第5章　可信计算平台

5.1　概述

为了解决软件及其计算环境的信任问题，可信计算组织（TCG）首先提出了可信计算平台（Trusted Computing Platform，TCP）的概念[1]，并将其具体化为可信个人计算机、可信服务器和可信移动设备等。可信计算平台的目标是实现系统行为的信任，即保证软件在给定的运行环境下，其行为与预期是一致的。构建可信计算平台的基本思路是在硬件平台上引入安全芯片（TPM/TCM）作为信任根，在此基础上扩展信任边界，最终将部分或整个普通的计算平台变为“可信”的计算平台。可信计算平台的安全性根植于上述具备一定安全防护能力的安全芯片（TPM/TCM），基于安全芯片实现隔离计算、计算环境完整性保证和远程证明等服务，从而保证计算平台上实体行为的可信性。

可信计算平台是利用安全芯片为通用计算平台构建的安全体系架构，为了构建可信计算平台必须具备两个基本要素：首先必须装配硬件安全芯片，这是保护目标平台安全功能的基础与前提；其次是实现相应的可信计算技术，包括信任链构建、可信度量和远程证明等安全机制，这是实现计算平台可信环境的具体方法[2]。总的来说，可信计算平台能够为用户环境提供以下信任保障：

（1）基于可信度量机制，建立平台启动过程中的信任链，为平台构建初始信任环境；通过验证运行时应用程序的完整性和合法性，保障平台内部应用程序的可信运行；基于安全芯片提供的密钥计算功能，为平台内部数据提供基于硬件的保护，从而构建平台内部信任。

（2）基于匿名证明及远程证明机制，提供平台身份及平台软硬件配置的正确性证明，构建平台之间的信任。

（3）基于可信计算平台的完整性收集与远程证明等机制，对将要接入网络的平台完整性状态进行验证，以确保网络中各个节点的可信性，为构建整个网络信任奠定基础。

5.1.1　发展现状

可信计算平台的需求来自解决终端平台行为信任问题，所以早期工作主要由IT产业界推动，这其中包括微软、IBM、HP和Intel等众多可信计算组织TCG的成员。可信计算平台利用硬件安全芯片，从体系结构层面解决平台信任问题，与传统的基于软件的安全解决方案相比有明显优势。可信计算平台作为一种安全增强的平台架构，在数据保护、计算环境保护、远程信任和系统安全架构等方面还存在着诸多挑战，这也激发了国内外相关领域对可信计算平台的研究热潮。

在国外，剑桥大学、卡内基·梅隆大学、斯坦福大学和IBM研究院等知名大学与科研机构纷纷展开可信计算平台相关项目的研究，并取得一系列研究成果；TCG针对不同形态的可信计算平台，分别制定了可信PC、可信服务器、可信手机及可信虚拟平台等相关技术与产品规范，为进一步推广应用可信计算技术提供标准支持；而产业界也据此研制了一系列可信

计算平台产品，包括 IBM、HP 等计算机厂商都推出众多从台式机、笔记本计算机到服务器的可信计算产品；而且，随着移动设备与应用的快速推广，诺基亚、三星等手机厂商正在研究相应的可信手机产品。

在国内，一方面，众多高校和科研机构，如中国科学院软件研究所、清华大学、武汉大学和北京工业大学等，针对可信计算平台技术与架构展开了深入研究，为自主可信计算技术发展与产品研制奠定了坚实基础；另一方面，自主可信计算平台得到了从芯片、计算机厂商到应用服务提供商、终端用户的大力支持与推动，联想、长城、同方等众多国内计算机厂商都分别推出各自的可信计算平台产品，在军队、银行及政府等关键部门得到广泛应用。2007 年，国家密码管理局推出自主可信计算产品相关技术规范，为可信计算平台的进一步研制与推广提供了标准支持。

目前，可信计算平台的技术研究和产业推广已形成良好的互动，形成了研究、产品、测评和标准循环前进的发展态势。随着物联网和云计算等新型技术的快速发展，进一步引发了用户对其计算环境的安全需求；为此，各厂商正逐步推出包括可信移动平台和可信嵌入式平台（车载设备）等新型可信计算平台，相信可信计算平台将随着应用技术的快速发展，也必将得到进一步快速推广与应用。

