TRUSTED COMPUTING GROUP WHITE PAPER

June 2012

TPM MOBILE with Trusted Execution Environment for Comprehensive Mobile Device Security

In this paper...

- The Need for a "TPM"
- The TPM MOBILE 1.0
- Running a TPM MOBILE 1.0 Instance in a TEE

Trusted Computing Group

3855 SW 153rd Drive
Beaverton, OR 97006

Tel (503) 619 – 0562
Fax (503) 644 – 6708

admin@trustedcomputinggroup.org
www.trustedcomputinggroup.org

TPM MOBILE formerly referenced as MTM

Introduction

In the past few short years the way we go about our daily lives has been fundamentally transformed by the growth and development of Smart Connected Devices – principally smart phones and tablets. We can access our bank accounts, our personal networks and our business documents wherever and whenever we please.

This added richness and connectivity also poses a problem though: increased malware. In order to take full advantage of the potential of these devices we must be able to control those risks, and two key platform security technologies have emerged from the Trusted Computing Group and GlobalPlatform standards initiatives which address the increasing set of software threats that smart connected devices face.

This whitepaper introduces how GlobalPlatform Trusted Execution Environment (TEE) and Trusted Computing Group Mobile Trusted Module (TPM MOBILE) can work together in mobile devices to provide security, peace of mind and enhanced services to users.

The need for a 'TPM'

Many types of devices are constrained in space, cost or power dimensions that make the use of a discrete Trusted Platform Module chip (TPM) difficult. However advances in on-processor technologies such as the TEE, combined with the flexibility of the TPM protocols mean that it is possible to implement the TPM as an integrated solution or in firmware.

In addition, as many more devices of different kinds begin to join together in networks, particularly in BYOD corporate scenarios, it is essential to enable new devices to participate in existing networks by implementing a diverse range of existing protocols including Trusted Network Connect (TNC) or measurement functionality.

> **… advances in on-processor technologies such as the TEE, combined with the flexibility of the TPM protocols mean that it is possible to implement the TPM as an integrated solution or in firmware.**

The TPM MOBILE 1.0

The Mobile Trusted Platform Module (TPM MOBILE) is a security component and approved TCG specification for use in mobile devices. Its origin lies in the TPM v1.2 and is intended to provide the same security and protocol interoperability, but with some enhancements for mobile devices:

1. The concept of **secure boot** is introduced i.e., the boot sequence is not only measured, but also

halted when non-approved software is detected. This improves the integrity of mobile (or ‘in-field’) devices and is a vital building block for security services or those subject to regulatory approvals.

2. The specification explicitly supports implementation of the TPM MOBILE in alternative implementations including as software. This makes it possible for device manufacturers to add the TPM MOBILE alongside existing device security. Such an alternative implementation may be considered a ‘firmware TPM’.

3. The reference architecture takes into account the support of several parallel TPM MOBILE instances in the same device that can be used to secure different stakeholders in the device while still adhering to a range of TCG specifications.

The GlobalPlatform TEE

The GlobalPlatform Trusted Execution Environment (TEE) defines a standardized isolation environment for Systems on Chip (SoC) in which sensitive code, data and resources are processed away from the main operating environment, software and memory on the device. This isolation is enforced by hardware architecture and the boot sequence uses a hardware root of trust in the SoC package making it highly robust against software and probing attacks. In addition, code running in the TEE and using protected resources (known as ‘Trusted Applications’) is cryptographically verified prior to execution, leading to high integrity assurance.

Because it provides an isolated runtime environment entirely inside the SoC (processor chip), the TEE enables advanced device or peripheral security use cases such as securing the user interface, or controlling access to an NFC chip. As such the TEE can be used as a distinct security coprocessor or to provide a trusted ‘bridge’ between the user and other security technologies such as secured UI or OS user permissions on one side, and Secure Element access control on the other.

The main operating system and rich applications then run as normal on the device, accessing the functionality of the Trusted Applications via a standardized ‘Client API’. Trusted Applications are written to an ‘Internal API’ which ensures portable trustworthy access to secure resources, cryptographic operations and secure storage regardless of the underlying SoC hardware.

Running a TPM MOBILE 1.0 instance in a TEE

Software organization

In the case of a ‘firmware TPM’, the TPM MOBILE functionality is implemented as a Trusted Application in the TEE. Executing an TPM MOBILE instance in this way requires several different pieces of software to work together to maintain system integrity.

