Mobile Trusted Module Specification FAQ

- Technical Overview -
June 2007

Q. In what ways do Mobile Trusted Modules (MTMs) and the Reference Architecture (RA) enhance security for mobile device?

A. MTMs are “safes” that protect stored information, and are optimized for mobile devices. They also enable a mobile device to be recognised as a trusted mobile device, while at the same time maintaining privacy. The RA describes how to incorporate MTMs into a mobile device in a way that protects information while it is being used, after it has been obtained from an MTM.

Q. How could you implement MTM in a mobile platform?

A. There are a number of implementation possibilities, such as:

a) A specialised MTM chip
b) A TPM 1.1 or 1.2 chips and some extra layer in software to implement extra commands
c) Another HW chip bound to the platform and running an MTM application amongst others
d) SW MTM running in a virtualised engine with the virtualisation environment protected by an underlying HW MTM
e) SW MTM running in a CPU chip.

Q. Will mobile devices based on the TCG mobile specification use the TPM chip that is used in PCs?

A. The TPM specification contains core functionality common to all platforms and allows the functionality to be implemented for specific platforms. The mobile specification builds on the TPM security specification and trust model. As the TPM in the form it appears in the PC environment is not directly applicable for mobile equipment, it needs to be modified for the mobile environment, taking into considerations unique features and requirements for mobile phones.

Q. 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?

A. 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.

Multiple MTMs provide the capability for allowing different security policies to be applied independently to the user’s data, the device itself, or other aspects of the phone. This allows the user

to determine and set their own privacy and security preferences. The regular TPM v1.2 used in PCs can have only one Owner, thus multiple MTMs were chosen to be the solution for mobile phones as it better serves the needs of the more complex mobile ecosystems.

Q. Are MTM and TPM compatible? Will the security in a mobile device be compatible with PC client?

A. With minor exceptions, the MTM and TPM are compatible. The MLTM is specified to be an embedded version of a v1.1b TPM. The MRTM is specified to be a MLTM with functions to ensure that selected parts of a mobile device are protected against unauthorised alteration. Nothing in TCG's specifications makes security in a mobile device incompatible with security in a PC client, although some functions in mobile devices are restricted by the capabilities of mobile devices. Functional compatibility between mobile devices and PC Clients will depend on individual vendors' implementations.

Q. What do the MPWG TCG specifications and a phone being TCG compliant really bring?

A. TCG compliance gives a way for manufacturers to assure customers (operators, enterprise and users) that a phone is securely implemented for many of its important security properties, which in turn enable many of the most important security use cases. The TCG MPWG work provides a standards-based specification for generic platform security functions such as secure boot, secure storage and runtime integrity.

Long term, the MPWG TCG specifications should bring the market efficiencies and dynamics that standardised specifications, and the open market they enable, bring. The MTM specification provide assurance to operators, enterprises and users that the mobile phone will function as intended under all use cases. Standardization offers market efficiencies and interoperability that benefit all the parties involved.

Q. What is the strength level of functions provided by an MTM? What security claims can be made about the MTM?

A. “Strength of function” loosely covers three areas for the MTM: (i) What cryptographic algorithms are implemented, and do they use sufficiently long keys? (ii) Are the MTM capabilities protected against various sorts of attack? (iii) What assurance can be given to show that the MTM capabilities are protected against these sorts of attack?

(i) In the first respect, the MTM spec references precisely the same mandatory algorithms, key-lengths and equivalences as the TPM 1.2 specification.

(ii) In the second respect, the MTM is - like a TPM 1.2 - regarded as a set of shielded locations and protected capabilities, and is designed to resist the same general sorts of attacks. Namely, software attacks and some hardware attacks, which might attempt to read or modify the contents of shielded locations while bypassing the protected capabilities, or might attempt to corrupt or manipulate the protected capabilities. Also, like the TPM 1.2, the MTM is not intended or expected to resist powerful hardware attacks.

The only difference in the MTM specification concerns monotonic counters: the minimum mandatory strength of function for a monotonic counter in the MTM specification is lower than for a TPM 1.2. This is a short term measure, arising because a true TPM 1.2 monotonic counter requires a memory location which is simultaneously shielded, non-volatile, and re-writable, and a number of likely candidates for an MTM implementation do not currently have a memory location satisfying all three properties. Also, the types of attacks which are resisted by a monotonic counter (such as re-flash and version rollback) can be resisted in the mobile phone specification by other means (such as timed revocation lists and access to a secure network time source). Nevertheless the MPWG intends to strengthen the requirements on monotonic counters at a later date, to match the TPM 1.2 level.

