



## 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).

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.

This EmSys WG architectural framework shall be an open and vendor neutral architecture that identifies how technical specifications and interoperability interfaces can be used to deploy trusted computing technologies and concepts in a way that meets the requirements of EmSys use cases. The EmSys WG will cooperate with other related external standardization committees for dissemination of TCG standards as well as getting inputs for fulfilling the markets needs.

## **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.

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 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.

More information on Mobile Phone 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 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.

More information on PC Client Work Group activities is available at:  
[http://www.trustedcomputinggroup.org/developers/pc\\_client](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 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.

More information on Storage System 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 dependence 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 TCG can establish standards on which improved information flow and infrastructure management efficiency are based, with consideration to making the infrastructure more cost effective for the customer. Whether these costs are a measure of energy, physical space, IT expertise, or some other aspect of IT infrastructure operation, it is becoming increasingly critical to enable trust models and interoperability that support secure multi-tenant use and management of back-end infrastructure, and permit the sharing of high-density IT resources.

The purpose of this work group is to define an architectural framework to enable IT infrastructure solutions which take advantage of trusted computing standards to achieve secure manageability and the safe sharing of resources between multiple, independent end-user organizations. The Trusted Multi-tenant Infrastructure WG is driven from solution architecture level expertise, to identify and document requirements, and then collaborate with the TCG Technical Committee to align those requirements to TCG technical working groups that are responsible for developing individual technical specifications.

### **Trusted Mobility Solutions (TMS) Work Group**

It is expected that the TMS WG efforts will be driven from use cases that are jointly sponsored by members of the Work Group. In addition, TMS Work Group efforts will rely on the solution architecture development level expertise of members to identify and document requirements, along with collaboration with the TCG technical committee to align those requirements to existing or future TCG technical Work Groups that may develop the necessary technical specifications.

The scope of this solution work group covers the documentation of use cases for managing and securing mobile, network-connected endpoints, and the articulation of a unifying, integrated TMS architectural framework that enables the use of trusted computing standards. . Implementation profiles and recommendations for updates to relevant TCG standards are included.

### **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. 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).

More information on TNC Work Group activities is available at:

[http://www.trustedcomputinggroup.org/developers/trusted\\_network\\_connect](http://www.trustedcomputinggroup.org/developers/trusted_network_connect)

### **Trusted Platform Module (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.

More information on TPM Work Group activities is available at:

[http://www.trustedcomputinggroup.org/developers/trusted\\_platform\\_module](http://www.trustedcomputinggroup.org/developers/trusted_platform_module)

### **TCG Software Stack (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.

More information on TPM Work Group activities is available at:

[http://www.trustedcomputinggroup.org/developers/software\\_stack](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.