R E F E R E N C E

Multiple Stakeholder Model

Published

Family "2.0"

Level 00 Revision 3.40

2 May 2016

Contact: admin@trustedcomputinggroup.org

TCG PUBLISHED

TCG

Disclaimer

THIS REFERENCE DOCUMENT IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, WHITE PAPER, OR SAMPLE. Without limitation, TCG disclaims all liability, including liability for infringement of any proprietary rights, relating to use of information in this reference document, and TCG disclaims all liability for cost of procurement of substitute goods or services, lost profits, loss of use, loss of data or any incidental, consequential, direct, indirect, or special damages, whether under contract, tort, warranty or otherwise, arising in any way out of use or reliance upon this document or any information herein.

No license, express or implied, by estoppel or otherwise, to any TCG or TCG member intellectual property rights is granted herein.

Contact the Trusted Computing Group at www.trustedcomputinggroup.org for information on TCG licensing through membership agreements.

Any marks and brands contained herein are the property of their respective owners.

Acknowledgments

The TCG wishes to thank all those who contributed to this reference document.

Ronald Aigner	Microsoft
Bo Bjerrum	Intel Corporation
Alec Brusilovsky	InterDigital Communications, LLC
David Challener	Johns Hopkins University, Applied Physics Lab
Michael Chan	Samsun Semiconductor Inc. / Qualcomm Inc.
Cedric Colnot	NXP Semiconductors
Carlin Covey	NXP Semiconductors
Jan-Erik Ekberg	Nokia
Paul England	Microsoft
Andreas Fuchs	Fraunhofer Institute for Secure Information Technology (SIT)
Jon Gaeter	ARM Ltd. / Trustonic Ltd
Steve Hanna	Infineon Technologies North America Corp.
Laszlo Hars	The Boeing Company
Carey Huscroft	HP Inc.
Bill Jacobs	Cisco
Greg Kazmierczak	Wave Systems
Seigo Kotani	Fujitsu Limited
Sung Lee	Intel Corporation
Ira McDonald	High North Inc.
Kathleen McGill	Johns Hopkins University, Applied Physics Lab
John Mersh	ARM Ltd.
Hadi Nahari	NVIDIA Corp
Ken Nicolson	Panasonic
Carlton Northern	The MITRE Corporation
Niall O'Donoghue	Microsoft
Michael Peck	The MITRE Corporation
Gilles Peskine	Trustonic Ltd
Stanley Potter	United States Government
Graeme Proudler	HP Inc.
Emily Ratliff	Advanced Micro Devices, Inc.
Joshua Schiffman	Advanced Micro Devices, Inc.
Ariel Segall	The MITRE Corporation
Hervé Sibert	STMicroelectronics
Sylvain Trosset	Trustonic Ltd
Janne Uusilehto	Microsoft
Paul Waller	CESG
Monty Wiseman	Intel Corporation
David Wooten	Microsoft
Esteban Yepez	Sandia National Laboratories

Table of Contents

List of Figures

List of Tables

1 Scope and Audience

This document describes the Multiple Stakeholder Model, which provides guidance to allow multiple stakeholders to coexist safely on a mobile platform. This document is coherent with the TPM 2.0 Mobile Reference Architecture [2]. This guidance is applicable to all mobile devices (smartphones, feature phones, basic phones, etc.) and may be useful for other computing devices. The target audience for this document includes designers, developers, and implementers of Trusted Computing technologies in mobile platforms.

This reference document is not a TCG Specification and therefore is not normative.

1.1 References

[1] Trusted Computing Group, Trusted Platform Module, Version 2.0, Parts 1-4

[2] Trusted Computing Group, TPM 2.0 Mobile Reference Architecture v2r142, December 2014

[3] Trusted Computing Group, TPM 2.0 Mobile Common Profile v2r29, July 2015, work-in-progress, public review draft

[4] Trusted Computing Group, TNC Architecture for Interoperability v1.5, May 2012

[5] Trusted Computing Group, Mobile Trusted Module 2.0 Use Cases, May 2011

[6] Trusted Computing Group, TMS Use Cases – Bring Your Own Device (BYOD), October 2013

[7] Trusted Computing Group, TSS TAB and Resource Manager, February 2015, work-in-progress public review draft

[8] Trusted Computing Group, TSS Feature API, November 2014, work-in-progress public review draft

[9] Global Platform Device Technology TEE System Architecture, GPD_SPE_009 [INFORMATIVE]

[10] Trusted Computing Group, TSS System Level API and TPM CTI, January 2015.

[11] Unified EFI Forum, UEFI Specification version 2.5, [INFORMATIVE], April 2015

[12] IETF, RFC 4122, A Universally Unique IDentifier (UUID) URN Namespace, July 2005

[13] Trusted Computing Group, Virtualized Platform Architecture Specification, September 2011

[14] NIST Special Publication SP800-90A, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, February 2013

[15] NIAP Protection Profile for Mobile Device Fundamentals Version 2.0, September 2014

[16] NIST FIPS Publication 140-2 Security Requirements for Cryptographic Modules, May 2001

[17] NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments, September 2012.

[18] IETF RFC 3552, Guidelines for Writing RFC Text on Security Considerations, July 2003

[19] NIST Special Publication 800-124, Revision 1, Guidelines for Managing the Security of Mobile Devices in the Enterprise, June 2013

[20] Trusted Computing Group, Trusted Multi-Tenant Infrastructure Reference Framework, December 2013

[21] Mobey Forum, Mobile Financial Terms Explained, 2014. [ONLINE] Available at: http://www.mobeyforum.org/whitepaper/mobile-financial-terms-explained-2/

[22] Mobey Forum, Prepaid Mobile Wallet, 2014. [ONLINE] Available at: http://www.mobeyforum.org/whitepaper/prepaid-mobile-wallet/

[23] Mobey Forum, Mobile Wallet Part 5: Strategic Options for Banks, 2013. [ONLINE] Available at: http://www.mobeyforum.org/whitepaper/mobile-wallet-part-5-strategic-options-for-banks/

[24] Mobey Forum, Mobile Wallet Part 4: Structures and Approaches, 2013. [ONLINE] Available at: http://www.mobeyforum.org/whitepaper/structures-and-approaches-the-changing-face-of-mobile-wallets/

[25] Trusted Computing Group, Glossary, [ONLINE] Available at: http://www.trustedcomputinggroup.org/developers/glossary

[26] ARM, ARM TrustZone, [ONLINE] Available at:http://www.arm.com/products/processors/technologies/trustzone/index.php

[27] IBM. What is an Address Space? [ONLINE] Available at: http://www-01.ibm.com/support/knowledgecenter/zosbasics/com.ibm.zos.zconcepts/zconcepts_82.htm

[28] Global Platform, Secure Element Secure Element Access Control v1.0, GPD_SPE_013

[29] IETF, RFC 4301 – 4309, Security Architecture for the Internet Protocol, December 2005

[30] IETF, RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2, August 2008

[31] Virtual Private Network Consortium, VPN Protocols, [ONLINE] Available at: http://www.vpnc.org/vpn-standards.html

[32] ETSI, ETSI TR 102 216 v3.0.0, Smart cards; Vocabulary for Smart Card Platform specifications, September 2003

[33] SD Association, SD Standards Overview, [ONLINE] Available at: https://www.sdcard.org/developers/overview/

[34] Department of Defense, DoD Common Access Card, [ONLINE] Available at: http://www.cac.mil/

[35] NIST, FIPS Publication 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors, August 2013

[36] Trusted Computing Group, TCG Storage Security Storage Class: Opal, August 2015

[37] IETF, RFC 5424, The Syslog Protocol, March 2009

[38] Google, Inc. Logger | Android Developers, [ONLINE] Available at: http://developer.android.com/reference/java/util/logging/Logger.html

[39] ISO, ISO/IEC 15408-1, Information technology — Security Techniques — Evaluation criteria for IT Security — Part 1:Introduction and general model

[40] NIAP Protection Profile for Mobile Device Management, Version 1.1, March 2014

[41] Open Mobile Alliance, OMA Device Management V2.0, January 2015, [ONLINE] Available at: http://technical.openmobilealliance.org/Technical/technical-information/release-program/current-releases/oma-device-management-v2-0.

