第5章

可信计算

5.1 可信度量技术信任链的传递

在信任度量模型中信任链是主要的技术实施方案，可以用信任链传递机制将信任边界从可信度量延伸至整个工业嵌入式设备平台。可信计算技术在工业嵌入式电子设备平台上的应用主要体现在可信链的产生与传递这两个方面。可信机制得以实现的原因在于三个可信根：度量可信根 RTM(Root of Trust for Measurement)、存储可信根 RTS(Root of Trust for Storage)、报告可信根 RTR(Root of Trust for Reporting)。RTM 是可信度量的起点，在度量过程中建立信任链。RTS 是一个能准确地记录完整性度量的摘要值和顺序的计算引擎，是一个能进行可靠加密的存储单元。RTR 是一个能可靠报告 RTS 的计算引擎，能可靠报告信息并标识平台身份的可信性。启动序列中的任意一个环节被破坏，都会完全或部分地危及工业嵌入式设备平台上所有应用。所以，研究一种强有力的信任机制去评估系统启动过程是否已经被篡改是十分必要的。信任链的传递流程如图 5-1 所示。

TPM(可信平台模块)对启动序列进行评估的核心是信任链机制。信任链就是在信任当前某一环节的前提下，由该环节去评估下一环节的安全性，确定下一个环节可信之后，再将控制权移交给下一个环节，从而扩展至整个嵌入式平台。具体实现过程如下。

第一步：工业嵌入式平台加电后，可信根 CTRM 作为信任链的源头，系统会最先执行可信根 CTRM 的代码。

第二步：系统从可信根开始，首先进行 BIOS 的可信度量，度量通过后启动 BIOS。

第三步：BIOS 度量 Boot loader，并将度量值扩展到 TPM 对应的 PCR 中，BIOS 完成对 Boot loader 的度量且度量通过后，将控制执行权移交给 Boot loader。

第四步：Boot loader 度量 OS kernel 的启动过程，并将其度量值记录在 TPM 的 PCR(平台配置寄存器) 中，度量通过后执行 OS 的启动流程。

