AUGUST 2018

TRUSTED COMPUTING GROUP®

TCG Guidance

For TPM 2.0 Mobile Implementations

Trusted Computing Group
3855 SW 153rd Drive
Beaverton, OR 97003
Tel (503) 619-0505
Fax (503) 644-6708
admin@trustedcomputinggroup.org
www.trustedcomputinggroup.org

THE RISE OF MOBILE DEVICES

Today, both at work and at home, more users than ever before rely on their mobile phones, tablets, and other mobile devices to keep in touch and get things done. With Bring Your Own Device, Choose Your Own Device, and other Enterprise- Owned Device models, business and personal data now coexist on the same device. More and more devices also means a growing attack surface for those who aim to cause harm.

The rise in mobile device usage comes with a commensurate requirement for mobile platforms to provide a secure foundation for many types of applications.

The rise in mobile device usage comes with a commensurate requirement for mobile platforms to provide a secure foundation for many types of applications. However, while there are a growing number of software-based security approaches and vendor solutions for the many bits and pieces of the mobile ecosystem, mobile device hardware itself has remained vulnerable to a variety of attacks.

For designers, manufacturers, system integrators, application developers, mobile network operators, and mobile service providers 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 Trusted Computing Group (TCG) has published a collection of specifications that define trusted computing technologies for mobile platforms. These specifications are applicable to all mobile devices (smartphones, feature phones, basic phones, etc.).

In collaboration with GlobalPlatform on alignment and compatibility of TPM 2.0 Mobile and GlobalPlatform Trusted Execution Environment (TEE), TCG has ensured TPM 2.0 Mobile could be implemented as a Trusted Application in a TEE in a standardized manner.

MOBILE APPLICATIONS

End users ultimately benefit from mobile applications that provide enhanced features, such as e-financial services, in a way that is both highly-secure and practical.

Trusted mobile platforms provide key benefits, such as device integrity, for mobile device operations, and offer significant improvement in securing device hardware. 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. Widespread adoption of standardized interfaces, however, is a prerequisite for the development of mobile applications which use the core TPM capabilities.

There are several ways to move toward widespread adoption:

- OEMs and system integrator implementation of the FAPI specifications and underlying TPM Interface specifications in the rich environment to ensure that applications have access to TPM services through a standard interface across multiple platforms.

- Application Developers being able to develop mobile applications that use the FAPI interface to access the TPM, and other building blocks of the trusted mobile platform, to provide a variety of services with security assurances.

REFERENCE DOCUMENTS

Mobile Trusted Module Use Cases
Reviews a broad range of usage scenarios where TCG MTM security technology can be applied in the mobile embedded devices context and ecosystem.

TMS Use Cases – Bring Your Own Device (BYOD)
Describes a broad range of scenarios where TCG technologies is applicable in the mobile ecosystem.

TCG Multiple Stakeholder Model
Introduces several use cases that illustrate support considerations for multiple stakeholders to coexist on a mobile platform.