[42] Intel, Intel Trusted Execution Technology Software Development Guide, May 2014

[43] Intel, Intel Software Guard Extensions Programming Reference, October 2014

[44] Intel, Intel Virtualization Technology (Intel VT). [ONLINE] Available at: http://www.intel.com/content/www/us/en/virtualization/virtualization-technology/intel-virtualization-technology.html

[45] ARM. Virtualization Extensions. [ONLINE] Available at: http://www.arm.com/products/processors/technologies/virtualization-extensions.php

[46] SELinux Project. SELinux Project Main Page. [ONLINE] Available at: http://selinuxproject.org/page/Main_Page

[47] Global Platform. Global Platform made simple guide: Secure Element, [ONLINE] Available at: https://www.globalplatform.org/mediaguideSE.asp

[48] Trusted Computing Group. Self-Encrypting Drives Take off for Strong Data Protection, [ONLINE] Available at: http://www.trustedcomputinggroup.org/community/2010/03/selfencrypting_drives_take_off_for_strong_data_protection

[49] IETF, RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008

[50] PCI Security Standards Council, Payment Card Industry (PCI) Hardware Security Module (HSM) Security Requirements

[51] Trusted Computing Group. Trusted Computing Group. [ONLINE] Available at: http://www.trustedcomputinggroup.org/

[52] IETF RFC 4949, Internet Security Glossary, Version 2, August 2007

[53] IETC RFC 7547, Management of Networks with Constrained Devices: Problem Statement and Requirements, May 2015

[54] Global Platform, Global Platform Device Technology TEE Sockets API v1.1, GPD_SPE_100

[55] Global Platform, Global Platform Device Technology Trusted User Interface API v1.0, GPD_SPE_020

[56] Global Platform, Global Platform Device Technology TEE Secure Element API v1.1, GPD_SPE_024

[57] IETF, RFC 6960, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP June 2013

[58] ISO, ISO/IEC 18031, Information technology — Security Techniques — Random bit generation

[59] ISO/IEC 19790, Information technology - Security Techniques - Security requirements for cryptographic modules

[60] ISO/IEC 31000, Risk management – Principles and guidelines

[61] ISO/IEC 31010, Risk management – Risk assessment techniques

2 Basic Definitions

Table 1 – Basic Definitions

Glossary Term	Description
Attestation	The process of vouching for the accuracy of information. External entities can attest to protected locations and Roots of Trust. A platform can attest to its description of platform characteristics that affect the integrity (trustworthiness) of a platform. Both forms of attestation require reliable evidence of the attesting entity [25].
Communications Carrier (CC)	An entity that provides wireless communications (e.g. Wi-Fi, Cellular) functionality to the mobile device [6].
Critical Security Parameter (CSP)	Security-related information (e.g., secret and private cryptographic keys, and authentication data, for example, passwords and Personal Identification Numbers [PINs]) whose disclosure or modification can compromise the security of a cryptographic module [16], [59].
Device Manufacturer (DM)	The manufacturer or brand of a Device, typically an Original Equipment Manufacturer (OEM) [2]. The DM is also commonly referred to as a Vendor.
Device Owner (DO)	The legal owner of the device. The device owner may be an End User (consumer), a communications carrier, or some other entity. The Device Owner can customize all aspects of the TPM except the Platform Hierarchy [2].
Digital Signature	A value computed with a cryptographic algorithm and associated with a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity [52].
End User	The ultimate consumer of mobile applications and services, particularly the user for whom the device is designed. The End User can also be the Device Owner [2].
Endorsement Key (EK)	An asymmetric key pair composed of a public key (EKpu) and private (EKpr). The EK is used to recognize a genuine TPM. The EK is used to decrypt information sent to a TPM in the Privacy CA and DAA protocols, and during the installation of an Owner in the TPM [25].
Enhanced Authorization(EA)	A TPM 2.0 Library capability that allows entity-creators or administrators to require specific tests or actions to be performed before an action can be completed [1].
Man-In-The-Middle (MITM) Attack	A form of active wiretapping attack in which the attacker intercepts and selectively modifies communicated data to masquerade as one or more of the entities involved in a communication association [52].
Measured Boot	A boot process where images are measured (for example by calculating their hashes) and the measurements are extended into

	the PCRs of a TPM [2].
Mobile Common Profile	TPM profile that is applicable to all mobile devices (smartphones, feature phones, basic phones, etc.) 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[3].
Mobile Device	A physical entity encompassing all the hardware, firmware, software, and data necessary for it to function and provide services to an end user. Also known as a Mobile Platform [2].
Mobile Network Operator (MNO)	Telecommunications network operator [6] – synonym for Communications Carrier [6].
Platform Configuration Register (PCR)	A shielded location within a TPM Mobile containing a digest of integrity digests [25].
Protected Environment	A functional element that has its own execution and memory resources that are isolated from other components [2].
Public Key Infrastructure	A public key infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption [49].
Residual Risk	The portion of an original risk or set of risks that remains after countermeasures have been applied [52].
Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result (see: residual risk) [52].
Root of Trust (RoT) component	A component that must always behave in the expected manner, because its misbehavior cannot be detected. The complete set of Roots of Trust has at least the minimum set of functions to enable a description of the platform characteristics that affect the trustworthiness of the platform [25].
Secure Boot	A boot process where each image is validated before execution [2].
Secure Element	A tamper-resistant platform (typically a one chip secure microcontroller) capable of securely hosting applications and their confidential and cryptographic data (e.g. key management) in accordance with the rules and security requirements set forth by a set of well-identified trusted authorities [47]. A Secure Element is an example of a Protected Environment [2] implementation.
Security Policy	A definite goal, course, or method of action to guide and determine present and future decisions concerning security in a system [52]. A set of policy rules (or principles) that direct how a system (or an organization) provides security services to protect sensitive and

	critical system resources [52].
Self-Encrypting Drive	A hard drive that encrypts data on the fly in hardware, transparent to the user and system [48].
Stakeholder	A person or group that has an investment, share, or interest in a given computing system, for example, a business or industry.
Subscriber Identity Module (SIM)	An integrated circuit chip that is intended to store securely the international mobile subscriber identity (IMSI) number and its related key, which are used to identify and authenticate subscribers on a mobile device [21]. The SIM circuit is part of the function of a Universal Integrated Circuit Card (UICC) physical smart card. SIM cards are designed to be transferable between different mobile devices.
Threat	A potential for violation of security, which exists when there is an entity, circumstance, capability, action, or event that could cause harm [52]. Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or an enterprise through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service [17], [60], [61].
Transitive Trust	In this process, the Root of Trust gives a trustworthy description of a second group of functions. Based on this description, an interested entity can determine the trust it is to place in this second group of functions. If the interested entity determines that the trust level of the second group of functions is acceptable, the trust boundary is extended from the Root of Trust to include the second group of functions. In this case, the process can be iterated. The second group of functions can give a trustworthy description of the third group of functions, etc. Transitive trust is used to provide a trustworthy description of platform characteristics, and also to prove that non-duplicable keys are non-duplicable [25].
Trust	A feeling of certainty (sometimes based on inconclusive evidence) either (a) that the system will not fail or (b) that the system meets its specifications (i.e., the system does what it claims to do and does not perform unwanted functions) [52].
Trust Anchor	An established point of trust (usually based on the authority of some person, office, or organization) from which a certificate user begins the validation of a certification path [52].
Trust Assertions	A set of attributes or claims regarding the state of an object or actor [6].
Trusted Execution Environment (TEE)	Isolated execution environment where trusted code can be executed and isolated from the rich mobile device environment. A Global Platform Trusted Execution Environment (TEE) [9] is one possible