这样交替执行，启动过程的每一部分在启动之前都进行了完整性度量，度量

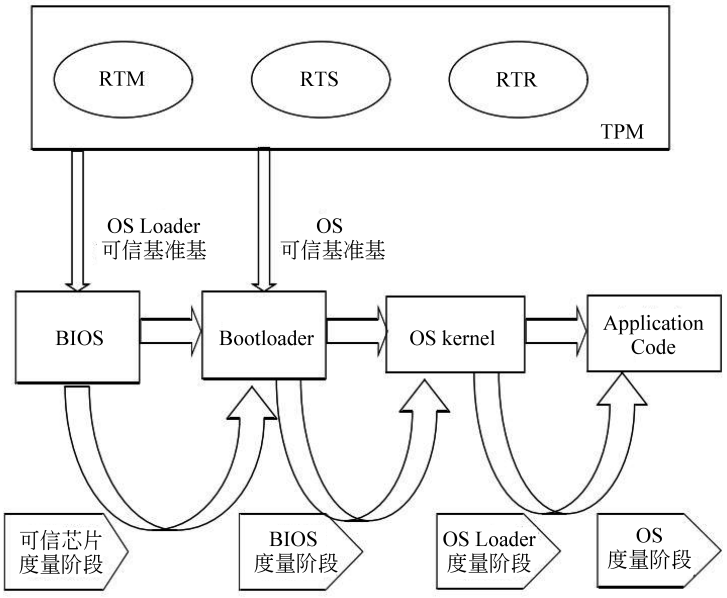

图 5-1　信任链传递过程

值也保存在了 TPM 对应的 PCR 中。当启动过程被攻击者篡改，完整性度量机制将终止程序的执行，从而保证了工业嵌入式平台的安全。

5.2　可信度量机制

可信计算平台的完整性度量技术包括完整性度量的运算、存储、报告和验证。

1）完整性度量的运算

信任链的起点是从可信根开始的，依据可信度量机制来完成信任链的传递。无论是顶层的应用还是底层的 BIOS 引导加载程序，在得到执行之前，都要经过完整性度量的验证操作。在完整性度量技术的应用中，使用散列消息认证码（Hash-bashed Message Authentication Code，HMAC）的一致性校验算法完成可信度量的操作。HMAC 运算利用 SHA-1 摘要算法，将密钥和要发送的消息作为输入，输出则为这个消息的摘要值，这也是目前应用最普遍的度量算法。可信平台模块 TPM 方案中的 HMAC 使用的是 SHA-1 哈希算法，为度量的实现提供了安全的保障。度量完整性的运算过程实质是执行哈希密码摘要算法的过程，摘要运算输入的数据是依据度量者所指定的可以证明被度量者特性的相关数据，输出的摘要值其实就是被度量者经过完整性度量的值。SHA-1 是美国国家标准与技术研究院在 1995 年提出并设计的，并成为美国的国家标准（FIPS PUB 180-1）。摘要算法 SHA-1 是对数据进行一系列加密的算法，随着人们的不断改进和发展而日趋成熟，被普遍采用。该摘要算法是用一种单向的方法，将一段明文转化为固定位数并且长度较短的摘要值的过程。摘要函数是表征明文某种特性的指纹。可信平台模块提供了既满足单向性又满足强抗碰撞性的安全摘要算法 SHA-1 引擎，配合 TPM 提供的用于安全存

储的平台配置寄存器 PCR 以及 TPM 的内部接口函数就可以把信任链传递下去。在信任链传递的过程中，任何组件在获得信任链之前都要进行可信度量，一级认证一级，前一个完整性度量值需要存储，而后一个度量值也需要进行存储，需要注意的是在对这些完整性度量值进行存储的过程中，必须要体现出完整性度量的前后顺序。一个新的度量值不能只是简单地覆盖现有的度量值，否则会无法判断完整性度量的源头。但是如果把每个完整性度量值都进行分别存储，就很难找到一个存储范围比较大的度量存储器。为了使存储到 PCR 中的度量值能够反映系统的启动顺序，TCG 使用一种迭代计算 Hash 值的方式，并称为“扩展”操作，即将 PCR 现在保存的值与新值进行连接，然后再计算摘要值并作为新的度量值保存到当前 PCR 中，算法的扩展如下：New PCRi = Hash(Old PCRi ‖ New Value)，其中，符号||表示连接。Old PCRi 是保存在 PCRi 中的原本的值，把新生成的度量值放到原有的值之后，再执行一次哈希运算，得到新的 PCRi 值。哈希算法有两个与 PCR 结构相关的重要属性：一个是与顺序有关的属性，即先度量 A 再度量 B 与先度量 B 再度量 A 是不一样的；另一个特性是单向性，这对于一个恶意攻击者来说，只知道 PCR 的值，是无法逆向判断出输入的消息。可信平台模块提供的 SHA-1 摘要算法引擎在 TPM 芯片的内部通过会话来实现，流程如图 5-2 所示。

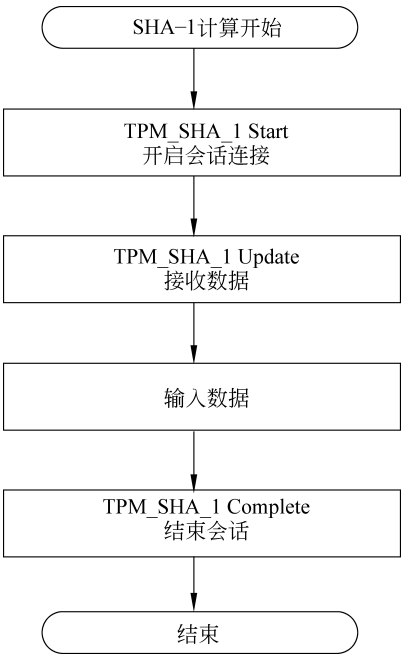

图 5-2　TPM 中的 SHA-1 会话流程图

TPM_SHA_1 Start 用于开启一个 SHA_1 计算对话，在计算期间，TPM 不允许有其他计算过程同时进行，SHA-1 将独占 TPM 资源。接着继续调用 TPM_SHA_1 Update 函数，TPM_SHA_1 Start 函数返回的是将要输入的参数，TPM_SHA_1 Update 函数遵循这些参数形式输入工业嵌入式设备平台中定义的完整数据结构。最后再调用 TPM_SHA_1 Complete 或 TPM_SHA_1 Complete Extend 执行 SHA-1 摘要运算，并对输入的

