(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 104618096 B
(45)授权公告日 2018.10.30

(21)申请号 201410849795.3

(22)申请日 2014.12.30

(65)同一申请的已公布的文献号
申请公布号 CN 104618096 A

(43)申请公布日 2015.05.13

(73)专利权人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

(72)发明人 施迅 叶思海

(74)专利代理机构 北京同达信恒知识产权代理有限公司 11291
代理人 冯艳莲

(51)Int.Cl.
H04L 9/08(2006.01)

(56)对比文件
CN 102549594 A,2012.07.04,说明书第[0016]、[0048]-[0050],附图3.
CN 102177678 A,2011.09.07,说明书第[0019]-[0020]段.

审查员 陈玲珑

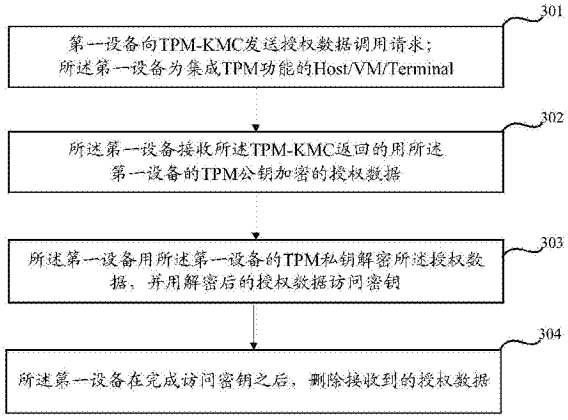
权利要求书2页 说明书13页 附图7页

(54)发明名称

保护密钥授权数据的方法、设备和TPM密钥管理中心

(57)摘要

本发明公开了一种保护密钥授权数据的方法、设备和TPM密钥管理中心，需要访问密钥时向TPM密钥管理中心临时申请授权数据，访问密钥之后再删除申请到的授权数据，从而提高了密钥授权数据的安全性，降低了授权数据泄露和被篡改破坏的可能性。该方法为：第一设备向TPM密钥管理中心发送授权数据调用请求；所述第一设备为集成TPM功能的物理服务器、虚拟机或终端；所述第一设备接收所述TPM密钥管理中心返回的用所述第一设备的TPM公钥加密的授权数据；所述第一设备用所述第一设备的TPM私钥解密所述授权数据，并用解密后的授权数据访问密钥；所述第一设备在完成访问密钥之后，删除接收到的授权数据。



CN 104618096 B

1.一种保护密钥授权数据的方法,其特征在于,包括:

第一设备向可信平台模块TPM密钥管理中心发送授权数据调用请求;所述第一设备为集成TPM功能的物理服务器、虚拟机或终端;

所述第一设备接收所述TPM密钥管理中心返回的用所述第一设备的TPM公钥加密的授权数据;

所述第一设备用所述第一设备的TPM私钥解密所述授权数据,并用解密后的授权数据访问密钥;

所述第一设备在完成访问密钥之后,删除接收到的授权数据。

2.如权利要求1所述的方法,其特征在于,所述方法还包括:

所述第一设备调用TPM的随机数接口,生成硬件随机数;

所述第一设备将所述硬件随机数作为指定密钥的授权数据,对该密钥进行加密;

所述第一设备用所述TPM密钥管理中心的TPM公钥对该授权数据进行加密;

所述第一设备将加密后的授权数据通过移动网络发送到所述TPM密钥管理中心进行保存;

所述第一设备接收到所述TPM密钥管理中心的成功响应消息后,删除所述第一设备中的授权数据。

3.一种保护密钥授权数据的方法,其特征在于,包括:

可信平台模块TPM密钥管理中心接收第一设备发送的授权数据调用请求;所述第一设备为集成TPM功能的物理服务器、虚拟机或终端;

所述TPM密钥管理中心在认证通过所述第一设备的访问权限后,根据所述授权数据调用请求,获取存储在数据库中的授权数据;

所述TPM密钥管理中心调用TPM,解密获取的授权数据;

所述TPM密钥管理中心用所述第一设备的TPM公钥对解密后的授权数据进行再加密;

所述TPM密钥管理中心将再加密后的授权数据通过移动网络发送给所述第一设备。

4.如权利要求3所述的方法,其特征在于,所述方法还包括:

所述TPM密钥管理中心接收所述第一设备通过移动网络发送的用所述TPM密钥管理中心的TPM公钥加密的授权数据;

所述TPM密钥管理中心用所述TPM密钥管理中心的TPM私钥解密该授权数据;

所述TPM密钥管理中心调用TPM对解密后的授权数据进行再加密后,保存到数据库中;

所述TPM密钥管理中心向所述第一设备发送成功响应消息。

5.一种保护密钥授权数据的设备,其特征在于,所述设备为集成可信平台模块TPM功能的物理服务器、虚拟机或终端,所述设备包括:

第一发送单元,用于向TPM密钥管理中心发送授权数据调用请求;

接收单元,用于接收所述TPM密钥管理中心返回的用所述设备的TPM公钥加密的授权数据;

解密单元,用于用所述设备的TPM私钥解密所述授权数据,并用解密后的授权数据访问密钥;

第一删除单元,用于在完成访问密钥之后,删除接收到的授权数据。

6.如权利要求5所述的设备,其特征在于,所述设备还包括:

随机数生成单元，用于调用TPM的随机数接口，生成硬件随机数；

第一加密单元，用于将所述硬件随机数作为指定密钥的授权数据，对该密钥进行加密；

第二加密单元，用于用所述TPM密钥管理中心的TPM公钥对该授权数据进行加密；

第二发送单元，用于将加密后的授权数据通过移动网络发送到所述TPM密钥管理中心进行保存；

第二删除单元，用于在接收到所述TPM密钥管理中心的成功响应消息后，删除所述设备中的授权数据。

7.一种可信平台模块TPM密钥管理中心，其特征在于，包括：

第一接收单元，用于接收第一设备发送的授权数据调用请求；所述第一设备为集成TPM功能的物理服务器、虚拟机或终端；

获取单元，用于在认证通过所述第一设备的访问权限后，根据所述授权数据调用请求，获取存储在数据库中的授权数据；

第一解密单元，用于调用TPM，解密获取的授权数据；

第一加密单元，用于用所述第一设备的TPM公钥对解密后的授权数据进行再加密；

第一发送单元，用于将再加密后的授权数据通过移动网络发送给所述第一设备。

8.如权利要求7所述的TPM密钥管理中心，其特征在于，所述TPM密钥管理中心还包括：

第二接收单元，用于接收所述第一设备通过移动网络发送的用所述TPM密钥管理中心的TPM公钥加密的授权数据；

第二解密单元，用于用所述TPM密钥管理中心的TPM私钥解密该授权数据；

第二加密单元，用于调用TPM对解密后的授权数据进行再加密后，保存到数据库中；

第二发送单元，用于向所述第一设备发送成功响应消息。

保护密钥授权数据的方法、设备和TPM密钥管理中心

技术领域

[0001] 本发明涉及信息安全领域，尤其涉及一种保护密钥授权数据的方法、设备和TPM密钥管理中心。

背景技术

[0002] 计算机系统中为提供信息安全防护机制而大量使用的对称密钥、私钥、共享秘密等均属于敏感数据，这些敏感数据一旦泄露，与其相关的被加密数据的机密性将受到严重影响。因此必须提供安全保护机制，防止其以明文的形式保存在系统或代码中。保护这些敏感数据的机密性，应考虑部署以下防护措施中的一种或多种：

[0003] 第一种：密钥加密存储，为了保护对称密钥、私钥、共享秘密等的机密性，需要对这些信息再进行加密。例如，使用密钥加密密钥再对对称密钥、私钥进行加密保存。

[0004] 第二种：基于硬件的安全保护，将明文对称密钥及私钥的使用限制于物理保护容器(如安全芯片)之内，密钥的使用(加密、解密等)始终不离开硬件模块。

[0005] 第三种：访问控制，设备提供权限控制功能，限制密钥仅允许密码模块访问或仅允许高权限的用户读取。

[0006] 可信平台模块(英文：Trusted Platform Module，简称：TPM)是业界认可的密钥保护方案，通过集成密钥和加解密运算引擎，能够提供基于硬件的敏感信息安全存储功能，大部分商用计算机都有TPM，主流的通用操作系统也都支持TPM功能，如Microsoft Bitlocker使用TPM保存加密密钥。

