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. More information on Authentication activities is available at: http://www.trustedcomputinggroup.org/solutions/authentication

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). The scope of the Compliance Work Group is the definition of the compliance and interoperability criteria, in the first iteration step for products designed according to the TPM Main spec and the PC Client-Spec (TPMs for PC Platforms); the development of the required test tools and methods to allow for a validation according to A) for vendors and users of products of the scope of this Work Group; the organization of events for TCG member companies to test their products especially with the scope of interoperability (i.e. Plugfests) in coordination with the TC and the Compliance Special Committee; and the support of the Compliance Special Committee in the implementation of a Certification and Logo Program as well as in the field of self-certification and 3rd party evaluation. More information on Compliance Work Group activities is available at: http://www.trustedcomputinggroup.org/certification

Embedded Systems Work Group
It is expected that the EmSys WG will be driven from solution architecture level expertise, to identify and document specification requirements, and then collaborate with the TCG technical committee to develop necessary specification extensions as EmSys specifications or to align those requirements to existing or future TCG technical working groups that may develop the necessary technical specifications. The scope covers the documentation of use cases for EmSys solutions, and the articulation of a unifying, integrated, EmSys architectural framework that enables the use of trusted computing standards in an interoperable fashion in order to securely manage an EmSys environment as well as producing additional technical architecture components, rules and specifications. The documentation of high level usage scenarios shall include vertical market requirements, demand signals, and overall solution requirements for specifications. Its scope will also include defining outbound messaging and marketing strategy for the organization in the field of EmSys WG solutions. More information on Embedded Systems Work Group activities is available at: http://www.trustedcomputinggroup.org/developers/embedded_systems

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 group will define an open and vendor neutral architectural framework, interfaces and metadata necessary to bridge infrastructure gaps. More information on Infrastructure Work Group activities is available at: http://www.trustedcomputinggroup.org/developers/infrastructure
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 Platform Work Group
The Mobile Platform Working Group (MPWG) produces use cases, requirements and specifications that a) facilitate a TCG-based platform for mobile platforms at the constrained end of the mobile device spectrum and b) which are applicable to the specification work done by other working groups in terms of being a TPM profile/subset reference point. More information on Mobile Platform Work Group activities is available at: http://www.trustedcomputinggroup.org/developers/mobile

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 does 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. More information on PC Client Work Group activities is available at: http://www.trustedcomputinggroup.org/developers/pc_client

Security Evaluation Work Group
The Security Evaluation 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. More information on Security Evaluation Work Group activities is available at: http://www.trustedcomputinggroup.org/certification

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. More information on Server Specific Work Group activities is available at: http://www.trustedcomputinggroup.org/developers/server

Storage 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. More information on Storage Work Group activities is available at: http://www.trustedcomputinggroup.org/developers/storage
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.

Trusted Multi-tenant Infrastructure (TMI) Work Group
With the increasing dependency on information systems, every end-user organization relies on high operational efficiency of the infrastructure while reducing the operational cost of maintaining standalone infrastructures. The purpose of this solution work group is to define an architectural framework to enable such IT infrastructure solutions to take advantage of trusted computing standards to achieve secure manageability and the safe sharing of resources between multiple independent end-user organizations. It is expected that the Trusted Multi-tenant Infrastructure Work Group will be driven from solution architecture level expertise, to identify and document requirements, and then collaborate with the TCG technical committee to align those requirements to existing or future TCG technical working groups that may develop the necessary technical specifications. More information on Trusted Multi-Tenant Infrastructure Work Group activities is available at:
http://www.trustedcomputinggroup.org/developers/trusted_multitenant_infrastructure

Trusted Mobility Solutions (TMS) Work Group
The Trusted Mobility Solutions Work Group will develop mobile solution frameworks for laptops, tablets, and smartphones and potentially some embedded systems. The scope of the TMS WG is the development and promotion of use cases and solution frameworks that enable trusted computing for mobile platforms. Along with requirements derived from mobile use cases, trusted mobility solutions frameworks and profiles will be developed in order to recommend and validate applicable TCG technical specifications, to identify gaps in existing TCG technical specifications, and to define new requirements that should be communicated to other TCG WGs. More information on Trusted Mobility Solutions Work Group activities is available at:
http://www.trustedcomputinggroup.org/developers/trusted_mobility_solutions

Trusted Network Connect (TNC) 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 and security automation. Network access control is a process and set of technologies that allow network operators to enforce policies regarding network access. The network access control specifications include (but are not limited to): reporting the posture of an endpoint, verifying the posture is consistent with policy, and provisioning access control consistent with the results of the verification. Security automation enables the integration of security components across the endpoint, network, and servers into an intelligent, responsive, coordinated defense. The security automation specifications include (but are not limited to) securely sharing actionable, machine-readable information among authorized security systems with low latency. Roots of trust such as TPM may be used in network access control and security automation to establish endpoint identity and integrity. More information on TNC Work Group activities is available at:
http://www.trustedcomputinggroup.org/developers/trusted_network_connect

Trusted Platform Module (TPM) Work Group
The TPM Workgroup (TPMWG) creates specifications for Trusted Platform Modules (TPM) to enable the creation of interoperable roots of trust on TCG-enabled platforms. The TPMWG shall serve an advisory role as needed to platform-specific workgroups to assist them in the creation of TPM 2.0 profiles and other specifications that require expertise and knowledge related to TPM. The TPMWG will serve an
TCG Software Stack (TSS) Work Group
The TSSWG creates specifications for software stacks to allow applications, operating systems, firmware and other software modules to access TPMs. The TSSWG shall develop TSS specifications that correspond to each release of TPM hardware, and which allow the appropriate exercise of TPM functionality; the TSS specification shall be hardware, Operating System, and environment neutral; and, develop vendor neutral header files to augment the TSS specification. TSS work group members should come from a variety of TCG platform backgrounds as the TSS is intended for use by the wide range of TCG platforms. They should be knowledgeable on operating systems and hypervisors that will provide TSS services and be knowledgeable on the TPM and its practical use. A strong knowledge of TSS use cases is desired so that the TSS can be applicable to both expert users and also a more general set of application developers who are not expert in the use of TPMs but desire to use TPMs nonetheless. The overarching goal of the TSS is to enable the use of TPMs with the broadest possible set of applications. More information on TSS Work Group activities is available at:
http://www.trustedcomputinggroup.org/developers/software_stack

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. More information on Virtualized Platform Work Group activities is available at:
http://www.trustedcomputinggroup.org/developers/virtualized_platform