(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 108351944 B
(45)授权公告日 2021.11.09

(21)申请号 201680065061.3
(22)申请日 2016.12.07
(65)同一申请的已公布的文献号
申请公布号 CN 108351944 A
(43)申请公布日 2018.07.31
(30)优先权数据
14/960,553 2015.12.07 US
(85)PCT国际申请进入国家阶段日
2018.05.07
(86)PCT国际申请的申请数据
PCT/US2016/065351 2016.12.07
(87)PCT国际申请的公布数据
WO2017/100303 EN 2017.06.15
(73)专利权人 亚马逊技术有限公司
地址 美国内华达州
(72)发明人 马修·约翰·坎帕尼亚
格雷戈里·艾伦·鲁宾
埃里克·詹森·布兰德温
马修·肖恩·威尔逊
克里斯蒂安·M·伊拉茨
(74)专利代理机构 北京超凡志成知识产权代理事务所(普通合伙) 11371
代理人 王晖 李丙林
(51)Int.Cl.
G06F 21/57(2006.01)
G06F 9/455(2006.01)
(56)对比文件
US 8176336 B1,2012.05.08
US 8627414 B1,2014.01.07
US 2014108784 A1,2014.04.17
US 2006256108 A1,2006.11.16
US 2014006776 A1,2014.01.02
CN 103795717 A,2014.05.14
审查员 周燕

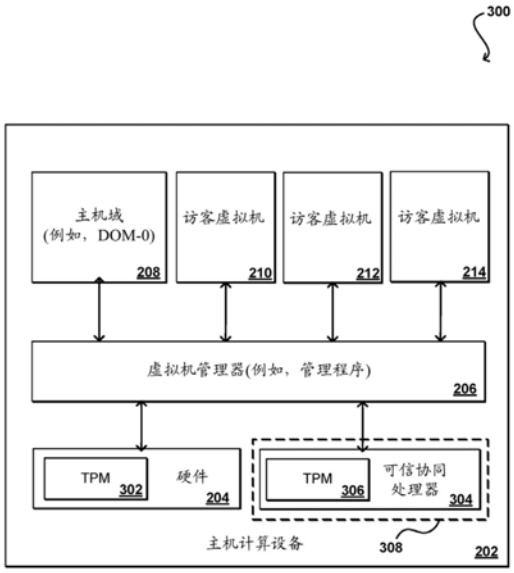
权利要求书3页 说明书14页 附图9页

(54)发明名称

链式安全系统

(57)摘要

一种分层授证方法向具有在远程环境中运行的虚拟机的客户提供这些机器的虚拟图像处于原始状态并在可信执行环境中运行的保证。所述环境可以被分成多个子系统,每个所述子系统具有其自身的密码界限、安全存储和可信计算能力。可信的有限子系统可以处理在主机计算设备的主系统上运行的虚拟机的管理任务。所述有限系统可以从证书机构接收证书,并且可以充当用于向所述主系统提供凭证的证书机构。在证明请求之后,所述子系统可以使用所述相应的凭证以及所述证书链来提供证明信息。具有所述适当凭证的实体可以根据响应确定所述系统的所述状态并且验证所述状态是符合预期的。



CN 108351944 B

1.一种主机计算机系统,其包括:

至少一个处理器,其被配置来操作多个虚拟机;

外围设备,其包括存储用于管理所述多个虚拟机的第一可执行指令的协同处理器和第一存储器,所述外围设备还包括:第一安全加密处理器,其被配置用于至少使用第一背书密钥和从证书机构接收的第一证书来与所述外围设备一起使用;以及

第二安全加密处理器和第二存储器,其存储第二可执行指令并且被配置用于至少使用第二背书密钥和从所述第一安全加密处理器接收的第二证书来与所述主机计算机系统一起使用,

其中所述第一可执行指令在被执行时致使所述外围设备:

接收与所述多个虚拟机中的客户虚拟机相关联的证明请求,使用客户机图像来启动所述客户虚拟机;

为所述外围设备生成第一已签名测量值,所述第一已签名测量值包括所述外围设备的识别信息和使用从所述证书机构接收的所述第一证书来生成的凭证;

致使所述第二安全加密处理器为所述主机计算机系统生成第二已签名测量值,所述第二已签名测量值包括所述主机计算机系统的识别信息、所述客户机图像的信息、以及使用从所述第一安全加密处理器接收的所述第二证书来生成的凭证;

汇编包括所述第一已签名测量值、所述第二已签名测量值、以及所述第一证书和所述第二证书的证书链的证明响应;以及

转发所述证明响应,其中使得客户系统能够至少验证所述客户虚拟机的完整性和所述主机计算机系统的安全性。

2.根据权利要求1所述的主机计算机系统,其中所述第二可执行指令在被执行时还致使所述系统操作所述主机计算机系统上的主子系统,所述主子系统负责使用所述客户机图像来执行所述客户虚拟机,并且

其中所述第一可执行指令在被执行时还致使所述协同处理器使用所述外围设备来操作有限子系统,所述有限子系统被配置来执行所述主子系统的管理任务,所述有限子系统进一步被配置来初始化所述主子系统并且致使使用从所述证书机构接收的所述第一证书来生成的所述凭证被提供给所述第二安全加密处理器。

3.根据权利要求1所述的主机计算机系统,其中所述第一已签名测量值还包括对应于所述第一安全加密处理器的第一证明完整性密钥对和第一主机身份密钥对,并且其中所述第二已签名测量值还包括对应于所述第二安全加密处理器的第二证明完整性密钥对和第二主机身份密钥对。

4.一种计算机实现的方法,其包括:

将来自客户系统的证明请求接收到计算设备的主子系统,所述计算设备操作与所述客户系统相关联的客户虚拟机;

向使用物理连接到所述计算设备的可信硬件提供的有限子系统发送请求,所述有限子系统被配置来执行所述客户虚拟机的管理任务;

从所述有限子系统接收包括所述有限子系统的第一凭证的第一测量值,使用由证书机构提供的第一证书来生成所述第一凭证;

生成包括所述主子系统的第二凭证和所述客户虚拟机的状态信息的第二测量值,使用

由所述有限子系统提供的第二证书来生成所述第二凭证;以及

向所述客户系统发送证明响应,所述证明响应包括所述第一测量值和所述第二测量值;

其中,所述计算机实现的方法还包括:

将所述第二证书接收到所述主子系统的第二安全加密处理器;以及

使用所述第二证书和所述第二安全加密处理器的第二背书密钥来生成所述第二凭证,所述第二背书密钥不可从所述第二安全加密处理器输出。

5.根据权利要求4所述的计算机实现的方法,其还包括:

将所述第一证书接收到所述有限子系统的第一安全加密处理器;以及

使用所述第一证书和所述第一安全加密处理器的第一背书密钥来生成所述第一凭证,所述第一背书密钥不可从所述第一安全加密处理器输出。

6.根据权利要求4所述的计算机实现的方法,其还包括:

在将所述请求发送到所述有限子系统之前,使用所述证明请求中包括的第一标识符验证所述计算设备的身份,以及使用所述证明请求中包括的第二标识符验证客户机图像的身份。

7.根据权利要求4所述的计算机实现的方法,其还包括:

使用所述第一测量值和所述第二测量值中的至少一个来生成至少一个散列值,并且将所述至少一个散列值包括在所述证明响应中,所述至少一个散列值与所述客户系统相关联。

8.根据权利要求4所述的计算机实现的方法,其中所述测量值是引证或加密可验证的测量值中的一个。

9.根据权利要求4所述的计算机实现的方法,其中所述可信硬件是包括由所述计算设备操作的环境的提供商配置的固件和指令的外设卡,其中所述外设卡具有比所述计算设备更高的信任等级。

10.根据权利要求4所述的计算机实现的方法,其还包括:

确定所述证明请求中包括的挑战信息;以及

将所述挑战信息包括在所述证明响应中。

11.一种在主机计算设备上操作的有限子系统,其包括:

至少一个处理器;以及

存储器,其存储指令,所述指令在由所述至少一个处理器执行时致使所述有限子系统:

接收针对在所述主机计算设备上的主子系统中运行的虚拟机的证明请求,使用可信硬件来提供所述有限子系统,所述可信硬件物理连接到所述主机计算设备并且被配置来执行所述虚拟机的管理任务;

生成包括所述有限子系统的第一凭证的第一测量值,使用由证书机构提供的第一证书来生成所述第一凭证;

致使所述主机计算设备的所述主子系统生成包括所述主子系统的第二凭证和所述虚拟机的状态信息的第二测量值,使用由所述有限子系统提供的第二证书来生成所述第二凭证;以及

发送包括所述第一测量值和所述第二测量值的证明响应;

其中所述指令在被执行时还致使所述主机计算设备：

致使将所述第二证书发送到所述主子系统的第二安全加密处理器;以及

致使使用所述第二证书和所述第二安全加密处理器的第二背书密钥来生成所述第二凭证,所述第二背书密钥不可从所述第二安全加密处理器输出。

12.根据权利要求11所述的有限子系统,其中所述指令在被执行时还致使所述主机计算设备：

确定所述证明请求中包括的密码随机数;以及

将所述密码随机数包括在所述证明响应中。

13.根据权利要求11所述的有限子系统,其中所述指令在被执行时还致使所述主机计算设备：

使用所述证明请求中包括的第一标识符将所述主机计算设备验证为所述证明请求的目标。

链式安全系统

背景技术

[0001] 随着越来越多的应用和服务在诸如互联网的网络上变得可用，越来越多的内容、应用和服务提供商求助于诸如云计算的技术。一般来说，云计算是通过诸如网络服务的服务提供对电子资源的访问的方法，其中用于支持那些服务的硬件和/或软件是动态可扩展的，以便在任何给定时间满足服务的需要。客户通常将通过云来租用、租出、或以其他方式支付对资源的访问，使得客户不必须购买和保持硬件和/或软件以提供对这些资源的访问。至少从客户角度来看，这种方法的潜在缺点是：资源通常位于那些资源的提供商控制下的位置处并且因此不在客户的直接控制下。此外，通常与其他客户共享资源，使得数据、软件和资源的安全性和完整性可能受损。

附图说明

[0002] 将参考附图描述根据本公开的各种实施方案，在附图中：

[0003] 图1示出可实现各种实施方案的示例性环境。

[0004] 图2示出可根据各种实施方案使用的运行多个访客虚拟机的虚拟机管理器的示例性配置。

[0005] 图3示出可根据各种实施方案利用的包括可信协同处理器的示例性环境。

[0006] 图4示出可根据各种实施方案利用的示例性授证过程。

[0007] 图5示出可根据各种实施方案利用的示例性证明过程。

[0008] 图6示出可根据各种实施方案利用的示例性证明验证过程。

[0009] 图7示出可根据各种实施方案利用的另一个示例性证明过程。

[0010] 图8示出可根据各种实施方案利用的另一个示例性证明验证过程。

[0011] 图9示出可根据各种实施方案利用的计算设备的示例性组件。

具体实施方式

[0012] 根据本公开的各种实施方案的系统和方法可以克服在用于管理共享计算环境中的安全性的常规方法中经历的前述缺点和其他缺点中的一个或多个。具体地，各种实施方案向具有在远程环境中运行的虚拟机的客户提供这些机器的虚拟图像处于原始状态并在可信执行环境中运行的保证。具体地，各种实施方案利用分层授证方法，其中环境在逻辑上被划分为诸如有限子系统(l-sys)和主子系统(m-sys)的子系统，其中l-sys可以托管在m-sys上运行的虚拟机的管理过程。例如，可以使用具有可信协同处理器的外围设备来提供l-sys，而可以由原始主机计算设备提供m-sys。由于l-sys具有比m-sys更高的信任级别并且物理连接到m-sys，因此l-sys可以从证书机构接收证书并且可以向m-sys提供凭证，由此l-sys充当m-sys的证书机构。在证明阶段期间，例如，每个子系统的相关信息可以被散列化并且与认证链组合以提供所期望的证明。相关信息可以包括适当的标识符以及每个子系统的凭证。接收信息的实体可以使用适当的凭证来提取系统的状态信息并验证信息是符合预期的，以便提供相应客户机的虚拟图像处于原始状态并且在可信执行环境中运行的保证。