[0007] TPM安全芯片是一种含有密码运算和存储部件的小型芯片系统，通常由中央处理器(英文：Central Processing Unit，简称：CPU)、存储器、输入/输出端口(英文：Input/Output，简称：I/O)、密码运算器、随机数产生器和嵌入式操作系统等部件组成。TPM标准是由国际工业标准组织——可信计算组织(Trusted Computing Group，TCG)制定的，该标准通过在计算机系统中嵌入一个包含密钥生成、加解密计算、安全存储和防篡改功能的芯片，使非法用户无法对其内部的数据进行访问更改，从而确保了身份认证和数据加密的安全性。

[0008] 以TPM为安全存储根密钥的信任根，向用户和应用程序提供TPM密钥管理应用程序编程接口(英文：Application Programming Interface，简称：API)，形成的密钥分层保护结构如图1所示，包括：

[0009] TPM硬件根密钥：用于为上层密钥(如密钥加密密钥)提供机密性保护，位于密钥分层保护结构的底端，由TPM芯片提供，仅限设备本地使用；包括一对公私钥，以及其它一些密钥参数信息。其中公钥是公开的信息，可以通过API读出；但私钥是私密的，存放在TPM的安全存储区域，只在TPM内部使用，没有任何途径被读出到TPM外部。

[0010] 密钥加密密钥：用于为上层工作密钥提供机密性保护，自身受根密钥保护。密钥加密密钥的职能可以直接由根密钥兼任。

[0011] 工作密钥：用于直接对业务数据或用户数据进行加解密、签名和消息认证码(英

文:Message Authentication Code,简称:MAC)等操作,包括存储加密密钥、预共享密钥、MAC密钥、签名密钥等。

[0012] API:用于为应用程序提供调用的TPM密钥访问接口,支持对上述根密钥、密钥加密密钥和工作密钥的创建、清除、更新和使用等操作。应用程序执行这些操作时都需要指定对应密钥的授权数据。

[0013] 在TCG密码管理体系中,在创建密钥时均会分配一个授权数据,访问密钥时需要输入与该密钥对应的授权数据。然而,由于在自动化运行的系统中,如互联网(英文:WEB)服务器、数据库等,无法通过交互的方式输入密钥的授权数据,因此授权数据只能和密钥一起持久化地保存在内存或存储设备上,因而授权数据存在泄露和被暴力破解的风险,安全性能低。

发明内容

[0014] 本发明提供一种保护密钥授权数据的方法、设备和TPM密钥管理中心,用以解决现有技术中在自动化运行的系统中,密钥授权数据只能和密钥一起不安全地保存在计算机静态存储设备上,安全性能低的问题。

[0015] 第一方面,本发明提供了一种保护密钥授权数据的方法,包括:

[0016] 第一设备向TPM密钥管理中心发送授权数据调用请求;所述第一设备为集成TPM功能的物理服务器、虚拟机或终端;

[0017] 所述第一设备接收所述TPM密钥管理中心返回的用所述第一设备的TPM公钥加密的授权数据;

[0018] 所述第一设备用所述第一设备的TPM私钥解密所述授权数据,并用解密后的授权数据访问密钥;

[0019] 所述第一设备在完成访问密钥之后,删除接收到的授权数据。

[0020] 结合第一方面,在第一方面的第一种可能的实现方式中,所述方法还包括:

[0021] 所述第一设备调用TPM的随机数接口,生成硬件随机数;

[0022] 所述第一设备将所述硬件随机数作为指定密钥的授权数据,对该密钥进行加密;

[0023] 所述第一设备用所述TPM密钥管理中心的TPM公钥对该授权数据进行加密;

[0024] 所述第一设备将加密后的授权数据通过移动网络发送到所述TPM密钥管理中心进行保存;

[0025] 所述第一设备接收到所述TPM密钥管理中心的成功响应消息后,删除所述第一设备中的授权数据。

[0026] 第二方面,本发明提供了一种保护密钥授权数据的方法,包括:

[0027] TPM密钥管理中心接收第一设备发送的授权数据调用请求;所述第一设备为集成TPM功能的物理服务器、虚拟机或终端;

[0028] 所述TPM密钥管理中心在认证通过所述第一设备的访问权限后,根据所述授权数据调用请求,获取存储在数据库中的授权数据;

[0029] 所述TPM密钥管理中心调用TPM,解密获取的授权数据;

[0030] 所述TPM密钥管理中心用所述第一设备的TPM公钥对解密后的授权数据进行再加密;

[0031] 所述TPM密钥管理中心将再加密后的授权数据通过移动网络发送给所述第一设备。

[0032] 结合第二方面，在第二方面的第一种可能的实现方式中，所述方法还包括：

[0033] 所述TPM密钥管理中心接收所述第一设备通过移动网络发送的用所述TPM密钥管理中心的TPM公钥加密的授权数据；

[0034] 所述TPM密钥管理中心用所述TPM密钥管理中心的TPM私钥解密该授权数据；

[0035] 所述TPM密钥管理中心调用TPM对解密后的授权数据进行再加密后，保存到数据库中；

[0036] 所述TPM密钥管理中心向所述第一设备发送成功响应消息。

[0037] 第三方面，本发明提供了一种保护密钥授权数据的设备，所述设备为集成TPM功能的物理服务器、虚拟机或终端，所述设备包括：

[0038] 第一发送单元，用于向TPM密钥管理中心发送授权数据调用请求；

[0039] 接收单元，用于接收所述TPM密钥管理中心返回的用所述设备的TPM公钥加密的授权数据；

[0040] 解密单元，用于用所述设备的TPM私钥解密所述授权数据，并用解密后的授权数据访问密钥；

[0041] 第一删除单元，用于在完成访问密钥之后，删除接收到的授权数据。

[0042] 结合第三方面，在第三方面的第一种可能的实现方式中，所述设备还包括：

[0043] 随机数生成单元，用于调用TPM的随机数接口，生成硬件随机数；

[0044] 第一加密单元，用于将所述硬件随机数作为指定密钥的授权数据，对该密钥进行加密；

[0045] 第二加密单元，用于用所述TPM密钥管理中心的TPM公钥对该授权数据进行加密；

[0046] 第二发送单元，用于将加密后的授权数据通过移动网络发送到所述TPM密钥管理中心进行保存；

[0047] 第二删除单元，用于在接收到所述TPM密钥管理中心的成功响应消息后，删除所述第一设备中的授权数据。

[0048] 第四方面，本发明提供了一种TPM密钥管理中心，包括：

[0049] 第一接收单元，用于接收第一设备发送的授权数据调用请求；所述第一设备为集成TPM功能的物理服务器、虚拟机或终端；

[0050] 获取单元，用于在认证通过所述第一设备的访问权限后，根据所述授权数据调用请求，获取存储在数据库中的授权数据；

[0051] 第一解密单元，用于调用TPM，解密获取的授权数据；

[0052] 第一加密单元，用于用所述第一设备的TPM公钥对解密后的授权数据进行再加密；

[0053] 第一发送单元，用于将再加密后的授权数据通过移动网络发送给所述第一设备。

[0054] 结合第四方面，在第四方面的第一种可能的实现方式中，所述TPM密钥管理中心还包括：

[0055] 第二接收单元，用于接收所述第一设备通过移动网络发送的用所述TPM密钥管理中心的TPM公钥加密的授权数据；

[0056] 第二解密单元，用于用所述TPM密钥管理中心的TPM私钥解密该授权数据；

[0057] 第二加密单元，用于调用TPM对解密后的授权数据进行再加密后，保存到数据库中；

[0058] 第二发送单元，用于向所述第一设备发送成功响应消息。

[0059] 本发明提供的方案，通过将密钥授权数据保存到TPM密钥管理中心，需要访问密钥时向TPM密钥管理中心临时申请授权数据，访问密钥之后再删除申请到的授权数据，从而提高了密钥授权数据的安全性，降低了授权数据泄露和被篡改破坏的可能性。

