(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102104597 A
(43)申请公布日 2011.06.22

(21)申请号 201010599715.5

(22)申请日 2010.12.17

(30)优先权数据
12/653,872 2009.12.18 US

(71)申请人 英特尔公司
地址 美国加利福尼亚

(72)发明人 M·哈斯拉 G·普拉卡什 S·达杜
M·米拉什拉斐 D·格伦迪宁

(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 刘瑜 王英

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/30(2006.01)
H04L 9/32(2006.01)

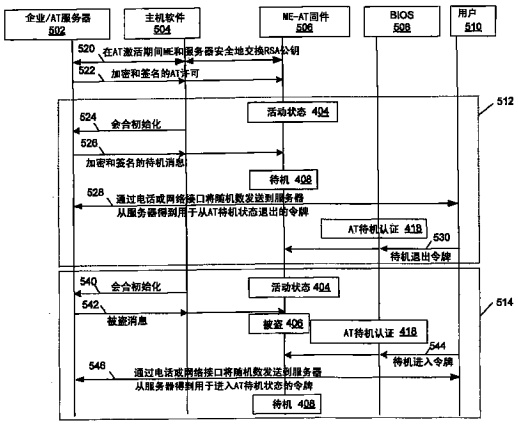
权利要求书 1 页 说明书 7 页 附图 6 页

(54)发明名称

用于防盗平台的复原的方法和装置

(57)摘要

本文总地描述了用于复原防盗平台的方法的实施例。所述方法包括:通过将平台公钥发送到服务器来启动进入待机状态;接收服务器公钥;接收加密和签名的AT许可;将会合消息发送到所述服务器;从所述服务器接收加密和签名的AT待机转变消息;验证所述待机转变消息;将RSA签名的确认发送到所述服务器;以及进入所述平台上的所述待机状态。从而得以进行防盗固件的重配置、修复和重置。可以描述并要求保护其他实施例。



CN 102104597 A

1. 一种用于访问具有防盗 (AT) 机制的平台的方法，包括 ：

通过将平台公钥发送到服务器来启动进入待机状态 ；

接收服务器公钥 ；

接收加密和签名的 AT 许可 ；

将会合消息发送到所述服务器 ；

从所述服务器接收加密和签名的 AT 待机转变消息 ；

验证所述待机转变消息 ；

将 RSA 签名的确认发送到所述服务器 ；以及

进入所述平台上的所述待机状态。

2. 根据权利要求 1 所述的方法，其中，所述平台是从活动状态转变到所述待机状态的。

3. 根据权利要求 2 所述的方法，还包括将所述平台从所述活动状态转变到被盗状态。

4. 根据权利要求 1 所述的方法，还包括生成平台 RSA 密钥对并且将所述 RSA 密钥对存储为加密的数据二进制大对象。

5. 根据权利要求 3 所述的方法，其中，所述待机转变消息是由管理引擎 (ME) 验证的。

6. 根据权利要求 5 所述的方法，其中，通过所述平台上的主机软件来交换所述平台公钥和所述服务器公钥。

7. 根据权利要求 4 所述的方法，其中，所述平台公钥可以是仅由管理引擎 (ME) 可读的。

8. 一种具有防盗 (AT) 机制的平台，包括 ；

用于通过将平台公钥发送到服务器来启动进入待机状态的模块 ；

用于接收服务器公钥的模块 ；

用于接收加密和签名的 AT 许可的模块 ；

用于生成随机数的模块 ；

用于使用所述随机数和所述平台公钥生成第一待机令牌的模块 ；

用于接收第二待机令牌的模块 ；

用于使用所述第一待机令牌来认证所述第二待机令牌的模块 ；以及

用于进入所述待机状态以提供对所述平台的访问的模块。

9. 根据权利要求 8 所述的平台，其中，所述平台是从活动状态转变到所述待机状态的。

10. 根据权利要求 8 所述的平台，其中，所述第二待机令牌是使用管理引擎 (ME) 通过所述第一待机令牌来认证的。

用于防盗平台的复原的方法和装置

技术领域

[0001] 本公开总体上涉及电子设备的防盗保护领域，并且更具体地涉及用于访问配置有防盗 (AT) 系统或机制的平台以进行防盗固件的重配置、修复和重置的方法和相关装置。

背景技术

[0002] 电子设备正变得越来越来普遍和移动化，并且随着用户数据越来越多地分布在膝上型计算机、台式计算机、服务器和手持设备中，从台式计算机到移动设备的电子设备盗窃也在增加。防盗保护是可以用于防止对用户数据的访问的工具并且可以通过软件、硬件和固件的一些组合用在电子设备中。当被触发时，防盗系统的应用可以启动一个或多个处理，例如电子设备的禁用以及从电子设备中删除数据。可以使用认证处理来允许电子设备或平台的修复和对用户数据的访问。

附图说明

[0003] 在说明书的结论部分具体指出并且清楚地要求保护视为本发明的主题。然而，通过在阅读附图时参考下文的详细描述，可以最佳地理解关于本发明的操作的组织和方法及其目的、特征和优点，在附图中 ：

[0004] 图 1 是本公开的各个实施例的框图概述。

[0005] 图 2 是根据本发明的实施例的被配置为使得能够进行平台复原的系统的框图。

[0006] 图 3 示出了根据本发明的实施例的、图 2 的使得能够进行平台复原的系统的进一步的细节。

[0007] 图 4 是根据本发明的实施例的状态图。

[0008] 图 5 是根据本发明的实施例的过程图。

[0009] 图 6 是根据本发明的实施例的用于访问平台的流程图 ；以及

[0010] 图 7 是说明根据本发明的实施例的用于访问平台的替代方法的流程图。

[0011] 将理解，为了说明的简洁和清楚，附图中说明的元件未必按照比例绘制。例如，为了清楚，可以相对于其他元件放大一些元件的尺寸。此外，当认为合适时，会在附图中重复标号以指示相应的或类似的元件。

具体实施方式

[0012] 在下面的详细地描述中，阐述了针对平台的安全和可靠的恢复的许多具体细节以提供对本发明的透彻理解。然而，本领域的技术人员将理解，可以在没有这些具体细节的情况下实现本发明。在其他的实例中，没有详细地描述公知的方法、过程、部件和电路，以免模糊本发明。

[0013] 提供用于访问具有防盗 (AT) 系统的平台以例如对其中 AT 系统已在平台上被激活的平台进行修复或恢复的方式将是本领域中的进步。在一些场景中，授权用户可能难以在修复场景中分析和检测平台故障的原因。AT 系统已在平台上被激活的平台的恢复通常需要