5.1.2 基本架构

可信计算平台是由 TCG 最早提出的，它为通用计算平台提供一种系统架构层面的安全增强，它以底层的安全芯片为核心，结合上层的可信计算关键机制，最终为用户计算平台建立完整的可信运行环境。我们将可信计算平台架构分为自底向上的 3 个层次，其基本架构如图 5.1 所示。

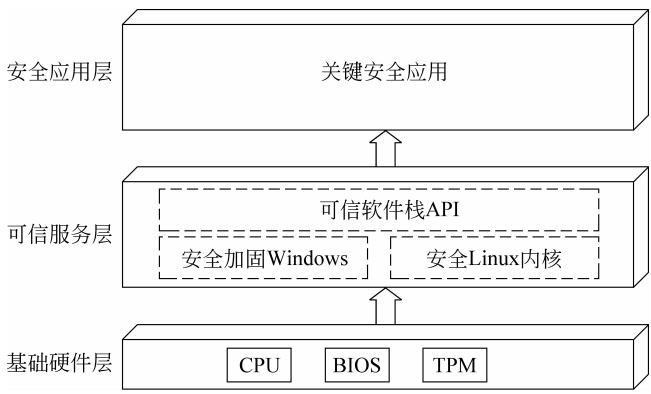

图 5.1 可信计算平台体系结构

这 3 个层次分别是基础硬件层、可信服务层和安全应用层，也就是说，可信计算平台涵盖了从底层的基础硬件、中间的操作系统内核、可信功能接口以及上层用户应用的整个计算平台体系。

（1）基础硬件层。该层主要是物理安全芯片，辅以可信 BIOS、安全 CPU 和安全 I/O 等结构，为整个计算系统提供信任根。

（2）可信服务层。该层跨越了系统内核层和用户应用层，主要包括操作系统内核及可

信软件接口，操作系统内核是运行计算系统的基础，而可信软件接口为上层应用提供可信计算服务的调用接口，比如针对不同安全芯片 TPM/TCM 的可信软件栈 TSS/TSM 等。

(3) 安全应用层。该层位于可信计算平台体系的最高层，它基于上述信任根与基础可信运行环境，通过调用不同的可信计算软件接口，实现针对不同安全应用需求的安全功能，保障用户应用软件的可信运行。

可见，以安全芯片为核心构建的可信计算平台架构中，基础硬件层提供原始的信任根，是可信计算平台构建的前提；可信服务层通过与硬件层的交互，完成信任链构建、完整性度量等关键可信机制，为用户应用提供基础可信运行环境；安全应用层基于硬件层与可信服务层提供的可信功能及调用接口，实现用户安全应用。各层功能相辅相成，缺一不可，最终为用户构建一个满足安全需求的可信计算平台。

5.2 个人计算机

个人计算机是应用最广泛的计算平台，终端用户需要能够提供应用与系统可信运行的保障机制，基于安全芯片构建的可信个人计算机能够满足上述需求。可信个人计算机不能影响原有系统的运行与实现，因此必须是在兼容原有体系结构的前提下，对原有系统进行相应的安全增强。为此，TCG 组织给出了可信个人计算机安全技术规范与标准，以引导相应产品的实现与应用。

5.2.1 规范

针对普通的用户计算平台 PC Client 架构，TCG 推出个人计算机 PC Client 规范(TCG PC Specific Implementation Specification)[3]，主要由 HP、IBM、Intel 及 Microsoft 公司制定，其目标是为可信个人计算平台的实现提供参考依据。考虑到 TCG 通用规范应该独立于平台架构，因此它并未给出在其抽象架构下的具体的实现要求。

该规范用于为具体的 PC 平台提供实现的参考依据，其主要内容包括 PC Client 的基本组件、主机平台启动与配置过程、系统状态转换及相应的证书定义等。其中，着重对静态 RTM 及动态 RTM 使用到的 Locality 及 PCR 的使用进行了具体定义与描述，并给出可信 PC Client 的参考实现架构及应用接口。