	implementation of a Protected Environment [2][9].
Trusted Network Communications (TNC)	A TCG workgroup that defines and promotes an open solution architecture for endpoint integrity that enables network operators to enforce policies regarding endpoint integrity at or after network connection. TNC standards ensure multi-vendor interoperability across a wide variety of endpoints, network technologies, and endpoints.
Trusted Path	A mechanism by which a person or process can communicate directly with a cryptographic module and that can only be activated by the person, process, or module, and cannot be imitated by untrusted software within the module [52]. A means to ensure the user can communicate with the target that the user intends with confidence [39].
Trusted Shared Component	A trusted shared component is a software or hardware component that is utilized by more than one stakeholder and relied upon to provide the Recommended Capabilities of the Multiple Stakeholder Model.
Trusted System	A system that operates as expected, according to design and policy, doing what is required -- despite environmental disruption, human user and operator errors, and attacks by hostile parties -- and not doing other things [52].
TPM Software Stack	Untrusted software services that facilitate the use of the TPM and do not require the protections afforded to the TPM [25].
Vulnerability	A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy [52]. Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source [17], [60], [61].

3 Acronyms

Table 2 – Acronyms

BYOD	Bring Your Own Device [6]
CC	Communications Carrier [6]
CAC	Common Access Card [34]
EA	Enhanced Authorization [1]
EK	Endorsement Key [25]
fTPM	Firmware TPM [2]
GP SE	Global Platform Secure Element [28]
HSM	Hardware Security Module [50]
IPSec	Internet Protocol Security [29]
MITM	Man-In-The-Middle (Attack) [52]
MNO	Mobile Network Operator [6]
MSM	Multiple Stakeholder Model [6]
PIV	Personal Identity Verification [35]
PKI	Public Key Infrastructure [49]
RoT	Root(s) of Trust [25]
pTPM	Physical Trusted Platform Module [13]
SED	Self-Encrypting Drive [48]
SIM	Subscriber Identity Module [21]
SK	Storage Key [1]
TCG	Trusted Computing Group [51]
TLS	Transport Layer Security [30]
TNC	Trusted Network Communications [4]
TPM	Trusted Platform Module [1]
TSS	TPM Software Stack [7]

UICC	Universal Integrated Circuit Card [12]
VPN	Virtual Private Network [31]
vTPM	Virtual Trusted Platform Module [13]

4 Introduction

The Multiple Stakeholder Model (MSM) is an informative reference document that describes use cases, recommended capabilities, and various implementation alternatives for multiple stakeholders to coexist safely on a mobile platform. This document includes guidance on how to leverage Trusted Computing Group (TCG) specifications to realize each alternative. In particular, this document emphasizes the role of the Trusted Platform Module (TPM) [1], the Mobile Common Profile [3], and the Mobile Reference Architecture [2] specifications to support these capabilities for multiple stakeholders. The goal of the MSM is to provide trusted services, for example, TPM [1] and Trusted Network Communications (TNC) [4], in a secure and efficient manner to all interested stakeholders (both local and remote) for a given mobile device.

4.1 Assumptions

For all use cases and implementation alternatives described in this document, the following premises are assumed:

1. There is a Protected Environment [2] on the mobile platform, and the Device Manufacturer has installed a TPM within it.

2. All participating Stakeholders trust the Device Manufacturer and other providers of fundamental components, for example, hardware Roots of Trust [25] and Protected Environment [2] firmware.

4.2 Key Concepts and Technologies

There are several concepts and technologies that are fundamental to a trusted mobile platform. The following sections present brief introductions to these concepts and technologies with references that provide detail on each topic.

4.2.1 Roots of Trust

A Root of Trust (RoT) is a component that must always behave in the expected manner, because its misbehavior cannot be detected [25]. Generally, it is the smallest distinguishable set of hardware, firmware, and/or software that performs one or more security-specific functions, for example, measurement, storage, reporting, verification, and/or update [2]. The complete set of RoT has at least the minimum set of functions to enable a description of the platform characteristics that affect the trustworthiness of the platform.

4.2.2 Transitive Trust

In the Transitive Trust process, the RoT gives a trustworthy description of a second group of functions. Based on this description, an interested entity can determine the trust it is to place in this second group of functions. If the interested entity determines that the trust level of the second group of functions is acceptable, the trust boundary is extended from the Root of Trust to include the second group of functions. This process can be iterated. The second group of functions can give a trustworthy description of the third group of functions, etc. Transitive trust is used to provide a trustworthy description of platform characteristics [25]. This process allows the trustworthy description to encompass a much larger portion of the platform than the minimal set of RoT.

4.2.3 Secure Boot

Secure Boot [2] is a process in which every software image is validated before execution. The boot process begins with execution of the Boot ROM. Whenever an additional module of code is loaded, it is measured and verified. If verification is successful, execution continues. Otherwise, the mobile device enters some remediation state. If the Boot ROM is immutable and trustworthy, any code that fails validation cannot be launched during the Secure Boot process. Secure Boot is sometimes used only for the early-booted device firmware up to the point of launching the main operating system (OS) boot loader [2].

4.2.4 Measured Boot

Measured Boot [2] is a process that can be optionally performed during and after the Secure Boot [2] process once a TPM [2] is available. In this process, code and data modules are measured (for example by calculating their hashes), and the measurements are extended into the PCRs of a TPM [2]. Then, the code module is executed or the data is used regardless of the values of the measurements. These measurements may be used subsequently to perform binding or attestation, as defined by the TPM 2.0 Library Specification [1].

4.2.5 Trusted Platform Module

The TPM is an implementation of the functions defined in the TCG TPM 2.0 Library Specification [1]. The TPM includes some RoT, shielded locations, and protected capabilities. In general, the TPM provides a set of functions and data that enable platforms to be trustworthy [25]. The TPM provides methods for collecting and reporting the identities of hardware and software components of a platform for the purposes of establishing trust in that platform [1].

4.2.6 TPM Mobile

A TPM Mobile is an adaptation of the TPM for mobile platforms. The TPM Mobile Reference Architecture Specification [2] defines the reference architecture for the implementation of a TPM mobile. The architecture allows any possible implementation of a TPM Mobile that meets the security requirements, and several example implementations are included in informative appendices [2].

4.2.7 Trusted Network Communication (TNC)

TNC is a TCG workgroup that defines and promotes an open solution architecture for endpoint integrity that enables network operators to enforce policies regarding endpoint integrity at or after network connection [4]. These policies may involve endpoint integrity parameters spanning a range of system components (hardware, firmware, software and application settings). The TNC architecture focuses on interoperability of network access control solutions and on the use of trusted computing as the basis for enhancing security of those solutions. The TCG TNC Working Group has published several specifications on various roles, functions, and interfaces of TNC [4].