数据进行分组操作。分组是每 64B 分为一组，得出摘要值。会话完成后，TPM_SHA_1 Complete 函数返回最终的运算结果。

2）完整性存储

信任链执行过程中，反映平台可信性的度量值必须能安全存储，但是硬盘的安全性较低。可信计算最突出的一个特点是采用了一个 TPM 芯片作为信任根，其安全性比硬盘要高。因此，TCG 将可信度量值存储到 TPM 中，即在 TPM 的存储器中专门开辟了一片区域作为平台配置寄存器 PCR，用于存储可信度量值。PCR 位于 TPM 的内部，表示当前平台的配置状态。TCG 规定 PCR 要支持 20B 的存储空间，这也是保证平台完整性的基础。在 TPM 启动时以一定的规则对 PCR 赋予初值，完整性度量结果是以 SHA-1 摘要的形式存储到 PCR 中。为了使一个 PCR 中能够存储更多的摘要值，度量的存储采用扩展机制。在保存完整性度量值时，完整性度量机制要求平台状态信息以日志的形式保存在 TPM 外部的度量日志文件中。平台状态信息不仅包括度量者信息和被度量者的信息，而且包含原本的 PCR 值和新的 PCR 值以及执行完成的时间等相关信息。完整性度量的存储操作是通过一系列的函数来实现的。

随着工业化和信息化的不断融合以及互联网技术的蓬勃发展，工业控制系统正通过工业以太网、互联网技术等进行新一轮的技术革新，其变化如图 5-3 所示。

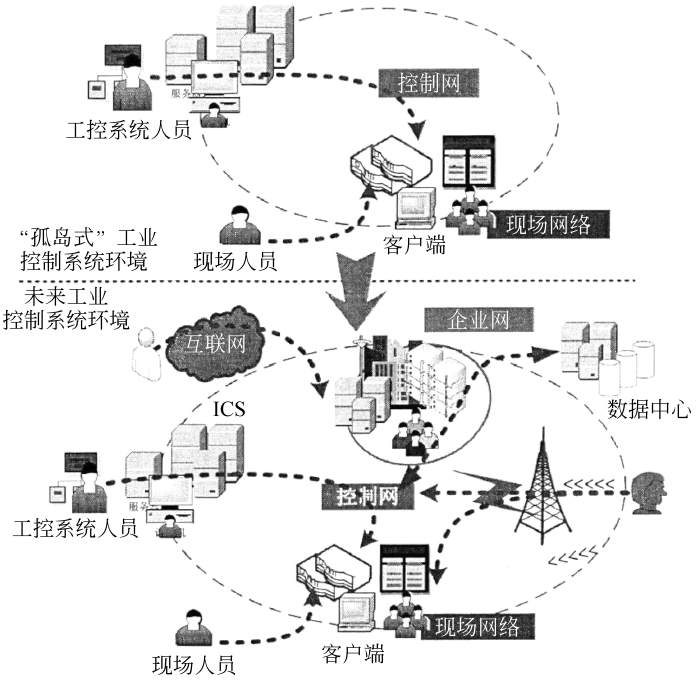

图 5-3　工业控制系统变化图

根据国内信息安全公司绿盟科技综合整理收录的工业控制系统的漏洞信息，可以看出从 2010 年开始，公开的工业控制系统漏洞呈井喷的趋势。在 2011 年之前，公开披露的工业控制系统相关漏洞数量相当少，但在 2010 年“震网”病毒爆发之后，人们对工业控制

系统的安全问题更为关注，工业控制系统厂商对自身产品的安全性进行重新审视，而使信息安全漏洞暴露出来。可以看出，随着各方面对工业控制系统的安全日益重视，工业控制系统的相关公开漏洞数量仍将保持一个快速增长的总体趋势。

面对 2010 年“震网”事件之后产生的各种针对工业控制系统的威胁，世界各国对工控系统的安全问题的关注被提升到一个新的高度，世界各国以及各行各业在政策法规、行业标准、解决方案等方面进行了深入的探讨，工业控制系统的信息安全更成为备受工业和信息安全领域研究机构关注的研究热点。