为了更好地为可信 PC Client 实现提供指导，TCG 还提供了其他相关的辅助规范，包括：

(1) 个人计算机专用 TPM 接口规范 TIS(PC Client Specific TPM Interface Specification)[4]。TCG 主规范中定义了非具体平台的通用的 TPM 使用接口，但是没有包含涉及具体平台(如个人 PC 或服务器)的 TPM 特殊功能(如支持动态 Locality、可重置 PCR 等)。为此，TCG 制定本规范，给出针对普通 PC 环境中使用支持特殊功能的 TPM 接口定义。

(2) 个人计算机防重启攻击规范(PC Client Work Group Platform Reset Attack Mitigation Specification)[5]。当一个平台重置或关闭时，易失内存的内容不是立刻消失。因此，攻击者能够通过重置目标平台，快速激活一个攻击程序来获取尚未消失的内存内容，比如加密密钥及其他秘密信息。为了避免这种威胁，本规范提供一种解决方案，通过为主机

平台重置事件设置一个内存重写 MOR(Memory Overwrite Request)位,使得平台非法重置时,在加载程序前清除原有内存内容(比如重写该内存为全零)以防止攻击者读取机密信息。本规范针对基于传统 BIOS 以及新的 UEFI(Unified Extensible Firmware Interface)方法启动主机的情况,给出实现上述方法的详细接口定义及使用方法。

(3) 两个关于可扩展固件接口 EFI(Extensible Firmware Interface)的规范[6,7]。

EFI 协议规范(TCG EFI Protocol Specification)针对不同的 EFI 平台场景,给出 EFI 平台上使用 TPM 的标准接口定义,利用该接口,OS Loader 和管理组件能够度量并记录 EFI 平台上的启动事件;EFI 平台规范(TCG EFI Platform Specification)针对具有 EFI 的平台启动过程,给出针对不同事件类型扩展 PCR 以及向事件日志添加新项的详细操作定义。

5.2.2 产品与应用

利用已推出的各种规范,不同的计算机厂商可建立各自的实现架构,生产不同的可信计算机。目前,国内外众多厂商,包括 IBM、HP、联想和同方等,针对不同的安全需求,已经推出一系列可信计算机产品。

IBM 公司于 2001 年 11 月率先推出了主板嵌有 TPM 芯片的台式机产品,2004 年又推出了嵌有 TPM 的笔记本电脑产品;HP 公司于 2003 年 6 月推出了嵌有 TPM 的计算机,富士通和宏碁公司也于 2004 年推出了嵌有 TPM 的计算机产品。市场上流行的台式机产品主要有 HP/Compaq 公司的 dc7100、IBM 公司的 Netvista desktops、Dell 公司的 OptiPlex GX520 等;笔记本电脑产品有 HP/Compaq 公司的 nw8000、IBM 公司的 T43 和 Sony 公司的 VAIO BX Series 等。

目前,有不少国内厂家也推出自主可信计算机产品,比如联想、瑞达、清华同方、浪潮、长城和方正等。其中,联想公司基于自主可信安全芯片 TCM 构建的可信计算平台有联想开天 M8000 和昭阳 K42A 等,并为可信计算机提供联想数据盾牌安全套件,该套件是在联想公司安全芯片基础上开发的应用软件,集成了一系列的主机安全保护工具,为用户提供本地加密并共享给指定用户等功能,用以保护用户的重要文件,防止数据泄漏;武汉瑞达信息安全产业股份有限公司基于自主安全芯片研制可信计算平台,推出了嵌入式密码计算机;同方公司基于自主 TCM 安全芯片构建的可信计算平台,能够为用户的计算机系统和数据提供全方位保护,支持对安全芯片的管理、用户文件加解密及数据恢复等功能,并基于可信计算平台提供可信网络接入服务;卫士通公司也基于可信计算平台,提供结合 TCM 和 USB Key 的用户计算机操作系统安全防护系统,为用户提供数据安全存储及网络访问控制等安全功能。

