Mobile Trusted Module Specification FAQ
- General Overview -
June 2007

Q. Why was the Trusted Computing Group (TCG) Mobile Trusted Module (MTM) specification developed?

A.. The TCG, as the trusted computing security authority, has developed the Mobile Trusted Module specification to enable mobile phone information security assurance and the potential application benefits associated with that assurance. TCG security assurance directly translates into trust in a platform's capability to protect its information and functional assets, and to attest to those protections.

TCG has always had the mission of providing specifications for any device that touches the network. While its initial work has been in PC clients, the network and servers, it is logical for TCG to apply its expertise and Trusted Computing concepts to mobile devices. From the perspective of users and vendors, mobile phones are becoming increasingly sophisticated and are being used for basic computing tasks, Internet connectivity, network access to corporate data, and mobile commerce and banking services. Smartphones also are being used as storage for personal, confidential information. All these new phenomena require increased trust and security functionality.

The TCG Mobile Phone Work Group has completed the world's first open security standard for Mobile Trusted Platforms, using the Mobile Trusted Module (MTM), whose specification was published already in September 2006.

Q. When will the actual specification be available? When will we see product implementations?

A. The specifications are now complete and available. The Mobile Phone Work Group released the Reference Architecture specification and the Mobile Trusted Module specification in June 2007. A draft version of the MTM specification, called "Commands and Structures", was released previously in September 2006. Like all TCG specifications, the specification is available on the organization's website, free of charge.

While we can't forecast specific product plans, generally products follow specifications by several quarters or so, depending on product development cycles.

Q. What do you mean by mobile security?

A. TCG's definition of trust as it applies to trusted computing is "hardware and software behaves as expected". With regard to mobile devices, this implies that the operating system, platform, and application level functionalities, as well as SIM, USIM, UICC cards etc, interact in a secure, trusted manner. The Mobile Trusted Module is designed to complement existing mobile phone security components. The Reference Architecture specification describes a platform that uses the MTM to provide enhanced platform security. While existing standards address subscriber information security from a network carrier perspective, the TCG specifications enable trust in the mobile phone equipment itself from the more interoperable and privacy sensitive TCG trust perspective.

Q. Who benefits from this specification?

A. Because the specification addresses both information and functional asset integrity, both functional users such as consumers, professional users, enterprises, industry and governments as well as content providers and information owners benefit from the assured protections enabled by this specification. As defined in the Mobile Trusted Module use cases (published in 2005) a variety of

practical applications match with current needs from both end-users' perspective and enterprises' viewpoint. Practical implementation of the use cases enable enterprises and other parties to develop more sophisticated services and expand their business field.

Q. What does the Mobile Trusted Module specification cover? How will it work?

A. The specification provides the core framework, commands and control specifications needed to provide a TCG based security building block solution in mobile phones. This will allow mobile chip, software, and handset companies to begin to design the MTM functions into their products.

Q. What else is required for a mobile phone handset maker or other party to use this specification?

A. Vendors need to provide software and hardware that provides standard TCG roots of trust, such as the root of trust for measurement, an additional root of trust to verify software before loading it, and (optionally) an additional root of trust for instantiating other roots of trust.

Vendors also need to provide software that can take advantage of the functions provided by TCG technology. This may include adaptation and further development of operating systems. These functions are described in the Reference Architecture component that forms the second half of TCG's Mobile specifications. The Reference Architecture was published in June 2007.

Q. What are the benefits of standardizing mobile security? Aren't handset OEMs, software makers and service providers working on this issue individually?

A. Standardization has proven to be a highly successful path to foster interoperability across computing and communications. Effective standards allow different manufacturers to streamline R&D, to take advantage of the combined expertise of the industry, to cut costs and to increase adoption by users and other participants in the economic ecosystem. By embedding standardized security into mobile devices, the various providers of hardware and services can ensure security and interoperability while adding value through their devices or applications.

Q. To what extent will today's phone architecture need to be modified to accommodate this specification?

A. As there are numerous different implementations across various handset OEMs, it is not possible to know how TCG's Mobile specifications might impact their current designs. However, the open standards for security functions included in the Mobile Trusted Module specification are in many cases similar to current functions implemented by each vendor and the specification is deliberately formulated to be abstract and implementation neutral. Participation of various organizations in the specification design process and continuous cross-industrial collaboration has supported the aim of developing an implementation neutral specification. The benefit of the specification is that it would provide a common description of the functions that need to be provided to meet platform security objectives and of the security propreties and capabilities of those functions.

Q. TCG has talked about the fact that enabling a TPM in a PC is an opt-in procedure, allowing users to decide whether they want that security or not. Will phones operate in the same way?

A. In the mobile phone environment, there are different requirements about what the user can and cannot do, and these are different from PCs. One example could be the subscriber information that is used for billing the phone usage – a user should not be able to change that.

Q. Does the work of the Mobile Phone Work Group cover just phones or does it include PDAs?

A. The published use cases and Mobile Trusted Module specification have been designed to address mobile phones. These could include smartphones with PDA functions.

Q. Do these use cases apply to other handheld devices?

A. The first set of use cases targets the products that include cellular technology. However, the specifications might be used to implement mobile security in other products.

Q. Where does the responsibility on security reside when a security module is built into a device; can the interests of the service providers be assured?

A. The responsibility for security is always a shared responsibility between the security service provider and the service user. Any security module can only offer assurance for the behavior and assets within its own domain. The behavior and the assurances of a security module include the protections employed to address the particular threats that exist in a specified environment. The interests of service providers are assured to the extent that they understand the protections offered by the module and their own responsibilities for its effective application.

Q. What will be the estimated cost of using the specification?

A. TCG cannot speculate about costs because the specifications are deliberately implementation agnostic. The costs mainly depend on the way the specification is implemented among volumes and environment.

Q. Which companies are participating in the TCG Mobile Phone Work Group?

A. A number of companies representing handset makers, service providers, silicon providers and applications are active in the Work Group. These companies include AuthenTec, Ericsson, France Telecom, HP, IBM, Infineon, Intel, Lenovo, Motorola, Nokia, Panasonic, Philips, Samsung, Sony, STMicroelectronics, Texas Instruments, VeriSign, Vodafone, Wave Systems and many others.

Q. Is TCG working with other standardization bodies?

A. TCG has an active liaison program with the purpose of coordinating its open specifications with other organizations. Open, interactive discussion between different organizations overcomes any potential gaps or overlaps in standardization work. Many of the TCG Mobile Phone Work Group members also participate in other key standardization organizations, such as OMA, OMTP, 3GPP, MIPI, ITU and others. In addition to ongoing liaison by members of the organization, TCG is publishing the relevant technical materials and inviting comments and participation of other companies.