授权用户对平台重新载入或刷新 (reflash) 映像。

[0014] 在基于 Intel ®芯片组的嵌入式处理器上使用管理引擎 (ME) 的实施例中，可以通过刷新 ME 固件映像来禁用 AT 系统。ME 固件映像是包含数据存储机构或设备上的防盗固件部件的完整内容和结构的 ME 的镜像 (reflection)。ME 固件映像的刷新可能导致独立软件提供商 (ISV) 丢失包括平台上防盗客户端激活状态的防盗配置数据。类似地，在 ISV 不再可用的情况下，被禁用或锁定的 Intel 防盗平台的恢复可能需要刷新完整的 ME 固件映像，这可能是昂贵的、耗时的并且在不替换平台上闪速存储部分的情况下还可能是无法完成的。提供用于以允许授权用户或修复人员在减少的努力、时间和成本的情况下安全地访问和修复平台的方式访问具有防盗系统的装置和方法是有用的。

[0015] 用于访问具有防盗 (AT) 机制的客户端设备或平台的一种这样的方法包括 :通过将平台公钥发送到服务器来启动进入待机状态，并接收服务器公钥 ;接收加密的和签名的 AT 许可 ;将会合 (rendezvous) 消息发送到服务器 ;从服务器接收加密的和签名的 AT 待机转变消息 ;验证待机转变消息 ;将 RSA 签名的确认发送到服务器 ;以及启动待机状态。

[0016] 图 1 说明了本公开的各个实施例的概述。如所说明的，可以为每一个客户端设备 102（也可交换地称为平台或站）提供有阻止盗窃能力的芯片组固件和 / 或硬件。在实施例中，芯片组固件和硬件包括阻止盗窃管理引擎 (TDME)112。还可以为客户端设备 102 提供阻止盗窃主机代理 (TD HA)114。特别地，TD ME 112 和 TD HA 114 可以被配置为与阻止盗窃服务 (TD SVC)122 共同地实现阻止盗窃协议，所述阻止盗窃服务 122 可以与客户端设备 102 远程地放置，用于阻止或阻碍对客户端设备 102 的盗窃。可以在一个或多个远程放置的服务器 106 上实现 TD SVC 122。可以使用中间服务器 108 来便利客户端设备 102 和服务器 106 之间的消息交换。并且，中间服务器 108 可以是经由网络 104 从客户端设备 102 和服务器 106 可访问的。

[0017] 可以将包括用于阻止或阻碍对客户端设备 102 的盗窃的动作指令的消息经由中间服务器 108 从服务器 106 发送到客户端设备 102。TD HA 114 可以被配置为在阻止盗窃协议中帮助客户端设备 102 中的 TD ME 112，例如包括 :确定网络 104 是否是可访问的、向中间服务器 108 查询来自 TD SVC122 的消息，和 / 或将消息中继到 TD ME 112。TD ME 112 可以被配置为检验从 TD HA 114 中继的消息并且命令客户端设备 102 执行相应地阻止盗窃动作。

[0018] 对于所说明的实施例，TD HA 114 可以被配置为在客户端设备 102 的处理器操作的应用执行环境中工作，而 TD ME 112 可以被配置为在该应用执行环境外工作。客户端设备 102 可以具有一个或多个处理器操作的应用执行环境，其为虚拟的环境或其他环境。

[0019] 此外，客户端设备 102 可以是多个基于处理器的设备中的任意一个，包括但不限于 :台式计算设备、便携式计算设备（膝上型计算机、上网本和其它手持设备）、机顶盒，和游戏控制台。手持设备可以包括但不限于 :个人数字助理、数码相机、媒体播放器，和移动电话。服务器 106 可以是任意多个服务器，包括但不限于刀片服务器。网络 104 可以包括一个或多个私人网络和 / 或公共网络、有线网络和 / 或无线网络、局域网和 / 或广域网。

[0020] 此外，对于所说明的实施例，每一个客户端设备 102 可以包括基本输入 / 输出系统 (BIOS)113，其被配置为与 TD ME 112 协作以在客户端设备 102 上实现防盗处理。BIOS 可以包括修复认证 AT 模块，其可以用于从 AT 禁用中恢复客户端设备 102 和将 AT 平台转变成待

机状态。

[0021] ME/ 防盗服务（例如，Intel ®服务）的隔离和安全的执行环境可以包括各种不同类型的分区，包括：整个分离的硬件分区（例如，使用 Intel ®公司的管理引擎（“ME”）、动态管理技术（“AMT”）、平台资源层（“PRL”）和 / 或其他类似的或相似的技术）和 / 或虚拟分区（例如，Intel ®公司虚拟化技术（“VT”）方案中的虚拟机）。对本领域的普通技术人员将显而易见的是，还可以使用虚拟化主机实现 ME、AMT 和 PRL 技术。

[0022] 图 2 是描述在其中可以实现本发明的实施例的平台的框图。对应于主计算机系统的平台 200 包括经由桌面管理接口 (DMI)211 连接到芯片组 220 的处理器 210。处理器 210 将处理功率提供给平台 200 并且可以是单核心或多核心处理器，并且平台 200 中可以包括多于一个处理器。可以经由一个或多个系统总线、通信路径或介质（未示出）将处理器 210 连接到平台 200 的其他部件。

[0023] 芯片组 220 包括用于管理平台 200 的配置和操作的管理引擎 (ME)230，其可以实现为独立于主机处理器 210 操作的嵌入式微处理器。在一个实施例中，处理器 210 在主机操作系统（未示出）的指引下操作，而管理引擎 (ME)230 提供不能被主机操作系统访问的安全和隔离的环境。在一个实施例中，管理引擎 (ME)230 对用户进行认证，控制对外围设备的访问，管理用于保护存储在平台 200 的存储设备中的数据的加密密钥，以及经由网络控制器 260 向企业服务 270 提供接口。使用企业服务 270，管理引擎 (ME)230 与针对例如平台 200 的平台的配置和管理的企业范围的策略保持一致。可以将防盗固件模块实现为由管理引擎 (ME 230) 执行的固件。

[0024] ME 230 与企业服务 270 之间的通信通过用于在 ME 和 AT 服务器之间中继消息的 AT 主机 OS 代理经由带外或带内 (oob/ib) 通信信道 271 来进行。在一个实施例中，oob/ib 通信信道 271 是主机系统上的管理引擎 (ME)230 与管理主机系统的企业服务 270 之间的安全通信信道。可以在芯片组 200 和管理引擎 (ME)230 的制造期间将用于实现平台 200 和企业服务 270 之间的安全通信的加密 / 解密密钥存储在闪速存储器 290 中。