总之,可信计算机融合了安全芯片、基础软件、计算机制造、网络设备制造和网络应用软件等多学科专业技术,集成相应的可信计算安全芯片、安全软件中间件、安全主板以及信任链平台软件,能够满足军事、金融、交通等特定行业苛刻的数据移动处理和安全防护要求。目前,可信计算机已在诸如交通管理、现场救援、数据采集、设备检测和通信保障等作业现场进行广泛应用,并在推出可信计算机产品后的短时间内迅速得到相关行业用户的认可和好评。随着用户对自己隐私信息和数据安全的保护需求越来越高,可信计算机将会得到更进一步的应用与推广。

5.3 服务器

服务器作为数据控制的中心，系统中通常运行着众多关键服务，并存储大量数据，因此也导致大量针对服务器系统的攻击。与个人计算机一样，为更好地保障位于服务器上的服务与数据的安全性，需要引入可信计算技术为服务器构建可信运行环境。

5.3.1 规范

与可信个人计算机相比，可信服务器对其安全芯片 TPM/TCM、信任链和 TSS/TSM 的要求有许多不同，主要包括：

(1) 由于服务器的处理速度比普通 PC 高得多，因此要求安全芯片的处理速度包括密码的运算速度也应很高，而现有的安全芯片的处理速度较低。

(2) 服务器的安全芯片应能支持并发控制，当多用户同时访问可信服务器时，安全芯片应该可以并发地处理访问请求，并确保数据的正确性与操作的原子性。服务器常采用多安全芯片机制(物理安全芯片和虚拟安全芯片)，单个安全芯片的改变不应影响其他安全芯片的安全性，此外还应具有对机密数据迁移、备份与恢复的能力。

(3) 现在 TCG 的 TPM 与主板的接口是 LPC 总线，而 LPC 的速率不高，不适合服务器高速通信的要求。

(4) 由于服务器通常具有多个处理器，而且支持虚拟化机制，因此它的启动方式与普通 PC 不同，所以其信任链也应与普通 PC 不同。

(5) 由于服务器开机后长时间不关机，因此需要能够多次执行的可信度量机制。

为此，TCG 专门制定并发布了一系列独立于物理实现架构的服务器规范，为可信服务器的研制提供标准支持。这些规范主要包括：

(1) 可信服务器主规范(Server Work Group Generic Server Specification)[8]。与可信 PC 规范对应，针对服务器架构中使用 TPM 的特点制定本规范，它基于 TPM 主规范，根据服务器利用 TPM 的特定需求，给出具体的术语及功能定义，比如服务器 TBB(Trusted Building Block)和 PCR 使用等。该规范与具体服务器平台架构无关，因此各服务器厂商需要针对具体平台定义自己的实现架构。

(2) 可信服务器命令规范(Server Work Group Mandatory and Optional TPM Commands for Servers Specification)[9]。对于服务器来说，适用于普通 PC 平台上的 TPM 命令可由强制转为可选，但不能直接从可选命令转换为强制命令，因此制订该规范。

(3) 其他相关规范。结合 TCG 主规范，TCG 又制定了相关的高级配置和电源管理接口(Advanced Configuration and Power Management Interface，ACPI)通用规范[10]，它为各种期望使用 ACPI 的平台(含服务器和客户机)提供一个符合 TCG 规范的使用框架，主要包括所需的 ACPI 表及基本方法定义。TCG 还给出一种安腾架构的服务器系统实施示例规范(Server Work Group Itanium Architecture Based Server Specification)[11]，可以作为其他系统架构实现的参考。

5.3.2 产品与应用

受市场需求的推动，国内外企业已经开始可信服务器的研究和开发。但是，目前 TCG

发布的有关服务器的规范与可信个人计算机规范相比，缺乏实现细节上的定义，而且服务器本身在技术上比个人计算机复杂，其技术性能要求也比个人计算机高很多。而由于服务器的上述特性，用于服务器的可信软件栈也应有所不同。因此，可信服务器的产品研发要比可信个人计算机滞后。

目前，国外的 HP、IBM 等众多知名公司也推出了部分可信服务器的产品，但主要都只是结合已有普通可信平台关键机制，并未得到广泛应用与推广。比如 HP ProLiant ML110 G6、HP ProLiant ML150 G6 系列的部分产品中嵌入了 TPM 芯片，在应用过程中，主要与 Windows 的 BitLocker 机制结合，为服务器的数据安全提供保障。