The fundamental software building blocks are:

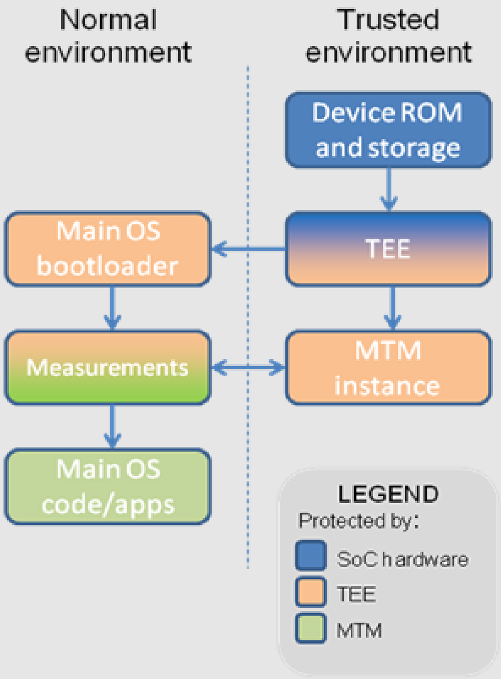
- Device ROM/boot code
- TEE kernel (for example GlobalPlatform TEE kernel) and system functions
- TPM MOBILE instance

This organization is shown in the figure 1 below. Once all these components are checked and running, the main OS boot sequence can be executed, loading and using an TPM MOBILE driver for measurement.

Security model

The security of the TPM MOBILE Trusted Application, and by extension the services that rely on it, starts with the boot process. In keeping with the fundamental principles of TCG, the TEE defines a hardware root of trust (usually an integrity key or value implemented inside the processor package) which underpins its boot security. From there progressive stages of the boot software are verified cryptographically to ensure that only correct, authorized software is executed in the device. This is shown diagrammatically in figure 1 below.

Figure #1: The boot process maintains device integrity right through to measured OS launch



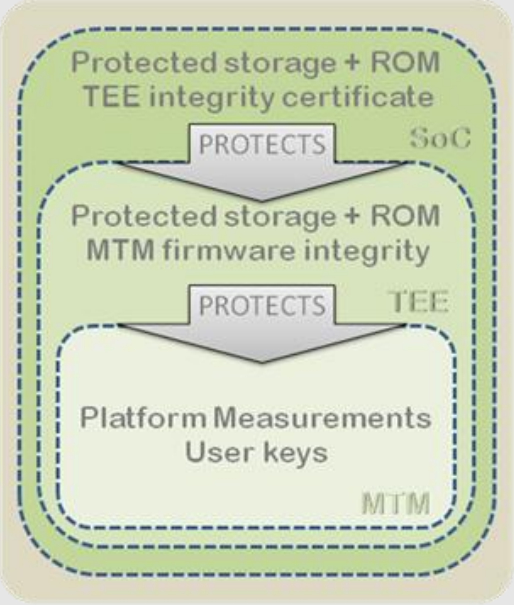
Once booted the TPM MOBILE functionality and cryptography can be accessed at any time by a call from the main operating system. However, although functionality is requested by the main operating system it is executed in the protected environment of the TEE, isolated by strong hardware mechanisms from the calling process.

In this way the device security is maintained at all times during the boot sequence. Starting with the mobile platform's base boot security, the secure boot process of the TEE completes before handing over to the TPM MOBILE instance to provide measured boot services for the main OS. This security 'bridge' provided by the TEE accommodates both the device's base security mechanisms and the TCG-based main OS security model simultaneously and so affords cooperative operation with minimal changes to software design.

The security model above works because the chain of trust from one component to the next is maintained and appropriately protected by the use of cryptography. While the specific details of implementations differ, all compliant implementations conforming to the GlobalPlatform TEE specification will provide the same fundamental level of protection to the TPM MOBILE implementation running on them, ensuring reliable protection *and* portability across devices.

The diagram on the next page shows the protection hierarchy in a typical system and how the pieces work together to provide a strong chain of trust and protection for the TPM MOBILE data and operation.

Figure #2: Device protection hierarchy



Conclusion

The TPM MOBILE standard continues to be developed specifically in line with other mobile device security technologies such as the GlobalPlatform TEE in order to create something which is not just secure in principle, but secure and usable in real devices. By deploying the TPM MOBILE instance as a trusted application on a GlobalPlatform TEE, users and services are afforded practical, secure and interoperable access to TCG standards on mobile devices.

Further Reading
The Trusted Computing Group TPM MOBILE:
http://www.trustedcomputinggroup.org/developers/mobile

TPM MOBILE Use Cases
http://www.trustedcomputinggroup.org/files/static_page_files/FA751710-1A4B-B294-D0F1698506A36AE8/TCG%20Mobile%20Trusted%20Module%202%200%20Use%20Cases%20v1%200.pdf

The GlobalPlatform TEE
http://www.globalplatform.org/documents/GlobalPlatform_TEE_White_Paper_Feb2011.pdf