4.2.8 Protected Environment

A Protected Environment is a functional element that has its own execution and memory resources that are isolated from other components of a mobile device. The TPM 2.0 Mobile Reference Architecture [2] specifies a set of requirements that a Protected Environment must satisfy in order to host a TPM Mobile. The architecture allows any implementation of the Protected Environment that conforms to the specified security requirements. A Global Platform Trusted Execution Environment (TEE) [9] is one possible implementation of a Protected Environment.

4.2.9 Trusted Path

A Trusted Path is a mechanism by which a person or process can communicate directly with a cryptographic module and that can only be activated by the person, process, or module, and cannot be imitated by untrusted software within the module [52].. For the purposes of this document, this definition includes communication and connectivity paths from a human user interface, software instance, or hardware module that interacts with security functionality. For example, using a Trusted Path, a user can communicate with a secure application or an enterprise environment without fearing MITM attacks. Similarly, a sensor on the device can communicate confidentially with an application in a Protected Environment.

4.2.10 Trust Assertions

The TMS Use Cases – Bring Your Own Device (BYOD) reference document [6] thoroughly introduces Trust Assertions for the BYOD use case. A Trust Assertion consists of a set of attributes or claims regarding the state of an object or actor [6]. A Policy Decision Point (PDP) may use a Trust Assertion to make confidentiality, integrity, and availability assessments about an object or actor. The construction of a Trust Assertion relies on trusted building blocks. A trusted building block is a component or collection of components required to instantiate a Root of Trust. Typically platform-specific, one example is the code that is first executed by the main processor after the platform is reset and which determines how the main processor will perform its initial measurement for Measured Boot [25]. These Trust Assertions are useful for establishing trust between multiple stakeholders of a single mobile platform. This bilateral trust is part of the device integrity on which multiple stakeholders rely.

5 Use Cases

There are many use cases today for the MSM. This section provides a few examples to motivate the recommendations of this document. More detailed treatment of these and other mobile use cases can be found in the Mobile Trusted Module 2.0 Use Cases [5] and TMS Use Cases – Bring Your Own Device (BYOD) [6] documents.

5.1 Bring Your Own Device (BYOD)

The BYOD use case allows an employee, partner, contractor or guest to have an appropriate level of access to an enterprise network through their personal mobile devices [6]. While there are clear advantages for both enterprise and individuals, there are potential consequences of this convenience, including compromised corporate IT security and leakage of individuals' private data. The following list provides examples of concerns for various stakeholders of the BYOD use case:

- Enterprise stakeholders are concerned that BYOD mobile devices with breached integrity will introduce malware to the enterprise.

- Enterprise stakeholders are concerned that corporate secrets or other intellectual property will be leaked from BYOD systems.

- Device Owners (i.e., End Users) are concerned that Enterprise monitoring software will leak private data from their personal mobile device.

5.2 Financial Services

Financial services in the mobile context imply the capability of the user to connect to their personal banking services or to perform financial transactions via their mobile device. Such services require user authentication for establishing sessions and authorization for approving transactions. Many existing financial services use their own proprietary methods and protocols for authentication and authorization. The intersection of the financial and mobile industries is a complex domain. The Mobey Forum, a global industry association, has published a glossary of common terms in the mobile and financial industries in order to provide clarity for interested readers and implementers [21].

In recent years, mobile financial services have evolved from browser-based transactions to wider use of dedicated applications. The integrity of these financial applications is imperative. Users would like to be certain the financial applications are authentic, which may mean downloading them from an app store or directly from the financial institution. This mobile industry practice of downloading from an app store is a departure from the PC approach in which users are typically advised to "go to the source" (i.e., developer of the application or OS).

The Mobile Wallet is an emerging capability in the financial services category. Several mobile wallet solutions exist today. However, many financial institutions and partnering service providers are still devising strategies to optimize the Mobile Wallet market [22], [23]. Today's solutions are in relatively early stages of development, and their trustworthiness depends on the proper deployment and configuration of the underlying technologies [24]. These underlying technologies may include mobile device operating systems as well as hardware support, including fingerprint readers and other biometric input devices, to enhance security [24]. Financial services are high-value targets for criminal activity and require demonstrable trust in multiple stakeholder environments [5]. The following list provides examples of concerns for various stakeholders of the financial services use case:

- Both financial institutions and End Users are concerned about fraud transactions, for example, spoofed servers, devices, or applications. End Users are concerned about stolen credentials or sensitive data, either on their mobile device or in transit to their financial institutions.

- Financial institutions are concerned that integration with mobile ecosystem stakeholders will potentially compromise their business model [23].

5.3 Health Monitoring Services

A health-monitoring device is a device worn on a person that tracks various statistics, for example, heartbeat, blood pressure, blood glucose levels, calorie consumption, sleep patterns, and more. Some of these are standalone devices, which may synchronize with software on the individual's mobile device, and some may be directly integrated with a mobile device. In concert with medical treatment, these health-monitoring devices offer significant benefits for personal health as well as diagnostics. However, End Users have privacy concerns about their health data that may prevent them from taking advantage of diagnostics.

End Users want control of their health data. They want guarantees that their data is protected both on and off their mobile device and is shared only with entities that they authorize. For example, if an individual uses a device to track his or her blood pressure, the individual may wish to share this information only with a specific trusted medical professional. The End User does not want this data distributed or sold such that they will receive advertisements for blood pressure treatments. The following list provides examples of concerns for various stakeholders of the health monitoring services use case:

- End Users are concerned that they are losing control of their health data.

- End Users are concerned that unauthorized entities on their mobile device might access personal user data.

- End Users are concerned about the protection of their health data on remote servers and also in transit. In the case of devices that synchronize with remote servers, whether they belong to manufacturers, medical facilities, insurance companies, etc., End Users want strong guarantees that their personal data will remain confidential and will not be shared with third parties. In many countries, there are regulations in place that require institutions to notify individuals of security breaches of information involving personally identifiable information. However, in some countries these regulations are not comprehensive and may exclude insurance companies.

- Institutions that use health-monitoring services may have concerns about integrating mobile devices with their enterprise systems which collect, transmit, and store health data securely. In some countries, there are regulated protections of individuals' health data that institutions legally must support.

6 Recommendations

The following capabilities are recommended for any mobile device that implements the MSM.

6.1 Recommended Capabilities

6.1.1 Integrity Protection of Trusted Shared Components

The MSM recommends providing integrity protection for all trusted shared components. The integrity of these components is crucial because several stakeholders rely on them to provide MSM capabilities. The mobile device architecture defines which components are shared, but, typically, these components include operating system software and device firmware. These components often also include mechanisms like Secure Boot, Digital Signature verification, and Transitive Trust chains to protect mobile device integrity. All of these concepts are described in greater detail in the TPM 2.0 Mobile Reference Architecture specification [2].

6.1.2 Isolation from Other Stakeholders

The MSM recommends providing isolation of all sensitive stakeholder resources. However, the specific use case often defines what resources are sensitive and need isolation. For example, the BYOD use case may warrant an entire rich environment, with its own set of applications, isolated from other environment(s) on the mobile device. Alternatively, a banking application may only require isolation of the application itself and any associated sensitive data.

This capability of isolation from other stakeholders includes prevention of information leakage about the existence of other stakeholders on the device. An application installed by one stakeholder can have access to a report of the integrity of the device as a whole, but this report should not normally include information about the existence of other stakeholders or their sensitive assets on the mobile device. In practice, the isolation of this information is typically policy-based. Some stakeholders, for example, the Device Manufacturer or Mobile Network Operator, may have greater privilege than other stakeholders have and, as a result, have access to this sensitive stakeholder existence information.