[0025] 在图 2 示出的实施例中，管理引擎 (ME)230 经由管理引擎控制器接口 (MECI)231 耦合到微控制器 240。在一个实施例中，微控制器 240 是执行存储命令解码和其它加速操作的通用控制器。在示出的实施例中，管理引擎 (ME)230 控制微控制器 240 的行为，微控制器 240 又控制存储控制器 250 的行为。微控制器 240 包括用于存储控制器 250 的驱动器以及涉及任何盘加密功能的逻辑。存储控制器 250 是用于例如存储设备 252 的存储设备的控制器，并且使得微控制器 240 和 ME 230 能够访问存储在存储设备 252 中的数据。

[0026] 平台 200 还包括存储器设备，例如动态随机存取存储器 (DRAM)212、芯片组 220 中的静态随机存取存储器 (SRAM)222，和闪速存储器 290，以及经由存储控制器 250 可访问的存储设备 252。这些存储器设备可以包括随机存取存储器 (RAM) 和只读存储器 (ROM)。为了本公开的目的，术语“ROM”可以用来总地指非易失性存储器设备，例如可擦可编程 ROM(EPROM)、电可擦可编程 ROM(EEPROM)、闪速 ROM、闪速存储器等。存储设备 252 可以包括大容量存储设备，例如电子集成驱动器 (IDE) 硬盘驱动器，和 / 或其他设备或介质，例如软盘、光学储存器、磁带、闪速存储器、记忆棒、数字视频盘、生物学储存器等。

[0027] 闪速存储器 290 是经由闪速接口 291 可由芯片组 220 访问的。可以对存储在存储设备 252 和 / 或存储器设备 DRAM 212、SRAM 222 和闪速存储器 290 中的数据进行加密。

[0028] 闪速存储器 290 包括用于初始化平台 200 的固件。这个初始化固件包括用于识别和初始化系统部件硬件（例如视频显示卡和硬盘）和一些其他硬件设备的基本输入 / 输出系统 (BIOS) 固件 292，所述一些其他硬件设备包括管理引擎 (ME)230。BIOS 固件 292 使平台 200 的系统部件硬件进行准备以在已知的低性能状态中操作，从而存储在各种介质中的其他软件程序（包括操作系统）可以被加载、执行并给予平台 200 的控制。ME 固件 296 使得能够在引导处理期间进行管理引擎 (ME)230 的初始配置。在一个实施例中，管理引擎 (ME)230 正好在为平台 200 加载操作系统之前注册 ME 固件 296 以接收通知。该通知使得管理引擎 (ME)230 执行某些指令以为加载操作系统做准备。

[0029] 闪速存储器 290 还包括用于配置网络控制器 260 的网络控制器固件 295，以及用于配置芯片组 220 的芯片组固件 296。闪速存储器 290 还包括数据区域 298。在一个实施例中，数据区域 298 被加密并且仅能由管理引擎 (ME)230 读取。可以将 ME 230 用于提供防盗服务的信息存储在闪速存储器 290 的数据区域 298 或存储设备 252 中。

[0030] 处理器 210 还可以通信地耦合到额外的部件，例如视频控制器、小型计算机系统接口 (SCSI) 控制器、网络控制器、通用串行总线 (USB) 控制器、诸如键盘和鼠标的输入设备等。平台 200 还可以包括用于通信地耦合各种系统部件的一个或多个桥或集线器，例如存储器控制器集线器、输入 / 输出 (I/O) 控制器集线器、PCI 根桥等。如本文所使用的，术语“总线”可以用来指共享通信路径以及点到点路径。

[0031] 诸如网络控制器 260 的一些部件可以实现为具有用于与总线通信的接口（例如，PCI 连接器）的适配卡。在一个实施例中，使用诸如可编程或不可编程的逻辑设备或阵列、专用集成电路 (ASIC)、嵌入式计算机、智能卡等的部件，可以将一个或多个设备实现为嵌入式控制器。

[0032] 如本文所使用的，术语“处理系统”和“数据处理系统”意图宽泛的包括单个机器，或将机器或设备通信地耦合在一起的系统。示例性处理系统包括而不限于 :分布式计算系统、超级计算机、高性能计算系统、计算集群、大型计算机、迷你计算机、客户端 - 服务器系统、个人计算机、工作站、服务器、便携式计算机、膝上型计算机、平板计算机、电话、个人数字助理 (PDA)、手持设备、诸如音频和 / 或视频设备的娱乐设备，以及用于处理或传输信息的其他设备。

[0033] 可以至少部分地通过来自传统输入设备（例如键盘、鼠标等）的输入和 / 或从另一个机器、生物计量反馈或其他输入源或信号接收的命令来控制平台 200。平台 200 可以例如通过网络接口控制器 (NIC)160、调制解调器或其他通信端口或耦合，来使用到一个或多个远程数据处理系统（未示出）的一个或多个连接。

[0034] 平台 200 可以通过物理和 / 或逻辑网络（例如局域网 (LAN)、广域网 (WAN)、内部网、互联网等）的方式互连到其他处理系统（未示出）。涉及网络的通信可以使用各种有线和 / 或无线的短距离或长距离的载波和协议，包括 :射频 (RF)、卫星、微波、电气与电子工程师协会 (IEEE)802.11、蓝牙、光、红外、电缆、激光等。

[0035] 图 3 示出了图 2 的在其中可以实现本发明的实施例的管理引擎 (ME)230 和企业 AT 服务 270 的进一步的细节。ME 230 包括逻辑并且经由带外 / 带内通信信道 271 与 Intel 防盗固件模块和企业服务 270 的 AT 状态管理模块服务 370（可以是 Intel ®服务）进行通信。

[0036] 在芯片组 220 中，示出的是在加载了图 2 的 ME 固件 296 之后的管理引擎 230。管理

引擎 230 包括为管理引擎 230 提供基本操作性能的 ME 内核 310，以及提供诸如网络通信、安全性、密码和计时器服务的基本服务的 ME 通用服务 320。管理引擎 230 还包括带外 (OOB)/带内通信模块 330。OOB 通信模块 330 便利平台 200 的部件与企业服务 270 相应的部件之间经由网络控制器 260 进行通信。管理引擎 230 还包括管理平台上的防盗服务的防盗服务模块 360。