作为信息产业发展的领导者，美国从 20 世纪开始一直致力于保护关键性工控行业的信息安全，并提升到国家安全的高度，将其列入美国国家急需特别关注和保障的关键基础设施范畴。2009 年颁布了《保护工业控制系统战略》等行业指导标准，指导能源、关键制造业等关键工业相关行业的信息安全。同时成立了相应的应对工控行业信息安全事件的小组，致力于工控行业相关安全事故监控、分析执行漏洞和恶意代码、为事故响应和取证分析提供现场支持，并共享信息安全事故中的具体数据，提供工控系统信息安全事件监控及行业安全态势分析，并以季度报告的方式公开发布。而且美国国土安全部启动的控制系统安全计划则依托工业控制系统模拟仿真平台，结合实际现场应用测试与实验环境下测试来应对工业控制系统信息安全漏洞难寻找、难解决等实际问题。美国国家标准与技术研究院发布了《工业控制系统安全指南 NISTSP800-82》等相关的工控系统的安全建设标准指南或最佳实践文档。另外，其国内的传统信息安全厂商赛门铁克、MCAFEE、思科以及传统工控厂商罗克韦尔、通用电气以及一些新兴的专业工控安全厂商在工控系统的安全防护及产品服务提供方面也都展开了深入研究、实践及产业化工作，并总体上处于领先的地位。在欧洲则以德国西门子、法国施耐德电气为代表的工业控制系统提供商为主，为用户提供相应的安全产品、服务及解决方案。例如西门子基于纵深防御理念的过程控制系统信息安全解决方案，在保证物理安全的前提下，对过程控制系统进行系统的风险分析与评估，针对不同性质的安全威胁，有针对性地研制并分层次部署具有不同特性的安全措施。该方案适用于流程行业的过程控制系统信息安全，包括石油石化行业、化工行业、电力行业、制药行业等领域，可极大地降低控制系统信息安全维护方面的综合成本以及工厂的信息安全风险，但是该方案采取深层次的隔离以及访问控制需要严格的风险评估，对现场员工的信息安全防御的能力要求较高，一般企业达不到要求。施耐德电气在中国拥有多年工控现场实践经验的前提下，提出了针对设备级、系统级和管理级的三级纵深防护体系从对控制现场物理设备层级的保护着手，向上级拓展，综合提高系统的防护能力，该方案类似于西门子的纵深防御理念，从系统脆弱性与安全管理着手用严格的网络安全设备进行层级布置，但没有从根源上解决传统防御措施的弊端。在专业的工控安全厂商方面，加拿大多芬诺公司著名的工控系统防火墙通过对工业控制现场的通信进行白名单过滤，其产品在石化等多个行业应用广泛。此外，还有一些开源组织提供相应的工控安全工具，例如 Nessus 利用相应的工控系统安全插件，对 SCADA 系统或 PLC 的控制设备的脆弱性进行检测评估。这些防范措施针对性强，适用解决特定场合特定现场的安全问题，但不利于系统的变化升级等管理，且整体性不强。在工控安全的国际标准研究方面，有国际电工委员会下的网络和系统信息安全工作组与国际自动化协会共同制定的 IEC62443，美

