Mobile Trusted Module Specification FAQ
September 2006

1. Why was the TCG Mobile Trusted Module specification developed?
The TCG, as the trusted computing security standards 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.

2. What do you mean by mobile security?
TCG's definition of trusted computing is "hardware and software behaves as intended". 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 TCG specification for the Mobile Trusted Module is designed to complement and strengthen the existing mobile phone security components. Where these 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.

3. Who benefits from this specification?
Because the specification addresses both information and functional asset integrity, both functional users and information owners benefit from the assured protections enabled by this specification.

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

5. How does the Mobile Trusted Module (MTM) specification relate to the Trusted Platform Module(TPM) shipping in PCs today?
The TCG specifications contain core functionality common to all platforms and allow the functionality to be implemented for specific platforms. The specification builds on existing TCG specifications. The Mobile Phone Work Group has extended the TCG specifications specifically to support mobile phone devices

6. Is the new specification in any way similar to the Trusted Platform Module specification?
The TCG has created a core set of security specifications to be used as standardized building blocks. Both the TPM and Mobile Trusted Module specification are based on this same core set of security functions providing the same essential TCG roots of trust. The MTM is tailored to the verified mobile phone framework and offers enhancements suitable for that framework.

7. What else is required for a mobile phone handset maker or other to use this spec?
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. This overall reference architecture will be described in a future companion specification whose development is already well advanced by the TCG.

8. Is TCG working with other standardization bodies?
TCG has an active liaison program with the purpose of coordinating its open specifications with other organizations. Many of the TCG Mobile Phone work group members also participate in other key standards organizations, such as OMA, OMTP, 3GPP, MIPI, ITU and others. In addition to maintaining liaison with members of the various organizations, TCG is publishing the relevant technical materials and inviting comment and participation of other groups.

The TCG believes that the specifications developed by the MPWG are complementary to the other mobile industry security efforts. The aim is always to offer the underlying endpoint security assurances associated with TCG root of trust technology.

9. Why does the specification define two types of MTMs (Mobile Local Owner Trusted Module and Mobile Remote Owner Trusted Module)?. And, in the specification, the TCG identifies multiple owners of a mobile phone. What does this really mean?
Mobile Local-Owner Trusted Modules (MLTMs) support usages similar to those of existing TPMs but are different from TPMs because they are designed to cope with restrictions inherent in today's phone technologies.

Mobile Remote-Owner Trusted Modules (MRTMs) are adaptation of MLTMs that enable remote entities (such as the phone manufacturer and the cellular network provider) to preset some parts of the phone (such as access to the IMEI and the cellular network).

Owners in this specification are a reference to the mobile phone that is abstracted as multiple layers, where each engine serves the security and trust interests of a single stakeholder and the owner. Therefore, owners are simply entities with information assets on the platform, given their authorization to be on the platform and their need to securely manage those assets.

10. To what extent will today's phone architecture need to be modified to accommodate this specification?
Since there are numerous different implementations across various handset OEMs, it is not possible to know how the Mobile Trusted Module specification 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. 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 properties and capabilities of those functions.

11. When will we see products implementing the specification?
TCG can't forecast specific product plans. Generally products follow specs by six to eighteen months, depending on product development cycles. Implementation depends on independent companies. Some participating companies have provided statements of support for the work done in TCG; you can see this at https://www.trustedcomputinggroup.org/groups/mobile.

12. What will be the estimated cost of using the specification?
TCG cannot speculate the costs as the implementation is not limited by purpose and the costs are mainly based on the way the specification is implemented among volumes and environment.

13. Does the work of the Mobile Phone Work Group cover just phones or does it include PDAs?
The published use cases and Mobile Trusted Module specification were designed to address mobile phones. These could include smartphones with PDA functions.

-- 30 --

For more information, go to https://www.trustedcomputinggroup.org/groups/mobile.

Contact: Anne Price
1-602-840-6495
press@trustedcomputinggroup.org