[0037] 根据本发明的实施例，管理引擎 (ME)230 还包括管理模块 350、安全模块 355 以及防盗服务模块 360。结合 AT 企业服务 270 使用这些模块来与针对例如平台 200 的平台的管理和配置的企业范围的策略保持一致。OOB/ 带内服务器通信模块 330 便利 AT 服务模块 360 和安全模块 355 与 AT 企业服务 270 的相应部件（未示出）之间经由网络控制器 260 进行通信。

[0038] 如前面所讨论的，可以在平台 200 上激活防盗 (AT) 系统，以使用包括防盗服务模块 360 的模块提供平台 200 的资产 (asset) 保护、数据保护和盗窃阻止。图 4 是表示平台 200 的 AT 的各个状态的状态机图；包括：非活动状态 402、活动状态 404、被盗状态 (stolen state)406 以及待机状态 408。在一个实施例中，非活动状态 402 表示平台 200 处于登记前 (pre-enrollment) 配置，其中平台 200 还没有向服务器（例如在下面的图 5 中描述的企业 /AT 服务器 502) 寻求激活 AT 的许可，或者其中在平台 200 上停用了 AT 技术。

[0039] 继续该实施例，登记 410 处理用于将平台 200 从非活动状态 402 转变成活动状态 404。如果平台 200 适合与 AT 系统进行操作，那么平台 200 满足登记 410 处理的条件。针对 AT 的登记代理可以向 ISV 服务器或企业 AT 服务器 402 请求激活 AT 的许可。作为响应，ISV 服务器可以验证请求，并且可以将 AT 许可（在实施例中，是用于激活平台上的防盗的 Intel 授权的、密码签名并加密的数据结构）发送到平台 200，以允许平台 200 验证来自 ISV 服务器或企业 AT 服务器 402 的签名的消息。当在活动状态 404 中时，可以使用会合计时器来确定平台 200 是否应当保持在活动状态 404，或是否应当实现触发和策略执行 414 处理以例如通过图 3 的防盗状态管理模块 340 将平台 200 的状态从活动状态 404 改到被盗状态 406。

[0040] 可以使用触发将平台 200 的状态从活动状态 404 转变到被盗状态 406。一个这样的触发是从 ISV 服务器发送到平台 200 的被盗（或 AT 平台锁定）消息。在其他的实施例中，触发可以是由 ME 固件 296 进行的防盗平台篡改检测或策略驱动的登陆到操作系统 (OS) 的本地登陆失败。转变平台 200 到被盗状态 406 指示平台 200 要实现策略动作。例如，当转变到被盗状态 406 时，平台 200 可以采取动作以立刻禁用或在给定的时间段内禁用平台 200。此外，或可替代地，AT 机制或系统可以通过删除所有数据中的一部分或禁止对数据的访问来保护平台 200 上的数据。

[0041] 本发明的实施例通过认证 418 处理将平台 200 从被盗状态 406 转变成待机状态 408，来提供进入修复场景或暂时禁用或中止 AT 平台状态的能力。认证 418 处理的应用允许在没有丢失 AT 许可（在实施例中，用于激活平台上的防盗的 Intel 授权的、密码签名并且加密的数据结构）的情况下通过修复场景访问平台 200。可替换地，客户端设备 102 或平台 200 可以使用旁路处理 422 从活动状态 404 直接转变到待机状态 408。旁路处理 422 可以被应用来从活动状态 404 访问待机状态 408，而不用将平台 200 转变成被盗状态 406。在下面的图 6 和图 7 中描述了认证 418 处理的实施例。在实施例中，AT 待机状态 408 是时间

受限且基于策略的，但是实施例不受此限制。

[0042] 待机状态 408 可以允许用户基于平台 200 中基于 AT 策略的计时器持续时间访问硬件和软件，并且允许服务 / 支持工程师在不刷新 / 重编程平台 200 中的 ME 固件 296 的情况下修复有 AT 能力的平台。如果没有根据策略要求修复或纠正平台 200，那么可以使用休眠 420 处理将平台 200 从待机状态 408 转变回被盗状态 406。例如，如果处于待机状态 408 时计时器期满，那么平台 200 可以进入休眠 420 处理以将平台 200 转变回被盗状态 406。

[0043] 可以使用根据本发明的实施例的、如在下面的图 6 和图 7 中所描述的复原 424 处理将平台 200 从待机状态 408 转变为活动状态 404。在另一实施例中，可以使用恢复 416 处理将平台 200 从被盗状态 406 转变为活动状态 404。恢复 416 处理可以包括在 AT 系统中输入口令（在 AT 激活期间提供的用户激活的密码）以检验用户凭证。可替换地，恢复 416 处理可以包括在 AT 系统中输入恢复令牌（ISV 服务器生成的平台恢复密码）以将平台 200 从被盗状态 406 转变为活动状态 404。通过其中 AT 系统在平台 200 上被停用的停用 412 处理，可以将平台 200 从活动状态 404 转变回非活动状态 402。

[0044] 图 5 是描述根据本发明的实施例的认证处理 418 的过程图。在后面的图 6 和图 7 中另外描述了认证处理的一些实施例。使用企业 /AT 服务器或 ISV 服务器 502、平台 200 上的主机软件 504、ME-AT 固件 (FW)506、平台 200 上的 BIOS 508 以及用户 510，可以通过认证 418 处理将具有激活的 AT 系统的平台 200 转变成待机状态 408。

[0045] 由 ME-AT 固件 506 生成 RSA(Rivest，Shamir 和 Adelman) 密钥对，并且在 AT 激活或登记 410 期间在 ME-AT 固件 506、主机软件 504 和服务器 502 之间安全地交换 RSA 公钥。RSA 密钥对被生成并且可以被存储为加密的数据二进制大对象 (blob)。可以由平台 200 的原始设备制造商 (OEM) 将公钥或“共享密钥”放置、编程或烧录到 SPI 闪速存储器中由管理引擎 (ME) 可读取的位置。在该实施例中，可以以仅 ME 可读的方式来限制公钥的位置。将加密和签名的 AT 许可 522 发送到主机软件 504 和 ME-AT 固件 506 以将平台 200 置于活动状态 404。

[0046] 在第一实施例 512 中，平台 200 处于活动状态 404。当处于活动状态 404 时，会合处理使用的会合初始化 524 消息被周期地发送到企业 /AT 服务器 502，以根据使用策略来更新盗窃状态。可以通过平台 200 中的会合计时器的期满，例如由主机软件 504 中的客户端代理来触发会合初始化 512 消息。将加密和签名的待机消息 526 从企业 /AT 服务器 502 发送到主机软件 504 和 ME-AT 固件 506，以启动待机状态 408。通过电话或诸如网络接口的其他接口将发出以用于认证的随机数 (nonce) 或诸如随机号或伪随机号的安全号从用户 510 发送到企业 /AT 服务器 502(528)，并且从服务器 502 获取用于从待机状态 408 退出的令牌。待机退出令牌从用户 510 发送到 BIOS508(530)，然后发送到 ME-AT 固件 506。