6.1.3 Trusted Path

The MSM recommends providing a Trusted Path [39], [52] for all sensitive stakeholder communications. For the purposes of this document, this definition includes both communication paths between a human user interface and a stakeholder environment as well as connectivity between software instances or hardware modules interacting with sensitive stakeholder resources. For example, with a Trusted Path, an End User can communicate with a banking application or an enterprise environment with confidence. Similarly, a biometric sensor on the mobile device can communicate with a stakeholder application in a Protected Environment with strong confidentiality. The MSM recommends that the mechanisms providing a Trusted Path also be resistant to all known side-channel attacks (e.g., timing, power, electromagnetic, etc.) on sensitive stakeholder communications.

6.1.4 Key Storage

The MSM recommends providing protected non-volatile storage for each stakeholder. Stakeholders need to store cryptographic keys and other critical security parameters (CSPs) [2] with data integrity and data confidentiality guarantees consistent with the use case [2].

6.1.5 Authentication of End Users and Device

The MSM recommends providing support for multifactor authentication of the End User and mobile device to trusted third parties. In most cases in the mobile ecosystem, trusted third parties require authentication of both entities. Authentication to trusted third parties may be specific to the stakeholder. For instance, authenticated users of the TPM, for example, human users, service providers, the operating system, or the BIOS, may utilize the attestation and signing capabilities of the TPM. Some stakeholder implementation methods may require support from other hardware security modules, for example, a Global Platform Secure Element [47] or Subscriber Identity Module (SIM) card [21]. Other authentication factors may include passwords or biometrics (fingerprint, retina scan, face recognition, etc.).

In addition to authentication to third parties, the MSM recommends providing support for authentication of End Users to the mobile device itself. This End User authentication support should include TPM authentication for access to sensitive data, as well as any additional authentication (e.g., biometrics) required by stakeholders of the mobile device.

The TCG Trusted Multi-Tenant Infrastructure Working Group has published a TMI Reference Framework [20] that provides a thorough treatment of the trusted multi-tenant infrastructure domain. This domain is pertinent to the MSM, and the TMI Reference Framework provides more detail on the interactions between multiple tenants, or stakeholders, of a common infrastructure domain.

6.1.6 Authentication of Remote Entities

The MSM recommends providing support for authentication of remote entities. Typically, mobile devices utilize a variety of services on remote servers and other infrastructure. In many cases, it is critical to authenticate these remote servers and/or service providers before transactions begin. Typically, the TPM itself or low-level OS software provides the necessary cryptographic libraries to support authentication of third party credentials. There may be additional stakeholder-specific authentication methods that require support from other hardware security modules, for example, a Global Platform Secure Element [47] or Subscriber Identity Module (SIM) card [21] card. Other privileged software components, for example, a TNC Client, may implement protocol stacks specific to the authentication method.

6.1.7 Authorization

The MSM recommends providing support for authorization to protect the mobile device and sensitive data from all unauthorized access. The TPM itself can provide support for this authorization for sensitive TPM data. There may be additional stakeholder-specific authorization methods that require support from other hardware security modules (HSMs).

6.1.8 Policy-based Access Control

The MSM recommends providing support for policy-based access controls on the mobile device. Stakeholders should be able to enforce a security policy that completely controls access to stakeholder sensitive data and applications, including stakeholder-specific upgrade policies. The TPM itself has an Enhanced Authorization (EA) mechanism [1] that can be used to implement this access control enforcement, or other infrastructure implementations may be available.

6.1.9 Data Encryption

The MSM recommends providing support for data encryption for confidentiality of data in transit and data at rest [14], [58]. In addition, the MSM recommends providing support for encryption of data in use to the greatest extent possible. For example, applications should limit the lifetime of unencrypted sensitive data in memory and should delete such data so that they destroy all cached copies as well. The mobile device should provide data encryption capabilities that have the same isolation properties that are required for the sensitive stakeholder data. Note that various cryptographic ciphers are used in authentication protocols, but this is not the bulk transaction data encryption to which this capability refers.

6.1.10 Attestation of Trusted Shared Components

The MSM recommends providing support for attestation of all trusted shared components. In an attestation process, a mobile device provides evidence of data and device integrity to stakeholders. The TPM itself can provide support for attestation, for example, vouching for the authenticity of integrity measurements or binding the attestation to a particular mobile device and current configuration.

6.2 Advanced Capabilities

6.2.1 Audit of System Events

The MSM recommends providing support for a reliable audit log of each system event on the mobile device. Stakeholders may need evidence of mobile device activity, for example, repeated authentication and authorization attempts, recent software upgrades, policy enforcement actions, etc., for verification or non-repudiation purposes [15], [16]. This capability may require support for application-specific audit logs, TPM audit logs, and system audit logs.

6.2.2 Audit of Stakeholder Events

The MSM recommends providing support for a reliable audit log of events on the mobile device that are specific to particular stakeholders. This capability may require support for application-specific audit logs, TPM audit logs, and system audit logs.

6.2.3 Active Environment Indication

The MSM recommends providing support for a reliable indication to human users of a Trusted Path [39] [52] of the currently active environment (e.g., enabled input interfaces). This capability can reduce the likelihood that an End User would inadvertently leak sensitive data. This recommendation is agnostic to the implementation of the active environment, e.g. as a conventional application, virtual machine, or other container.

7 Implementation Alternatives

The following sections demonstrate alternatives for implementing the MSM.

7.1 Single TPM

The MSM can be implemented on a mobile device with a single TPM (discrete, integrated, or firmware) in a Protected Environment. In this case, multiple stakeholder applications, or execution environments, typically share significant portions of the operating environment. Stakeholders can rely on system software that uses the TPM to protect their sensitive data. Figure 1 shows an example of a single TPM implementation of the MSM. The TPM Mobile Reference Architecture [2] presents additional examples of hardware and software architectures with a single TPM.

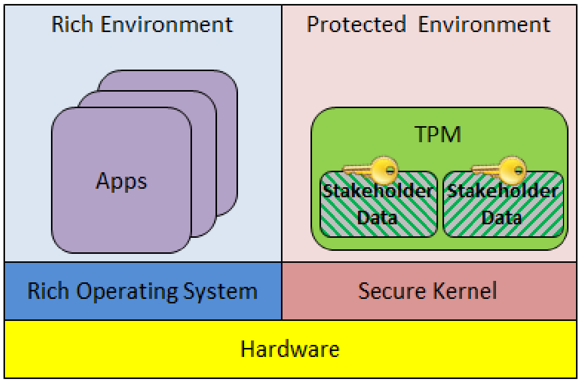

Figure 1 – Notional diagram of a Single TPM MSM implementation

An important feature of a TPM with multiple stakeholders is its ability to support multiple key hierarchies, in particular the Endorsement and Storage hierarchies. An Endorsement Key (EK) is a key used for attestation. A Storage Key (SK) is a key used to protect sensitive data. Stakeholders can use their own attestation and encryption keys to protect their sensitive resources from all other entities.

When multiple entities use the same TPM, it is necessary to manage the TPM resources to prevent interference. The TPM Software Stack (TSS) is a software stack designed to isolate users from the low-level details of the TPM and manage resource isolation. The TSS includes several layers, but two are particularly important to the MSM: the Resource Manager and the TPM Access Broker (TAB). The Resource Manager manages the TPM contexts in a manner similar to a virtual memory manager. It swaps objects, sessions, and sequences in and out of the limited TPM onboard memory as needed [7]. The TAB manages multi-process access to the TPM to guarantee that TPM commands will complete without interference from other competing processes [7].

