(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 1997955 B
(45)授权公告日 2011.07.13

(21)申请号 200580020738.3
(22)申请日 2005.06.03
(30)优先权数据
10/876,994 2004.06.24 US
(85)PCT申请进入国家阶段日
2006.12.22
(86)PCT申请的申请数据
PCT/US2005/019724 2005.06.03
(87)PCT申请的公布数据
WO2006/011943 EN 2006.02.02
(73)专利权人 英特尔公司
地址 美国加利福尼亚州
(72)发明人 V·斯卡拉塔 C·罗扎斯
(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 陈斌
(51)Int.Cl.
G06F 1/00(2006.01)

(56)对比文件
同上.
同上.
同上.
US 20030163711 A1,2003.08.28, 说明书第2,29-30,39段.
US 20030226031 A1,2003.12.04, 说明书第45-46,49,53,62,69,78,81,99,101-103,105,107,110,114-115段、图2,8.

审查员 杨洁

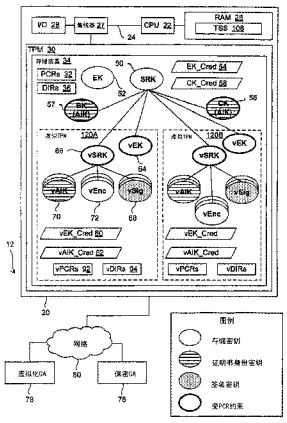
权利要求书 3 页 说明书 11 页 附图 4 页

(54)发明名称

提供可信平台模块的安全虚拟化的方法和装置

(57)摘要

一种方法和相关装置提供一虚拟可信平台模块(TPM)。在一个示例实施例中,虚拟TPM服务创建一在含有物理TPM的处理系统内使用的虚拟TPM。该虚拟TPM服务可以存储用于物理TPM内的虚拟TPM的密钥。该虚拟TPM服务随后可以使用虚拟TPM以提供仿真的物理TPM特征。在一个实施例中,该虚拟TPM服务可以在处理系统中使用虚拟TPM来仿真用于虚拟机的物理TPM。对其他实施例也进行了描述和声明。



CN 1997955 B

1. 一种用于创建可信的虚拟可信平台模块的方法，包括：

创建在包含物理可信平台模块的处理系统中的虚拟机所使用的虚拟可信平台模块；

生成用于所述虚拟可信平台模块的虚拟保证密钥，其中所述虚拟保证密钥至少部分基于所述物理可信平台模块的保证密钥，并且所述虚拟保证密钥被绑定到用于所述虚拟机的环境；

生成用于所述虚拟可信平台模块的虚拟存储根密钥；

在所述物理可信平台模块内存储所述虚拟保证密钥和所述虚拟存储根密钥中的至少一个；

使用用于证实密钥的凭证以及由所述证实密钥签署的用于虚拟保证密钥的认证信息从虚拟化认证授权机构获取用于所述虚拟保证密钥的经签署的保证凭证；

生成用于所述虚拟可信平台模块的虚拟证明书身份密钥；

使用所述虚拟证明书身份密钥以及用于所述虚拟保证密钥的经签署的保证凭证从保密认证授权机构获取用于所述虚拟证明书身份密钥的身份凭证；

在所述虚拟可信平台模块的存储器空间中创建用于所述虚拟可信平台模块的虚拟平台配置寄存器；

使用所述虚拟可信平台模块来提供用于所述虚拟机的仿真的物理可信平台模块特征；

其中使用所述虚拟可信平台模块来提供用于所述虚拟机的仿真的物理可信平台模块特征的操作包括使用所述虚拟可信平台模块来仿真用于虚拟机的物理可信平台模块；以及

其中使用所述虚拟可信平台模块来提供用于所述虚拟机的仿真的物理可信平台模块特征的操作包括：使用来自所述虚拟可信平台模块的存储器空间的所述虚拟平台配置寄存器来仿真标准的平台配置寄存器操作。