国国家标准技术研究院制定的工控系统的安全指南 NISTSP800-82 等，都为工业控制系统提供了重要的参考标准。

中国自从《关于加强工业控制系统信息安全管理的通知》发布之后，国内各行各业都对工控系统安全的认识达到一个新的高度，电力、石化、制造、烟草等多个行业，陆续制定了相应的指导性文件，来指导相应行业的安全检查与整改活动。国家标准相关的组织 TC260、TC124 等标准组也已经启动了相应标准的研究制定工作。具体政策法规有《关于加强工业控制系统信息安全管理的通知》《电力二次系统安全防护规定》《电力工控信息安全专项监管工作方案》等。并且在工控行业相关研究科研单位、企业等 24 家单位领导下于 2014 年 4 月成立了工业控制系统信息安全产业联盟，以此推动工业控制系统信息安全研究进展，为我国工业化生产提供信息安全的保障，维持整个工控行业的稳定发展。国内工控安全行业根据工控系统和信息安全背景分为两类。工控系统、信息安全背景的企业各具有优势，但都缺乏对方所具有的能力和人才储备。工控系统背景的厂商代表性企业有和利时、浙大中控等，因缺少信息安全攻防人才储备，短期内难以大幅度提升其在工控系统上面的信息安全攻防实力，国内整个工控安全市场也刚刚起步，尚没有明显具有竞争优势的企业或产品。信息安全背景的厂商代表性企业有绿盟科技、启明星辰、天融信、中科网威等这些传统的信息安全厂商，它们的优势在于多年的信息攻防、安全服务经验的积累以及完善的信息安全产品线，当工控系统面对来自系统、网络层面的黑客攻击时，相对于工控系统背景的厂商来说，其优势自然是不言而喻的。但其因工业控制系统行业并非是信息安全背景的厂商的传统关注对象，对工控系统领域相关技术与人才的储备也是从事工控安全研究及产品产业化的最大短板。

研究机构根据工业控制系统的特点，给出很多提高系统安全性的解决方案，较单一的控制现场，对于综合性和交互性强的控制现场会带来更为严峻的控制安全问题。国内工业控制系统信息安全解决方案相对国外的解决方案，整体应用面更窄，更多是根据传统的防御手段进行搭配组合，而且技术也相对落后。对于稳定运行的工控系统，过程系统架构和业务流程对于特定的行业相对更具专业特点，常见的防御信息泄露、抵御攻击的手段直接应用效果并不好，而且容易对工控系统本身造成影响。目前通用的防火墙、杀病毒、漏洞扫描“老三样”防御措施针对工业上的应用也未有进行针对性的应变，整体性的解决方案又没有达到行业的要求。

针对上述问题，下面介绍一种基于可信计算的工业控制系统解决方案，来从整体上解决工业控制系统的信息安全问题，对系统外部接入、内部防御进行统一控制，对系统的业务流程进行保障，使系统能够按照既定的运行方式进行工作。

可信计算是可信计算组织（Trusted Computing Group，TCG）提出从微机芯片、主板、硬件结构、BIOS 和操作系统等软硬件底层出发，从数据库、网络、应用等方面综合考虑以保证微机系统信息安全为目标的平台，旨在提供可靠、可用、安全的计算机系统。从信息安全的角度出发，计算机系统按照既定的运行方式、运行顺序进行操作，那么说明该系统是可以信任的，可以保证系统的安全性。可信计算正是利用这种思想进行拓展，以硬件结构可信平台模块（Trusted Platform Module，TPM）作为信任的根基，通过 TPM 的可信保障将信任进行传递，进而拓展建立相应的可信平台，并把这种信任传递到其余的可信平

台，从而建立起可信环境来确保整个信任链的可信。其中 TPM 集成了可信计算所需的安全模块功能，其主要组成结构如图 5-4 所示，主要由密码引擎部件、存储器组成，实现了作为硬件可信根基所需的基本功能。

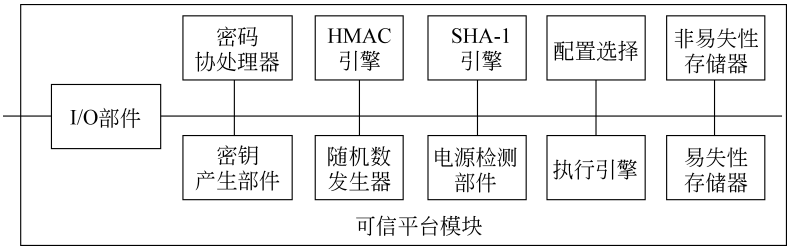

图 5-4　TPM 组成结构

内部工作的数据，与密码学引擎进行协同工作。所以 TPM 作为整个平台的硬件信任根基，必须确保自身的安全性，正是其基于硬件的属性，同时提供多种密码和访问控制技术，保证了 TPM 自身以及内部数据不被非法攻击的基本能力。以此为基础，TPM 通过 LPC 总线与主板上的芯片进行相连，这样实现了 TPM 作为可信计算平台的硬件基础结构。