[0047] 可以经由待机状态 408 的使用例如通过以下方式来修复平台 200 ：允许将串行外围接口 (SPI) 闪速存储器重置成期望的设置，和 / 或移除由恶意独立软件供应商 (ISV) 或不再可用的 ISV 进行的错误或未授权的 AT 系统的激活。

[0048] 在图 5 中说明的第二实施例 514 中，处于活动状态 404 的平台 200 将会合初始化 540 消息从主机软件发送到企业 /AT 服务器 502。将被盗消息 542 从企业 /AT 服务器 502 发送到主机软件 504，然后发送到 ME-AT 固件 506 以将平台 200 置于被盗状态 406。启动 AT 待机认证 418 处理，并且将待机进入令牌 544 从用户 510 发送到 BIOS 508 和 ME-AT 固

件 506。通过电话或诸如网络接口的其他接口将随机数从用户 510 发送到企业 /AT 服务器 502(546)，并且从服务器 502 获取用于进入待机状态 408 的令牌。

[0049] 图 6 是根据本发明的实施例的用于从活动状态 404 访问平台 200 的流程图。在项 600 中，启动从活动状态 404 进入平台 200 的防盗 (AT) 待机状态 408。在项 610 中，基于操作系统 (OS) 的 AT 系统启动与企业 /AT 服务器 502 的会合。在项 620，企业 /AT 服务器 502 接收客户端设备 102 或平台 200 针对新的 AT 策略的请求，并且在项 630 中，企业 /AT 服务器 502 基于用户请求生成待机消息。ME-AT 固件 (FW)506 通过主机软件 504 从企业 /AT 服务器 502 接收加密和签名的 AT 待机转变消息 (项 640)。在项 640 中，ME-AT 固件 (FW)506 验证签名的 AT 待机转变消息并且将 RSA 签名的确认发送到企业 /AT 服务器 502。在项 660 中，启动待机状态 408 以提供对平台 200 的访问。

[0050] 图 7 是说明根据本发明的实施例的用于从活动状态 404 或被盗状态 406 访问平台 200 的替代方法的流程图。如该方法所说明的，在项 700 中，通过 BIOS 从被盗状态 406 或活动状态 404 启动进入 AT 待机状态 408。在项 710 中，通过 BIOS 从 ME-AT 固件 506 请求随机数，并且将随机数显示给用户 510。在项 720，由企业 /AT 服务器 502 使用随机数生成待机进入令牌，然而，在生成待机进入令牌时还可以使用额外的信息。在该实施例中，在项 730 中，用户 510 输入待机进入令牌以由 ME-AT 固件 506 进行认证。在项 740 中，ME-AT 固件 506 使用公钥或共享密钥和随机数生成待机令牌。在项 750 中，将来自用户 510 的待机令牌与由 ME-AT 固件 506 生成的待机令牌进行比较以确定是否存在匹配。在项 760 中，启动待机状态 408 以提供对平台 200 的访问。

[0051] 在可应用的情况下，经由执行实施为主机处理器和微控制器上的代码指令的合适固件或软件通常可以便利进行本文所讨论的操作。因此，本发明的实施例可以包括在某种形式的处理核心上执行的或在机器可读介质上或机器可读介质中实现或实施的指令集。机器可读介质包括用于以机器 (例如，计算机) 可读形式存储或传输信息的任何机构。例如，机器可读介质可以包括制品，例如闪速存储器 290 ；动态随机存取存储器 (DRAM)212 ；磁盘存储介质 ；光存储介质 ；以及静态随机存取存储器 222 等。此外，机器可读介质可以包括传播信号，例如电的、光的、声的或其他形式的传播信号 (例如，载波、红外信号、数字信号等)。

[0052] 尽管本文已经说明和描述了本发明的某些特征，但是本领域的技术人员现在将可以想到许多修改、替代、改变以及等价物。因此，应当理解，所附权利要求意图覆盖落在本发明的真实精神内的所有此类修改和改变。

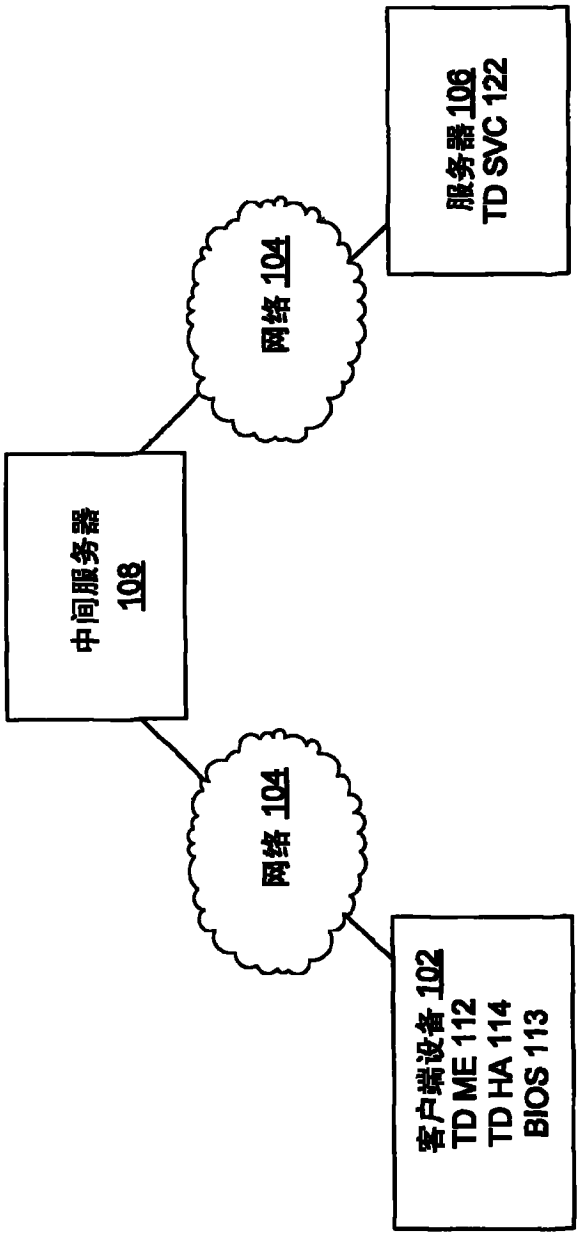

服务器 106
TD SVC 122
网络 104
中间服务器
108
网络 104
客户端设备 102
TD ME 112
TD HA 114
BIOS 113