2. 如权利要求 1 所述的方法，其特征在于，所述虚拟可信平台模块包括第一虚拟可信平台模块，而所述虚拟机包括第一虚拟机，所述方法还包括：

在所述处理系统中创建第二虚拟可信平台模块，所述虚拟机还包括第二虚拟机；

在所述物理可信平台模块内存储用于所述第二虚拟可信平台模块的密钥；

使用所述第二虚拟可信平台模块仿真用于所述第二虚拟机的物理可信平台模块。

3. 如权利要求 1 所述的方法，其特征在于，使用所述虚拟可信平台模块以提供仿真的物理可信平台模块特征的操作包括：

从保密认证授权机构中获取用于与虚拟机相关联的虚拟证明书身份密钥的身份凭证；以及

将所述身份凭证发送给质询器。

4. 如权利要求 1 所述的方法，其特征在于：

所述虚拟化认证授权机构提供用于所述虚拟保证密钥的保证凭证，并能够区分经批准的虚拟可信平台模块环境与未经批准的虚拟可信平台模块环境；以及

当所述虚拟保证密钥被绑定到经批准的虚拟可信平台模块环境时，所述保密认证授权机构信赖所述虚拟化认证授权机构，所述虚拟化认证授权机构提供用于虚拟保证密钥的保证凭证。

5. 一种用于提供可信平台模块的安全虚拟化的方法，包括：

创建在包含物理可信平台模块的处理系统中的虚拟机所使用的虚拟可信平台模块；

由虚拟机生成用于处理系统中的虚拟机的虚拟保证密钥，所述虚拟保证密钥至少部分基于所述处理系统内用于物理可信平台模块的保证密钥；

在所述物理可信平台模块中存储所述虚拟保证密钥；

使用用于证实密钥的凭证以及由所述证实密钥签署的用于虚拟保证密钥的认证信息从虚拟化认证授权机构获取用于所述虚拟保证密钥的经签署的保证凭证；

由虚拟机生成用于所述虚拟机的虚拟证明书身份密钥；以及

使用所述虚拟证明书身份密钥以及用于所述虚拟保证密钥的经签署的保证凭证从保密认证授权机构来获取用于所述虚拟证明书身份密钥的身份凭证。

6. 一种用于提供可信平台模块的安全虚拟化的装置，包括：

用于创建在包含物理可信平台模块的处理系统中的虚拟机所使用的虚拟可信平台模块的装置；

用于生成用于所述虚拟可信平台模块的虚拟保证密钥的装置，其中所述虚拟保证密钥至少部分基于所述物理可信平台模块的保证密钥，并且所述虚拟保证密钥被绑定到用于所述虚拟机的环境；

用于生成用于所述虚拟可信平台模块的虚拟存储根密钥的装置；

用于在所述物理可信平台模块内存储所述虚拟保证密钥和所述虚拟存储根密钥中的至少一个的装置；

用于使用用于证实密钥的凭证以及由所述证实密钥签署的用于虚拟保证密钥的认证信息从虚拟化认证授权机构获取用于所述虚拟保证密钥的经签署的保证凭证的装置；

用于生成用于所述虚拟可信平台模块的虚拟证明书身份密钥的装置；

用于使用所述虚拟证明书身份密钥以及用于所述虚拟保证密钥的经签署的保证凭证从保密认证授权机构获取用于所述虚拟证明书身份密钥的身份凭证的装置；

用于在所述虚拟可信平台模块的存储器空间中创建用于所述虚拟可信平台模块的虚拟平台配置寄存器的装置；

用于使用所述虚拟可信平台模块来提供用于所述虚拟机的仿真的物理可信平台模块特征的装置；

其中用于使用所述虚拟可信平台模块来提供用于所述虚拟机的仿真的物理可信平台模块特征的装置使用所述虚拟可信平台模块来仿真用于虚拟机的物理可信平台模块；以及

其中用于使用所述虚拟可信平台模块来提供用于所述虚拟机的仿真的物理可信平台模块特征的装置使用来自所述虚拟可信平台模块的存储器空间的所述虚拟平台配置寄存器来仿真标准的平台配置寄存器操作。

7. 如权利要求 6 所述的装置，其特征在于，所述虚拟可信平台模块包括第一虚拟可信平台模块，而所述虚拟机包括第一虚拟机，并且所述装置还包括：

用于在所述处理系统中创建第二虚拟可信平台模块的装置，所述虚拟机还包括第二虚拟机；

用于在所述物理可信平台模块内存储用于所述第二虚拟可信平台模块的密钥的装置；

用于使用所述第二虚拟可信平台模块仿真用于所述第二虚拟机的物理可信平台模块

的装置。

8. 一种用于提供可信平台模块的安全虚拟化的处理系统，包括：

处理器，执行虚拟机，并执行虚拟可信平台模块服务以生成用于所述虚拟机的虚拟证明书身份密钥；

物理可信平台模块，与所述处理器通信耦合，用于存储保证密钥；

其中所述虚拟可信平台模块服务使用所述物理可信平台模块来创建用于所述虚拟机的虚拟可信平台模块，所述虚拟可信平台模块用于基于存储在所述物理可信平台模块内的所述保证密钥来生成与所述虚拟机相关联的虚拟保证密钥；以及