根据 TCG 规范，一个实体要满足可信的状态，需要具有能对本身的状态进行保护的能力，同时证明自身的可信状态，并对自身完整性进行存储与报告。

(1) 保护能力：通过可信平台模块芯片中证书、密码学等功能，以及可信储存根中平台寄存器 PCR 的硬件存储功能，实现对计算机系统中数据以及软件的安全保护和网络连接的控制。

(2) 证明：根据可信芯片的保护能力对实体的状态进行保护，对自身的可信性进行度量证明，再以此为基础通过可信芯片的身份证明密钥 AIK 进行签名，并通过表明自身可信性的证明证书向需要进行连接的终端进行报告来实现可信证明。这样就保证了自身的身份、可信性，来达到证明的可行性。

(3) 完整性的度量存储和报告：系统文件的度量 Hash 值可以用来判断检测系统资源是否遭到破坏，对于正确的系统资源数据计算器 Hash 值并存储于平台配置寄存器 PCR 中，在系统启动时重新计算系统资源数据的 Hash 值，并与事先存储的正确值进行比较、印证，在度量、储存之后，当访问客体询问时可以提供报告，判断平台的可信状态。

TCG 为了规范对硬件的访问以提供更为安全的操作规范，TCG 提供两种平台模式。

(1) 内核模式：内核模式为用户模式提供相应的服务基础，涵盖了 TPM 设备驱动和 TPM 芯片。

(2) 用户模式：用户模式处于 TPM 设备驱动以上，用于处理响应用户请求或者系统启动时载入的程序和服务的执行。对于系统启动时载入的程序和服务通常嵌入系统的启动脚本，操作系统对此进行处理，具有较高的安全性。

5.3 云计算的可信平台构建

云计算是一种新兴的共享基础架构，能够为广大用户提供丰富的虚拟化资源和服务，用户仅需支付少量的费用就能够享受这些服务和资源。其中，云计算架构主要包括三层：基础设施即服务（Infrastructure as a Service，IaaS）、平台即服务（Platform as a Service，PaaS）、软件即服务（Software as a Service，SaaS），如图 5-5 所示。

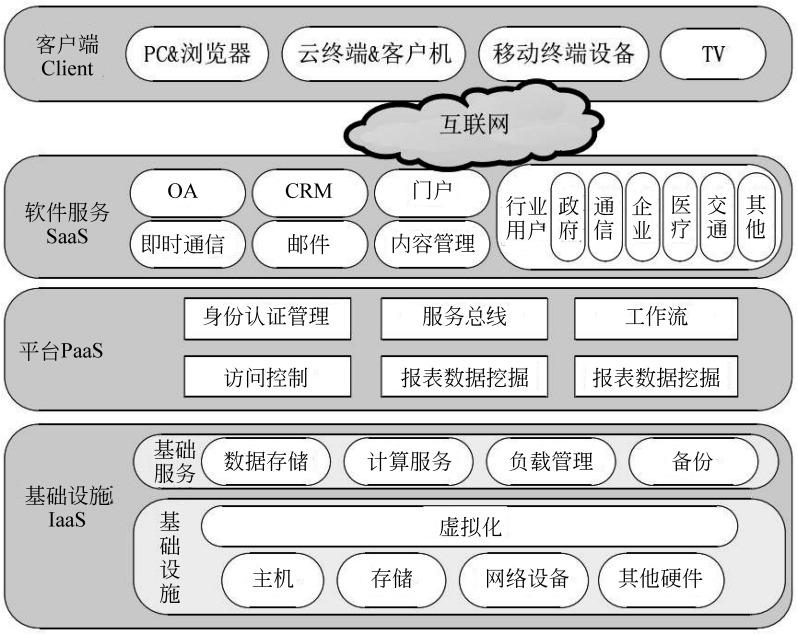

图 5-5 云计算架构层次结构图

下面对这三层进行具体描述。

SaaS：用户通过网络向云服务提供商提出软件资源请求，云服务提供商根据用户的请求将用户所需的资源以软件服务的形式提供给用户。

PaaS：云服务提供商向用户提供虚拟化的平台运行环境，而用户不必购买软件或硬件来搭建平台就能得到所需要的平台系统，并能根据自身需要在平台上部署各种应用。

IaaS：云服务提供商向用户提供计算过程所需的软硬件资源，包括计算资源、备份资源和存储资源等。这些资源被整合到一个虚拟化资源池中，以服务的形式提供给用户。虽然用户使用的这些资源都是虚拟的，但能享受到与真实资源所提供的同等功能。