Table 3 – Single TPM MSM Implementation describes how a system with a single TPM may provide the recommended capabilities.

Table 3 – Single TPM MSM Implementation

Recommended Capability	Examples of Supporting Technologies in a Single TPM Implementation
Integrity Protection of Trusted Shared Components	• Integrity relies on sound Roots of Trust [2]. • Secure Boot provides transitive chain of trust from Roots of Trust to trusted shared components [2]. • Measured Boot may also maintain measurement evidence of component integrity [2].
Isolation From Other Stakeholders	• A TPM can provide isolation of sensitive data by storing it internally and enforcing strong access controls. The data of different users of the TPM can be further isolated in separate storage hierarchies [1]. • Isolation of applications and/or environments can be facilitated by software isolation, for example, separate address spaces [27]. • In some cases, the processor hardware architecture enforces separation of execution environments [26], [42], [43]. • A Global Platform Secure Element (GP SE) [28], for example, an embedded SE, Universal Integrated Circuit Card (UICC) [32], or micro SD [33]**Error! Reference source not found.**, or other proprietary HSMs may also provide isolated data storage and execution resources.
Trusted Path	• Processor architecture [26], [42], [43] or HSMs may support secure input mechanisms [55] and secure communication channels [54], [56] to provide secure communications between the End User and the target mobile device. • After an initial Trusted Path is established, data encryption capabilities (see Data Encryption Recommended Capability below in this table) can protect data in transit and digital signatures on data can enable verification of data integrity.
Key Storage	• A TPM can provide storage of keys with strong access controls and different End Users of the TPM can store their keys in separate key hierarchies [1]. • A GP SE [28] or other HSM can provide secure key storage.
Authentication of the End Users and Device	• Various biometric technologies and security tokens, for example, a Smart Card, Common Access Card (CAC) [34], or Personal Identity Verification (PIV) [35], can authenticate mobile device End Users. • A TPM EK [25] provides a cryptographically verifiable identity for the mobile device TPM-supported attestation [1]. • Public Key Infrastructure (PKI) [36] technologies can manage digital certificates and public keys. • A GP SE [28] or other HSMs may support stakeholder-specific device authentication protocols. • Application-level software clients can implement various authentication protocols, for example, TNC [4] or other Mobile Device Management solutions.
Authentication of Remote Entities	• A TPM and other cryptographic libraries can support verification of cryptographic identities. • A TPM may store credentials, certificates, or other sensitive

	data in NVRAM. • PKI technologies can manage digital certificates and public keys. • A GP SE or other HSMs may support stakeholder-specific authentication protocols. • Application-level software clients can implement various authentication protocols, for example, TNC or other stakeholder-specific MDM solutions.
Authorization	• A TPM can support access controls, both simple and policy-based, can restrict visibility of sensitive data to authenticated users [1]. • A GP SE [28] or other HSMs may support authorization to stakeholder-specific resources.
Policy-based Access Controls	• A TPM can support policy-based access controls [1]. • A GP SE [28] or other HSMs may also support policy-based access controls. • Operating Systems solutions, e.g. SELinux, may also support policy-based access controls [46].
Data Encryption	• A TPM can support encryption of data at rest using separate storage hierarchies [1]. • Encryption of data at rest may also be provided by Self Encrypting Drives (SEDs) [36]**Error! Reference source not found.**, a GP SE [28], or other HSMs**Error! Reference source not found.**. • Data in transit over networks can be encrypted using Internet Protocol Security (IPsec) [29], Transport Layer Security (TLS) [30], and Virtual Private Network (VPN) [31] solutions.
Attestation of Trusted Shared Components	• A TPM can support attestation by storing integrity metrics in PCRs and through Measured Boot [2]. • A TPM EK [25] can provide a cryptographically verifiable identity for TPM-based attestation [1]. • Application-level software clients can implement various attestation protocols, for example, TNC [4]. Other proprietary Mobile Device Management (MDM) solutions may support stakeholder-specific protocols [19], [40], [41], [53].
Audit	• A TPM can support audit functions [1]. Syslog [39], Android's logger facility [37], or other OS logging facility may provide additional auditing capability.
Active Environment Indication	• Hardware-specific solutions may be available.

One important advantage of this implementation approach is that it minimizes the footprint of code supporting multiple stakeholders. This is beneficial for mobile platforms, which often have a memory-constrained Protected Environment hosting the TPM Mobile.

7.2 Multiple TPMs

The MSM can be implemented using multiple TPMs. These TPMs may reside in a single or in multiple Protected Environments. In this case, multiple stakeholder applications, or environments, still share significant portions of the operating environment. However, stakeholders use separate TPMs to protect their sensitive data. Figure 2 shows an example of a multiple TPM implementation of the MSM. The TPM Mobile Reference Architecture specification [2] discusses other mobile device architectures that utilize multiple TPMs.

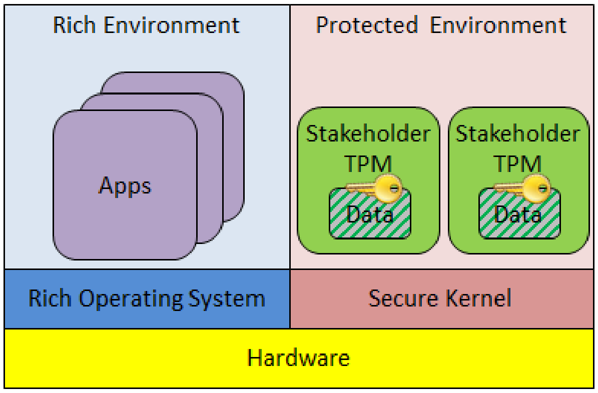

Figure 2 – Notional diagram of a Multiple TPM MSM implementation

The motivation for multiple TPMs is that some stakeholders may prefer not to share the services of a single TPM with others. These stakeholders may have more confidence in the protection offered by a distinct TPM instance, than they do in the granular protections of data within a shared TPM. However, it is important to note that this option may not be available to all stakeholders (e.g., due to resource constraints). Even in the case of multiple TPMs, the data and properties associated with the Device Manufacturer will be the same and the TPMs will rely on common resources provided by the operating environment.

A more general case of this implementation alternative may be multiple TPMs that support different levels of stakeholder privilege. In this case, there may be a "premium" TPM with Device Manufacturer and Mobile Network Operator (MNO)[6] as the only configured authorized users and a "regular" TPM for all other stakeholders. This option may provide a reasonable compromise that enables stakeholders to establish trust in mobile devices while maintaining tractable mobile device and TPM provisioning processes.

A system with multiple TPM Mobiles requires a means to distinguish them. The TSS supports multiple TPMs, both local and remote. Each TPM has a dedicated TPM Command Transmission Interface (TCTI), TAB, and Resource Manager. The highest layer of the TSS stack is the Feature API[8]. The purpose of the Feature API is to make TPM programming as simple as possible for ordinary applications. The Feature API includes a command to initialize a TPM context and establish a connection with a particular TPM stack, specified by URI. For the purposes of interoperability, stakeholder applications utilizing TPM services should be agnostic about the use of a shared TPM or a dedicated TPM.

Table 4 – Multiple TPM MSM Implementation describes how a system with a multiple TPMs can provide the recommended capabilities.