其中所述处理器与一虚拟化认证授权机构通信，所述虚拟化认证授权机构使用用于证实密钥的凭证以及由所述证实密钥签署的用于虚拟保证密钥的认证信息来生成用于所述虚拟保证密钥的经签署的保证凭证；

其中所述处理器与一保密认证授权机构通信，所述保密认证授权机构使用所述虚拟证明书身份密钥以及用于所述虚拟保证密钥的经签署的保证凭证来生成用于所述虚拟证明书身份密钥的身份凭证。

9. 一种用于提供可信平台模块的安全虚拟化的处理系统，包括：

用于创建在包含物理可信平台模块的处理系统中的虚拟机所使用的虚拟可信平台模块的装置；

用于由虚拟机生成用于处理系统中的虚拟机的虚拟保证密钥的装置，其中所述虚拟保证密钥至少部分基于所述处理系统内用于物理可信平台模块的保证密钥；

用于在所述物理可信平台模块内存储所述虚拟保证密钥的装置；

用于使用用于证实密钥的凭证以及由所述证实密钥签署的用于虚拟保证密钥的认证信息从虚拟化认证授权机构获取用于所述虚拟保证密钥的经签署的保证凭证的装置；

用于由虚拟机生成用于所述虚拟机的虚拟证明书身份密钥的装置；

用于使用所述虚拟证明书身份密钥以及用于所述虚拟保证密钥的经签署的保证凭证从保密认证授权机构获取用于所述虚拟证明书身份密钥的身份凭证的装置。

10. 一种用于提供可信平台模块的安全虚拟化的装置，包括：

物理可信平台模块，用于存储保证密钥；以及

其中一虚拟可信平台模块服务使用所述物理可信平台模块来创建用于一虚拟机的虚拟可信平台模块，所述虚拟可信平台模块，用于为虚拟机生成虚拟保证密钥，所述虚拟保证密钥至少部分基于所述保证密钥，并且使用用于证实密钥的凭证以及由所述证实密钥签署的用于虚拟保证密钥的认证信息从虚拟化认证授权机构获取用于所述虚拟保证密钥的经签署的保证凭证，生成用于所述虚拟机的虚拟证明书身份密钥，并且使用所述虚拟证明书身份密钥以及用于所述虚拟保证密钥的经签署的保证凭证从保密认证授权机构获取用于所述虚拟证明书身份密钥的身份凭证。

11. 如权利要求 10 所述的装置，其特征在于，所述虚拟保证密钥被存储在所述物理可信平台模块中。

提供可信平台模块的安全虚拟化的方法和装置

技术领域

[0001] 本公开一般涉及数据处理领域，尤其涉及用于提供可信平台模块的安全虚拟化的方法和装置。

背景技术

[0002] 传统的处理系统可以包括硬件资源，诸如中央处理单元 (CPU) 和随机存取存储器 (RAM)，以及软件资源，诸如操作系统 (OS) 和一个或多个最终用户程序或应用程序。应用程序通常被开发成只能在某一特定的 OS 上运行。当启动一典型的传统计算系统时，该系统在装载最终用户程序或应用程序之前载入 OS。OS 在一处理系统中通常用作软件应用程序和硬件之间的中介。

[0003] 除了 RAM 和一个或多个 CPU 之外，处理系统还可以包括可信平台模块 (TPM)。TPM 是位于处理系统内的硬件组件，并提供了用于增强处理系统的安全性的各种机制和服务。例如，TPM 可用于保护数据并证明一平台的配置。TPM 的子组件可以包括执行引擎和安全非易失性 (NV) 存储器或存储。安全 NV 存储器可用于存储诸如密钥之类的敏感信息，而执行引擎则根据将由 TPM 实现的安全策略来保护这些敏感信息。

