Trusted Computing Group Mobile Trusted Module and Use Cases
Frequently Asked Questions
May 2011

Mobile Trusted Module (MTM)

Q. What is new with Trusted Computing Group's efforts around mobile device security?
A. TCG has been working actively to enable security for mobile devices. Several years ago, it developed a specification for the Mobile Trusted Module, or MTM. Because of changing market requirements, TCG is working to evolve that effort. This month, we are releasing updated use cases for the MTM and proceeding with work on MTM 2.0.

Q: Is TCG's Mobile Trusted Module (MTM) 1.0 specification still valid for use today?
A: The MTM 1.0 specification is still valid for use today. However, the MTM specification is now evolving and work on an MTM 2.0 specification is in progress.

In addition, support for local and remote ownership remains a mainstay of the MTM architectural framework, and is a differentiator from the TPM specification, whereby mobile device manufacturers and network service providers utilize a Mobile Remote-Owner Trusted Module (MRTM) and end users benefit from a Mobile Local-Owner Trusted Module (MLTM) to address corresponding requirements in cellular security.

Q: The original MTM original specification was never widely implemented. How do you intend to enable adoption of the new MTM specification?
A: The MTM was implemented primarily in company-internal and lab research projects. It was perceived that easy deployment on legacy trust roots would make MTM happen. Clearly this was not enough. The implication is the need for better and more use cases. And implementation in a variety of ways is still very important.

The newest use cases, addressed later in this FAQ, introduce concepts where common interfaces for messaging – protocol data units (PDUs) and application programming interfaces (APIs) – are utilized, primarily between the operating system (OS) and the trusted execution environment, but also between applications and the OS, to provide added value for service deployment. This should ease both implementation and adoption.

Q: Who ought to become involved in MTM 2.0 development and why?
A: Stakeholders include mobile equipment vendors, silicon vendors, BIOS/OS vendors, mobile financial and payments services, network service providers, content services developers, and end user experience experts who need to facilitate security and privacy in a standards-based fashion, without compromising usability and end user satisfaction.

Q: What are the key concepts that the MTM 2.0 specification will bring to the mobile industry, and what are the benefits of these for stakeholders?
A: The MTM 2.0 specification will, for example, make the MTM more relevant for aforementioned stakeholders by facilitating easier application provisioning, facilitating a trusted execution environment, and related application programming interfaces (APIs). TCG's MTM specification development builds upon the existing MTM specification and

TCG's current Trusted Platform Module (TPM) security concepts to offer more flexibility and easier integration of trusted mobile devices to other systems.

New MTM use cases recommend that legacy algorithm support should be specified within MTM 2.0, by providing trusted execution environment interfacing that leverages MTM interfaces including platform binding and authorization.

Q: Does the MTM, whether present or future, have to be implemented in dedicated silicon? If not, how can it be implemented?
A: The choice of MTM implementation is flexible. It can be implemented in hardware, in both hardware and software, or as software only. Implementation choices will depend on business objectives for the implementation, as well as security levels deemed appropriate on a business case-by-case basis.

For all implementations, the MTM roots of trust define the minimal platform (hardware) binding, and in general the means to estimate, for example, the security level of a given MTM.

Q: Is TCG working with any other industry groups during the development of the new MTM 2.0 specification?
A: TCG recognizes the value of industry liaisons for enabling trusted end-to-end solutions which serve multiple actors and support several business models. We are working to identify such liaisons.

Q: What software is required to enable the security of the MTM specification?
A: The security of the MTM 2.0 specification is based on trust roots, and the notion that the devices that implement the specification use some legacy hardware-assisted security architecture, in many cases a processor mode with isolated execution.
The binding between the legacy architecture and the MTM will be device-specific in accordance with the definitions of the MTM trust roots – there is no common bootstrap.

Q: What is the approximate timeframe for the new MTM 2.0 specification?
A: The objective is to make available the first public release of the MTM 2.0 specification in a second half-2012 to first half-2013 timeframe.

Q: How can stakeholders not yet involved in this effort become part of the development and adoption of the Mobile Trusted Module?
A: Companies having an interest in contributing to open mobile security standards development for embedded devices are encouraged to contact Trusted Computing Group at www.trustedcomputinggroup.org

Use Cases

Q. What are the new use cases for the MTM 2.0 specification?
A: While mobile financial services use cases were previously comprehended in the original MTM use cases, new use cases include secure provisioning of e-health applications, strong mobile authentication of enterprise employees, secure device and identity management, application store security, and secure interconnectivity in vehicles.

Q. Can you describe two examples of these new use cases?
A. One of the new use cases deals with e-Health applications for storing and transmitting sensitive patient health data that have security, privacy and interoperability

requirements. The challenge is how to leverage the ubiquity of mobile devices to securely support the transmission and sharing of patient health data among providers and services. Mobile devices with MTMs based on TCG specifications, a trusted execution environment, MTM application programming interface (API), and attestation capability, can facilitate secure mobile healthcare data and transactions. The user's health credentials are secured in the MTM, are securely processed in a trusted execution environment, and communications to health services are attested. TCG anticipated this to be a strong drive of MTM adoption; Gartner's Dataquest Insight puts mobile health amongst the Top Ten consumer mobile applications in 2012 (http://www.fiercewireless.com/press-releases/gartner-identifies-top-10-consumer-mobile-applications-2012?cmp-id=OTC-RSS-FW0).

Another use case deals with strong mobile enterprise authentication; the challenge is to enforce robust and scalable mobile user authentication. TCG's MTM can enable such authentication and replace expensive and cumbersome tokens. An enterprise user authentication certificate can be enrolled into the MTM to enable logical (and optionally physical) access to the corporate environment. An MTM-facilitated user authentication can reinforce an enterprise's defense-in-depth.

Existing MTM use cases, created with the original MTM specification, remain valid (http://www.trustedcomputinggroup.org/resources/mobile_phone_work_group_selected_use_case_analysis_specification_version_10). For example, the financial services industry needs methods to secure mobile payments at a comparable level of security to smart cards.

Refer to the published MTM 2.0 use cases and the existing use cases for more details. Add links

Q: Who do you anticipate would most benefit from the MTM 2.0 use cases and impending specification?
A: The target beneficiaries are the same stakeholders that were identified for MTM 1.0, with additional beneficiaries that can benefit from the newest use cases. Mobile equipment vendors, silicon vendors, BIOS/OS vendors, network service providers, third party service providers, and end users all benefit from correct and trustworthy behavior not only of the mobile device but of end-to-end mobile communication as a whole.

Of course, the main beneficiary is the consumer, or end user of the mobile device. For example, user privacy and secure transactions could greatly benefit mobile device users