国内的联想公司 2011 年新推出的一款主流塔式服务器 T168 G7，在安全设计方面，主要是采用基于国产 TCM 安全芯片的可信加密防护技术，目的是为服务器构建计算环境的可信，主要优势表现在 3 个方面：首先是构建服务器平台的可信性，安全芯片在开机时就会监控系统程序的装载，一旦发现某个程序状态异常就发出警报乃至禁止其运行；其次是服务器用户身份的证明，TCM 安全芯片中存储有标识平台身份的密钥，会在必要时通过签名或者数字证书的相关机制，向外界表明自己的身份，而且标识号是全球唯一的；最后是加密保护，经过 TCM 芯片进行加密的数据就只能在该服务器平台上进行解密和处理，从而把机密数据绑定在该平台上，即使数据被盗，因为脱离了对应平台而离开了解密密钥，数据将无法被识别，从而实现数据保护。该产品已经通过国家保密局和国家密码管理局等权威机关的认证。

随着服务器技术的快速发展与应用，对安全的需求也越来越高，作为数据与服务的管理中心，亟需可信计算技术为其提供安全保障。可信服务器能够满足上述需求，一方面为本地服务运行提供可信执行环境，另一方面能够为用户提供服务与数据的信任证明，使用户能够验证位于远程服务器方的数据正确性和完整性。

5.4 可信移动平台

随着移动通信技术的快速发展，移动计算平台的使用越来越普及，用户通过自行安装第三方服务商提供的程序，如应用软件、游戏等，来扩充移动计算平台应用功能，使得移动计算平台不再是单纯的通信工具，还可以用来对用户敏感数据进行发送、接收和存储等操作，这就导致了可信移动平台存在着较大的安全隐患。安全问题已经成为移动平台用户关注的焦点，尤其要求移动平台能够为用户提供高可信服务的保证。

由于移动计算平台与普通计算平台在硬件架构、处理能力、存储空间、通信带宽及实现成本等方面的差异，因此普通计算平台上利用硬件安全芯片来构建其可信运行环境的方法不再适用于移动平台。为此，TCG 与相关移动设备厂商一起推出了针对可信移动计算平台的相关规范；同时，一些研究机构也给出了可行的可信移动平台实现方案。本节将从规范、系统架构、技术实现与应用等方面简要介绍可信移动平台。

5.4.1 规范

由于移动计算平台自身的特殊性，导致我们不能直接使用 TPM/TCM 安全芯片来增强移动平台的安全性。为此，相关移动设备厂商及 TCG 都推出了一系列规范，以满足可信移

动平台的功能需求，同时为可信移动平台的实现提供标准支持。

2004 年 10 月，Intel、IBM 和 NTT DoCoMo 等公司针对移动平台安全，制订了基于可信计算的可信移动平台（Trusted Mobile Platform，TMP）规范[12]；2006 年 9 月，TCG 针对移动平台的特点，通过对 TPM 规范进行部分修改，发布了移动可信模块规范（Mobile Trusted Module，MTM）[13]，作为构建可信移动平台的基础，目前该规范已更新[14]；之后，TCG 又推出相关的可信移动平台技术与实现规范，并给出可能的使用场景：

（1）移动参考架构规范（TCG Mobile Reference Architecture）[15]。为了提供移动可信平台在实现上的参考，TCG 发布了可信移动平台参考架构规范。该规范是在可信移动平台主规范基础上，针对可信移动平台的初始化启动过程及其功能使用方法，提供一种可信移动平台参考使用架构。它主要给出了可信移动平台功能架构、度量与验证方法、信任链构建、可信启动及生命周期管理等具体功能实现方案。

（2）可信移动平台抽象层规范（TCG Mobile Abstraction Layer）[16]。为了给厂商及开发者提供具体的应用接口，TCG 还发布了可信移动平台抽象层规范。该规范是在 MTM 主规范和参考架构规范基础上，给出针对可信移动平台可信组件的抽象层定义，主要内容涵盖使用 MTM 过程中的各种数据类型与结构、各种具体的可信软件栈接口等，主要用于为各厂商生产可信移动产品提供标准化参考。