[0004] TPM 可以依照含有诸如设计原则、TPM 结构和 TPM 命令等部分的规范，诸如于 2003 年 10 月 2 日发布的 Trusted Computing Group(可信计算小组，TCG)TPMSpecification(TPM 规范)1.2 版 (下称“TPM 规范”) 来实现。该 TPM 规范由 TCG 公布并可从网址 www.trustedcomputinqqroup.org/home 处获取。

[0005] 一般而言，遵从 TCG 的 TPM 基于平台特性提供诸如证明身份和 / 或平台完整性等安全服务。TPM 通常考虑的平台特性包括平台的硬件组件，诸如处理器和芯片组，以及位于平台内的软件，诸如固件和 OS。TPM 还可以支持软件进程的审查和日志记录，平台引导完整性、文件完整性的验证，以及软件许可。因此就可认为 TPM 提供针对平台的信任根。因此，第三方可以实现需要请求系统提供基于 TPM 的平台证明书的安全策略。例如，第三方可以将服务器配置成拒绝客户机的请求，除非这些请求附有来自客户机系统的基于 TPM 的有效平台证明书。

[0006] 但是，当传统处理系统使用 TPM 时，该处理系统一次仅能支持一个软件环境。

[0007] 最近，Intel 公司开始研发用于在单个处理系统内提供多个独立的软件环境的技术。例如，由 Intel 公司研发的技术包含以允许多个 OS 在同一机器上并发执行的方式划分并管理处理系统的硬件资源的特征，其中每个 OS 实质上都能像在自己的独立物理机器上那样运行。在这一处理系统中，每个 OS 都在实质上独立的软件环境中运行。这些独立的环境被称为分区或虚拟机 (VM)。

发明内容

[0008] 本发明的一个方面提供了一种用于创建可信的虚拟可信平台模块的方法，包括：创建在包含物理可信平台模块的处理系统中的虚拟机所使用的虚拟可信平台模块；生成用

于所述虚拟可信平台模块的虚拟保证密钥，其中所述虚拟保证密钥至少部分基于所述物理可信平台模块的保证密钥，并且所述虚拟保证密钥被绑定到用于所述虚拟机的环境；生成用于所述虚拟可信平台模块的虚拟存储根密钥；在所述物理可信平台模块内存储所述虚拟保证密钥和所述虚拟存储根密钥中的至少一个；使用用于证实密钥的凭证以及由所述证实密钥签署的用于虚拟保证密钥的认证信息从虚拟化认证授权机构获取用于所述虚拟保证密钥的经签署的保证凭证；生成用于所述虚拟可信平台模块的虚拟证明书身份密钥；使用所述虚拟证明书身份密钥以及用于所述虚拟保证密钥的经签署的保证凭证从保密认证授权机构获取用于所述虚拟证明书身份密钥的身份凭证；在所述虚拟可信平台模块的存储器空间中创建用于所述虚拟可信平台模块的虚拟平台配置寄存器；使用所述虚拟可信平台模块来提供用于所述虚拟机的仿真的物理可信平台模块特征；其中使用所述虚拟可信平台模块来提供用于所述虚拟机的仿真的物理可信平台模块特征的操作包括使用所述虚拟可信平台模块来仿真用于虚拟机的物理可信平台模块；以及其中使用所述虚拟可信平台模块来提供用于所述虚拟机的仿真的物理可信平台模块特征的操作包括：使用来自所述虚拟可信平台模块的存储器空间的所述虚拟平台配置寄存器来仿真标准的平台配置寄存器操作。

[0009] 本发明的另一个方面提供了一种用于提供可信平台模块的安全虚拟化的方法，包括：创建在包含物理可信平台模块的处理系统中的虚拟机所使用的虚拟可信平台模块；由虚拟机生成用于处理系统中的虚拟机的虚拟保证密钥，所述虚拟保证密钥至少部分基于所述处理系统内用于物理可信平台模块的保证密钥；在所述物理可信平台模块中存储所述虚拟保证密钥；使用用于证实密钥的凭证以及由所述证实密钥签署的用于虚拟保证密钥的认证信息从虚拟化认证授权机构获取用于所述虚拟保证密钥的经签署的保证凭证；由虚拟机生成用于所述虚拟机的虚拟证明书身份密钥；以及使用所述虚拟证明书身份密钥以及用于所述虚拟保证密钥的经签署的保证凭证从保密认证授权机构来获取用于所述虚拟证明书身份密钥的身份凭证。