附图说明

[0060] 图1为现有技术下密钥分层保护结构图；

[0061] 图2为本发明实施例提供的一种保护密钥授权数据的系统示意图；

[0062] 图3为本发明实施例提供的一种Host/VM/Terminal侧保护密钥授权数据的流程图；

[0063] 图4为本发明实施例提供的一种TPM-KMC侧保护密钥授权数据的流程图；

[0064] 图5为本发明实施例提供的一种创建和保存密钥授权数据的流程图；

[0065] 图6为本发明实施例提供的一种使用密钥授权数据的流程图；

[0066] 图7为本发明实施例提供的一种保护密钥授权数据的设备的结构图；

[0067] 图8为本发明实施例提供的一种KTM-KMC的结构图。

具体实施方式

[0068] 本发明实施例提供了一种保护密钥授权数据的方法、设备和TPM密钥管理中心(英文:TPM Key Management Center，简称:TPM-KMC)，通过将密钥授权数据保存到TPM-KMC，需要访问密钥时向TPM-KMC临时申请授权数据，访问密钥之后再删除申请到的授权数据，从而提高了密钥授权数据的安全性，降低了授权数据泄露和被篡改破坏的可能性。

[0069] 下面结合说明书附图和各实施例对本发明技术方案进行说明。

[0070] 参阅图2所示，本发明实施例提供了一种保护密钥授权数据的系统，包括TPM-KMC以及主机(英文:Host)/虚拟机(英文:Virtual Machine，简称:VM)/终端(英文:Terminal)，其中，这里的Host/VM/Terminal为集成TPM功能的计算平台，TPM-KMC为Host/VM/Terminal的远端服务器，具体的：

[0071] TPM-KMC，用于实现和TPM密钥相关的密钥内容、授权数据等信息的集中管理。其中一个功能是对密钥内容的备份，能够在Host/VM/Terminal发生故障并导致密钥不可用时，在新的Host/VM/Terminal中恢复已备份的密钥，避免出现由于密钥丢失而导致加密数据丢失的情况。TPM-KMC的另一个功能是对密钥授权数据的备份，其中，授权数据包括口令、证书等凭证，用于证明Host/VM/Terminal上的某个应用程序(英文:Application，简称:APP)拥有访问某个TPM密钥的权限。通过将TPM密钥的授权数据保存在Host/VM/Terminal之外的TPM-KMC服务器上，在需要使用TPM密钥时才将相应的授权数据发送给Host/VM/Terminal，避免了在Host/VM/Terminal的本地硬盘存放授权数据，或在程序代码中用固定常量写死授权数据等场景下导致授权数据泄露的风险。可选的，TPM-KMC所在的系统中还可选用TPM等硬件安全模块来保护密钥、授权数据等机密。TPM-KMC中的备份恢复模块是TPM-KCM和Host/VM/Terminal之间的接口模块，处理二者之间与密钥及密钥授权数据的备份、恢复和查询等

操作有关的消息。

[0072] Host/VM/Terminal，为集成了TPM功能的计算平台，其中，Host是提供计算资源的物理服务器，例如：企业应用服务器、数据中心服务器、云计算架构中的计算节点等；VM是由虚拟化软件将物理服务器的资源进行划分和隔离得到的虚拟计算系统，VM内运行着客户操作系统；Terminal是表现为个人计算机(Personal Computer，PC)、便携式电脑(英文：Laptop)、平板电脑(英文：PAD)等形式的终端计算设备。对于Host和Terminal而言，其中的TPM是硬件形式的密码模块，提供随机数生成、密码算法、机密信息存储等功能。不同于Host和Terminal，VM内的客户操作系统可使用的TPM设备是由虚拟化软件提供的模拟TPM或共享物理TPM，称为虚拟TPM(英文：VirtualizedTPM，简称：vTPM)。本发明的处理流程和安全机制对于硬件形式和虚拟形式的TPM均适用。Host/VM/Terminal包括了APP、TPM密钥管理模块(英文：TPM Key Management，简称：TPM-KM)和KMC接口，具体的：

[0073] APP，是需要使用TPM来创建和访问密钥的密钥访问例程。

[0074] TPM-KM，位于APP和TPM驱动程序之间的软件中间件，为APP提供操作TPM密钥功能的接口(即API应用程序接口)。

[0075] KMC接口，面向TPM-KMC的接口模块，处理二者之间与密钥及密钥授权数据的备份、恢复、查询等操作有关的消息。

[0076] 基于图2所示的系统架构，如图3所示，Host/VM/Terminal侧保护密钥授权数据的实施流程如下：

[0077] 步骤301：第一设备向TPM-KMC发送授权数据调用请求；所述第一设备为集成TPM功能的Host/VM/Terminal。

[0078] 步骤302：所述第一设备接收所述TPM-KMC返回的用所述第一设备的TPM公钥加密的授权数据。

[0079] 本发明实施例用第一设备的TPM公钥对授权数据进行加密后再发送给第一设备，可以保证授权数据在传输过程中的安全性，避免被第三方截获和破解。

[0080] 步骤303：所述第一设备用所述第一设备的TPM私钥解密所述授权数据，并用解密后的授权数据访问密钥。

[0081] 步骤304：所述第一设备在完成访问密钥之后，删除接收到的授权数据。

[0082] 进一步地，在创建和保存密钥授权数据时，所述第一设备首先调用TPM的随机数接口，生成硬件随机数。由于密钥是通过授权数据加密后，以文件的形式存储在第一设备的静态存储器上的，因此用于对密钥进行加密的授权数据需要具有足够的强度，即授权数据需要具有足够的信息熵(即随机性)。但现有技术中授权数据要么是写死在代码中的固定常量(例如：授权数据是一个固定的字符串)，要么是通过软件随机数算法产生的可预测的随机数，这两种方式产生的授权数据的信息熵都比较低。而本发明实施例的授权数据来自于TPM芯片，能够确保授权数据的强度，避免低信息熵的授权数据所面临的暴力破解等攻击风险。实际应用中，硬件随机数除了可以从TPM芯片得到外，还可以从可信密码模块(英文：Trusted Cryptography Module，简称：TCM)、硬件密码芯片、加密卡或CPU等硬件中得到。需要说明的是，硬件随机数的使用并不依赖于本发明的技术方案，可以与其它技术手段配合实施，也可以单独实施，均能够达到增强授权数据的信息熵、降低被破解的可能性的目的。然后，所述第一设备将所述硬件随机数作为指定密钥的授权数据，对该密钥进行加密。其

中，这里所说的指定密钥可以是新创建的密钥，也可以是需要修改授权数据的密钥。接下来，所述第一设备用TPM-KMC的TPM公钥对该授权数据进行加密，并将加密后的授权数据通过移动网络发送到所述TPM-KMC进行保存。最后，所述第一设备接收到所述TPM-KMC的成功响应消息后，删除所述第一设备中的授权数据。

[0083] 与图3所示的Host/VM/Terminal侧保护密钥授权数据的方法相对应的，本发明实施例还提供了一种TPM-KMC侧保护密钥授权数据的方法，如图4所示，该方法的实施流程如下：

[0084] 步骤401：TPM-KMC接收第一设备发送的授权数据调用请求；所述第一设备为集成TPM功能的Host/VM/Terminal。

[0085] 步骤402：所述TPM-KMC在认证通过所述第一设备的访问权限后，根据所述授权数据调用请求，获取存储在数据库中的授权数据。

[0086] 步骤403：所述TPM-KMC调用TPM，解密获取的授权数据。

[0087] 为了保证授权数据在TPM-KMC上的安全性，数据库中的密钥授权数据都是密文存储，且加密密钥来自于TPM-KMC的TPM，所以TPM-KMC需要先用自身的TPM对该记录中的密钥授权数据进行解密。

[0088] 步骤404：所述TPM-KMC用所述第一设备的TPM公钥对解密后的授权数据进行再加密。

[0089] 再加密的目的是为了确保仅有具备对应的TPM私钥的第一设备能够唯一解密授权数据，以及确保授权数据在传输过程中的安全性。

[0090] 步骤405：所述TPM-KMC将再加密后的授权数据通过移动网络发送给所述第一设备。

[0091] 进一步地，当所述TPM-KMC接收到第一设备通过移动网络发送的用所述TPM-KMC的TPM公钥加密的授权数据时，所述TPM-KMC用所述TPM-KMC的TPM私钥解密该授权数据，然后所述TPM-KMC调用TPM对解密后的授权数据进行再加密后，保存到数据库中，并向所述第一设备发送成功响应消息。

[0092] 基于图3和图4所示的保护密钥授权数据的方法，下面对创建、保存和使用密钥授权数据的流程进行详细说明。

[0093] 参阅图5所示，为创建和保存密钥授权数据的实施流程，其中，图5中以Host/VM/Terminal的APP控制整个流程运行为例进行描述，实际应用中，除了APP外，还可以由Host/VM/Terminal的TPM-KM来控制整个流程的运行。