[0013] 下文参照各种实施方案来呈现各种其他应用、过程和用途。

[0014] 图1示出可实现各种实施方案的方面的示例性环境100。在这个实例中，用户能够利用计算设备102以便跨至少一个网络104提交有待接收到共享资源环境106(诸如数据中心或“云”环境等其他此类选项)的调用或请求。计算设备102可以包括任何适当的设备，如可以包括诸如个人计算机、手机、手持式消息传递设备、膝上计算机、机顶盒、个人数据助理、电子书阅读器等的客户端设备。至少一个网络104可包括任何适当的有线和/或无线网络，其包括内联网、互联网、蜂窝网、局域网或任何其他此类网络或上述网络的组合。用于这种系统的组件可至少部分地取决于所选择的网络和/或环境的类型。用于通过这种网络通信的协议和组件是众所周知的，因而本文将不再详细讨论。

[0015] 这个实例中的资源环境106包括接口层118，如可以包括诸如以下的组件：应用程序编程接口(API)、路由器、交换机、网络服务器、以及已知或用于将通信从用户计算设备102路由到环境中的适当资源的其他此类组件。在这个实例中，资源环境106包括许多机架108，每个机架包括许多主机计算设备110、以及这个示例性实施方案中的任选机架支持计算系统116。在所示机架108中的一个上的主机计算系统110各自托管这个实例中的一个或多个虚拟机114、以及与该主机计算系统上的虚拟机相关联的不同虚拟机管理器112。虚拟机管理器(VMM)的任务是管理相应主机设备上的虚拟机(VM)以及处理虚拟化的各个方面。每个虚拟机114可以充当用于代表用户执行一个或多个任务的独立计算资源，其中虚拟机用作用户的专用资源。环境还可以包括附加主机计算系统，所述附加主机计算系统不包括不同的虚拟机，尽管如此但可能各自充当一个或多个用户的计算资源。机架支持计算系统116可以为其机架本地的其他计算系统提供各种公用服务(例如，长期程序存储、计量以及对由机架本地的其他计算系统履行的程序执行和/或非本地块数据存储访问的其他监测等)，以及可能向位于环境106中的其他计算系统提供所述公用服务。每个计算系统也可以具有诸如用于存储由正在执行的程序创建或以其他方式使用的程序和/或数据的本地副本的一个或多个本地附接存储设备(未示出)、以及各种其他组件。

[0016] 应当理解的是，为了解释的目的，图1的实例已经被简化，并且主机计算系统和其他设备的数量和组织可能比图1中描绘的数量和组织大得多。例如，作为一个说明性实施方案，云环境中可能存在约几万个计算系统，其中那些计算系统中的至少一些是可以各自托管多个虚拟机的主机计算系统。

[0017] 可以使用许多虚拟化技术来在给定主机上同时操作多个访客虚拟机(VM)或访客操作系统(OS)。图2示出根据各种实施方案的使用虚拟机管理器(VMM)(诸如管理程序)来利用一个虚拟化技术的实例200。主机计算设备202的硬件204(例如，中央处理器和其他此类组件)能够与直接在硬件204上运行的VMM 206进行连接，诸如在“裸机”或本地管理程序的情况下。用于此类目的的管理程序的实例包括Xen、Hyper-V®等。管理程序通常在比机器上的任何其他软件更高、更特许的处理器状态下运行，并提供诸如用于依赖层和/或域的存储器管理和处理器调度的服务。此类层和/或域的最大特许存在于可包括主机域208的服务域层中，所述主机域208可包括管理操作系统，所述管理操作系统用于配置管理程序206的操作和功能性、以及较低特许的域(诸如访客虚拟机210、212、214或其他操作系统的域，其可以是异构性的(即，运行不同于彼此的操作系统))的操作和功能性。主机域208(例如，DOM-0)可以通过管理程序206直接访问主机计算设备202的硬件资源204，而访客虚拟机域210、

212、214可能不能如此。

[0018] 在某些实施方案中，可能存在各种操作模式。例如，为了更新主机计算设备上的微代码，主机计算设备可以从可信源接收更新并且进入系统管理模式(SMM)，诸如通过接收系统管理中断(SMI)来中断正常的管理程序执行。在至少一些常规设计中，进入SMM导致处理器中的除了单个物理核心(例如，自举核心)之外的所有物理处理器核心的执行被暂停。保持执行的单个物理核心将负责应用更新。在一些实施方案中，可以确保的是：在暂停物理核心的执行之前，处理器完成执行其在检测到SMI或其他中断信号时正在执行的特定指令的全部更新。所接收的更新(例如，针对固件、软件或微代码)可以由可信源(诸如服务提供商或处理器制造商)签名和/或加密。在一个实例中，可以使用私钥或可信源的其他此类凭证对更新进行签名以便确保更新的真实性。如果使用私钥对更新进行签名，则主机计算设备可能需要在应用修补程序之前确认更新的签名。在一些实施方案中，用于验证签名的公钥可以存储在主机计算设备上的可信平台模块(TPM)(未示出)中。在一些实施方案中，可以使用不对称密码或对称密码来加密更新。例如，可以使用公钥对更新进行加密以便确保更新的隐私。如果更新被加密，则处理更新的任何中间方都不能读取更新或确定其内容，除非他们有权访问用于解密更新的私钥。如果更新被加密，则用于解密更新的私钥可以被存储到TPM，类似于如前所述的用于验证更新的公钥。一旦更新被查证和/或解密，则可以将更新应用于主机计算设备202。如果使用SMM来应用更新，则可以在SMI处理程序中实现用于应用更新的指令，或者SMI处理程序可能以加密方式验证并调用在管理程序中预配置的修补程序功能。然而，这种方法的潜在缺点是：暴露给一个或多个外部用户的主机上的虚拟机管理器(VMM)可能受损。因此，主机计算设备202上的访客虚拟机(VM)210、212、214中的一个可以潜在地通过管理程序206来访问主机硬件204中的TPM。

[0019] 根据各种实施方案的方法可以尝试改善这种环境中的安全性，同时确保客户机密、密钥、安全数据和其他此类对象在该环境中得到充分保护，并且不会发生无意识的或意外的环境修改。图3示出可以用于提供这种安全性的示例性环境300。应当指出的是，出于简化解释的目的，类似组件的附图标号可以在附图之间继续存在，但是除非另外具体说明，否则这种使用不应当被解释为对各种实施方案的范围的限制。在这个实例中，主机计算设备202包括(或能够接收)可以与VMM 206和主机的其他组件通信的可信协同处理器304或安全协同处理器。可以通过外围设备(例如像，可从主机计算设备202移除的PCI设备)来提供可信协同处理器304。可信协同处理器可以包括一个或多个处理器、存储器、一个或多个接口、以及已知用于向这种系统提供外围设备或附加处理器的任何其他组件或连接。在一个实施方案中，可信协同处理器是采用包括特定固件的单独PCIE卡的形式的独立硬件组件。可信协同处理器的配置使得其能够在逻辑上被认为在与客户VM相关联的信任界限、密码界限、信任区域或可信飞域内。在至少一些实施方案中，可以由资源环境的提供商或由提供商信任的实体来制造、配置或以其他方式提供外设卡，使得提供商可以对外设卡或其他此类附加或可移除硬件的安全性具有比对原始主机计算设备202的安全性更高的信任等级。

[0020] 可信协同处理器304或其他此类硬件设备可以提供以下优点：能够从主机计算设备202卸载许多管理任务，以使得主机计算设备可以基本上专用于托管客户虚拟机、处理客户数据或执行其他此类任务。专用于客户的计算资源因此可以由主机计算设备提供，从而使得针对客户任务的主机硬件使用率最大化，同时那些资源的管理由可信协同处理器负

责。这具有另外的优点，即所有管理过程将在可信计算环境308中运行，或者在与具有更高提供商信任级别的硬件相对应的信任界限内运行。另外的优点是提供商可以提供安全保证，即提供商访问仅限于必要的资源并且系统正在运行可信软件。

[0021] 因此，可信计算环境308内的诸如可信协同处理器304的组件可以在逻辑上被认为是主机设备上的子系统，其中该子系统具有相对有限的功能性。这个单独的“有限”子系统被包含在相关联的密码界限内，并且在本文中被称为“l-sys”。然后，主机硬件的至少一部分可以专用于提供和保持在主机上运行的虚拟机或虚拟主机。包含在单独密码界限内的这个“主”子系统在本文中被称为“m-sys”。因此，为了m-sys中托管的访客机的提供商管理功能的目的，提供商访问至少可以在一定程度上限于l-sys。

[0022] 即使在提供商访问的这种分离和限制的情况下，然而，提供商仍将需要能够向客户(具有虚拟环境中运行的虚拟实例)提供以下保证：每个客户实例的虚拟映像处于“原始”或预期状态，而没有意外的修改，并且实例正在可信执行环境中运行。根据各种实施方案的方法可以使用分层或链式的授证机制来提供此类保证，由此子系统可以具有其自己的授证机制，从而使得子系统能够被识别，并且在子系统顶上运行的软件和虚拟系统被验证为真实的。至少一些实施方案中的每个子系统可以具有其自己的密码界限、安全存储和可信计算能力、以及运行附加固件和软件的能力。

[0023] 此外，至少一些子系统可以利用单独的存储器和处理器空间作为可信计算环境的一部分，诸如可以被建模为可信平台模块(TPM)或其他此类组件。TPM可用于执行远程证明，诸如用于远程验证在主机上运行的系统的真实性。例如，通过提供TPM的系列、链或层次结构，可以识别子系统，并且可以将在那些子系统顶上运行的软件和虚拟系统验证为真实的。尽管本文讨论的实例涉及包括l-sys和m-sys的双系统主机，但应当理解的是，可以在各种实施方案的范围内酌情地使用各种其他数量和/或配置的子系统。

[0024] 如所提及的，使用资源提供商环境中的嵌入式系统来执行敏感或机密任务的客户将通常希望能够确保远程嵌入式系统未被意外修改或篡改，并且嵌入式系统和虚拟机将按预期运行。用于验证这种操作的一种方法涉及远程证明。远程证明提供对计算环境(诸如本文所述的各种子系统)的未经授权或意外的改变的检测。这些改变可以包括用于尝试规避安全措施的修改。在常规远程证明过程期间，主机可以生成指示当前在主机上运行的软件的证书。然后，可以将证书提供给客户或另一适当方，以便证明当前在环境中执行的软件未被修改或如预期的那样。例如，远程证明可以利用公钥加密来确保关于软件的信息仅暴露给请求证明的一方或获得了适当密钥的其他方。通常TPM是可以通过将密钥安装到硬件中来保护硬件的专用微处理器。TPM可以利用在TPM外部不可访问的唯一加密密钥，以便在主机的硬件和软件上实施预期的行为。在一些实施方案中，唯一密钥是不可改变且不可从TPM输出的背书密钥，诸如2048位的RSA公钥和私钥对。背书密钥的公钥可以包含在TPM的证书内。在一些实施方案中，TPM可以通过生成对应环境或子系统的硬件和软件配置的散列汇总来执行远程证明。可以使用任何适当的加密散列算法来生成散列值，诸如可以生成MD5、SHA-1、SHA-2或SHA-3散列。