图 1

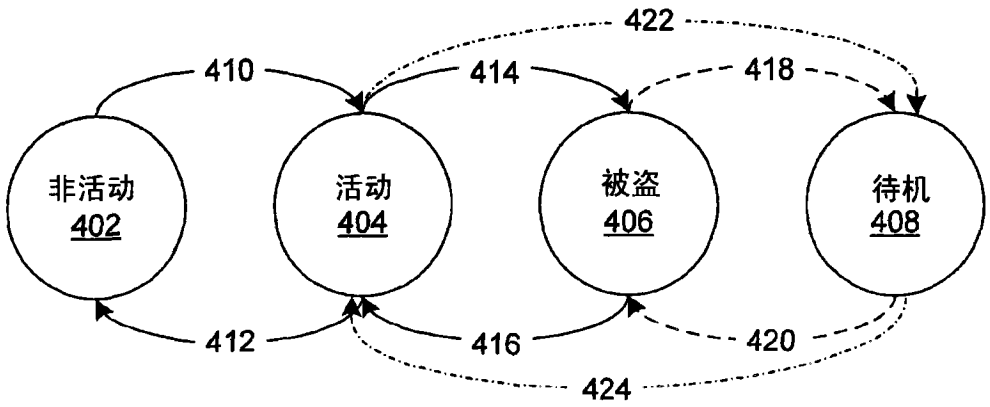


图 4

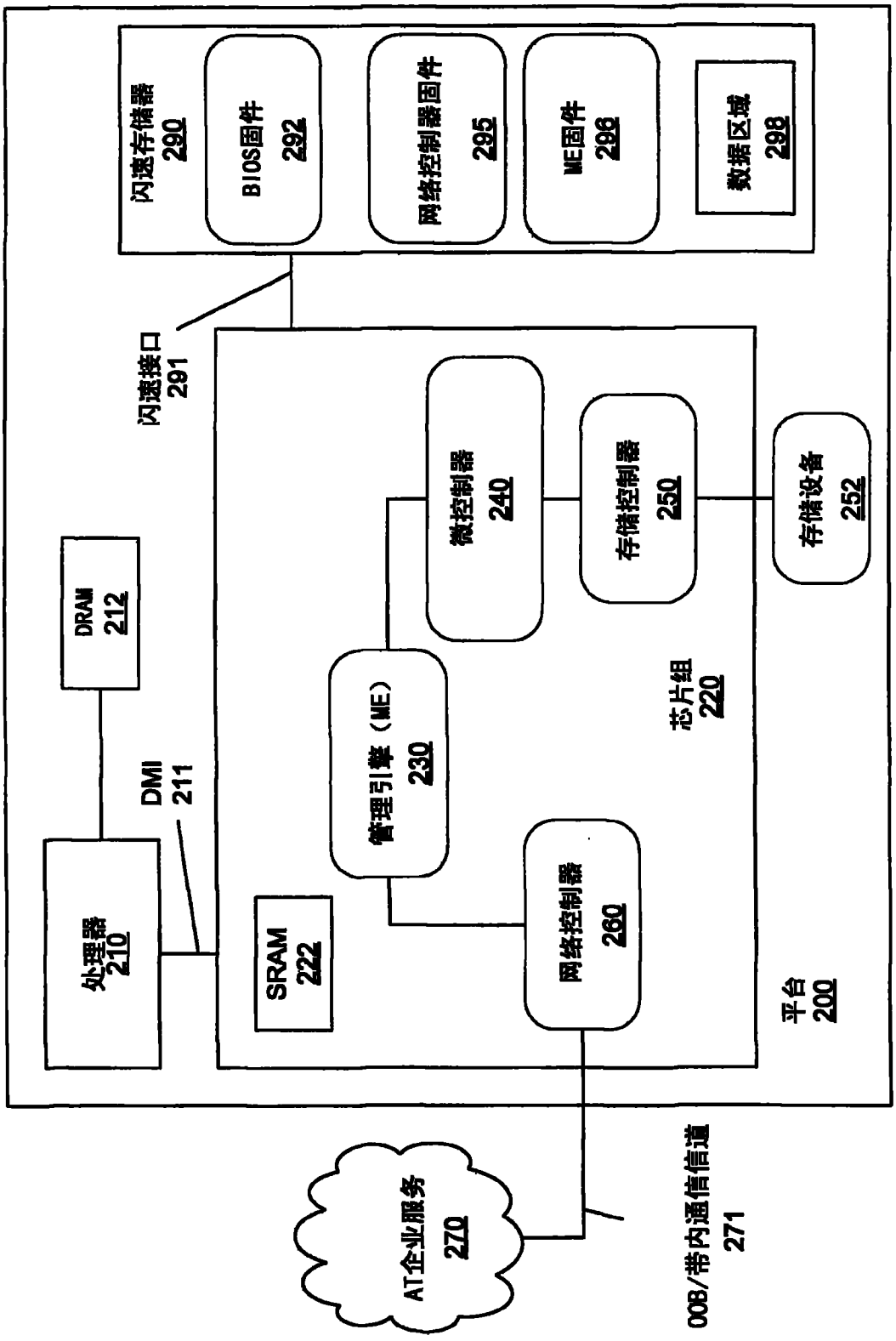

闪速存储器
290
BIOS固件
292
网络控制器固件
295
ME固件
296
数据区域
298
闪速接口
291
微控制器
240
存储控制器
250
存储设备
252
DRAM
212
DMI
211
管理引擎（ME）
230
芯片组
220
处理器
210
SRAM
222
网络控制器
260
平台
200
AT企业服务
270
OOB/带内通信信道
271

