group.

TPM Work Group

The TPM Work Group is chartered to create the Trusted Platform Module (TPM) specification. The definition of the TPM architecture comes from the TC and the TPM Work Group defines the implementation of that architecture. Work group members should have a working knowledge of security in relation to the design and usage of cryptographic modules. Members should also



have a working knowledge of cryptographic techniques including public-key cryptography, cryptographic algorithms and protocols.

Trusted Network Connect Work Group

The Trusted Network Connect Work Group will continue to refine, promote, and expand as needed the Trusted Network Connect open architecture and specifications for network access control. Network access control is a process and set of technologies that allow network operators to enforce policies regarding endpoint integrity when granting access to a network and after such access is granted.

Operator policies regarding endpoint integrity may involve integrity parameters that span the range of endpoint system components (hardware, firmware, software and application settings). Network operators are typically free to determine any policy they wish (which may or may not include evidence associated with a TPM).

TSS Work Group

The purpose of the TSS Work Group is to provide a standard set of APIs for Application vendors who wish to make use of the TPM. The work group will produce a vendor neutral specification which will provide an abstraction of the hardware differences so that application vendors can write applications that will work regardless of the hardware, Operating System, or environment is used. The TSS will also provide means for applications to talk to TPMs either locally or remotely.

Virtualized Platform Work Group

The Virtualized Platform Work Group will produce specifications that define trust properties of virtualized trusted computing platforms, interfaces used to express the trust properties of virtualized trusted computing platforms, trust properties of platforms that host a virtualized trusted computing platform, TPM functions and interfaces to support virtualized trusted computing platforms, and properties of virtualized TPMs.