（3）可信移动平台使用场景[17]。针对移动平台和嵌入式系统等面临的安全威胁，考虑利用 MTM 来对其进行安全增强。本规范以具体的可信移动平台使用场景为例（比如电子支付和电子医疗等），给出一些使用可信移动平台的技术需求及使用指南。

5.4.2 通用架构

TCG 根据移动平台相关的移动电话规范及 MTM 规范，提出一个通用的抽象可信移动平台功能架构，如图 5.2 所示。在该架构中，可信移动平台被抽象为一系列可信引擎结构的组合，通过处理可信服务请求、报告当前引擎的状态并提供其可信证明等机制来构建本地或远程的可信移动环境。该架构由 3 部分组成：各种抽象的功能引擎、可信服务以及可信移动模块（MTM）。

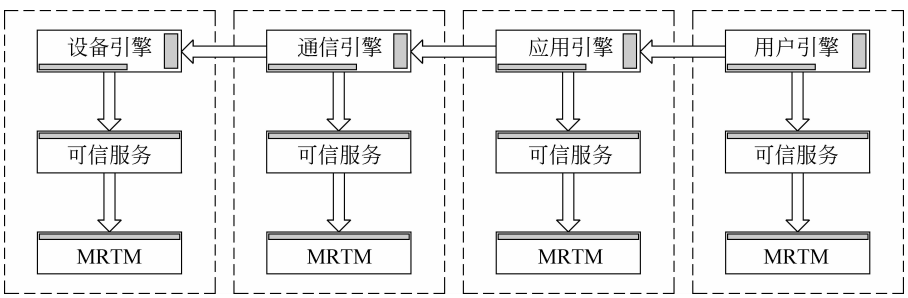

图 5.2 通用可信移动平台架构

1. 抽象功能引擎

通用的可信移动平台架构中包含多个抽象的功能引擎，分别对应在移动场景中不同的利益相关者（stakeholder），并提供相应的服务。这些引擎分别是设备引擎、通信引擎、应用

引擎和用户引擎，每个引擎为其使用者（即利益相关者）提供服务，而各个引擎的资源决定了该引擎能提供什么服务，引擎所有者则决定它如何提供服务。其中，设备引擎提供基本的平台资源，主要包括用户接口、调试链接器、信号发射和接收器、随机数产生器、国际移动设备身份码（International Mobile Equipment Identity，IMEI，即常见的手机序列号）和用户识别模块（Subscriber Identity Module，SIM）接口；通信引擎主要负责实现数据交互接口，提供网络连接并保障通信安全性；应用引擎则包含众多移动平台上可扩展的应用程序，如网络游戏客户端等；用户引擎是直接为用户提供服务的，主要利用其他功能引擎来保护用户数据。总之，设备引擎为通信引擎提供必需的硬件，通信引擎为应用引擎提供基础的数据交互服务，应用引擎则为用户引擎提供具体的数据应用服务，用户引擎负责为用户提供丰富的移动平台功能。图中，实心矩形表示接口，箭头表示依赖关系。

2. 可信服务

每个抽象的功能引擎都对应一个可信服务，主要用于对该抽象引擎中包含的各个具体功能模块实施度量，并将度量值扩展至底层的移动可信模块（MTM）中。

3. 可信移动模块（MTM）

MTM 作为可信移动平台的信任根，是可信移动平台功能架构的核心。考虑到在移动平台使用过程中需要为多个利益相关方提供信任服务（如手机用户和远程移动运营商等），因此，将 MTM 分为远程所有者可信模块（Mobile Remote-Owner Trusted Module，MRTM）和本地所有者可信模块（Mobile Local-Owner Trusted Module，MLTM）两个部分，分别作为本地及远程平台用户的信任锚点。其中，设备、通信（如手机）和应用引擎利用的是 MRTM，这些引擎的远程用户不能物理访问移动设备，但仍然需要安全启动进程来确保相应引擎能够按其预期执行。本地用户引擎主要利用的是 MLTM，本地用户能够物理访问移动设备，但也需要该引擎的可信加载和执行。可信移动平台能够利用 MTM 报告相应功能引擎当前的可信状态，并且对外提供可信状态证明。