[0094] 步骤501：APP获取硬件随机数。

[0095] 具体地，APP通过TPM-KM的API接口调用TPM-KM的随机数接口，TPM-KM接收到该调用后，组装TPM接口命令发送给TPM，由TPM内部的随机数生成模块产生硬件随机数。此步骤可以调用标准的TPM随机数接口命令，如表1和表2所示，分别为TPM2.0规范定义的获取随机数请求消息和获取随机数响应消息的结构。

[0096] 表1 获取随机数请求消息(GetRandom Command)

[0097]

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	会话类型：TPM_ST_NO_SESSIONS非会话命令接口，无需提供授权数据
UINT32	commandSize	命令消息长度
TPM_CC	commandCode	命令码：TPM_CC_GetRandom取随机数
UINT16	bytesRequested	请求的随机数字节长度，例如要求产生20字节的随机数

[0098] 表2 获取随机数响应消息(GetRandom Response)

[0099]

Type	Name	Description
TPM_ST	tag	会话类型：TPM_ST_NO_SESSIONS非会话命令接口
UINT32	responseSize	响应消息长度
TPM_RC	responseCode	返回码：TPM_RC_SUCCESS成功
TPM2B_DIGEST	randomBytes	TPM产生的随机数，例如长度为10字节的数据：0x11223344556677889900

[0100] 步骤502:APP将该硬件随机数作为指定密钥的授权数据,对该密钥进行加密。

[0101] 其中,该指定密钥可以是新创建的密钥,也可以是已存在并需要修改授权数据的密钥。以在创建密钥时指定这个硬件随机数作为密钥的授权数据为例,TPM-KM接收到APP的API接口调用后,组装TPM接口命令发送给TPM,由TPM创建密钥并关联APP指定的硬件随机数为该密钥的授权数据。此步骤可以调用标准的TPM对象创建接口命令,如表3和表4所示,分别是TPM2.0规范定义的创建请求消息和创建响应消息结构。

[0102] 表3 创建请求消息(Create Command)

[0103]

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	会话类型：TPM_ST_SESSIONS会话命令接口，需要提供授权数据
UINT32	commandSize	命令消息长度
TPM_CC	commandCode	命令码：TPM_CC_Create创建对象
TPMI_DH_OBJECT	@parentHandle	父密钥对象句柄及其授权数据
TPM2B_SENSITIVE_CREATE	inSensitive	待创建密钥对象的授权数据（即访问口令，例如10字节的随机数：0x11223344556677889900）
TPM2B_PUBLIC	inPublic	待创建密钥对象的公共部分，用于指定密钥类型等特征
TPM2B_DATA	outsideInfo	待创建密钥对象的外部数据，用于和所有者建立关联
TPML_PCR_SELECTION	creationPCR	如果密钥和平台配置关联，则指定PCR（平台配置寄存器）

[0104] 表4 创建响应消息(Create Response)

[0105]

Type	Name	Description
TPM_ST	tag	会话类型：TPM_ST_SESSIONS会话命令接口
UINT32	responseSize	响应消息长度
TPM_RC	responseCode	返回码：TPM_RC_SUCCESS成功
TPM2B_PRIVATE	outPrivate	已创建密钥的私密部分，如私钥（密文形式）
TPM2B_PUBLIC	outPublic	已创建密钥的私密部分，如公钥（明文形式）
TPM2B_CREATION_DATA	creationData	该密钥的创建信息，如PCR、outsideInfo等
TPM2B_DIGEST	creationHash	对该密钥的创建信息的数字摘要
TPMT_TK_CREATION	creationTicket	密钥凭证，用于证明该密钥为此TPM创建

[0106] 步骤503：APP用TPM-KMC的TPM公钥对该授权数据进行加密，并将加密后的授权数据发送到TPM-KMC进行保存。

[0107] 具体的，APP将加密后的授权数据携带在备份授权数据请求消息中发送给TPM-KMC。如表5所示，为本发明定义的备份授权数据请求消息结构。

[0108] 表5 备份授权数据请求消息(Create Command)

[0109]

Type	Name	Description
UINT32	commandSize	命令消息长度
UINT32	commandCode	命令码：KMC_Backup_Authdata备份密钥授权数据
Bytes[]	authData	密钥对象的授权数据（即访问口令），使用TPM-KMC的TPM密钥加密，这里填写加密后的密文
UINT32	keyIndex	已创建密钥的索引

[0110] 步骤504：TPM-KMC用TPM-KMC的TPM私钥解密该授权数据，并保存到数据库。

[0111] 具体地，TPM-KMC收到Host/VM/Terminal的APP发送的备份授权数据请求消息后，根据该消息中的密钥索引检索数据库中的密钥记录，如果不存在与该密钥索引对应的数据库记录则新建一条记录，然后调用TPM接口命令，使用TPM-KMC的TPM私钥解密该消息中携带的授权数据密文，再调用TPM对解密后的授权数据进行再加密，最后将解密并再加密后的授权数据保存到检索到的或者新建的数据库记录中。

[0112] 步骤505：当接收到TPM-KMC的备份授权数据响应消息后，APP删除本地内存中的密钥授权数据。

[0113] 如表6所示，为本发明定义的备份授权数据响应消息结构。

[0114] 表6 备份授权数据响应消息(Create Response)

[0115]

Type	Name	Description
UINT32	responseSize	响应消息长度
UINT32	responseCode	返回码：SUCCESS成功

[0116] 参阅图6所示，为使用密钥授权数据的实施流程，其中，图5中以Host/VM/Terminal的APP控制整个流程运行为例进行描述，实际应用中，除了APP外，还可以由Host/VM/Terminal的TPM-KM来控制整个流程的运行。

[0117] 步骤601：APP在使用密钥之前，发送获取授权数据请求消息到TPM-KMC。

[0118] 如表7所示，为本发明定义的获取授权数据请求消息结构。

[0119] 表7 获取授权数据请求消息(Get_Authdata Command)

[0120]

Type	Name	Description
UINT32	commandSize	命令消息长度
UINT32	commandCode	命令码：KMC_Get_Authdata获取备份密钥授权数据
UINT32	keyIndex	已创建密钥的索引

[0121] 步骤602：TPM-KMC根据该获取授权数据请求消息中的密钥索引，查找到对应的授权数据，用APP所属的Host/VM/Terminal的TPM公钥加密后发送给APP。

[0122] 具体地，TPM-KMC按照通常的认证流程对发送该获取授权数据请求消息的Host/VM/Terminal的访问权限进行认证，认证通过后TPM-KMC使用该请求消息中的密钥索引

(keyIndex)检索数据库，查找到对应的记录，由于数据库中的密钥授权数据是密文，且加密密钥来自于TPM-KMC的TPM，所以TPM-KMC先用自身的TPM对该记录中的密钥授权数据进行解密，再将解密得到的该授权数据明文用该APP所属的Host/VM/Terminal的TPM公钥进行加密，然后发送给APP，从而确保仅有具备对应TPM私钥的Host/VM/Terminal能够唯一解密该授权数据，并且确保授权数据在传输过程中的安全性，避免被恶意第三方截获。

[0123] 步骤603：APP用其所属的Host/VM/Terminal的TPM私钥对接收到的授权数据进行解密，使用解密后的授权数据访问对应的密钥。

[0124] 具体地，APP接收到授权数据后，首先通过TPM-KM的API接口调用TPM接口，解密授权数据。此步骤可以调用标准的TPM解密接口命令，如表8和表9所示，分别为TPM2.0规范定义的加解密请求消息和加解密响应消息的结构。

[0125] 表8 加解密请求消息(EncryptDecrypt Command)

[0126]

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	会话类型：TPM_ST_SESSIONS会话命令接口，需要提供授权数据
UINT32	commandSize	命令消息长度
TPM_CC	commandCode	命令码：TPM_CC_EncryptDecrypt对称加解密
TPMI_DH_OBJECT	@keyHandle	用于解密的对称密钥对象句柄及其授权数据
TPMI_YES_NO	decrypt	加解密标志，YES代表解密
TPMI_ALG_SYM_MODE+	mode	对称密码算法的计算模式
TPM2B_IV	ivIn	对称密码算法的初始向量
TPM2B_MAX_BUFFER	inData	密钥授权数据（即访问口令）的密文

[0127] 表9 加解密响应消息(EncryptDecrypt Response)

[0128]