由于云计算独特的结构和计算模式，使得云计算具有超大规模、虚拟化、高可靠性、通用性、高扩展性、按需服务和极其廉价等特点，但也正是这些特点，给云计算带来了严重的缺陷：来自云服务提供商的不可信、网络的不安全因素以及虚拟化问题，这些都已成为阻碍云计算发展的重要因素。

密钥管理是可信计算技术实现的一个重要组成部分，在 TCG 软件规范中一共为可

信计算定义了七种不同功能类型的密钥，主要包括存储密钥（Storage Keys，SK）、签名密钥（Signing Keys，SK）、身份认证密钥（Attestation Identity Keys，AIK）、绑定密钥（Bind Keys，BK）、背书密钥（Endorsement Key，EK）、鉴别密钥（Authentication Keys，AK）和继承密钥（Legacy Keys，LK）。这七种密钥根据用途又可分为签名密钥和加密密钥，签名密钥主要用来实现 TPCM 中的签名操作，而加密密钥主要用来实现 TPCM 中的加密相关操作。此外，对称密钥作为 TPCM 内部的鉴别密钥单独分类，仅供 TPCM 内部使用，与用户操作无关。TPCM 中密钥的层次结构图，如图 5-6 所示。

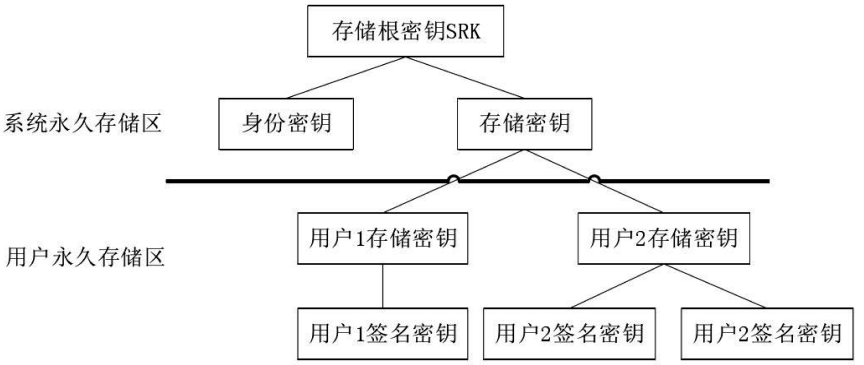

图 5-6　TPCM 中密钥的层次结构图

下面对 TPCM 中这七种密钥进行简要介绍。

（1）存储密钥。主要用来封装和存储 TPCM 中除对称密钥之外的其他密钥和 TPCM 内部数据，还可以保护 TPCM 外部的密钥和数据。其中位于图 5-6 中树根位置所指示的根存储密钥拥有最高的系统权限，伴随着用户的生成而生成，是平台系统的可信存储根。

（2）签名密钥。签名密钥是采用 RSA 算法实现的非对称密钥。其中，公钥对外开放，能够实现签名的认证；而私钥保护在 TPCM 内部，主要负责对数据进行签名，不可用于加密操作。

（3）身份认证密钥。由 TPCM 内部的 EK 产生的一种签名密钥，能够通过对 PCR 值进行签名来标识平台的真实身份，从而在不泄露平台身份信息的前提下能够提供平台状态和配置的可信证明。

（4）绑定密钥。与系统平台绑定在一起，只能用来对对称密钥进行简单的 RSA 加密存储操作。

（5）背书密钥。背书密钥是 TPCM 密钥的核心，属于不可迁移密钥，嵌入在 TPCM 安全芯片内部，是可信平台的唯一、永久身份标识。此外，背书密钥能够用于对用户的授权信息和与 AIK 相关的数据进行解密，但不能够实现对数据的加密或签名，也不能直接向外界提供平台的身份证明。