下面以 MRTM 为例，简要说明其使用过程，如图 5.3 所示。其中，MRTM 作为可信移动平台的存储信任根（Root of Trust for Storage，RTS）和报告信任根（Root of Trust for Reporting，RTR），为其他系统组件提供基本的存储保护功能以及相应的可信资源（比如 PCR 和签名密钥等）；度量信任根（Root of Trust for Measurement，RTM）和验证信任根（Root of Trust for Verification，RTV）作为基本功能组件，位于 MRTM 外部，利用 MRTM 提供的保护机制实现相应的度量与验证功能。利用 MRTM 构建可信移动环境时，首先，加载 RTM 和 RTV，并由它们对自身的执行状况进行诊断，如果与存储于 MRTM 中的 RIM 值匹配，则将结果扩展到 MRTM 中（第 1 步）；然后由 RTM 对度量验证代理的完整性进行度量（第 2、3 步），并利用 RTV 将所得到的实际度量值与参考完整性值（Reference Integrity Metrics，RIM）证书中的 RIM 值进行比较，如果验证通过，则将该度量值扩展到 MRTM 中，并将执行控制权交给度量验证代理；最后，度量验证代理对移动平台操作系统的完整性进行类似的度量、验证和存储（第 4、5、6 步），验证通过后就运行操作系统。远程利益相关者（如设备提供商或通信运营商）收到上述启动过程的度量值，可与标准值进行验证，以判定相应的功能引擎运行是否可信（如设备服务引擎和通信服务引擎等）。

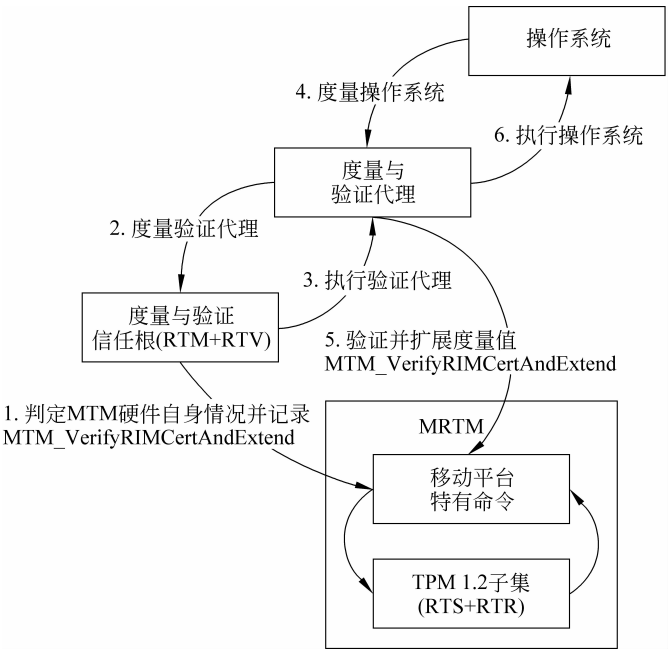

图 5.3　MRTM 使用流程

5.4.3　可信移动平台实现

由于移动平台形态的多样性，TCG 在发布相应可信移动平台规范时并没有明确移动可信模块(MTM)的具体体现方式，也未对可信移动平台的实现给出明确定义。因此，各个移动设备厂商可以用不同的方法实现 MTM，按照 5.4.2 节所述的通用架构构建不同的可信移动平台。

本节简要介绍两种具有代表性的可信移动平台实现方案，它们所使用的 MTM 分别基于 Java 智能卡和 ARM TrustZone 技术来实现。

1. 基于 Java 智能卡的可信移动平台

目前，在普通的移动平台中通常都提供额外的智能卡 Smart Card(如扩展卡或 SIM 卡)，这些智能卡能够支持众多常用的密码算法并提供一定的数据存储和处理能力。这种智能卡非常适合作为运行 MTM 的硬件安全构件，它们能够为 MTM 提供一种类似硬件 TPM 一样的独立硬件固件，使 MTM 能够作为移动平台中独立的硬件信任根，为移动平台构建可信运行环境。下面以 Java 智能卡为例，首先简要介绍基于 Java 智能卡实现的 MTM 架构[18,19]，然后说明以这种 MTM 构建的可信移动平台的方法[20]。