Table 4 – Multiple TPM MSM Implementation

Recommended Capability	Examples of Supporting Technologies in a Multiple TPMs Implementation
Integrity Protection of Trusted Shared Components	• Same as Single TPM implementation
Isolation From Other Stakeholders	• Same as Single TPM implementation with the following exceptions: ○ Different stakeholders have separate TPM instances to provide TPM isolation [1]. ○ If processor architecture enforces separation of execution environments [26], [42], [43], the separation of environments may be per stakeholder or by different levels of stakeholder privilege.
Trusted Path	• Same as single TPM implementation
Key Storage	• Same as Single TPM implementation with the following exception: ○ Different stakeholders have separate TPM instances to provide TPM key storage and access controls [1].
Authentication of the End Users and Device	• Same as Single TPM implementation with the following exception: ○ Different stakeholders have separate TPM instances and EKs to support attestation [1].
Authentication of Remote Entities	• Same as single TPM implementation with the following exception: ○ Different stakeholders have separate TPM instances and NVRAM for storing credentials, certificates, or other sensitive data.
Authorization	• Same as Single TPM implementation with the following exception: ○ Different stakeholders have separate TPM instances with both simple and policy-based access controls [1].
Policy-based Access Controls	• Same as Single TPM implementation with the following exception: ○ Different stakeholders have separate TPM instances with individual policy-based access control [1].
Data Encryption	• Same as Single TPM implementation with the following exception: ○ Different stakeholders have separate TPM instances to support encryption at rest [1].
Attestation of Trusted Shared Components	• Same as Single TPM implementation
Audit	• Same as Single TPM implementation with the following exception: ○ Note that separate TPM audit logs would be discrete
Active Environment Indication	• Same as Single TPM implementation

This approach demands more memory resources in the Protected Environment(s) than a Single TPM solution.

7.3 Virtualization

The MSM can be implemented using virtualization to support multiple stakeholder environments. Each environment would have its own set of applications and access to TPM services.

The TCG Virtualized Trusted Platform Architecture Specification [13] provides a general architecture and set of deployment models for virtualized trusted computing platforms. These deployment models support either sharing or virtualizing a physical TPM (pTPM). TPM sharing refers to the logical or physical partitioning of a pTPM between hypervisors and/or operating systems, similar to the Single TPM implementation alternative. A virtualized TPM (vTPM), however, provides the appearance of a single dedicated TPM for each virtual machine (VM). This implementation alternative emphasizes the virtualized TPM model. For a detailed discussion of the architecture, see the specification [13]. Figure 3 shows a notional diagram of a virtualized implementation of the MSM. The figure displays a simplified architecture with a pTPM in the hardware. Solutions have been proposed which virtualize firmware TPMs (fTPMs), but these solutions are not addressed in the Virtualized Trusted Platform Architecture or TPM Mobile Reference Architecture Specification and are beyond the scope of this document. Figure 3 shows a potential implementation architecture. The TPM Mobile Reference Architecture specification [2] discusses other mobile device architectures that leverage virtualization.

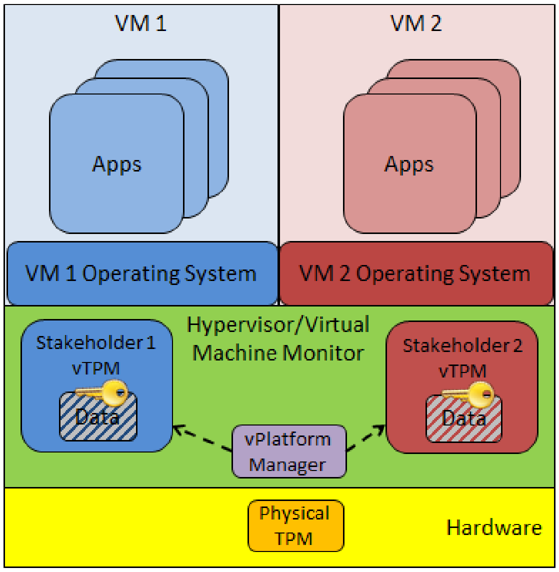

Figure 3 – Notional diagram of a virtualized MSM implementation

One motivation for virtualization is that stakeholders can isolate entire environments and the services of a vTPM from all other stakeholders, typically with hardware support for isolation. However, as in the multiple TPM case, it is important to note that this option may not be available to all stakeholders (e.g., due to resource constraints). Not all stakeholders may have control over or awareness of the platform architecture. The stakeholder VMs and vTPMs will typically rely on common resources provided by a hypervisor or Virtual Machine Manager (VMM) as well as a common underlying mobile device pTPM.

There are several challenges associated with the virtualized TPM model that affect stakeholders on the device. One challenge is the instantiation of keys and certificates [57] for a new vTPM in a way that enables remote entities to verify the TPM. One approach is to use a Certificate Authority (CA) on the virtualized platform network to obtain the necessary keys and certificates, if one is available. Another approach is to have a locally available CA on the virtualized platform. While the second approach is easier to implement, it may require stakeholders to trust a large number of CAs or CAs, which cannot be verified outside the network [13]. Another challenge is VM migration, in which the VM may be migrated from one physical platform to another. There are many use cases for VM migration, but it is crucial for the migration mechanisms to maintain the security of stakeholder resources within the VM and its unique vTPM [13]. These and other challenges are addressed in more detail in the TCG Virtualized Trusted Platform Architecture Specification [13]

Table 5 – Virtualized MSM Implementation describes how a virtualized system can provide the recommended capabilities.

Table 5 – Virtualized MSM Implementation

Recommended Capability	Examples of Supporting Technologies in a Virtualized Implementation
Integrity Protection of Trusted Shared Components	• Same as Single TPM implementation o Note that the technologies apply to entire virtualization stack.
Isolation From Other Stakeholders	• Same as Single TPM implementation with the following exceptions: o A vTPM can provide isolation of sensitive data by storing it internally and enforcing strong access controls [1], [13]. Different stakeholders would have separate vTPMs. o Isolation of stakeholder environments can be facilitated by virtual machine isolation, in some cases with hardware support for virtualization [44], [42]. o A GP SE [28], for example, an embedded SE, UICC [32], or micro SD[33], or other proprietary HSMs can also provide isolated data storage and execution resources.
Trusted Path	• Same as Single TPM implementation with the following exception: o Virtualization technologies may support additional secure input mechanisms and communication channels between the user and the target.
Key Storage	• Same as Single TPM implementation with the following exception: o Different stakeholders have separate vTPMs to provide TPM key storage and access controls [1], [13].
Authentication of the End Users and Device	• Same as Single TPM implementation with the following exception: o Different stakeholders have separate vTPMs and EKs to support attestation [1], [13].
Authentication of Remote Entities	• Same as single TPM implementation with the following exception: o Different stakeholders have separate vTPMs and NVRAM for storing credentials, certificates, or other sensitive data.
Authorization	• Same as Single TPM implementation with the following exception:

	o Different stakeholders have separate vTPMs with both simple and policy-based access controls [1], [13].
Policy-based Access Controls	• Same as Single TPM implementation with the following exception and addition: o Different stakeholders have separate vTPMs with individual policy-based access control [1], [13]. o Virtualization technologies may have other policy-based access control mechanisms.
Data Encryption	• Same as Single TPM implementation with the following exception: o Different stakeholders have separate vTPMs to support encryption at rest [1], [13].
Attestation of Trusted Shared Components	• Same as Single TPM implementation with the following exception and addition: o A vTPM, which is associated with an underlying mobile device pTPM, supports attestation of VMs [2], [13] and provides the EK. o A deep attestation service can support attestation of multiple layers of a virtualized system, including the VMs, hypervisor/VMM, and underlying mobile device pTPM [13].
Audit	• Same as Single TPM implementation with the following exception and addition: o The hypervisor or VMM may have additional logging facilities.
Active Environment Indication	• Hardware- or hypervisor-specific solutions may be available.