(iii) In the third respect, the published MTM specifications only specify the functional or compliance requirements of the MTM. The conformance requirements and the conformance plan for the MTM will determine its fundamental threat protections, and have not as yet been finalized. These protections

will however be written in the form of a Common Criteria (CC) Protection Profile (PP). The PP is an implementation independent statement of security requirements that is shown to address threats which exist in the specific environment.

Whether or not every MTM needs to undergo CC approved third party evaluation is a separate matter that the MPWG and the TCG is still addressing from both a TCG and mobile phone industry perspective. While the TCG typically recommends CC evaluation for TCG certification, there needs to be agreement within the mobile space on how to address its security needs for some of the rather rapid/short product lifecycles encountered. In particular, there is a need to address the different conformance requirements that will occur at the MTM and at the product/platform or TBB level.

Q. Does each MTM have its own certificate/credential?

A. The MLTM (Mobile Local-Owner Trusted Module) must always be supplied with an Endorsement key (EK) and associated credentials, to enable anonymity and pseudonymity via generation and certification of AIKs. An MRTM (Mobile Remote-Owner Trusted Module) could be supplied with an Endorsement key (EK) and associated credentials, but some might instead be supplied with just preassigned AIKs and associated credentials. This is because mobile phones must unambiguously identify themselves to cellular networks, and some MRTMs will be used to identify the phone just to cellular networks.

Q. Is an MTM needed for a secure and authenticated boot?
A. No. Secure and authenticated boot is a byproduct and the responsibility of the new TCG/MPWG root of trust, the Root-of-Trust-for-Verifiication, which locally verifies and enforces the authenticity of all components during the boot process. An MTM is needed to protect the identity of a platform entity and to ensure that this platform entity can authenticate the integrity measurements it produces. An MTM then is needed to offer verifiable and TCG certifiable measurements of integrity to any remote entity on demand. An MTM therefore is necessary to participate in the Trusted Computing Infrastructure to enable remote entities to make a trust decision for secure interoperability.

Q. Why wasn't the existing TPM enough?

A. The existing TPM isn’t enough because a mobile phone is often an embedded implementation and because protections for the regulatory parts of a mobile phone should never be turned off. Both the MLTM and MRTM were therefore designed to enable embedded implementations, and the MRTM was additionally designed to ensure continual availability of security functions for the regulatory functions in a mobile phone.

Q. Is there a TSS in the MTM specification?

A. The TCG Software Stack is not defined in the MTM specification.

Q. How will mobile phone industry vendors protect the data and privacy of users with Trusted Mobile devices?

A. Data and privacy will be protected as they are in trusted PCs. In phones, techniques such as access control, integrity check, controlled boot sequence etc. will be used, just as in PCs. The EULA signed by each subscriber today sets regulation on user information by the service provider. The TCG specifications for security do not contradict privacy and regulation already stipulated.

Q. Will the MTM based trusted services be offered in SW or HW?

A. Market requirements will determine whether dedicated HW, software, or a hybrid solution will be used. The specification allows for any kind of implementations.

Q. Does the MTM specification offer any TCG protections for Device Owner confidentiality and privacy?

A. Yes. The multiple stakeholder/MTM architecture enables confidentiality and privacy by enabling secure identification of active stakeholders and the partitioning and isolation of their functional and information assets. This serves not only to enable stakeholders to assume control of their own information integrity but also places responsibility on them for their handling of those assets. For example, the manufacturer is responsible for the security of the IMEI integrity and for ensuring that this information is only revealed to the Mobile Phone Service Provider [which is the only other entity with a need to know]. As the principal communication gateway manager, the Mobile Phone Provider has an obligation to maintain customer/subscriber privacy concerns from both a regulatory and a customer-loyalty/business-practice perspective.

Q. I see that content protection is one of the use cases (published in 2005) for mobile phones. Does this represent a change to TCG policy?

A. No. The potential for using the TCG building blocks for DRM, as with the protection of personal privacy and other applications, is well known. TCG is not developing specifications for DRM solutions, per se. We have noted that it is possible for adopters of the specifications to use the specifications to enable DRM solutions, as the specifications are open and do not discriminate what type of applications can be developed for them. In the mobile market segment specifically, companies have indicated that securing content such as messaging, games, music, graphics, videos and information services should be protected in such a way that enables strong authentication for the user and platform. Ultimately, a Trusted Mobile device could enable more applications such as content and sharing for users as well as protection of individual data.