Type	Name	Description
TPM_ST	tag	会话类型：TPM_ST_SESSIONS会话命令接口
UINT32	responseSize	响应消息长度
TPM_RC	responseCode	返回码：TPM_RC_SUCCESS成功
TPM2B_MAX_BUFFER	outData	密钥授权数据（即访问口令）的明文，即解密结果（例如10字节的随机数：0x11223344556677889900）
TPM2B_IV	ivOut	对称密码算法的初始向量（供下一轮计算使用）

[0129] 然后，APP使用解密后的授权数据访问密钥。以数字签名为例，此步骤调用标准的TPM数字签名接口命令，如表10和表11所示，分别为TPM2.0规范定义的签名请求消息和签名响应消息的结构。

[0130] 表10 签名请求消息(Sign Command)

[0131]

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	会话类型：TPM_ST_SESSIONS会话命令接口，需要提供授权数据
UINT32	commandSize	命令消息长度
TPM_CC	commandCode	命令码：TPM_CC_Sign 数字签名
TPMI_DH_OBJECT	@keyHandle	密钥对象句柄及其授权数据（访问口令，例如10字节的随机数：0x11223344556677889900）
TPM2B_DIGEST	digest	待生成数字签名的摘要信息
TPMT_SIG_SCHEME+	inScheme	数字签名方式
TPMT_TK_HASHCHECK	validation	数字签名的验证值，用于证明数字签名由此TPM生成

[0132] 表11 签名响应消息(EncryptDecrypt Response)

[0133]

Type	Name	Description
TPM_ST	tag	会话类型：TPM_ST_SESSIONS会话命令接口
UINT32	responseSize	响应消息长度
TPM_RC	responseCode	返回码：TPM_RC_SUCCESS成功
TPMT_SIGNATURE	signature	数字签名结果

[0134] 步骤604:APP删除接收到的授权数据。

[0135] 完成密钥使用之后,APP删除本地内存中的授权数据,避免泄露风险。

[0136] 参阅图7所示,本发明实施例提供了一种保护密钥授权数据的设备,用于实现本发明图3所示的一种保护密钥授权数据的方法,所述设备为集成TPM功能的Host/VM/Terminal,所述设备包括:

[0137] 第一发送单元701,用于向TPM-KMC发送授权数据调用请求。

[0138] 接收单元702,用于接收所述TPM-KMC返回的用所述设备的TPM公钥加密的授权数据。

[0139] 解密单元703,用于用所述设备的TPM私钥解密所述授权数据,并用解密后的授权数据访问密钥。

[0140] 第一删除单元704,用于在完成访问密钥之后,删除接收到的授权数据。

[0141] 所述设备还包括:

[0142] 随机数生成单元705,用于调用TPM的随机数接口,生成硬件随机数。

[0143] 第一加密单元706,用于将所述硬件随机数作为指定密钥的授权数据,对该密钥进行加密。

[0144] 第二加密单元707,用于用所述TPM-KMC的TPM公钥对该授权数据进行加密。

[0145] 第二发送单元708，用于将加密后的授权数据通过移动网络发送到所述TPM-KMC进行保存。

[0146] 第二删除单元709，用于在接收到所述TPM-KMC的成功响应消息后，删除所述第一设备中的授权数据。

[0147] 参阅图8所示，本发明实施例提供了一种TPM-KMC，用于实现本发明图4所示的一种保护密钥授权数据的方法，所述TPM-KMC包括：

[0148] 第一接收单元801，用于接收第一设备发送的授权数据调用请求；所述第一设备为集成TPM功能的Host/VM/Terminal。

[0149] 获取单元802，用于在认证通过所述第一设备的访问权限后，根据所述授权数据调用请求，获取存储在数据库中的授权数据。

[0150] 第一解密单元803，用于调用TPM，解密获取的授权数据。

[0151] 第一加密单元804，用于用所述第一设备的TPM公钥对解密后的授权数据进行再加密。

[0152] 第一发送单元805，用于将再加密后的授权数据通过移动网络发送给所述第一设备。

[0153] 所述TPM-KMC还包括：

[0154] 第二接收单元806，用于接收第一设备通过移动网络发送的用所述TPM-KMC的TPM公钥加密的授权数据。

[0155] 第二解密单元807，用于用所述TPM-KMC的TPM私钥解密该授权数据。

[0156] 第二加密单元808，用于调用TPM对解密后的授权数据进行再加密后，保存到数据库中。

[0157] 第二发送单元809，用于向所述第一设备发送成功响应消息。

[0158] 综上所述，本发明实施例提供的技术方案，可以直接作为TCG系列标准的完善和补充，在保存密钥授权数据时，通过将密钥授权数据保存到TPM-KMC，需要访问密钥时向TPM-KMC临时申请授权数据，访问密钥之后再删除申请到的授权数据，从而提高了保护密钥授权数据的安全性，降低了授权数据泄露和被篡改破坏的可能性。

[0159] 本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0160] 本发明是参照根据本发明实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0161] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指

令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0162] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0163] 尽管已描述了本发明的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例作出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本发明范围的所有变更和修改。

[0164] 显然，本领域的技术人员可以对本发明实施例进行各种改动和变型而不脱离本发明实施例的范围。这样，倘若本发明实施例的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

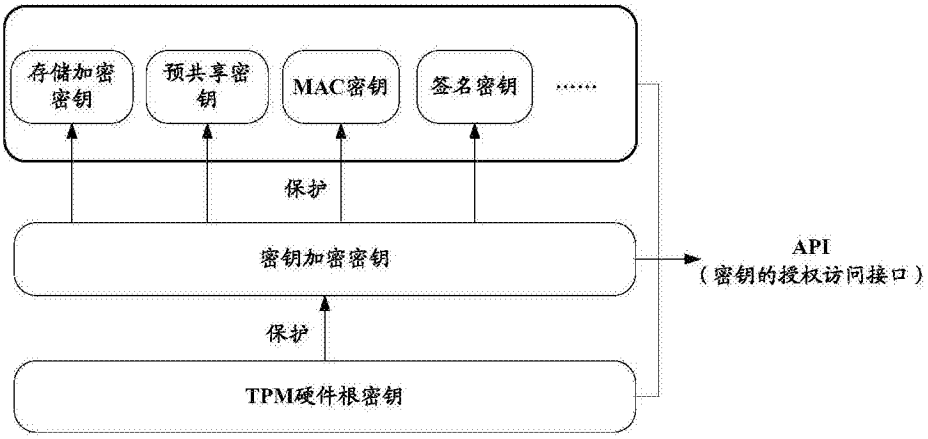

存储加密密钥
预共享密钥
MAC密钥
签名密钥
……
保护
密钥加密密钥
保护
TPM硬件根密钥
API
（密钥的授权访问接口）

图1

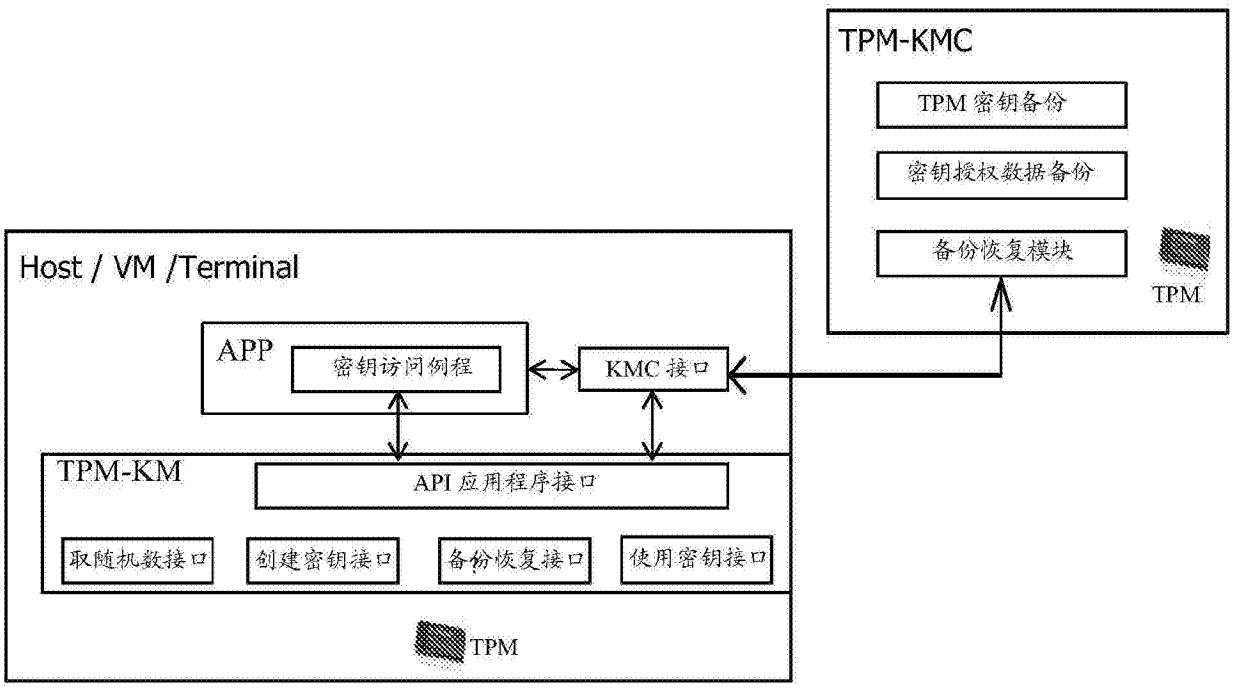

TPM-KMC
TPM 密钥备份
密钥授权数据备份
备份恢复模块
TPM
Host / VM /Terminal
APP
密钥访问例程
KMC 接口
TPM-KM
API 应用程序接口
取随机数接口
创建密钥接口
备份恢复接口
使用密钥接口
TPM