[0025] 根据各种实施方案的方法可以利用l-sys(或这个实例中的具有可信协同处理器304的外围设备)中的第一TPM 306以及m-sys(或这个实例中的主机计算设备202的剩余部分)中的第二TPM 302来执行远程证明。可信l-sys环境308可以用作用于证明设备上的一个

或多个其他子系统(诸如m-sys)的信任根,其能够执行m-sys的证明。l-sys可以生成证明完整性密钥对和主机身份密钥对,其中如先前所讨论的,将公钥绑定到来自证书机构的证书。该信息可以用于唯一地识别基础设施内的设备,以及为证明生成散列。在一些实施方案中,证明请求将包括某种类型的问题、任务或挑战,并且接收请求的设备可以收集具有所述问题、任务或挑战的信息并生成要返回到请求源(或另一适当方或目的地)的散列。可以通过API接收证明请求以及通过控制台或其他此类接口触发证明请求。在一些实施方案中,证明请求可以来自客户虚拟机内,诸如来自虚拟TPM或其他此类证明设备。然后,请求方可以使用其适当密钥副本来确保包括正确的挑战、以及针对挑战的所有信息的预期值。这可以有助于确保l-sys的软件、硬件、配置和/或其他方面如预期所料并且没有发生意外的修改。一旦l-sys被验证为按预期操作,则l-sys(其可以包括在提供商控制下的固件)可以引导或以其他方式初始化m-sys或上层系统。m-sys还可以具有TPM,所述TPM可以生成证明完整性密钥对和主机身份密钥对,其中公钥绑定到适当的证书。该信息可以用于唯一地识别基础设施内的设备,以及为证明生成散列。在这个实例中,l-sys可以是m-sys的证书颁发机构。因此,l-sys或可信协同处理器可以颁发证书、充当证书子机构并且证明它物理附接到m-sys TPM,因为可信协同处理器具有与主机的物理连接。这种方法可以提供完整的证明链。想要证明主机的客户或其他实体可以通过对应于指定虚拟机的主机的m-sys的证书来获得证明,所述m-sys链接到l-sys(以及外设卡或可信协同处理器),所述l-sys(以及外设卡或可信协同处理器)链接到原始证书机构。

[0026] 在一个实例中,客户系统正与资源提供商环境中的虚拟主机上运行的客户虚拟机进行通信。客户系统可以了解诸如绑定到虚拟机的实例标识符(ID)、以及运行虚拟机的主机计算设备的主机ID的信息。客户系统然后可以向客户虚拟机发送证明命令或证明请求。在一些实施方案中,虚拟机可以接收可通过外围设备或l-sys到达的请求。虚拟机可以接收实例ID和主机ID,并且确定虚拟机已正确接收请求并应当提供证明。为了提供证明,需要为可信根系统(或l-sys)以及主系统(或m-sys)返回信息。在这个实例中,虚拟机可以向l-sys发送证明命令,所述l-sys可以使用证明命令的期望信息和挑战来生成适当的散列。l-sys还可以向m-sys发送证明命令,所述m-sys可以为m-sys信息生成类似的散列。m-sys的散列可以包含虚拟机客户的预期引导图像的信息。例如,虚拟机可以获得两个散列值,并且可以发送回用于证明的适当信息。这可以包括例如l-sys和m-sys的散列值以及l-sys和m-sys的证书链。接收信息的客户系统可以验证图像是符合预期的以及可以信任证明链。获取每个子系统的引证(quote)(或可以被签名的其他测量值)的客户系统也可以验证每个引证上的签名以及那些签名中的值。客户系统还可以验证m-sys证书是由l-sys颁发的,而l-sys证书是由可信证书机构颁发的。只要客户信任证书机构,客户就应当能够验证指示客户虚拟机按预期操作的信息。

[0027] 作为用于验证目的的散列的一部分提供的信息可以包括相关子系统的任何适当信息。例如,针对可信协同处理器位于外设卡上的l-sys,散列可以包括PCR寄存器的值或可信协同处理器的固件的信息。也可以利用各种其他类型的信息。确定要包括哪些信息可以平衡包括大量信息的有用性(这提供了增强的安全性,即系统或环境按照预期操作)与保持对系统或环境当前状态的了解(以使得客户系统可知道或确定针对当前状态所期望的适当散列)的需要。使用证明链的优势是:由于子系统的性质,l-sys除了是更可信的环境之外,

还是更受控制且简单的环境，使得散列化或匹配错误的可能性显著减小，并且损害的可能性也显著减小。由于m-sys的硬件和软件都将来源于资源提供商环境的外部，因此在很多情况下，对环境安全的保证可能会更少或更弱。子系统的性质使得可信子系统由于l-sys中的信任级别和l-sys与m-sys的物理连接等其他此类优点而能够证明另一方是有益的。

[0028] 为了使用分层子系统方法来启用远程证明，首先在至少一些实施方案中使用授证过程以便确保子系统具有用于证明的适当凭证。图4示出可根据各种实施方案利用的用于向分层子系统提供凭证的示例性过程400。应当理解，在各种实施方案的范围内，对于本文所述的任何过程都可以存在按类似或不同次序执行或者并行地执行的另外步骤、更少步骤或替代步骤，除非另外说明。在这个实例中，为了在主机计算设备上管理主系统的目的，可以提供402有限系统，其中有限系统可以具有如本文讨论的可信硬件和软件并且可以包含在相关联的密码和/或信任界限内。l-sys可以使用本文讨论或建议的或本领域已知用于获得数字证书的各种过程中的任何一种来从证书机构接收404证书。l-sys可以生成406证明完整性密钥对和主机身份密钥对，其中公钥绑定到相应证书机构所颁发的证书并使用来自l-sys的TPM的认证背书密钥来生成。各种技术中的任一种可以用于通过认证机构从已知或认证的背书密钥自举至认证的主机证明或身份密钥。在得出结论后，l-sys TPM可以具有经证书机构认证的证明完整性密钥和主机身份密钥。可以存储408这些经认证的密钥并且通过$Cert_{l\text{-}sys}$来匿名表示所述密钥。

[0029] 进一步在授证阶段中，可以从m-sys访问m-sys TPM。l-sys可以与m-sys进行通信而不需要离线网络流量。可以致使m-sys TPM从l-sys获取410凭证，其可以用于生成412证书链。证书机构因此认证l-sys，并且l-sys认证m-sys密钥。m-sys授证可以采用一种方法，由此证书机构被l-sys的经机构认证的主机身份密钥替换。m-sys可以生成414证明完整性密钥对和主机身份密钥对，其中公钥绑定到由l-sys颁发的凭证并使用来自m-sys的TPM的认证背书密钥来生成。一旦结束，m-sys TPM可以具有经l-sys认证的证明完整性密钥和经l-sys认证的主机身份密钥。可以存储416这些经认证的密钥并且通过$Cert_{m\text{-}sys}$来匿名表示所述密钥。

[0030] 一旦两个子系统(或者在多于两个子系统的情况下的所有子系统)被授证，则可以证明在系统上运行的客户部署。图5示出可根据各种实施方案利用的用于证明客户部署的示例性过程500。在至少一些实施方案中，这种过程可以分解成各个部分，包括证明请求部分和证明响应部分。在至少一些实施方案中，还可以存在证明响应确认过程或部分。涉及证明请求的第一部分涉及需要证明客户部署的实体。在这个实例中，接收502证明请求，其中证明请求包括诸如客户部署的主机计算设备的主机身份(h-id)的信息。如本文其他地方所讨论的，证明请求最初可以被接收到控制平面组件，然后被转发到有限系统组件或接口等其他此类选项。作为过程的一部分，可以生成随机密码随机数N或其他任意单次使用号码，其中证明请求然后至少由值h-id和N组成。在至少一些实施方案中，输出证明请求可以被接收到主机h-id。

[0031] 具有主机身份h-id的已授证主机可以接收可能通过l-sys的请求。如所讨论的，已授证主机将具有由m-sys和l-sys的值组成的身份h-id，其中l-sys已经由证书机构认证。例如，接收或被通知请求的m-sys或其他组件可以触发504所述l-sys的证明。响应于证明请求，可以验证预期证明目标的h-id。可以使用随机数N和由证书机构认证的l-sys凭证来创

建506第一证明引证Quote1(或其他已签名测量值)。l-sys可以进而向m-sys发送508证明请求。m-sys可以使用随机数N和由l-sys认证的m-sys凭证来创建510第二证明引证Quote2。如本文其他地方所提及的,在至少一些实施方案中,每个引证可以包括相应信息的散列。然后,l-sys可以从m-sys接收Quote2和凭证$Cert_{m\text{-}sys}$,并且汇编512证明响应,所述证明响应在一些实施方案中包括Quote1、Quote2、以及证书$Cert_{m\text{-}sys}$和$Cert_{l\text{-}sys}$或证书链,其可以形成有待作为证明响应返回的输出。然后,l-sys可以将请求转发514到适当的目的地或地址。

[0032] 在至少一些实施方案中,接收证明响应并且具有状态的真实性保证的实体(或另一感兴趣的和授权的实体)可能想要验证所述证明。图6示出可根据各种实施方案利用的用于验证证明响应的示例性过程600。在这个实例中,对验证证明感兴趣的实体(诸如与在资源提供商环境中(诸如在m-sys子系统中)运行的部署相关联的客户)接收602证明响应。作为验证过程的一部分,可以确定604报告的系统状态。例如,状态信息可以包括来自证书机构的公钥的真实副本、以及用于生成对主机身份h-id的证明请求的随机数N。状态还可以包括针对m-sys的第一组可接受的证明响应值(PCR值)、针对l-sys的第二组可接受的证明响应值(PCR值)。输入可以包括证明引证和凭证,即包括Quote1、Quote2以及证书$Cert_{m\text{-}sys}$和$Cert_{l\text{-}sys}$。作为验证过程的一部分,可以执行第一验证606,即$Cert_{l\text{-}sys}$是来自证书机构的针对h-id有效的证书。如果不是,则可以返回608证明失败响应,或采取其他补救行动。如所提及的,尽管为了方便起见以特定顺序列出这些验证,但应当理解的是,在不同实施方案的范围内可能以不同顺序或同时或以其他方式执行这些确定。可以执行610第二验证,即第一引证Quote1使用$Cert_{l\text{-}sys}$中的适当h-id凭证来进行签名、包含随机数N并且具有正确的PCR值。如果不是,则可以返回608证明失败响应,或采取其他补救行动。可以执行第三验证612,即$Cert_{m\text{-}sys}$是来自l-sys的针对h-id有效的证书。如果不是,则可以返回608证明失败响应,或采取其他补救行动。可以执行614第四验证,即第二引证Quote2使用$Cert_{m\text{-}sys}$中的适当h-id凭证来进行签名、包含随机数N并且具有正确的PCR值。如果不是,则可以返回608证明失败响应,或采取其他补救行动。如果全部验证成功通过,则可以返回616通过或成功消息,或者响应于证明的验证而采取其他类似行动。

[0033] 图7示出用于证明的类似过程700,但是在这种情况下是针对系统上运行的特定虚拟机或客户实例的证明。在这个实例中,接收702远程虚拟机的证明请求,其中证明请求包括诸如虚拟机的虚拟图像的身份(v-id)以及其上加载虚拟图像的主机计算设备的主机身份(h-id)的信息。作为过程的一部分,可以生成随机密码随机数N或其他任意单次使用号码,其中证明请求然后至少由值v-id、h-id和N组成。在至少一些实施方案中,输出证明请求可以被接收到主机h-id。

