



**Trusted Mobility Solutions Work Group
Frequently Asked Questions
December 2011**

Q. Why did the Trusted Computing Group (TCG) form the Trusted Mobility Solutions (TMS) Work Group (WG)?

A. The TMS WG was formed to provide real-world solutions guidance for adopters and users who are interested in using TCG technologies for mobile devices in enterprise or business-to-consumer environments, with their evolving security challenges (which the TCG is well-equipped to address). The TMS WG is chartered to facilitate the demonstration of trusted mobility solutions, which make use of the TCG capabilities developed by different TCG Technical Work Groups, and to provide comprehensive guidance on how these TCG technologies can be leveraged in mobile devices and enterprise networks.

Q. What problems does the TMS WG intend to address?

A. With growing enterprise and consumer reliance on mobile platforms, such as smartphones, laptops and tablets, the need for enhanced protection of these devices as well as controlling their access to networks is paramount. Effective use of mobile devices requires the communication of trustworthy information about device identity and device integrity along with the availability of a secure storage. In addition, mobile platforms must be integrated with robust provisioning, access control, and application/data protection mechanisms to enable trusted connections to enterprise networks, mobile payment and financial services, health care, and other sensitive application systems within the mobile devices ecosystem.

Q. How will the TMS WG address these problems?

A. In order to deal with the aforementioned issues effectively, it is vital to enable trust models and interoperability of components which support trusted mobile platforms and the remote management of these mobile devices. One of the main goals of the TMS WG is to define an architectural framework, use cases, implementation guidelines, and best practices in order to ensure effective deployment of trusted mobility solutions. The TMS WG will facilitate the practical demonstration of trusted mobility solutions that leverage TCG and other trusted computing specifications to achieve trusted operation, trusted remote manageability and safe collaboration between multiple independent stakeholders (e.g., financial institutions and application developers) and user organizations.

Q. What is a “trusted mobility solution”?

A. The TMS WG defines a “trusted mobility solution” as one that addresses all of the following features and concepts:

- Mobile endpoints are managed computing resources.

- One or more mobile endpoint management functions are defined and operate as part of the solution.
- Mobile endpoints can connect to a network, preferably using TCG TNC network attachment integrity verification.
- Mobile endpoints can be physically moved by a person with ease, or in conjunction with the movement of a person (e.g., in an automobile).
- Mobile endpoint trustworthiness is enabled and/or supported by one or more capabilities that are conformant to TCG technical specifications (e.g., TPM or MTM).
- Mobile endpoint trusted boot, applications, databases, security policies, etc., can be reliably deployed in order to support a trusted execution environment (e.g., using a TCG Opal SED).

Laptops, tablets, and smartphones are the mobile endpoints that are the primary focus for the TMS WG. Other portable consumer devices (e.g., radios, cameras, music players, sensors, and analog devices) are out-of-scope in the TMS WG charter.

Q. What types of deliverables will the TMS WG produce?

A. The TMS WG will define **use cases** and **solution requirements** for managing and provisioning trusted mobile, network-connected endpoints, and will document a unifying, integrated **architectural framework** that will enable the interoperable use of trusted computing standards. Although, the TMS WG will not develop new TCG technical standards, the work group will define **implementation guidance, best practices, and also recommendations for updates** to existing relevant TCG standards. Furthermore, new approaches to demonstrate the solution certification and compliance may also be developed.

Q. What is the relationship between TMS WG and other TCG Work Groups, such as the Mobile Phone Work Group (MPWG)?

A. TCG Work Groups, such as the Mobile Phone Work Group (MPWG), define security-related use cases, requirements and technical specifications. For MPWG, the focus is on securely booting mobile and embedded systems that provide TCG TPM-compliant features like remote attestation, key management, and authentication and secure storage for applications and OS services, as well as support for local and remote ownership to address corresponding security requirements.

Moreover, the purpose of the TMS WG is to synthesize requirements and technical specifications from multiple TCG technical WGs to provide an integrating framework for mobility solutions architectures.

The objectives of the TMS WG may also expose additional requirements for future TCG specifications or even for new TCG WGs in order to deploy a TMS solution. In these cases, the TMS WG will engage with the respective technical WGs to help refine the requirements.

Also, the trusted platform concepts developed by the TCG will require specific lifecycle management and integration into mobile solution architectures. The TMS WG will aim to assist other TCG work groups in demonstrating how the current and future

specifications could contribute in enabling the trust models, which make new mobile compute paradigms possible.