图 2

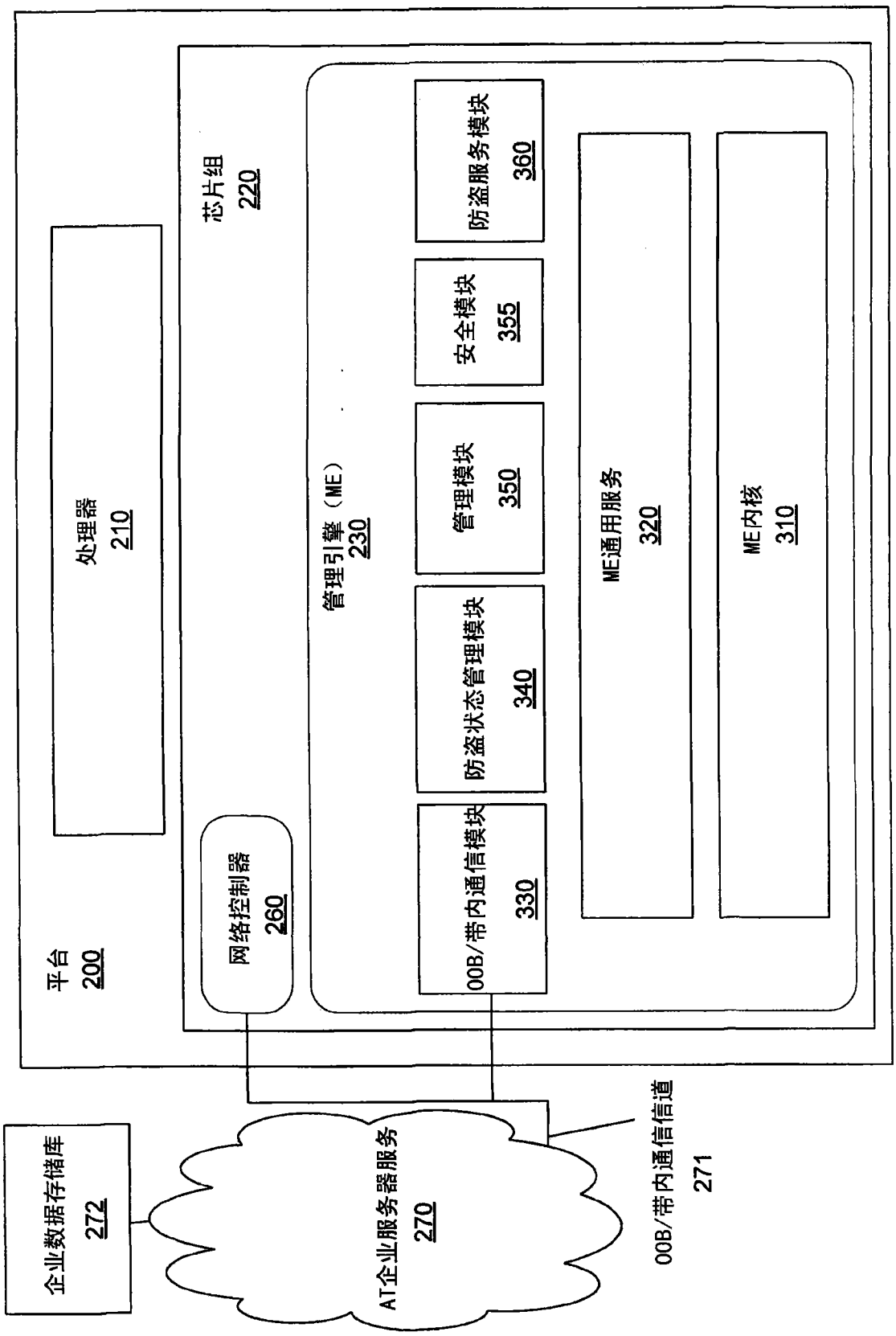

平台
200
处理器
210
芯片组
220
网络控制器
260
管理引擎（ME）
230
OOB/带内通信模块
330
防盗状态管理模块
340
管理模块
350
安全模块
355
防盗服务模块
360
ME通用服务
320
ME内核
310
企业数据存储库
272
AT企业服务器服务
270
OOB/带内通信信道
271