图2

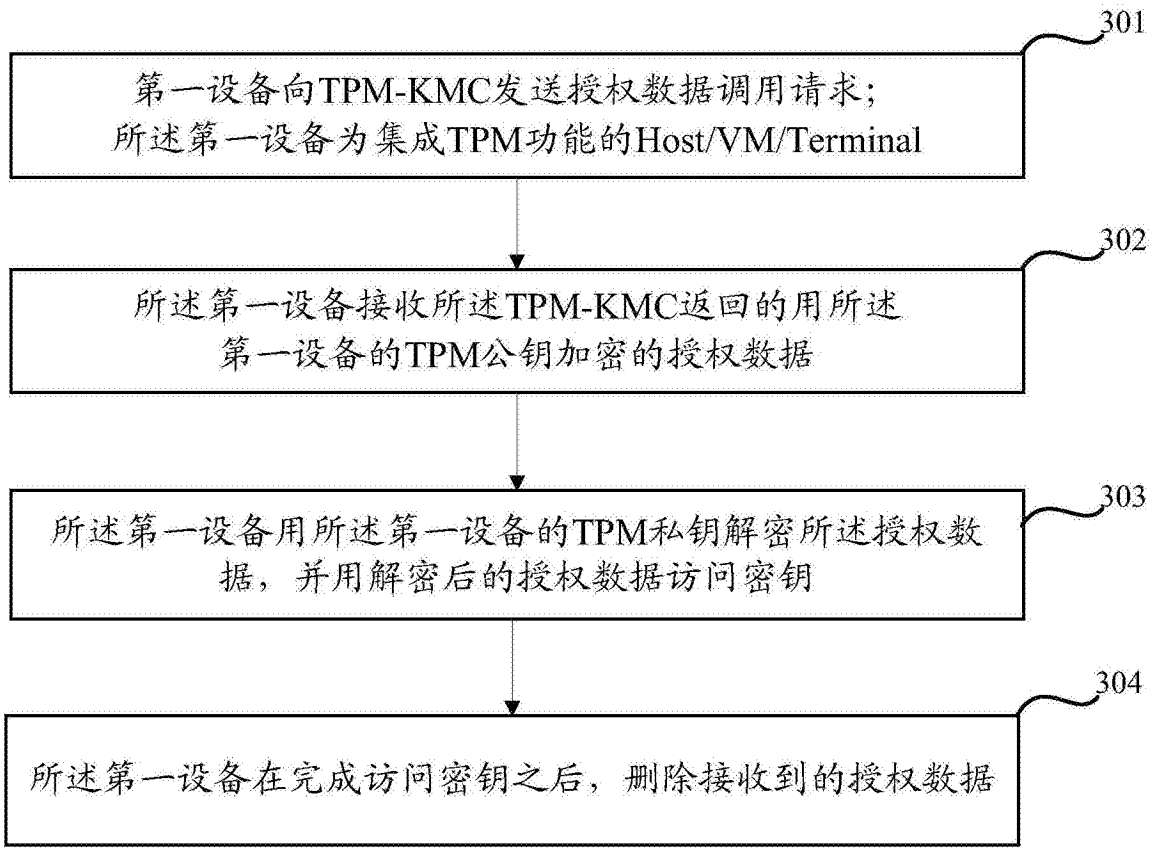

301
第一设备向TPM-KMC发送授权数据调用请求；
所述第一设备为集成TPM功能的Host/VM/Terminal
302
所述第一设备接收所述TPM-KMC返回的用所述
第一设备的TPM公钥加密的授权数据
303
所述第一设备用所述第一设备的TPM私钥解密所述授权数
据，并用解密后的授权数据访问密钥
304
所述第一设备在完成访问密钥之后，删除接收到的授权数据

图3

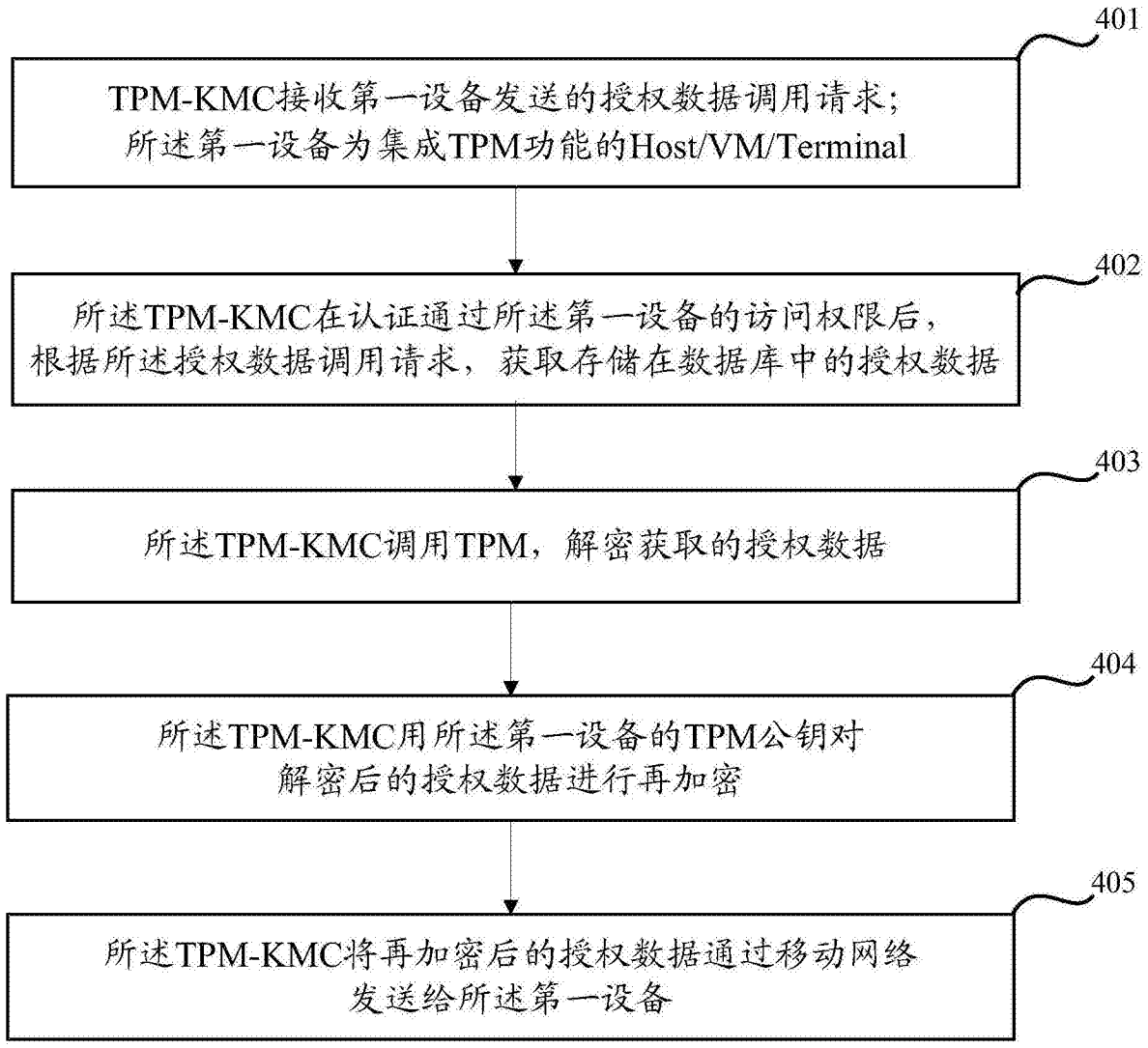

401
TPM-KMC接收第一设备发送的授权数据调用请求；
所述第一设备为集成TPM功能的Host/VM/Terminal
402
所述TPM-KMC在认证通过所述第一设备的访问权限后，
根据所述授权数据调用请求，获取存储在数据库中的授权数据
403
所述TPM-KMC调用TPM，解密获取的授权数据
404
所述TPM-KMC用所述第一设备的TPM公钥对
解密后的授权数据进行再加密
405
所述TPM-KMC将再加密后的授权数据通过移动网络
发送给所述第一设备