[0034] 具有主机身份h-id的已授证主机可以接收可能通过l-sys的请求。如所讨论的,已授证主机将具有由m-sys和l-sys的值组成的身份h-id,其中l-sys已经由证书机构认证。例如,接收或被通知请求的m-sys或其他组件可以触发704所述l-sys的证明。响应于证明请求,可以验证预期证明目标的h-id。可以使用随机数N和由证书机构认证的l-sys凭证来创建706第一证明引证Quote1。l-sys可以进而向m-sys发送708证明请求。m-sys可以使用随机数N和由l-sys认证的m-sys凭证来创建710第二证明引证Quote2。在一些实施方案中,第二证明引证将包括一个或多个PCR寄存器中表示的虚拟图像v-id。也可以针对特定虚拟机或客户实例确定或生成712测量值(诸如已签名测量值或引证),其中在这个实例中,测量值采

用v-id的形式。然后，l-sys可以从m-sys接收Quote2和凭证$Cert_{m-sys}$，并且汇编714证明响应，所述证明响应包括Quote1、Quote2、以及证书$Cert_{m-sys}$和$Cert_{l-sys}$或证书链，其可以形成有待作为证明响应返回的输出。然后，l-sys可以将请求转发716到适当的目的地或地址。

[0035] 在至少一些实施方案中，接收证明响应并且具有状态的真实性保证的实体(或另一感兴趣的和授权的实体)可能想要验证所述证明。图8出可根据各种实施方案利用的用于验证证明响应的示例性过程800。在这个实例中，对验证证明有感兴趣的实体(诸如与在资源提供商环境中(诸如在m-sys子系统中)运行的虚拟机相关联的客户)接收802证明响应。作为验证过程的一部分，可以确定804报告的系统状态。例如，状态信息可以包括来自证书机构的公钥的真实副本、以及用于生成对虚拟图像v-id和主机身份h-id的证明请求的随机数N。状态还可以包括针对m-sys的第一组可接受的证明响应值(PCR值)、针对l-sys的第二组可接受的证明响应值(PCR值)、以及针对虚拟图像v-id的可接受的证明响应值。输入可以包括证明引证和凭证，即包括Quote1、Quote2以及证书$Cert_{m-sys}$和$Cert_{l-sys}$。作为验证过程的一部分，可以执行806第一验证，即$Cert_{l-sys}$是来自证书机构的针对h-id有效的证书。如果不是，则可以返回808证明失败响应，或采取其他补救行动。如所提及的，尽管为了方便起见以特定顺序列出这些验证，但应当理解的是，在不同实施方案的范围内可能以不同顺序或同时或以其他方式执行这些确定。可以执行810第二验证，即第一引证Quote1使用$Cert_{l-sys}$中的适当h-id凭证来进行签名、包含随机数N并且具有正确的PCR值。如果不是，则可以返回808证明失败响应，或采取其他补救行动。可以执行812第三验证，即$Cert_{m-sys}$是来自l-sys的针对h-id有效的证书。如果不是，则可以返回808证明失败响应，或采取其他补救行动。可以执行814第四验证，即第二引证Quote2使用$Cert_{m-sys}$中的适当h-id凭证来进行签名、包含随机数N并且具有正确的PCR值。如果不是，则可以返回808证明失败响应，或采取其他补救行动。可以执行816第五验证，即Quote2中的值包含针对虚拟图像v-id的可接受的证明响应值，其在至少一些实施方案中最有可能是专用或添加的PCR值。如果不是，则可以返回808证明失败响应，或采取其他补救行动。如果全部验证成功通过，则可以返回818通过或成功消息，或者响应于证明的验证而采取其他类似行动。

[0036] 在一些实施方案中，TPM或其他可信环境可能不被设置有诸如证书的可验证凭证。针对这些情况，可以利用特定的设置过程，其中可以代替地使用对主机的物理访问。在一些实施方案中，远程系统的证明可能需要特殊权限。在可能的情况下，可以建立请求实体的经认证凭证，并且使用其来确认证明请求的真实性。最值得注意的是，可以使用经认证的非对称密钥对，并且对证明请求进行签名。在一些实施方案中，针对证明创建，既不需要知道主机身份h-id也不需要知道虚拟图像标识符v-id。在证明请求生成时，不一定需要知道主机身份，并且可以将虚拟图像标识符作为证明引证的一部分进行回报，由此可以确定可接受值。

[0037] 在至少一些实施方案中，引证不需要限于TPM限定的引证机制，并且可以包括使用系统身份密钥来附加签名的信息。m-sys证明响应可以包括足够的信息来确定多个虚拟图像的真实性。在一些实施方案中，这可以通过返回多个引证或将多个结果组合成单个引证来执行。此外，尽管出于解释的目的呈现了两个系统层次结构，但应当说明的是，也可以在各种实施方案的范围内使用具有证书机构的父节点的任何适当的树或层次结构，其中树中的每个节点由父节点进行签名。类似地，在至少一些实施方案中可以存在任意数量的根证

书机构。在一个这种系统中，l-sys形成单个主机内包含的子系统族的根。

[0038] 此外，可鉴于以下条款对本公开的实施方案进行描述：

[0039] 1.一种主机计算机系统，其包括：

[0040] 至少一个处理器，其被配置来操作多个虚拟机；

[0041] 外围设备，其包括存储用于管理所述多个虚拟机的第一可执行指令的协同处理器和第一存储器，所述外围设备还包括：第一安全加密处理器，其被配置用于至少使用第一背书密钥和从证书机构接收的第一证书来与所述外围设备一起使用；以及

[0042] 第二安全加密处理器和第二存储器，其存储第二可执行指令并且被配置用于至少使用第二背书密钥和从所述第一安全加密处理器接收的第二证书来与所述主机计算机系统一起使用，

[0043] 其中所述第一指令在被执行时致使所述外围设备：

[0044] 接收与所述多个虚拟机中的客户虚拟机相关联的证明请求，使用客户机图像来启动所述客户虚拟机；

[0045] 为所述外围设备生成第一已签名测量值，所述第一已签名测量值包括所述外围设备的识别信息和使用从所述证书机构接收的所述第一证书来生成的凭证；

[0046] 致使所述第二安全处理器为所述主机计算系统生成第二已签名测量值，所述第二已签名测量值包括所述主机计算机器的识别信息、所述客户机图像的信息、以及使用从所述第一安全加密处理器接收的所述第二证书来生成的凭证；

[0047] 汇编包括所述第一已签名测量值、所述第二已签名测量值、以及所述第一证书和所述第二证书的证书链的证明响应；以及

[0048] 转发所述证明响应，其中使得客户系统能够至少验证所述客户虚拟机的完整性和所述主机计算系统的安全性。

[0049] 2.如条款1所述的主机计算机系统，其中所述第二指令在被执行时还致使所述系统操作所述主机计算设备上的主子系统，所述主子系统负责使用所述客户机图像来执行所述客户虚拟机，并且

[0050] 其中所述第一指令在被执行时还致使所述协同处理器使用所述外围设备来操作有限子系统，所述有限子系统被配置来执行所述主子系统的管理任务，所述有限子系统进一步被配置来初始化所述主子系统并且致使所述凭证被提供给所述第二安全加密处理器。

[0051] 3.如条款1所述的主机计算机系统，其中所述第一已签名测量值还包括对应于所述第一加密处理器的第一证明完整性密钥对和第一主机身份密钥对，并且其中所述第二已签名测量值还包括对应于所述第二加密处理器的第二证明完整性密钥对和第二主机身份密钥对。

[0052] 4.如条款1所述的主机计算机系统，其中所述指令在执行时进一步致使所述系统：

[0053] 生成所述第一已签名测量值的第一散列和所述第二已签名测量值的第二散列，并且将所述第一散列和所述第二散列包括在所述证明响应中。

[0054] 5.一种计算机实现的方法，其包括：

[0055] 将来自客户系统的证明请求接收到计算设备的主子系统，所述计算设备操作与所述客户系统相关联的客户虚拟机；

[0056] 向使用物理连接到所述计算设备的可信硬件提供的有限子系统发送请求，所述有

限子系统被配置来执行所述客户虚拟机的管理任务；

[0057] 从所述有限子系统接收包括所述有限子系统的第一凭证的第一测量值，使用由证书机构提供的第一证书来生成所述第一凭证；

[0058] 生成包括所述主子系统的第二凭证和所述客户虚拟机的状态信息的第二测量值，使用由所述有限子系统提供的第二证书来生成所述第二凭证；以及

[0059] 向所述客户系统发送证明响应，所述证明响应包括所述第一测量值和所述第二测量值。

[0060] 6.如条款5所述的计算机实现的方法，其还包括：

[0061] 将所述第一证书接收到所述有限子系统的第一安全加密处理器；以及

[0062] 使用所述第一证书和所述第一安全加密处理器的第一背书密钥来生成所述第一凭证，所述第一背书密钥不可从所述第一安全加密处理器输出。

[0063] 7.根据条款6所述的计算机实现的方法，其中所述第一凭证包括与所述有限子系统相关联的第一证明完整性密钥对和第一主机身份密钥对。

[0064] 8.如条款6所述的计算机实现的方法，其还包括：

[0065] 将所述第二证书接收到所述主子系统的第二安全加密处理器；以及

[0066] 使用所述第二证书和所述第二安全加密处理器的第二背书密钥来生成所述第二凭证，所述第二背书密钥不可从所述第二安全加密处理器输出。

[0067] 9.根据条款8所述的计算机实现的方法，其中所述第二凭证包括与所述主子系统相关联的第二证明完整性密钥对和第二主机身份密钥对。

[0068] 10.如条款5所述的计算机实现的方法，其还包括：

[0069] 在将所述请求发送到所述有限子系统之前，使用所述证明请求中包括的第一标识符验证所述主机的身份，以及使用所述证明请求中包括的第二标识符验证客户机图像的身份。

[0070] 11.如条款5所述的计算机实现的方法，其还包括：

[0071] 使用所述第一测量值和所述第二测量值中的至少一个来生成至少一个散列值，并且将所述至少一个散列值包括在所述证明响应中，所述至少一个散列值与所述客户系统相关联。

[0072] 12.根据条款5所述的计算机实现的方法，其中所述证明响应还包括虚拟实例的测量值或所述第一证书和所述第二证书的证书链中的至少一个。

[0073] 13.如条款5所述的计算机实现的方法，其中所述测量值是引证或加密可验证的测量值中的一个。

[0074] 14.如条款5所述的计算机实现的方法，其中所述可信硬件是包括由所述计算设备操作的环境的提供商配置的固件和指令的外设卡，其中所述外设卡具有比所述计算设备更高的信任等级。

[0075] 15.如条款5所述的计算机实现的方法，其还包括：

[0076] 确定所述证明请求中包括的挑战信息；以及

[0077] 将所述挑战信息包括在所述证明响应中。

[0078] 16.一种在主机计算设备上操作的有限子系统，其包括：

[0079] 至少一个处理器；以及

[0080] 存储器，其存储指令，所述指令在由所述至少一个处理器执行时致使所述有限子系统：

[0081] 接收针对在所述主机计算设备上的主子系统中运行的虚拟机的证明请求，使用可信硬件来提供所述有限子系统，所述可信硬件物理连接到所述主机计算设备并且被配置来执行所述虚拟机的管理任务；

[0082] 生成包括所述有限子系统的第一凭证的第一测量值，使用由证书机构提供的第一证书来生成所述第一凭证；

[0083] 致使所述主机计算设备的所述主子系统生成包括所述主子系统的第二凭证和所述客户虚拟机的状态信息的第二测量值，使用由所述有限子系统提供的第二证书来生成所述第二凭证；以及