Q. What existing TCG specifications are relevant to the efforts of the TMS WG?

A. Since the activities of the TMS WG are solutions-oriented, several TCG technical specifications may be applicable to our trusted mobile solutions architecture. The key examples include:

- MTM – Mobile Trusted Module (mobile and embedded subset of TPM)
- TPM – Trusted Platform Module (encryption and other keys, hardware security)
- TNC – Trusted Network Connect (integrity measurement and verification)
- IF-MAP – Metadata Access Point (interworking across security architectures)
- OPAL – Self-Encrypting Drive (secure OS and application data storage)
- TMI – Trusted Multi-Tenant Infrastructure (separation of consumer and business applications)

The TMS WG use cases should include a selection of these TCG technical specifications to show how the integration of these capabilities can be deployed, managed, and operated to meet the security objectives of particular reference implementations. Financial, telecommunications, and government TMS WG members and liaisons should propose and evaluate key TMS use cases.

Q. Some people think that a TPM is hard to provision and manage for PCs. How is the mobile world different than PCs and how does the TMS WG aim to address this issue?

A. Certainly there are many issues that must be considered when provisioning and managing TPM or MTM-enabled devices, and the diversity of devices and interconnection technologies in the mobile world introduces even more complexity. This realization motivated the formation of the TMS WG to leverage the work of the other TCG WGs and other non-TCG standards groups that address the mobile world and explore the issues that enterprises face when provisioning and managing TCG technologies within mobility-enabled infrastructures. Using real-world use cases, the TMS WG will apply TCG standards within the mobile world and demonstrate how management challenges and technical risks can be handled in a cohesive and comprehensive manner. The TMS WG will work with other TCG WGs to resolve difficulties that are identified in the demonstration of these capabilities and propose recommendations for updates to TCG standards.

Q. Are there any mobile devices that currently ship with a TPM or MTM?

A. To date, the MTM has been implemented primarily in company-internal and lab research projects. For example, Nokia Research Center has produced a GPL open source MTM add-on to the TPM emulator by Mario Strasser et al, and a reference implementation of the manufacturer profile of MTM (MRTM) for ARM TrustZone. Also, the Terminal Mode V1.0 standard recommends hardware-assisted MTM security for key storage and usage.

To ease both implementation and adoption, the newest MTM use cases introduce concepts where common interfaces for messaging – protocol data units (PDUs) and application programming interfaces (APIs) – are utilized, primarily between the OS and

the trusted execution environment, but also between applications and the OS, to provide added value for service deployment.

Q. How does the TMS WG collaborate with and complement the efforts of other forums or standards bodies involved in mobile security?

A. The primary focus of the TMS WG is to synthesize TCG-based technical specifications into an architectural framework, set of relevant use cases, demonstrated capabilities, and lessons learned. Other standards groups and forums also are working on secure mobility specifications, projects, and use cases such as the Global Platform, the Mobey Forum, the U.S. Government Mobile Applications Group and National Institute of Standards and Technology (NIST), and the German Federal Ministry of Education and Research through the ESUKOM project. The TMS WG plans to collaborate with these groups as their efforts relate to trusted computing and where TCG specifications can be applied.

Q. What types of members participate in the TMS WG?

A. Current members of the TMS WG include a wide variety of participants: handset and other mobile platform providers, system integrators, chip manufacturers, network systems providers, hard drive manufacturers, system and application software vendors, and voices from academia, and government. This diversity of viewpoints and capabilities is essential to the development of robust solutions frameworks. The TMS WG cordially invites new or existing TCG members to participate in our development of trusted mobile solutions requirements and real-world demonstrations.

Q. What kinds of expertise are needed for a member to contribute to the TMS WG?

A. The TMS WG welcomes members with all types and levels of expertise, who could contribute in exploring and resolving different issues associated with deploying the TCG technologies within the mobile devices ecosystem. A diversity of backgrounds will assist the TMS WG in ensuring that its recommendations have a widespread applicability within the mobile-device-equipped enterprises.

Q. How can builders or users of trusted mobile solutions benefit from the work of the TMS WG?

A. The TMS WG will define specific recommendations for the use of TCG technologies in trusted mobile solutions. The builders of trusted mobile solutions can use these recommendations to ensure that their products meet the needs of diverse mobility communities. Users of trusted mobile solutions can use the recommendations that are specific to their needs to plan the purchase, deployment and management of appropriate and scalable trusted mobility solutions.

Q. When do you expect builders or users of mobile solutions to benefit from the work of the TMS WG?

A. Mobile solutions providers or adopters can benefit immediately in improving their understanding of the application of TCG capabilities through participating in the ongoing work of TMS WG activities, such as the development of white papers, solution requirements, use cases, and the TMS architecture framework. In addition, the WG plans to deliver initial versions of these documents starting in the first and second quarters of 2012. The TMS WG deliverables should assist solutions providers and adopters to plan the development and deployment of trusted and scalable mobile solutions.