图4

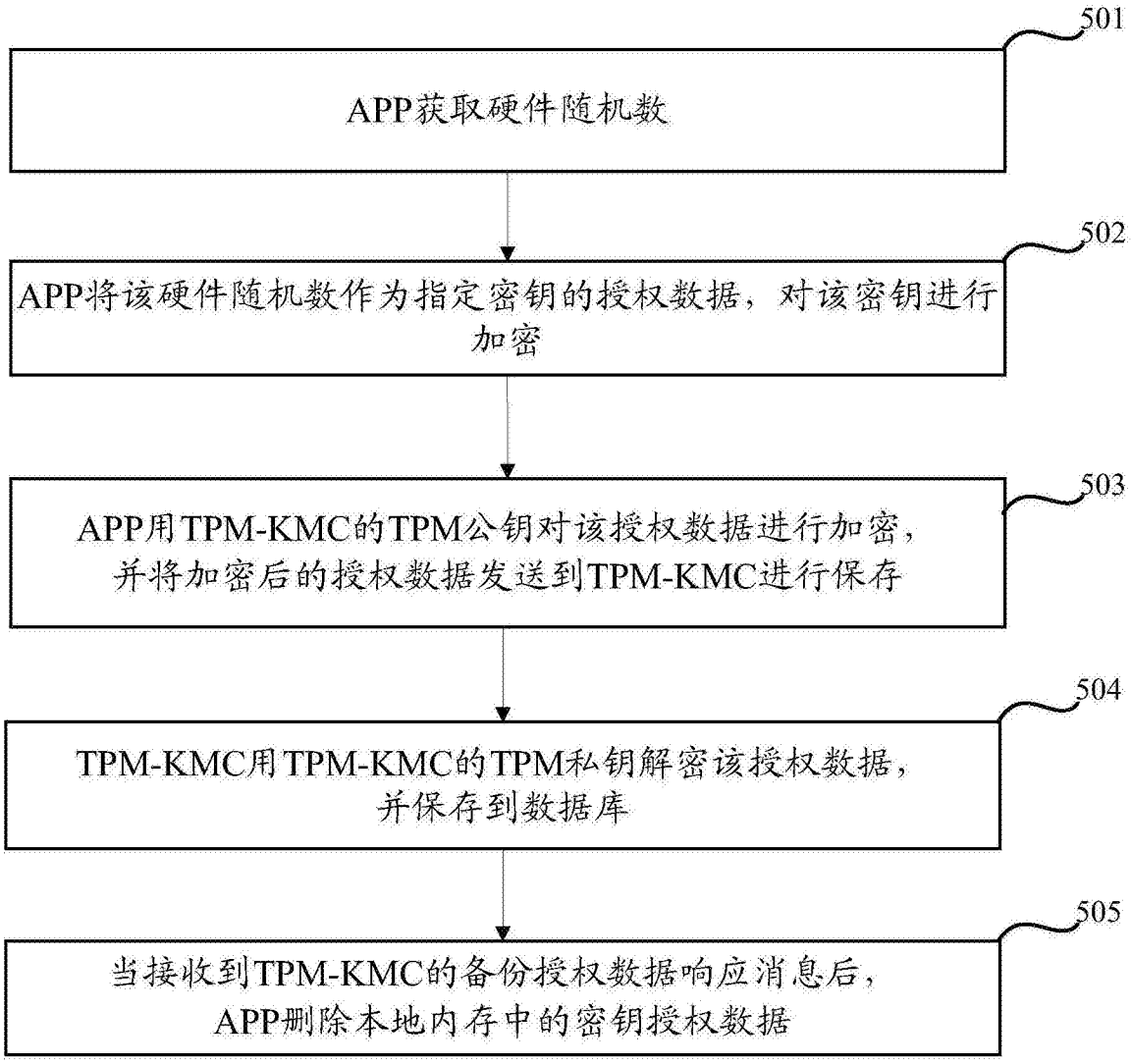

501
APP获取硬件随机数
502
APP将该硬件随机数作为指定密钥的授权数据，对该密钥进行加密
503
APP用TPM-KMC的TPM公钥对该授权数据进行加密，并将加密后的授权数据发送到TPM-KMC进行保存
504
TPM-KMC用TPM-KMC的TPM私钥解密该授权数据，并保存到数据库
505
当接收到TPM-KMC的备份授权数据响应消息后，APP删除本地内存中的密钥授权数据

图5

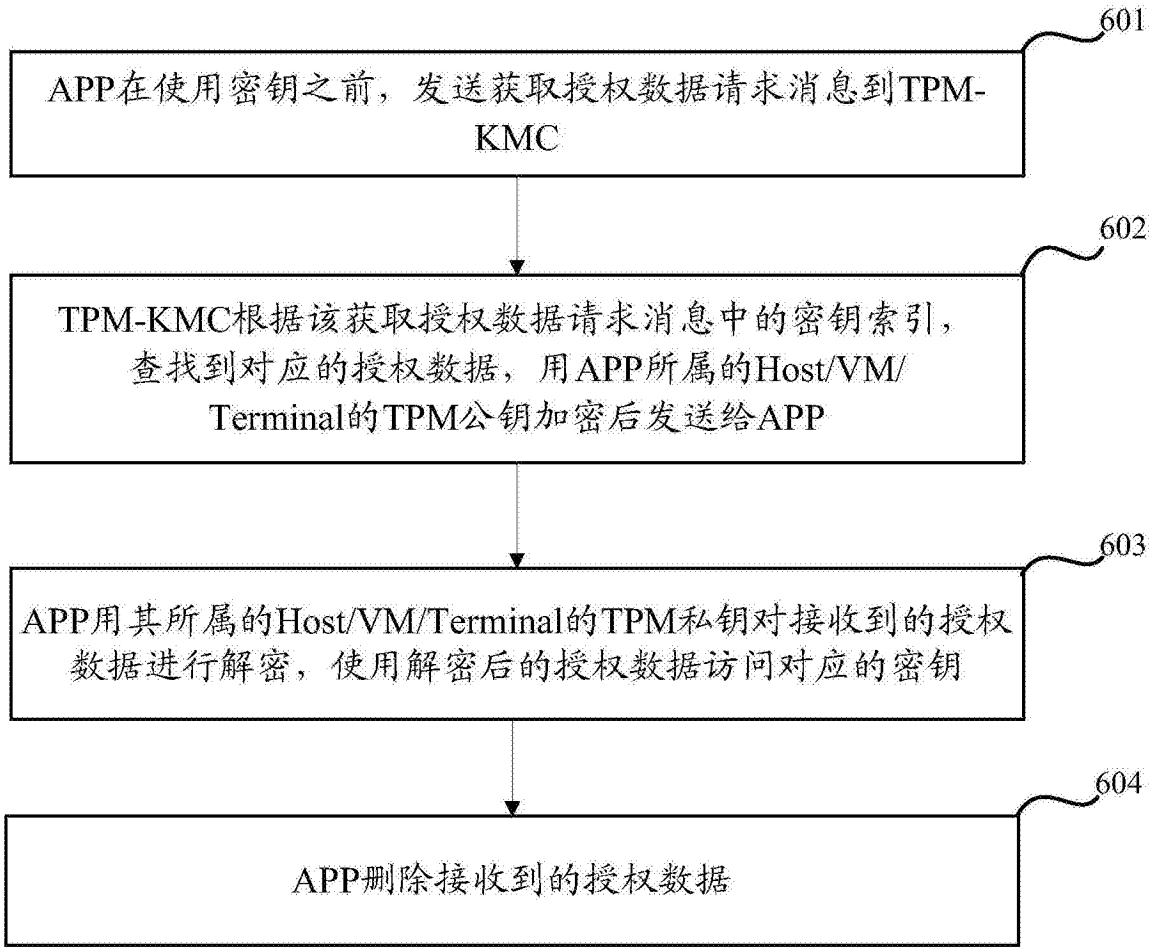

601
APP在使用密钥之前，发送获取授权数据请求消息到TPM-KMC
602
TPM-KMC根据该获取授权数据请求消息中的密钥索引，查找到对应的授权数据，用APP所属的Host/VM/Terminal的TPM公钥加密后发送给APP
603
APP用其所属的Host/VM/Terminal的TPM私钥对接收到的授权数据进行解密，使用解密后的授权数据访问对应的密钥
604
APP删除接收到的授权数据