[0084] 发送包括所述第一测量值和所述第二测量值的证明响应。

[0085] 17.如条款16所述的有限子系统，其中所述指令在被执行时还致使所述主机计算设备：

[0086] 致使将所述第二证书发送到所述主子系统的第二安全加密处理器；以及

[0087] 致使使用所述第二证书和所述第二安全加密处理器的第二背书密钥来生成所述第二凭证，所述第二背书密钥不可从所述第二安全加密处理器输出。

[0088] 18.如条款16所述的有限子系统，其中所述指令在被执行时还致使所述主机计算设备：

[0089] 确定所述证明请求中包括的密码随机数；以及

[0090] 将所述密码随机数包括在所述证明响应中。

[0091] 19.如条款16所述的有限子系统，其中所述指令在被执行时还致使所述主机计算设备：

[0092] 使用所述证明请求中包括的第一标识符将所述主机计算设备验证为所述证明请求的目标。

[0093] 20.如条款16所述的有限子系统，其中从所述虚拟机的内部生成所述证明请求。

[0094] 图9示出示例性计算设备900的一组通用组件的逻辑布置。在这个实例中，设备包括用于执行可存储在存储器设备或元件904中的指令的处理器902。如本领域的普通技术人员显而易见的，设备可包括许多类型的存储器、数据存储或非暂时性计算机可读存储介质，诸如用于处理器902执行的程序指令的第一数据存储，用于图像或数据的独立存储，用于与其他设备共享信息的可移动存储器等等。设备通常将包括某种类型的显示元件906，诸如触摸屏或液晶显示器(LCD)，但是诸如便携式媒体播放器的设备可能通过其他方式(诸如通过音频扬声器)来传送信息。如讨论的，在很多实施方案中，设备将包括能够从用户接收常规输入的至少一个输入设备908。这种常规输入可例如包括按钮、触摸板、触摸屏、方向盘、操纵杆、键盘、鼠标、小键盘或用户可以借助用来向设备输入命令的任何其他此种设备或元件。然而，在一些实施方案中，这种设备可能根本不包括任何按钮，且可能仅可通过视觉和音频命令的组合来控制，使得用户可在无需与设备接触的情况下控制设备。在一些实施方案中，图9的计算设备900可以包括用于在各种网络上通信的一个或多个网络接口元件908，诸如Wi-Fi、蓝牙、RF、有线或无线通信系统。许多实施方案中的设备可与诸如互联网的网络通信，并且可以能够与其他此类设备通信。

[0095] 在本文中讨论的用于实现根据各种实施方案的各方面的示例性环境主要是基于网络的，如涉及网络服务和云计算，但是应当理解的是，尽管基于网络的环境被用于解释的目的，但是可以酌情使用不同的环境来实现各种实施方案。用于与各种环境相互作用的客户端设备可包括可操作来在适当网络上发送和接收请求、消息或信息并且传送信息回设备用户的任何适当设备。此类客户端设备的实例包括个人计算机、智能电话、手持式消息传递设备、膝上计算机、机顶盒、个人数据助理、电子书阅读器等等。网络可包括任何适当的网络，其包括内联网、互联网、蜂窝网、局域网或任何其他此类网络或上述网络的组合。用于这种系统的组件可至少部分地取决于所选择的网络和/或环境的类型。用于通过这种网络通信的协议和组件是众所周知的，因而本文将不再详细讨论。通过网路进行的通信可通过有线或无线连接及其组合来实现。

[0096] 应理解，可存在可链接起来或以其他方式来配置的若干应用程序服务器、层或其他元件、进程或组件，它们可交互以执行如本文中讨论和建议的任务。如本文所使用的，术语“数据存储器”指代能够存储、访问和检索数据的任何设备或设备组合，所述设备或设备组合可包括任何标准、分布式环境或集群式环境中任何组合和任何数量的数据服务器、数据库、数据存储设备和数据存储介质。应用程序服务器可包括任何适当的硬件和软件，所述硬件和软件视执行客户端设备的一个或多个应用程序的方面的需要与数据存储器集成并且处理应用程序的大多数数据访问和业务逻辑。应用程序服务器提供与数据存储器协作的访问控制服务，并且能够生成将要传送到用户的诸如文本、图片、音频和/或视频的内容，在这个实例中所述内容可以HTML、XML或另一适当结构化语言的形式通过网络服务器向用户提供服务。所有请求和响应的处理以及客户端设备与资源之间的内容递送可由网络服务器来处理。应当理解，网络服务器和应用程序服务器不是必要的，且仅仅是示例性组件，因为本文所论述的结构化代码可在如本文其他地方所论述的任何适当设备或主机上执行。

[0097] 数据存储器可包括若干独立的数据表、数据库或其他数据存储机构和介质，以用来存储与特定方面相关的数据。数据存储器可通过与其相关联的逻辑来操作，以便从服务器接收指令，并且响应于所述指令获得数据、更新数据或以其他方式处理数据。在一个实施方案中，用户可以提交针对某种类型的项目的搜索请求。在此情况下，数据存储器可能访问用户信息来验证用户的身份，并且可访问目录详细信息以获得有关所述类型的项目的信息。接着可将信息以诸如网页上的结果列表的形式返回给用户，用户能够通过用户设备上的浏览器来查看所述网页。可在专用浏览器页面或窗口中查看感兴趣的特定项目的信息。

[0098] 每个服务器通常会包括提供针对该服务器的一般管理和操作的可执行程序指令的操作系统，且通常包括存储指令的非暂时性计算机可读介质，所述指令在被所述服务器的处理器执行时允许所述服务器执行其期望的功能。操作系统的合适的实现方式和服务器的一般功能是众所周知的或可商购获得的，并且易于由本领域普通技术人员实现，尤其是根据本文中的公开内容来实现。

[0099] 在一个实施方案中，环境是利用通过通信链路、使用一个或多个计算机网络或直接连接来互连的多个计算机系统和组件的分布式计算环境。但是，本领域普通技术人员应理解，这种系统可在具有比所描述的更少或更多组件的系统中同样顺利地操作。因此，对本文中的各种系统和服务的描绘本质上应视为说明性的，并且不限制本公开的范围。

[0100] 各个方面可实施为至少一个服务或网络服务的部分，诸如可为服务导向型架构的

部分。诸如网络服务的服务可使用任何适当类型的发信来通信，诸如通过使用呈可扩展标记语言(XML)格式的消息，且使用诸如SOAP(起源于“简单对象访问协议”)等适当协议来交换。这类服务提供或执行的进程可以任意适当语言编写，诸如网络服务描述语言(WSDL)。使用诸如WSDL等语言允许诸如各个SOAP框架中客户端代码的自动生成等的功能性。

[0101] 大多数实施方案利用本领域技术人员所熟悉的至少一个网络，所述网络使用可商购的各种协议中的任何协议来支持通信，所述协议诸如TCP/IP、FTP、UPnP、NFS和CIFS。举例来说，网络可以是局域网、广域网、虚拟专用网、互联网、内联网、外联网、公共交换电话网、红外线网络、无线网络和上述网络的任意组合。

[0102] 在利用网络服务器的实施方案中，网络服务器可运行各种服务器或中间层应用中的任意应用，包括HTTP服务器、FTP服务器、CGI服务器、数据服务器、Java服务器和业务应用服务器。服务器还能够响应来自用户设备的请求而执行程序或脚本，诸如通过执行可以实施为以任何编程语言(诸如Java®、C、C#或C++)或任何脚本语言(诸如Perl、Python或TCL)以及其组合写成的一个或多个脚本或程序的一个或多个网络应用程序。服务器还可包括数据库服务器，包括但不限于可商购自Oracle®、Microsoft®、Sybase®和IBM®的那些数据库服务器。

[0103] 环境可包括如上文讨论的多种数据存储器以及其他存储器和存储介质。这些可驻留在多种位置中，诸如在一个或多个计算机本地(和/或驻留在一个或多个计算机中)的存储介质上，或远离网络上的计算机中的任何或所有计算机。在一组特定实施方案中，信息可驻留于在本领域技术人员熟悉的存储区域网(“SAN”)中。类似地，可视情况本地和/或远程存储用于执行归属于计算机、服务器或其他网络设备的功能的任意必要文件。在系统包括计算机化设备的情况下，每种此类设备可以包括可通过总线进行电耦合的硬件元件，所述元件包括，例如，至少一个中央处理单元(CPU)、至少一个输入设备(例如，鼠标、键盘、控制器、触摸屏或小键盘)和至少一个输出设备(例如，显示设备、打印机或扬声器)。这种系统还可包括一个或多个存储设备，诸如硬盘驱动器、光存储设备和诸如随机存取存储器(“RAM”)或只读存储器(“ROM”)的固态存储设备、以及可移动媒体设备、存储卡、闪存卡等。

[0104] 此类设备还可包括计算机可读存储介质读取器、通信设备(例如，调制解调器、网卡(无线或有线)、红外线通信设备等)和工作存储器，如上文所描述。计算机可读存储介质读取器可与计算机可读存储介质连接或被配置来接收计算机可读存储介质，计算机可读存储介质表示远程、本地、固定和/或可移动存储设备以及用于临时和/或更永久地包含、存储、发射和检索计算机可读信息的存储介质。系统和各种设备通常也将包括多个软件应用、模块、服务或位于至少一个工作存储器设备内的其他元件，包括操作系统和应用程序，诸如客户端应用或网络浏览器。应了解，替代性实施方案相比上文描述的实施方案可具有众多变化。举例来说，也可使用定制硬件，和/或特定元件可以硬件、软件(包括便携式软件，诸如小程序)或者硬件和软件两者来实施。此外，可以采用与其他计算设备(诸如网络输入/输出设备)的连接。

[0105] 用于包括编码或部分编码的存储介质和其他非暂时性计算机可读介质可包括本领域已知或已使用的任何适合介质，包括存储介质和通信介质，诸如但不限于用于存储信息(诸如计算机可读指令、数据结构、程序模块或其他数据)的任何方法或技术中所实施的易失性和非易失性、可移动和不可移动介质，包括RAM、ROM、EEPROM、闪存或其他存储器技

术、CD-ROM、数字通用光盘(DVD)或其他光学存储器、磁盒、磁带、磁盘存储器或其他磁性存储设备，或可用于存储所要信息且可供系统设备访问的任何其他介质。基于本文所提供的公开内容和教义，本领域普通技术人员将了解实现各种实施方案的其他方式和/或方法。

[0106] 因此，应以说明性意义而不是限制性意义来理解本说明书和附图。然而，将明显的是：在不脱离如权利要求书中阐述的本发明的更宽广精神和范围的情况下，可以对本发明做出各种修改和改变。

