TPM 2.0 Mobile Architecture Frequently Asked Questions

December 2014

Executive Summary:
The Trusted Computing Group has published two Trusted Platform Module (TPM) 2.0 Mobile Specifications:

TPM 2.0 Mobile Reference Architecture
TPM 2.0 Mobile Command Response Buffer Interface

The TPM 2.0 Mobile Reference Architecture Specification defines architecture for the implementation of a TPM 2.0 Library Specification-compliant TPM executing within a Protected Environment in mobile platforms. It includes examples of several implementation approaches.

The Command Buffer Response (CRB) Interface is an interface between a TPM and software and is intended to work with a large number of implementation options. With the CRB Interface it is possible to write a driver that can interact with a TPM, whether implemented as a discrete component on a peripheral bus, or in an execution mode in a Protected Environment. The CRB Interface can be implemented on any TPM architecture, including PC client.

Further to the precursor Mobile Trusted Module (MTM) v1.0 Specification, enhancements defined in the TPM 2.0 Mobile Specification include:

- A firmware TPM 2.0 Mobile architecture implementable in a system-on-a-chip isolated Protected Environment
- Revised definitions of the inherently trusted Roots of Trust
- Enhancements to the availability of TPM 2.0 Mobile to trusted applications
- Enhanced authorization for improved TPM 2.0 Mobile management
- Support for algorithm agility
- Secure Boot and Measured Boot

The intended mobile platforms for these specifications range from the most basic ebook readers, to basic phones and feature phones, up to smartphones and tablets.

The security services that the TPM 2.0 Mobile Specifications facilitate are aimed at consumers (end users), enterprises, mobile device manufacturers, mobile network operators, mobile service providers, the public sector, and others.

Standardized mobile endpoint security provides essential TPM security services for a wide range of mobile use cases and applications. It enables protection of private and sensitive assets, cross-platform security compatibility, and interoperability across mobile device types.

TPM 2.0 Mobile Architecture Frequently Asked Questions

Q. Why were the TPM 2.0 Mobile Specifications developed?
A. One of the most rapidly developing sectors of computing is mobile. Mobile communications evolution has introduced completely new classes of devices, architectures, use cases, challenges and opportunities. Modern mobile platforms have rapidly evolved into increasingly open and powerful computing environments and have already replaced traditional PCs as the platform of choice. The rise in mobile device usage also comes with a commensurate requirement for mobile platforms to securely underpin and support many types of applications.

With all of this in mind, the newest mobile specifications adapt mechanisms specified in the latest TPM 2.0 Library Specification to extend the latest Trusted Computing concepts into modern mobile platforms.

Q. Who benefits from the TPM 2.0 Mobile Specifications?
A. The main beneficiaries are the consumers (end users) and enterprises who require enhanced mobile device integrity, trustworthy acquisition and use of mobile applications and mobile services, including enterprise services, and protection of private data assets. The public sector can also benefit by hardening the mobile security aspects of their public services. Mobile device manufacturers, suppliers, mobile network operators and mobile service providers are both ecosystem facilitators and beneficiaries. See the Mobile Trusted Module 2.0 Use Cases for such stakeholder (use case actor) roles.

Q. What can the TPM 2.0 Mobile Specifications be used for in practice?
A: Mobile device manufacturers can implement the TPM 2.0 Mobile Specifications in products to facilitate robust device integrity and identity, to facilitate remote attestation (evidence of device integrity to third parties such as service providers), to facilitate secure environments for Trusted Applications, and to facilitate secure storage of credentials and data.

In enterprise there is the Bring Your Own Device (BYOD) trend whereby employees are bringing their personal devices to work and accessing corporate resources with the same devices. Enterprises want the cost-savings and efficiency that BYOD offers and to do so must securely manage access to corporate networks to maximize the value to staff, contractors, and even guests with mobile devices, while minimizing risk to the organization.

The public sector is placing greater emphasis on utilization of trustworthy mobile technology for reinforcing the security of critical infrastructure, healthcare data, and emergency response services.

Q. How can mobile device manufacturers use the TPM 2.0 Mobile Specifications?
A. Mobile device manufacturers are aware of the security demanded of their products by mobile network operators, mobile services, enterprises and end users. These TPM 2.0 Mobile Specifications provide a standardized means for mobile device manufacturers to evolve their products to meet those security demands wherever TPM 2.0 Mobile is implemented in Protected Environments.

Q. Are the TPM 2.0 Mobile Specifications backwards compatible with MTM v1.0?
A. No. TPM 2.0 Mobile is significantly different from MTM v1.0 since the respective architectures differ. The TPM 2.0 Mobile architecture and data structures also differ in some details to the TPM 2.0 Library Specification. Therefore implementing TPM 2.0 Mobile requires the development of new firmware.

Q. What is the relationship between MPWG and the Trusted Mobility Solutions Work Group (TMS- WG)?
A. TMS-WG provides 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. TMS-WG is chartered to facilitate the demonstration of trusted mobility solutions that make use of the TCG capabilities developed by work groups such as Mobile Platform WG, and to provide comprehensive guidance on how these TCG technologies can be leveraged in mobile devices and enterprise networks. For more on TMS-WG, see their FAQ.

Q. Is TCG collaborating with other standardization bodies in the mobile ecosystem?
A. TCG has liaison relationships with several organizations for the purpose of coordinating specifications and for alignment of mutually interesting use cases. Open and interactive discussion between the liaising organizations overcomes gaps or overlaps in standardization work. Some examples:

- TCG has liaised with GlobalPlatform on alignment and compatibility of TPM 2.0 Mobile and GlobalPlatform Trusted Execution Environment (TEE) so that TPM 2.0 Mobile could be implemented as a Trusted Application in a TEE in a standard manner.
- TCG has liaised with Mobey Forum, a global, bank-driven business association working to accelerate the evolution and adoption of mobile financial services. The TPM 2.0 Mobile use cases include secure mobile banking and payment; TCG's Trusted Mobility Services (TMS) Work Group is working closely with Mobey Forum in terms of BYOD and mobile payment use cases.
- TMS-WG is actively pursuing further liaisons with other industry organizations.

Q. How have end users responded to the latest mobile trusted computing developments?
A. End users have responded positively. For example, RSA Conference delegates have reacted supportively to Trusted Computing-enabled Secure Boot and to BYOD exhibits involving mobile devices.

Q. If mobile platforms ship before a certification program is available, how do we know these are compliant with the TPM 2.0 Mobile Specifications?
A. Vendors will indicate their compliance with TCG specifications.