1) 基于 Java 智能卡实现的 MTM

以 Java 智能卡作为运行 MTM 安全构件的主要思想是将 MTM 功能实现为智能卡内部具有独立功能的应用程序，这些程序能够支持符合 TCG 规范的命令执行。移动平台将运行着 MTM 的智能卡作为信任根，构建所需要的可信移动环境，其基本架构如图 5.4 所示。

其中，MTM 的功能实现于智能卡内部，主要分为 MRTM 和 MLTM 两部分，分别以不

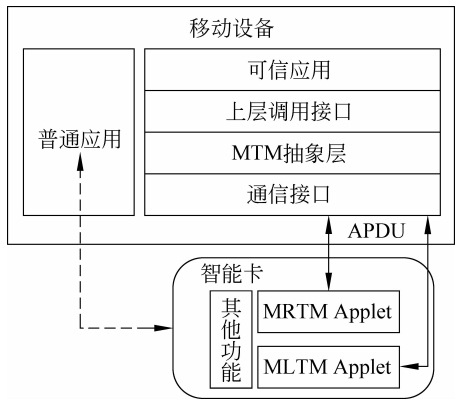

图 5.4 基于 Java 智能卡的可信移动平台软件架构

同的 Java Applet(小应用程序)运行于智能卡中。在智能卡的非易失性存储器内存储 MTM 的背书密钥 EK、授权数据 authdata 等,用硬件密码模块实现 MTM 所需的密码算法运算。基于 Java 智能卡实现的 MTM,需要为移动平台上层用户应用提供调用接口,以访问智能卡中的 MTM,因此需要提供相应的可信软件栈;而且,由于移动平台自身资源有限,需要重新设计其与智能卡之间的通信协议,在保证数据通信的前提下,防范对智能卡中 MTM 的攻击。

2) 基于 Java 智能卡构建的可信移动平台

在使用 Java 智能卡的移动平台中,智能卡能够为移动平台提供多种服务,而作为信任根的 MTM 只是其中的一项重要功能。因此,上述移动平台在使用可信计算技术时,不能影响到其他普通应用的运行。移动设备上的可信应用需要使用 MTM 的可信软件栈及相应的抽象接口来调用底层的可信计算服务,这些接口主要包括上层调用接口、MTM 抽象层和底层通信接口。其中,MTM 抽象层与可信设备驱动类库 TDDL 类似,主要是为访问下层 MTM 实现提供一个类库接口,它接收来自上层应用指令库的命令并将其转换至 MTM 需要的格式,而且还负责处理 MTM 命令的发送与接收。底层通信接口主要用于确保在智能卡与用户可信应用之间的数据安全交换,目前智能卡与外界的通信数据接口采用标准的数据通信协议 APDU(Application Protocol DataUnits,应用协议数据单元)。

为了构建可信移动平台,必须首先保障 MTM 自身的安全性,基于 Java 智能卡实现 MTM 的方法能够较好地满足这种需求。利用智能卡自身的硬件保护机制,能够防范对 MTM 功能实现的篡改;同时,MTM 的两种功能(MRTM 和 MLTM)是以 Java 小应用程序 applet 的形式并发地运行于 Java 智能卡内部的虚拟机上,利用虚拟机提供的安全机制能够确保它们的隔离运行。另外,基于智能卡实现 MTM 也使得它继承了智能卡固有的安全属性,由于对智能卡安全性评估目前已有非常成熟的方法,这也为基于智能卡实现的 MTM 的安全性检测评估提供了方便。

2. 基于 TrustZone 的可信移动平台

基于 ARM TrustZone 实现的 MTM 是另一种常见的构建可信移动平台的方法[19]。TrustZone 技术是 ARM 公司在嵌入式领域里提出的,其目标是在资源受限的特定平台,如手机、PDA 和机顶盒等设备中为敏感应用提供一个安全可信的环境,主要是在其微处理器(CPU)中加入域隔离功能,提供代码的隔离环境和安全服务。TrustZone 的这方面特性可