（6）鉴别密钥。主要用来保护 TPCM 在传输会话中所使用的对称密钥。

（7）继承密钥。当需要执行加密或签名操作时才会载入到 TPCM 内部，主要用来实现不同平台间数据的传输。为实现对 TPCM 中密钥的管理，保护密钥的隐秘性、完整性以及可认证性，防止非法用户对密钥的泄露和破坏，通常采用分层机制对密钥进行保护，如图 5-7 所示。SRK 作为主密钥，存储在 TPCM 的安全保护区域内，由 TPCM 对其进

行保护，再由 SRK 加密保护 k-1 层密钥，k-1 层密钥保护第 k 层密钥，待加密的数据或密钥由第 k 层密钥进行加密或签名保护。加密或签名后的数据存储在 Data Blob 中；加密或签名后的密钥存储在 Key Blob，由密钥缓存管理器（Key Cache Manager，KCM）进行管理和维护。此后，在一段时间内不活动的加密数据或密钥会被存储到外部存储设备上。

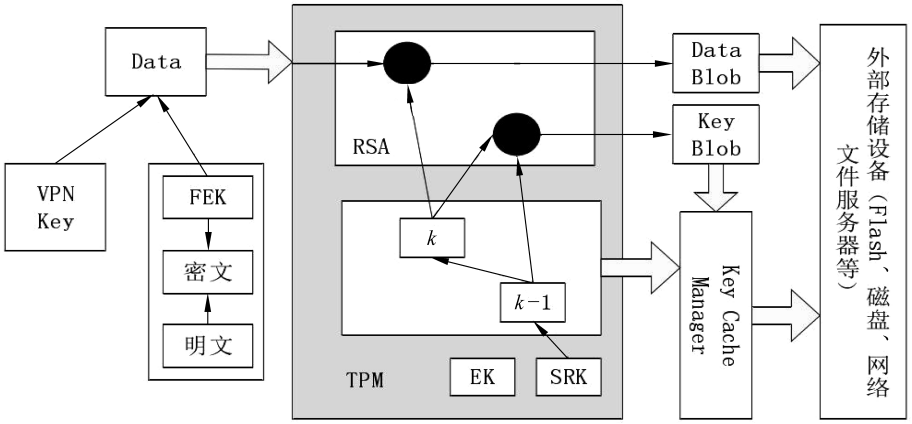

图 5-7　密钥存储保护结构

为实现云计算模式中整体系统机制的高效运行，特建立系统、安全、可信三方独立运行的子系统，其中云可信子系统透明运行，为云安全提供可信支撑，如图 5-8 所示为可信云层次结构。

其中横向可以分为云计算子系统、云安全子系统和云可信子系统；纵向分为管理层、平台层和虚拟化层。在实际运行中安全系统的运行对云计算系统来说是完全透明的，不会对系统运行产生任何影响；安全子系统虽然能够通过可信子系统调用底层的可信功能，但是这些可信功能的具体实现是在可信子系统内部完成，对安全子系统是完全透明的。这样就做到了云计算系统、云安全系统和云可信系统功能的分离，各层次更加鲜明，下面对该可信子系统中各层次进行具体描述。

1）虚拟化层

虚拟化层主要包含客户虚拟机，能通过虚拟化层应用程序为云计算系统上层应用提供具体服务。客户虚拟机的安全是通过云安全子系统来实现的，云安全系统根据客户的安全需求为虚拟机部署对应的安全机制。此外，为支持云系统的可信，特在云可信子系统上建立虚拟机可信服务程序，虚拟机可信服务通过调用第三方可信服务中心的可信策略来为虚拟机安全机制和平台可信服务提供可信支撑。在整个可信云支撑子系统中，应用系统、安全系统和可信系统既相互关联又能独立运行，各模块功能的具体实现在各子系统内部完成，对外仅提供数据功能交互的接口，实现了数据的透明传输。

2）平台层

平台层主要用于部署虚拟化平台，包括云平台中间件、平台安全机制和平台可信服务。其中，云平台中间件位于云计算系统中，主要用于不同虚拟化平台间的交互；平台安全机制采用安全技术来保障虚拟化平台的安全；平台可信服务通过与可信管理中心、虚拟机可信服务进行通信，获取可信管理中心发送的可信管理策略以及虚拟机的可信需求，对