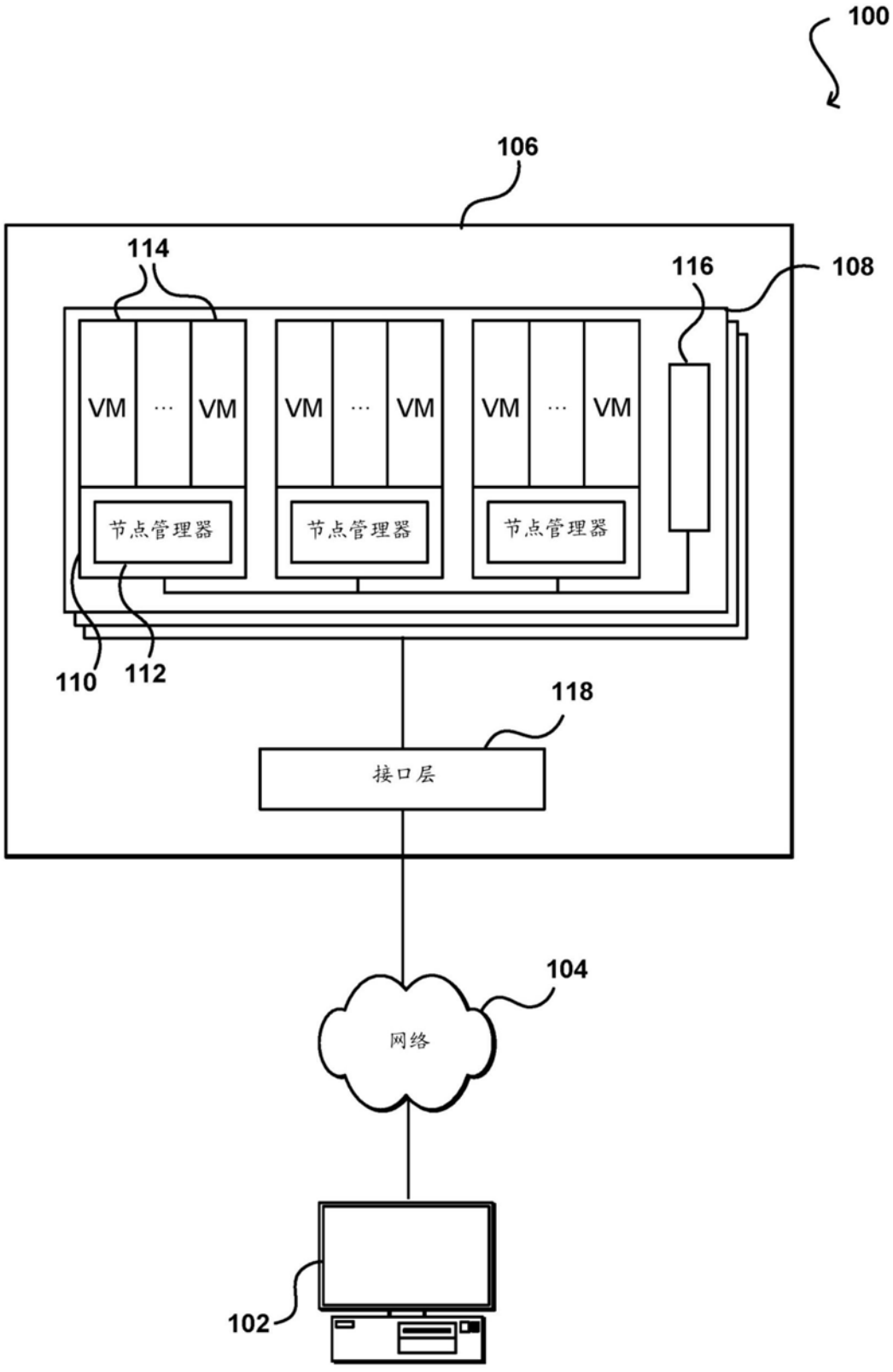

100
106
114
116
108
VM
…
VM
VM
…
VM
VM
…
VM
节点管理器
节点管理器
节点管理器
110
112
118
接口层
104
网络
102

图1

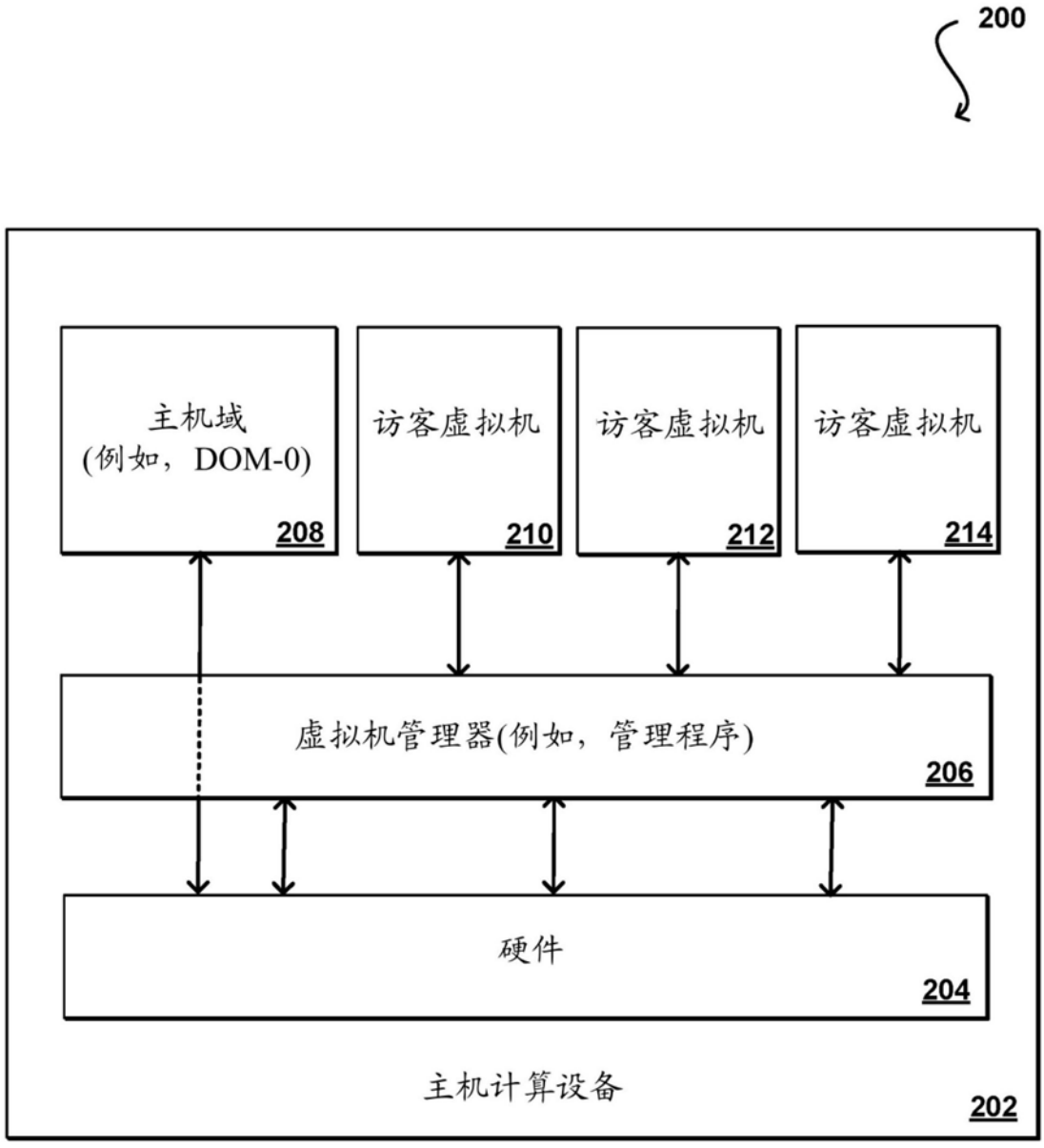

200
主机域
(例如，DOM-0)
208
访客虚拟机
210
访客虚拟机
212
访客虚拟机
214
虚拟机管理器(例如，管理程序)
206
硬件
204
主机计算设备
202

图2

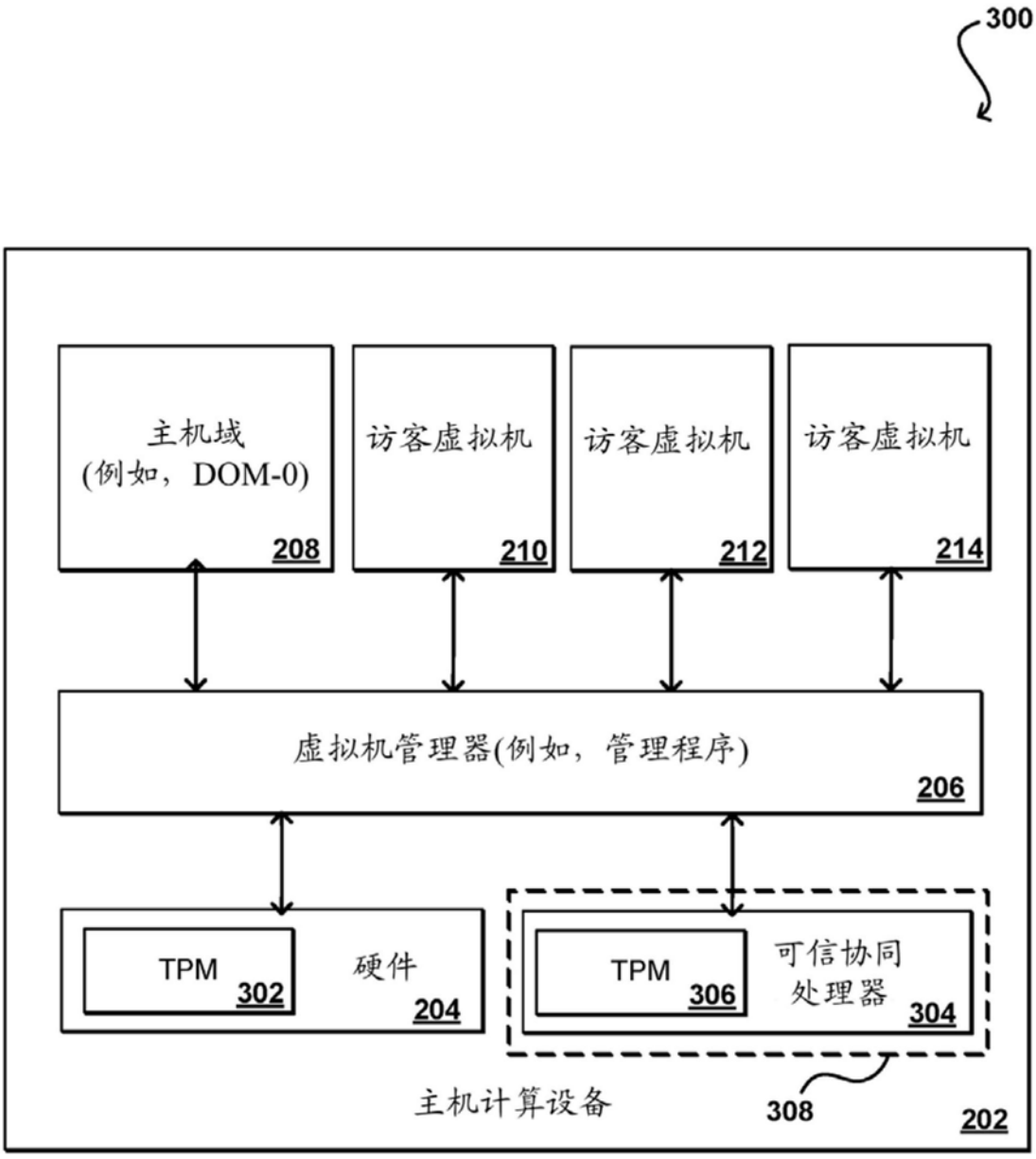

300
主机域
(例如，DOM-0)
208
访客虚拟机
210
访客虚拟机
212
访客虚拟机
214
虚拟机管理器(例如，管理程序)
206
TPM
302
硬件
204
TPM
306
可信协同
处理器
304
主机计算设备
308
202