8 Threats and Mitigations

As mobile devices become primary computing devices for individual and business applications, they become more attractive targets for malicious activity. In addition, relative to traditional PCs, mobile devices support far more diverse network interfaces and communication protocols, providing additional vectors for malicious attack. As a result, mobile devices require a broad range of capabilities to preserve their integrity. In the case of a multiple stakeholder mobile device, individual stakeholders require protection from external entities as well as from other stakeholders on the mobile device.

The recommended capabilities of the MSM are intended to reduce the vulnerability of mobile devices to increasingly sophisticated threats. For the purposes of this document, a threat is defined as the potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability [17], [60], [61]. A vulnerability is defined as a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised and result in a security breach or violation of the system's security policy [17], [60], [61].

The TMS Use Cases – Bring Your Own Device (BYOD) reference document [6] includes a discussion of information security threats pertinent to the MSM. The document derives the following list of threats from the IETF RFC 3552, Guidelines for Writing RFC Text on Security Considerations [18]*:*

T1. Eavesdropping on transmitted data
T2. Unauthorized read access to stored data
T3. Unauthorized use of sensitive authentication data
T4. Replay Attacks
T5. Data Insertion
T6. Data Deletion
T7. Data Modification
T8. Cloning of the mobile device

Table 6 – Threats and Mitigations is adapted from the TMS Use Cases – Bring Your Own Device (BYOD) document [6] in order to summarize how the recommended MSM capabilities can mitigate the impacts of mobile device threat sources.

Table 6 – Threats and Mitigations

Threat Source	**Threat**	**Recommended Mitigation Capabilities**
Attacker attempts to connect using an unauthorized device	• T1. Eavesdropping on transmitted data • T2. Unauthorized use of sensitive authentication data • T4. Replay Attacks • T5. Data Insertion • T7. Data Modification	• Key Storage: prevents access and manipulation of data by restricting key use to authorized entities (T1, T2) • Authentication of End Users and Device: prevents unauthenticated **mobile devices** from obtaining access to the network and sensitive data (T1,T2, T4) • Authorization: prevents unauthorized **mobile devices** from gaining privileges on network (T2) • Data Encryption: hinders unauthorized entities from inserting or modifying sensitive data (T5, T7) • Attestation of Trusted Shared Components: verifies genuine device state before allowing the **mobile device** to connect or to access

		sensitive data (T2, T4) • Audit: tracks attempts by unauthorized **mobile devices** to connect or to access data inappropriately (T2, T4)
Attacker attempts to connect using a lost or stolen (but normally) authorized device	• T1: Eavesdropping on transmitted data • T2: Unauthorized read access to stored data • T3: Unauthorized use of sensitive authentication data • T4: Replay Attacks • T5: Data Insertion • T7: Data Modification	• Key Storage: prevents access and manipulation of data by restricting key use to authorized entities (T1, T2, T3) • Authentication of End Users and Device: prevents unauthenticated **End Users** from obtaining access to the network and sensitive data (T1, T2, T3) • Authorization: prevents unauthorized **End Users** from gaining privileges on network (T2) • Policy-based Access Control: prevents unauthorized **End Users** from gaining privileges on network, even if the device has authorization (T2) • Data Encryption: prevents unauthorized entities from using sensitive data and hinders unauthorized entities from eavesdropping, inserting, or modifying sensitive data (T1, T2, T3, T5, T7) • Audit: tracks attempts by unauthorized **End Users** to connect or to access data inappropriately (T2, T3, T4)
Man-In-The-Middle (MITM) attack	• T1:Eavesdropping on transmitted data • T3:Unauthorized use of sensitive authentication data • T4:Replay Attacks • T5:Data Insertion • T6:Data Deletion • T7:Data Modification	• Trusted Path: ensures the **mobile device** or **End User** is communicating with the intended receiver (T1, T3) • Authentication of Remote Entities: prevents unauthenticated entities from intercepting communications (T1, T3) • Data Encryption: prevents unauthorized entities from using sensitive data and hinders unauthorized entities from effectively eavesdropping, inserting, deleting, or modifying sensitive data (T1, T3, T5, T6, T7) • Attestation of Trusted Shared Components: verifies genuine state of communication endpoints(T1, T3, T4)
Eavesdropping on RF transmission	• T1:Eavesdropping on transmitted data • T3:Unauthorized use of sensitive authentication data	• Key Storage: prevents access to and manipulation of data by restricting key use to authorized entities (T1, T3) • Data Encryption: prevents unauthorized entities from using sensitive data and hinders unauthorized entities from eavesdropping sensitive data (T1, T3). Here, data encryption refers to application-specific encryption of

		stakeholder data, rather than the radio transmission channel encryption.
User installs app that contains malware	• T1:Eavesdropping on transmitted data • T2:Unauthorized read access to stored data • T3:Unauthorized use of sensitive authentication data • T4:Replay Attacks • T5:Data Insertion • T6:Data Deletion • T7:Data Modification	• Integrity Protection of Trusted Shared Components: prevents installation of a malicious app which is a trusted shared component (T2, T3, T4, T5, T6, T7) • Isolation from Other Stakeholders: prevents a user-installed malicious app from accessing or compromising other stakeholders' data (T2, T3). • Trusted Path: ensures the malicious app cannot intercept communications intended for other entities (T1, T2,T3) • Authorization: prevents user-installed malicious app from accessing other stakeholders' data (T2, T3, T5, T6, T7) • Policy-based Access Control: prevents unauthorized apps from accessing other stakeholders' data (T2, T3, T5, T6, T7) • Data Encryption: prevents malicious app from using sensitive data and hinders malicious app from effectively eavesdropping, inserting, deleting, or modifying sensitive data (T1, T2, T3, T5, T6, T7) • Attestation of Trusted Shared Components: verifies that trusted shared components do not include malicious apps (T4) • Audit: tracks installation of malicious app and attempts by app to access data inappropriately (T2, T3, T4, T5, T6, T7) • Active Environment Indication: prevents users from unintentionally sharing data directly with the malicious app (T5, T6, T7)
User downloads data that exploits flaw in trusted app	• T1:Eavesdropping on transmitted data • T2:Unauthorized read access to stored data • T3:Unauthorized use of sensitive authentication data • T4:Replay Attacks • T5:Data Insertion • T6:Data Deletion • T7:Data Modification	• Isolation from Other Stakeholders: prevents a flaw in trusted app from compromising other stakeholders' data (T2, T3) • Key Storage: prevents the flawed trusted app from accessing and manipulating other stakeholder data by restricting key use to authorized entities (T1, T2, T3) • Policy-based Access Control: prevents flawed trusted app from accessing other stakeholders' data (T2, T3)

		• Data Encryption: prevents flawed trusted app from using other stakeholders’ sensitive data and hinders flawed trusted app from eavesdropping, inserting, deleting, or modifying other stakeholders’ sensitive data (T1, T2, T3, T5, T6, T7) • Attestation of Trusted Shared Components: verifies whether the flawed version of the trusted app is installed on the device (T4) • Audit: tracks attempts by flawed trusted app to access data inappropriately (T2, T3, T4, T5, T6, T7)
End User, knowingly or unknowingly, attempts to connect to the Enterprise network with a cloned mobile device	• T8:Cloning of the mobile device	• Key Storage: prevents the cloned device from connecting without required hardware (or un-cloneable) keys (T8) • Authentication of End Users and Device: prevents unauthenticated devices from obtaining access to the network (T8) • Attestation of Trusted Shared Components: verifies genuine device state before allowing the device to connect to the network (T8) • Audit: tracks attempts by cloned device to access the network(T8)