图 3

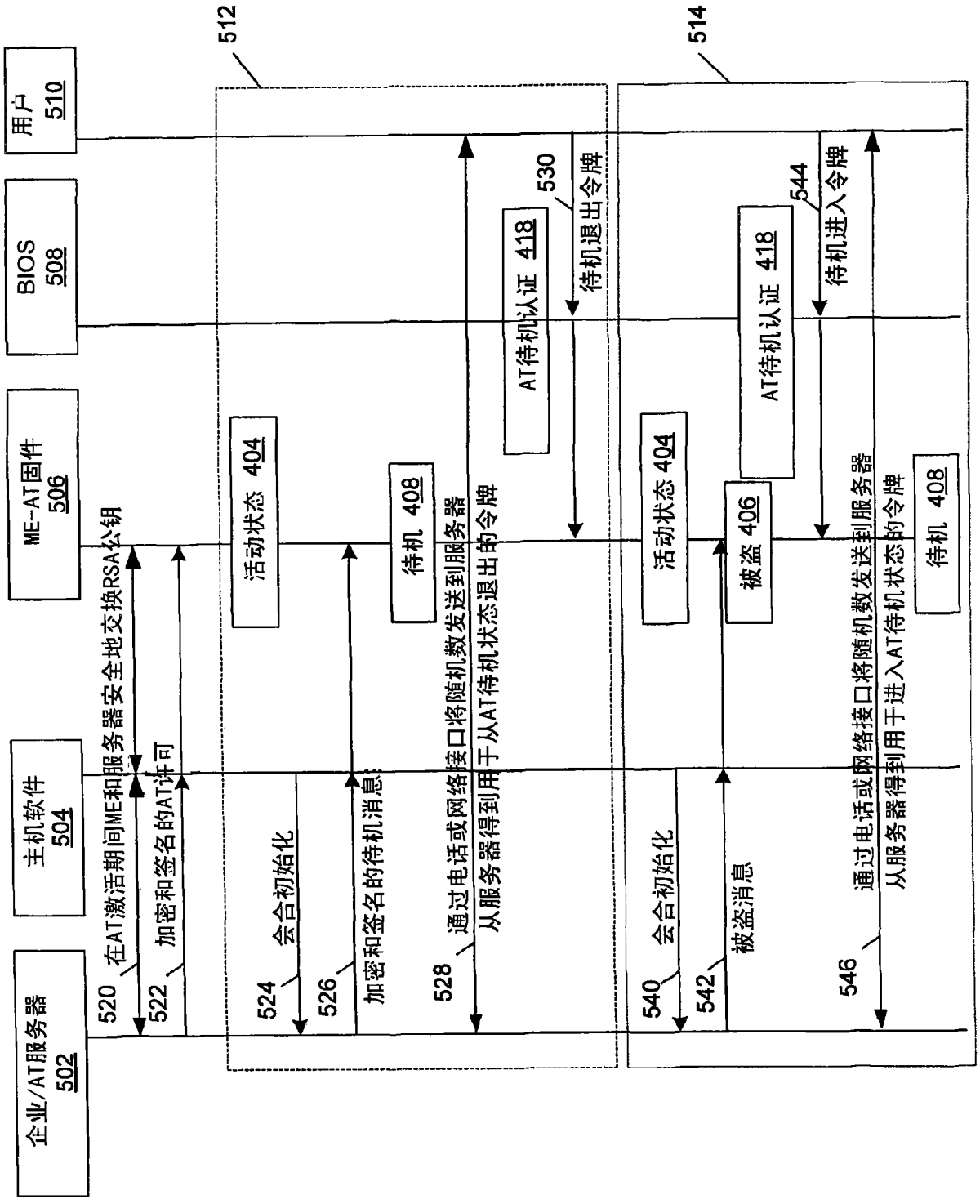

企业/AT服务器 502
主机软件 504
ME-AT固件 506
BIOS 508
用户 510
512
514
520 在AT激活期间ME和服务器安全地交换RSA公钥
522 加密和签名的AT许可
524 会合初始化
526 加密和签名的待机消息
528 通过电话或网络接口将随机数发送到服务器
从服务器得到用于从AT待机状态退出的令牌
活动状态 404
待机 408
AT待机认证 418
530 待机退出令牌
540 会合初始化
542 被盗消息
546 通过电话或网络接口将随机数发送到服务器
从服务器得到用于进入AT待机状态的令牌
活动状态 404
被盗 406
AT待机认证 418
544 待机进入令牌
待机 408

图 5

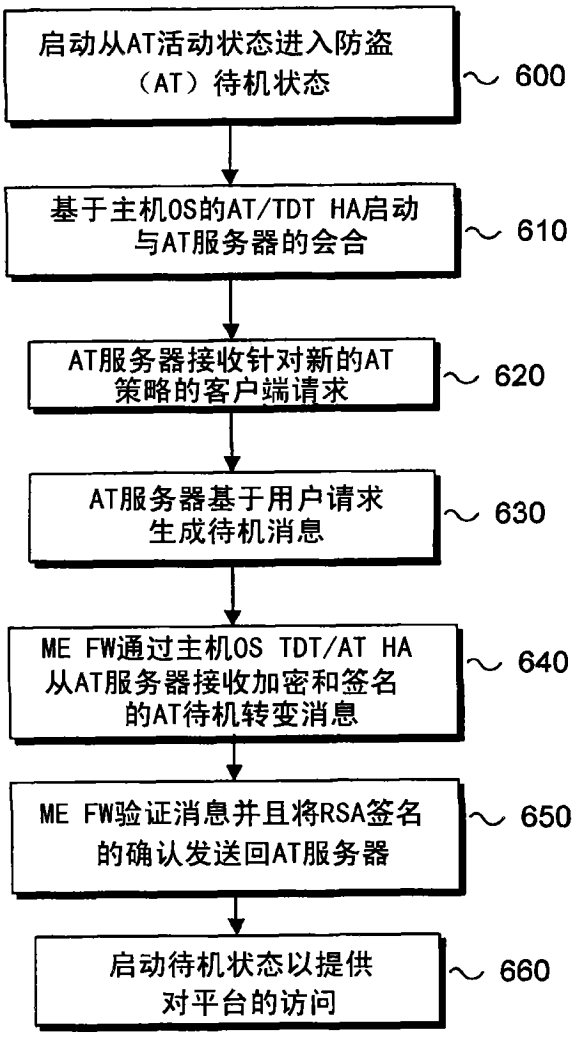

启动从AT活动状态进入防盗（AT）待机状态
600
基于主机OS的AT/TDT HA启动与AT服务器的会合
610
AT服务器接收针对新的AT策略的客户端请求
620
AT服务器基于用户请求生成待机消息
630
ME FW通过主机OS TDT/AT HA从AT服务器接收加密和签名的AT待机转变消息
640
ME FW验证消息并且将RSA签名的确认发送回AT服务器
650
启动待机状态以提供对平台的访问
660

图 6

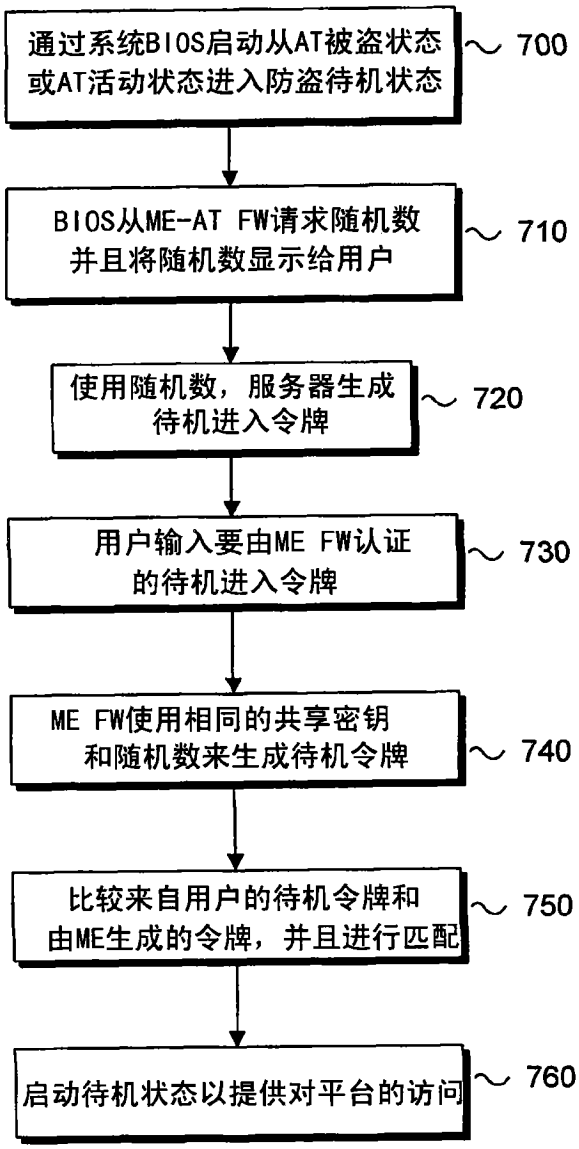

通过系统BIOS启动从AT被盗状态或AT活动状态进入防盗待机状态
700
BIOS从ME-AT FW请求随机数并且将随机数显示给用户
710
使用随机数，服务器生成待机进入令牌
720
用户输入要由ME FW认证的待机进入令牌
730
ME FW使用相同的共享密钥和随机数来生成待机令牌
740
比较来自用户的待机令牌和由ME生成的令牌，并且进行匹配
750
启动待机状态以提供对平台的访问
760

图 7