图3

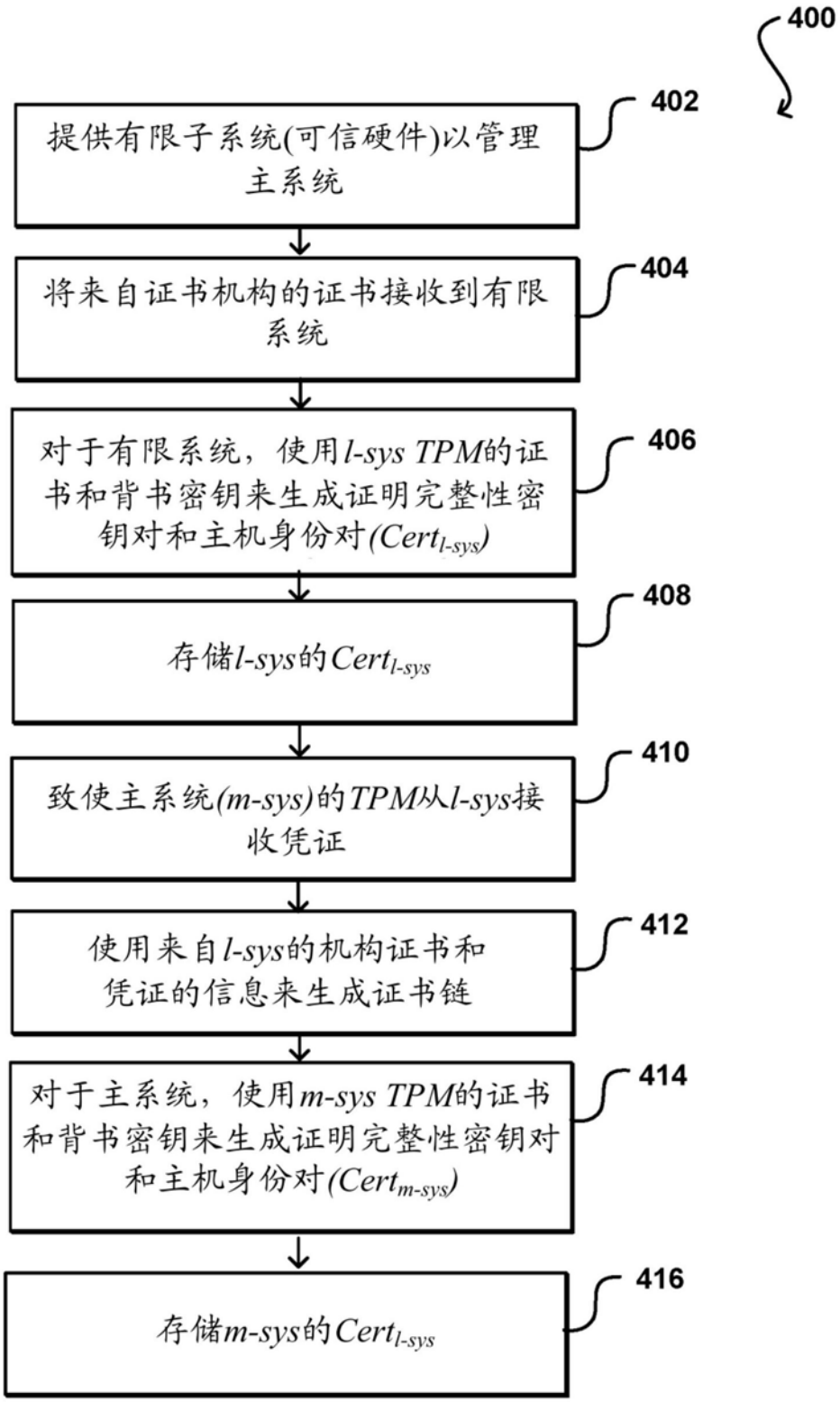

400
402
提供有限子系统(可信硬件)以管理主系统
404
将来自证书机构的证书接收到有限系统
406
对于有限系统，使用l-sys TPM的证书和背书密钥来生成证明完整性密钥对和主机身份对($Cert_{l\text{-}sys}$)
408
存储l-sys的$Cert_{l\text{-}sys}$
410
致使主系统(m-sys)的TPM从l-sys接收凭证
412
使用来自l-sys的机构证书和凭证的信息来生成证书链
414
对于主系统，使用m-sys TPM的证书和背书密钥来生成证明完整性密钥对和主机身份对($Cert_{m\text{-}sys}$)
416
存储m-sys的$Cert_{l\text{-}sys}$

图4

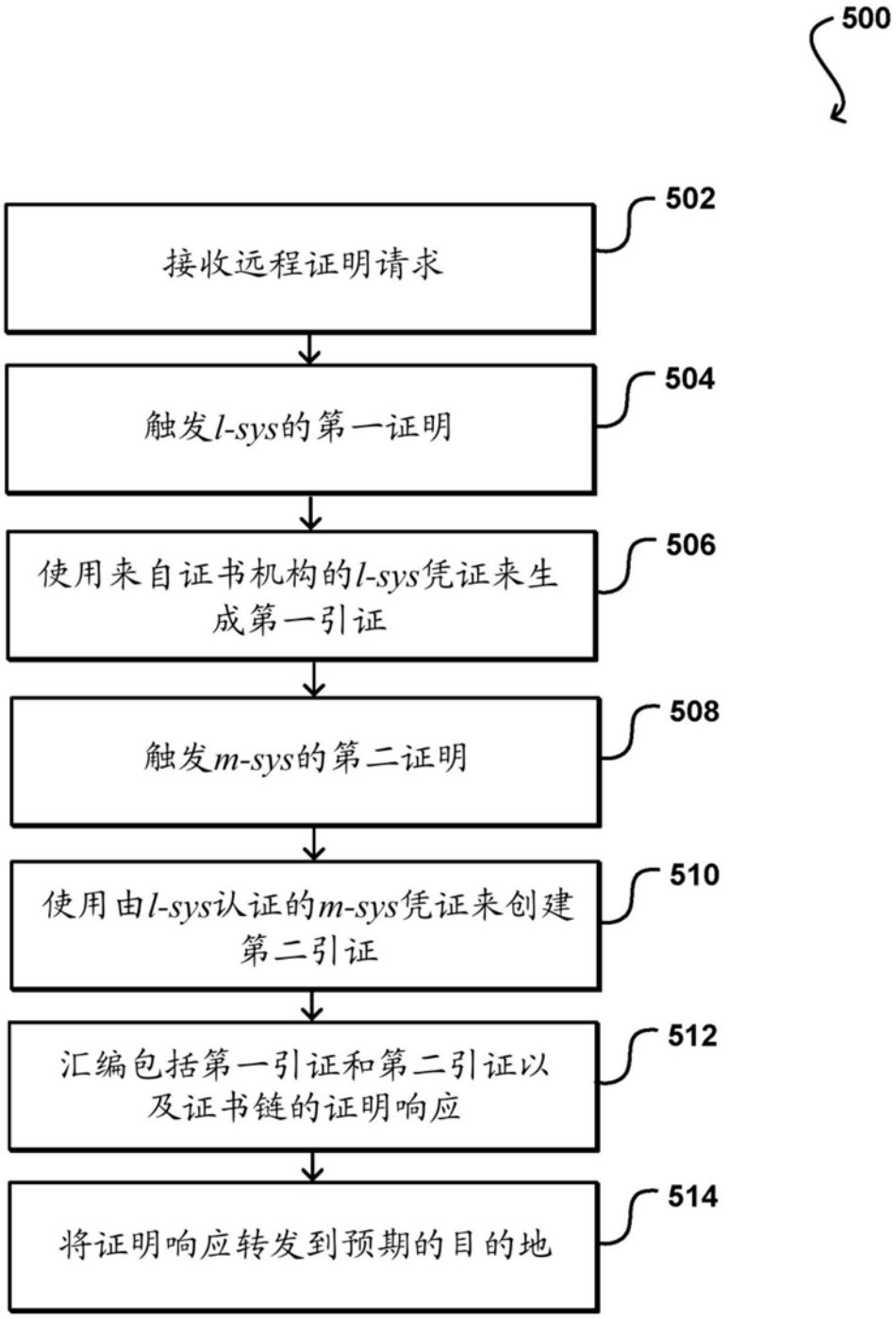

500
502
接收远程证明请求
504
触发l-sys的第一证明
506
使用来自证书机构的l-sys凭证来生成第一引证
508
触发m-sys的第二证明
510
使用由l-sys认证的m-sys凭证来创建第二引证
512
汇编包括第一引证和第二引证以及证书链的证明响应
514
将证明响应转发到预期的目的地

图5

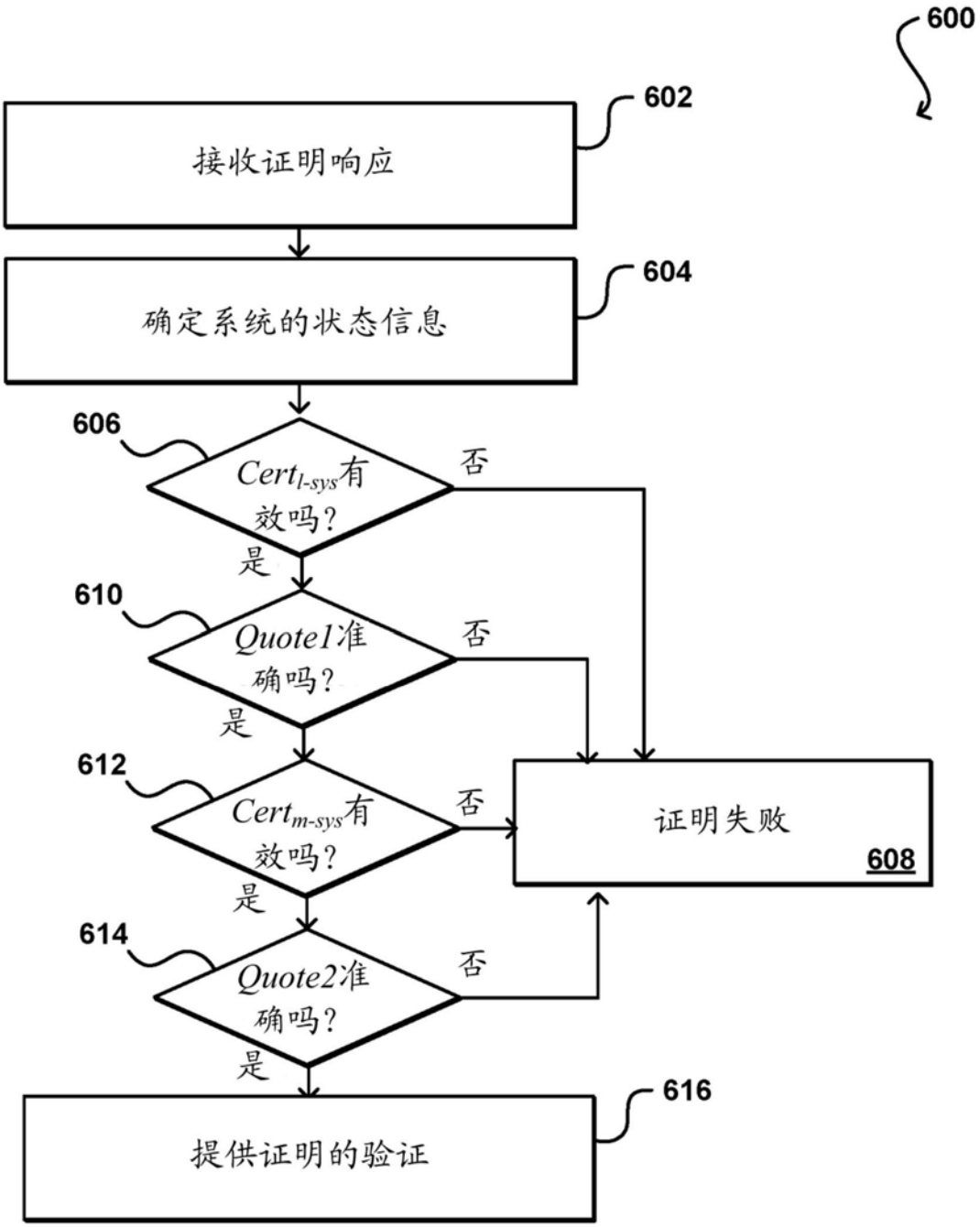

600
602
接收证明响应
604
确定系统的状态信息
606
$Cert_{l\text{-}sys}$有效吗?
否
是
610
Quote1准确吗?
否
是
612
$Cert_{m\text{-}sys}$有效吗?
否
是
证明失败
608
614
Quote2准确吗?
否
是
616
提供证明的验证