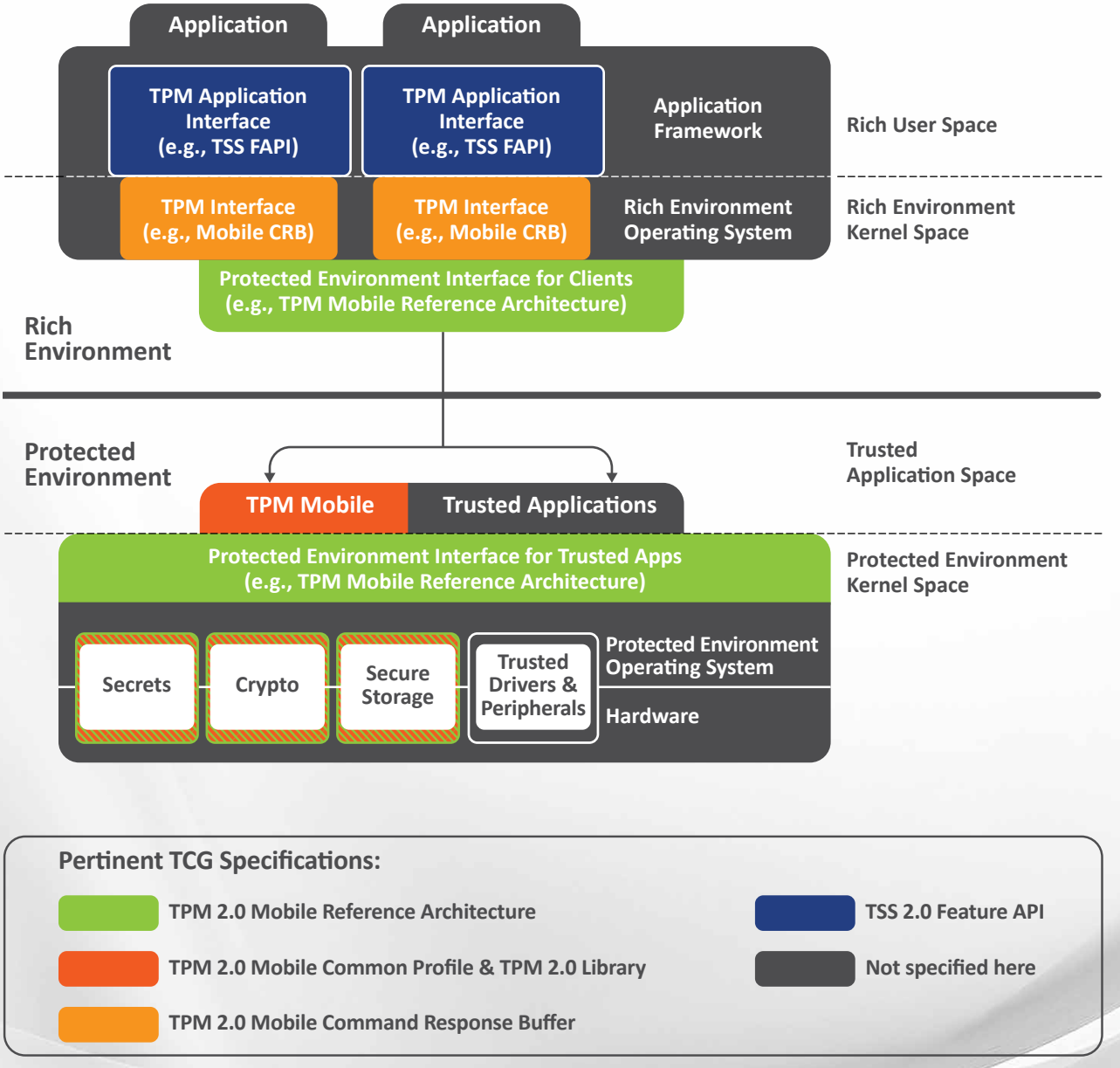
TPM 2.0 Mobile Architecture FAQs
A response guide to the most Frequently Asked Questions on TPM 2.0 Mobile Architecture

THE TRUSTED MOBILE PLATFORM

The accompanying image provides an example of a notional architecture that can be used to implement a trusted mobile platform.

Note, there are many possible architectures and implementations, using technologies such as hypervisors, micro-kernels, hardware mechanisms, and others, that can support trusted mobile platforms. In this example, the TPM 2.0 is hosted by a Protected Environment, which is isolated from the Rich Execution Environment (REE) of the mobile platform.

For more architecture examples, see the TPM 2.0 Mobile Reference Architecture Specification.



REFERENCES

The Trusted Computing Group has published three Trusted Platform Module (TPM) 2.0 Mobile Specifications. These resources provide reference on how to implement a trusted mobile platform:

TPM 2.0 MOBILE REFERENCE ARCHITECTURE SPECIFICATION

Provides a normative reference on how to implement mobile platform architecture to support a TPM Mobile. The TPM Mobile executes within a Protected Environment which is defined by a collection of security requirements. The Mobile Reference Architecture includes an informative example of a Protected Environment as an implementation of the ***Global Platform Trusted Execution Environment (TEE) System Architecture*** and related API specifications, such as the ***TEE Client API Specification***, ***TEE Internal API Specification***, and others. Read more at: https://trustedcomputinggroup.org/tpm-2-0-mobile-reference-architecture-specification

TCG TPM 2.0 MOBILE COMMON PROFILE SPECIFICATION

Defines a profile of the TPM 2.0 Library Specification that is applicable to all mobile devices that claim conformance to the ***TPM 2.0 Mobile Reference Architecture***, and is optimized for ease-of-implementation in feature phones, basic phones, eBook readers, and other similar constrained mobile devices. The specification defines the actual TPM Mobile implementation (platform constants, algorithm support, commands, and required resources). Read more at: https://trustedcomputinggroup.org/tcg-tpm-2-0-mobile-common-profile/

TCG TPM 2.0 MOBILE COMMAND RESPONSE BUFFER INTERFACE SPECIFICATION

Defines an interface between a TPM and software. This interface is the Command/Response Buffer Interface (CRB). The ***TCG Software Stack (TSS) 2.0 Feature API Specification (FAPI)*** defines a very high level API with the intention of supporting most of the commands that an application programmer would need to use the services of the TPM. Read more at:
https://trustedcomputinggroup.org/tpm-2-0-mobile-command-response-buffer-interface-specification/

For recent updates to this guidance, visit https://trustedcomputinggroup.org/work-groups/mobile/.

Note: *Implementers of portions of this guidance may require access to low level platform hardware, software, and documentation.*