图6

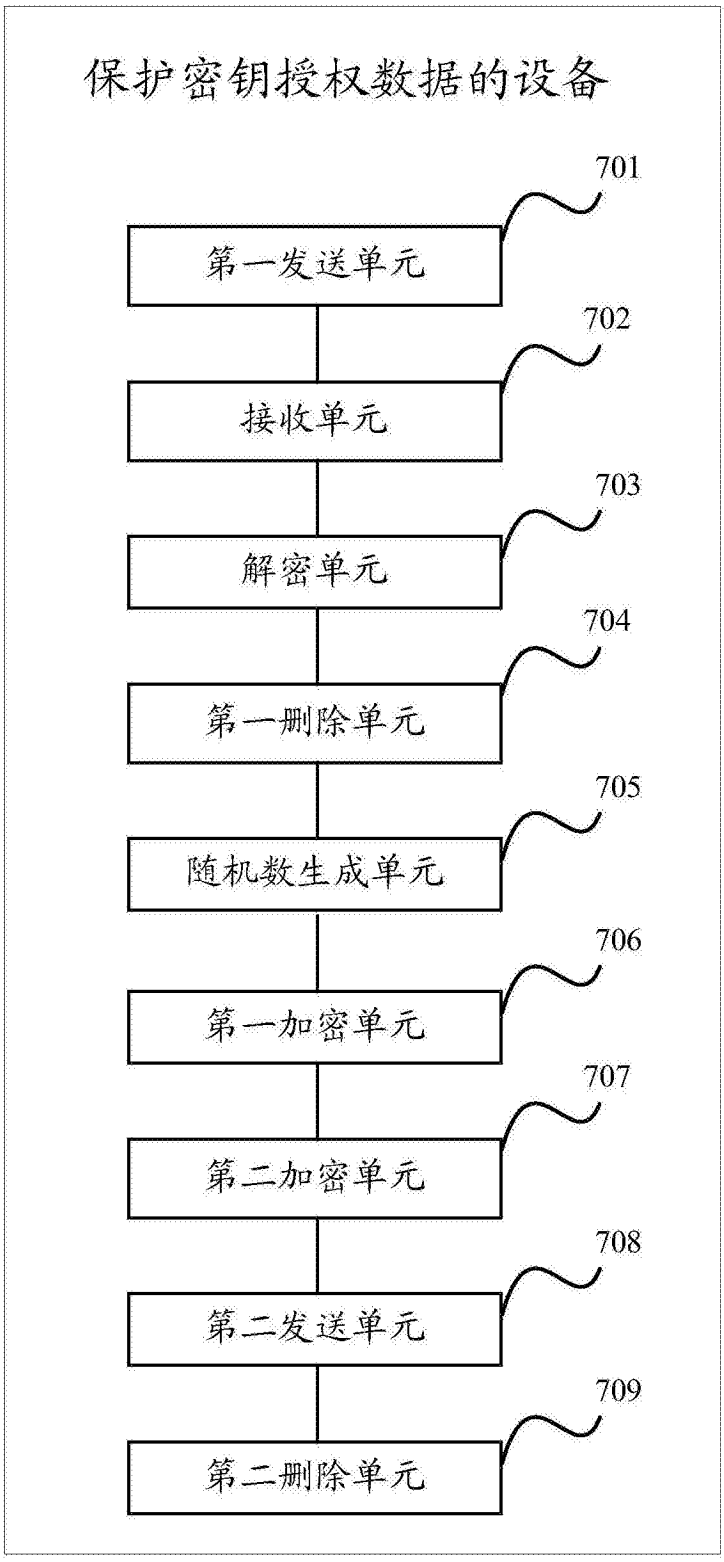

保护密钥授权数据的设备
701
第一发送单元
702
接收单元
703
解密单元
704
第一删除单元
705
随机数生成单元
706
第一加密单元
707
第二加密单元
708
第二发送单元
709
第二删除单元

图7

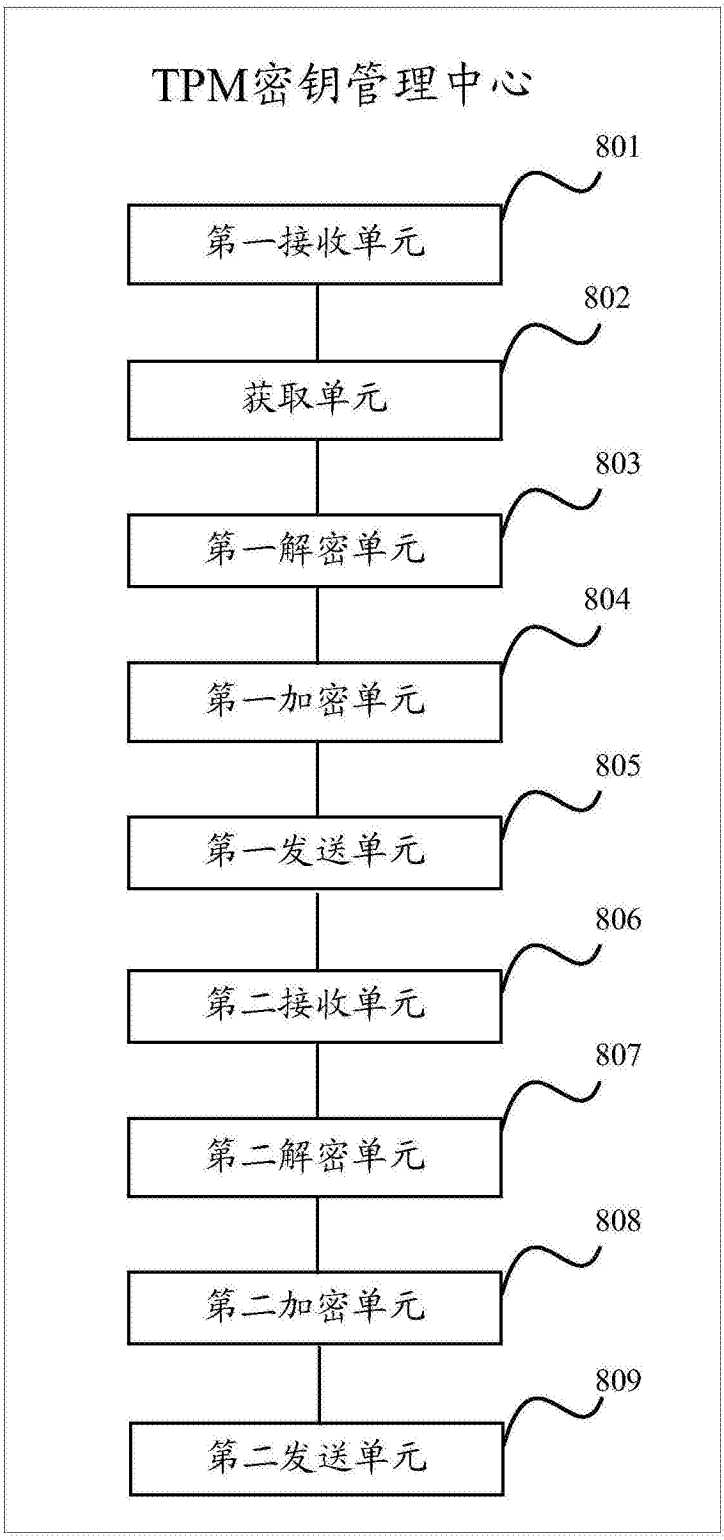

TPM密钥管理中心
801
第一接收单元
802
获取单元
803
第一解密单元
804
第一加密单元
805
第一发送单元
806
第二接收单元
807
第二解密单元
808
第二加密单元
809
第二发送单元

图8