图6

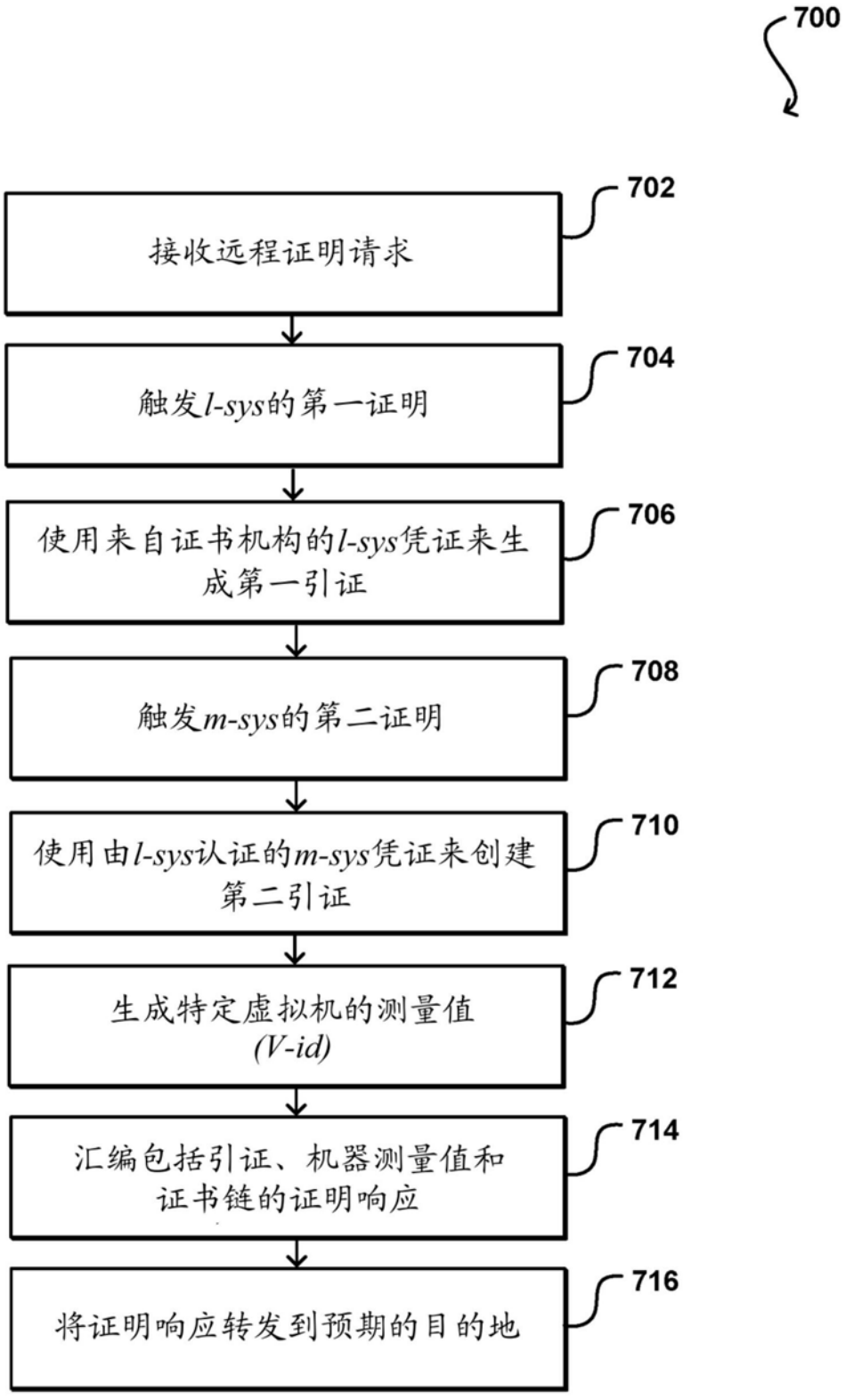

700
接收远程证明请求
702
触发l-sys的第一证明
704
使用来自证书机构的l-sys凭证来生成第一引证
706
触发m-sys的第二证明
708
使用由l-sys认证的m-sys凭证来创建第二引证
710
生成特定虚拟机的测量值(V-id)
712
汇编包括引证、机器测量值和证书链的证明响应
714
将证明响应转发到预期的目的地
716

图7

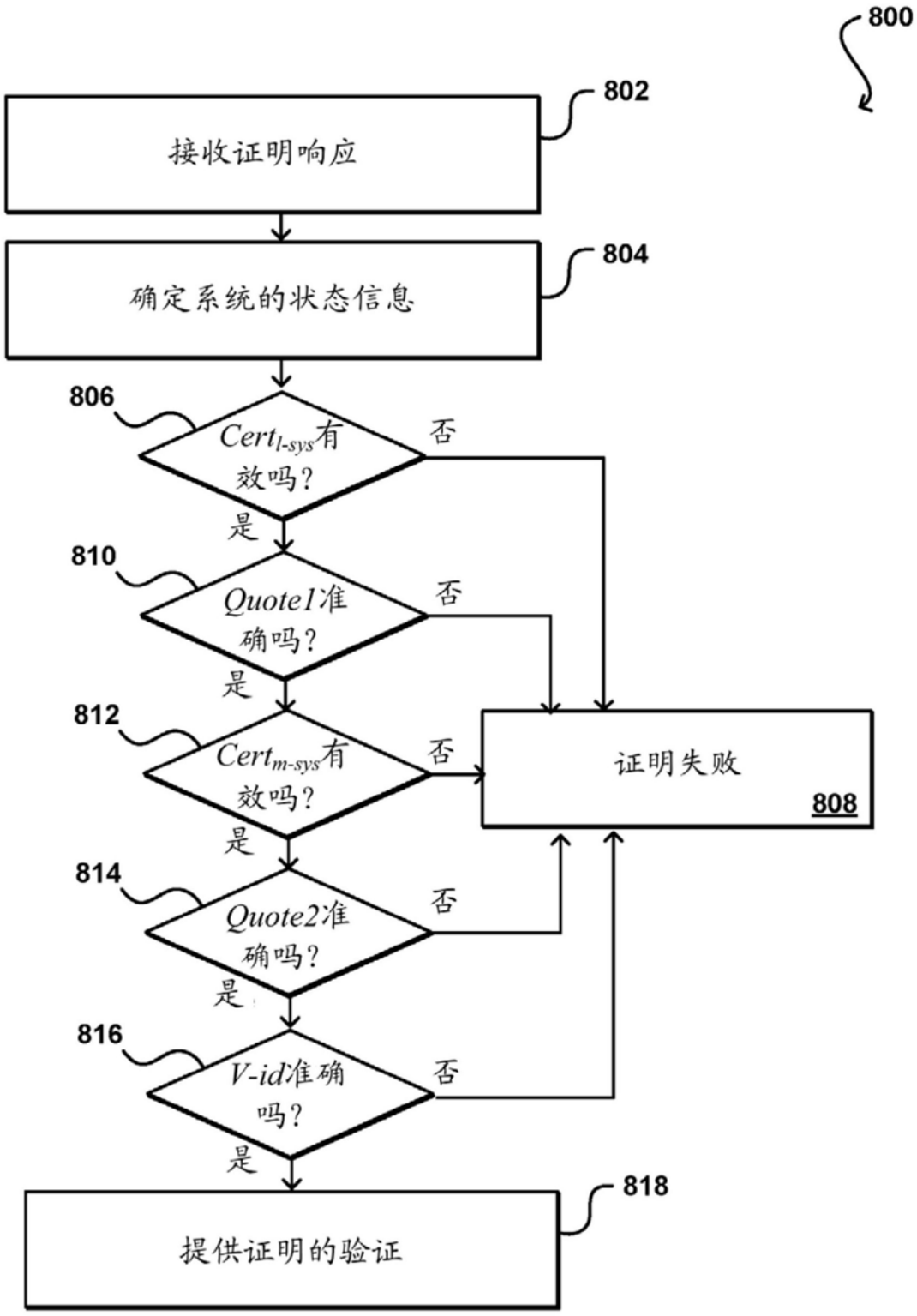

800
802
接收证明响应
804
确定系统的状态信息
806
$Cert_{l\text{-}sys}$有效吗?
否
是
810
Quote1准确吗?
否
是
812
$Cert_{m\text{-}sys}$有效吗?
否
是
证明失败
808
814
Quote2准确吗?
否
是
816
V-id准确吗?
否
是
818
提供证明的验证

图8

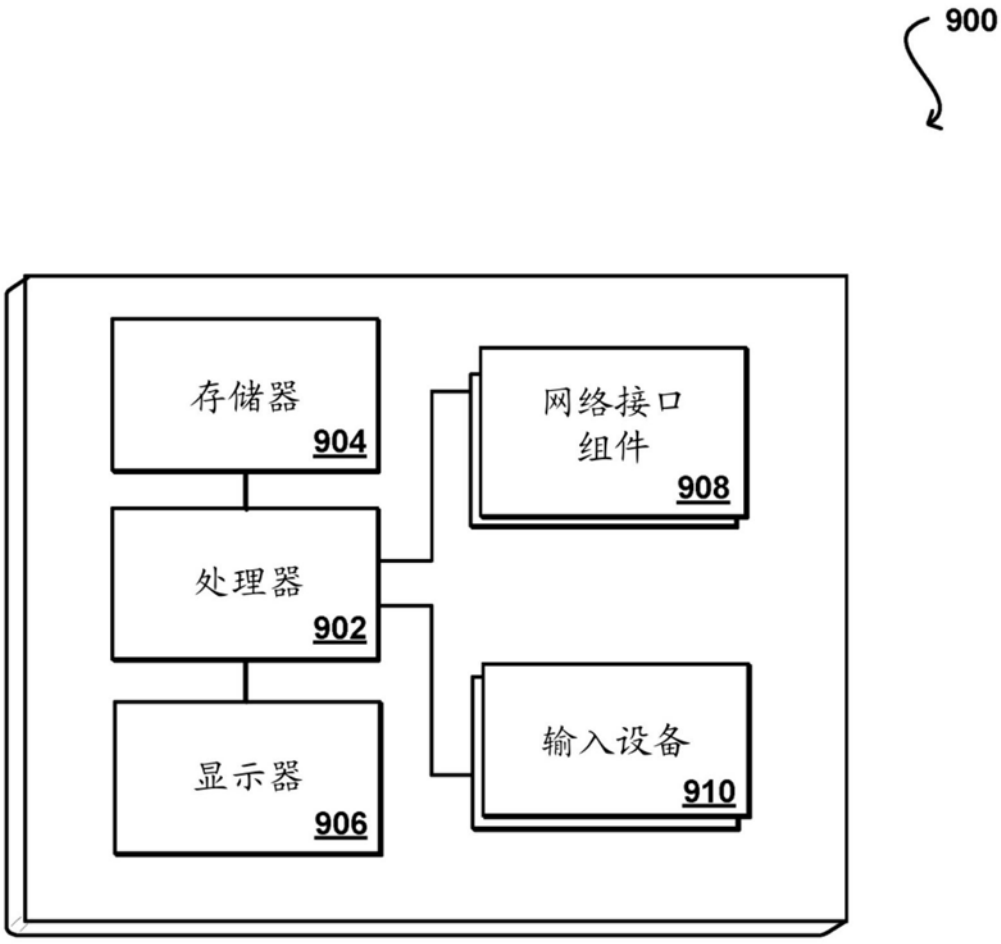


图9