[0010] 本发明的另一个方面提供了一种用于提供可信平台模块的安全虚拟化的装置，包括：用于创建在包含物理可信平台模块的处理系统中的虚拟机所使用的虚拟可信平台模块的装置；用于生成用于所述虚拟可信平台模块的虚拟保证密钥的装置，其中所述虚拟保证密钥至少部分基于所述物理可信平台模块的保证密钥，并且所述虚拟保证密钥被绑定到用于所述虚拟机的环境；用于生成用于所述虚拟可信平台模块的虚拟存储根密钥的装置；用于在所述物理可信平台模块内存储所述虚拟保证密钥和所述虚拟存储根密钥中的至少一个的装置；用于使用用于证实密钥的凭证以及由所述证实密钥签署的用于虚拟保证密钥的认证信息从虚拟化认证授权机构获取用于所述虚拟保证密钥的经签署的保证凭证的装置；用于生成用于所述虚拟可信平台模块的虚拟证明书身份密钥的装置；用于使用所述虚拟证明书身份密钥以及用于所述虚拟保证密钥的经签署的保证凭证从保密认证授权机构获取用于所述虚拟证明书身份密钥的身份凭证的装置；用于在所述虚拟可信平台模块的存储器空间中创建用于所述虚拟可信平台模块的虚拟平台配置寄存器的装置；用于使用所述虚拟可信平台模块来提供用于所述虚拟机的仿真的物理可信平台模块特征的装置；其中用于使用所述虚拟可信平台模块来提供用于所述虚拟机的仿真的物理可信平台模块特征的装置使用所述虚拟可信平台模块来仿真用于虚拟机的物理可信平台模块；以及其中用于使用所述虚拟可信平台模块来提供用于所述虚拟机的仿真的物理可信平台模块特征的装置使用

来自所述虚拟可信平台模块的存储器空间的所述虚拟平台配置寄存器来仿真标准的平台配置寄存器操作。

[0011] 本发明的还有一个方面提供了一种用于提供可信平台模块的安全虚拟化的处理系统，包括：处理器，执行虚拟机，并执行虚拟可信平台模块服务以生成用于所述虚拟机的虚拟证明书身份密钥；物理可信平台模块，与所述处理器通信耦合，用于存储保证密钥；其中所述虚拟可信平台模块服务使用所述物理可信平台模块来创建用于所述虚拟机的虚拟可信平台模块，所述虚拟可信平台模块用于基于存储在所述物理可信平台模块内的所述保证密钥来生成与所述虚拟机相关联的虚拟保证密钥；以及其中所述处理器与一虚拟化认证授权机构通信，所述虚拟化认证授权机构使用用于证实密钥的凭证以及由所述证实密钥签署的用于虚拟保证密钥的认证信息来生成用于所述虚拟保证密钥的经签署的保证凭证；其中所述处理器与一保密认证授权机构通信，所述保密认证授权机构使用所述虚拟证明书身份密钥以及用于所述虚拟保证密钥的经签署的保证凭证来生成用于所述虚拟证明书身份密钥的身份凭证。

[0012] 本发明的还有一个方面提供了一种用于提供可信平台模块的安全虚拟化的处理系统，包括：用于创建在包含物理可信平台模块的处理系统中的虚拟机所使用的虚拟可信平台模块的装置；用于由虚拟机生成用于处理系统中的虚拟机的虚拟保证密钥的装置，其中所述虚拟保证密钥至少部分基于所述处理系统内用于物理可信平台模块的保证密钥；用于在所述物理可信平台模块内存储所述虚拟保证密钥的装置；用于使用用于证实密钥的凭证以及由所述证实密钥签署的用于虚拟保证密钥的认证信息从虚拟化认证授权机构获取用于所述虚拟保证密钥的经签署的保证凭证的装置；用于由虚拟机生成用于所述虚拟机的虚拟证明书身份密钥的装置；用于使用所述虚拟证明书身份密钥以及用于所述虚拟保证密钥的经签署的保证凭证从保密认证授权机构获取用于所述虚拟证明书身份密钥的身份凭证的装置。

[0013] 本发明的还有一个方面提供了一种用于提供可信平台模块的安全虚拟化的装置，包括：物理可信平台模块，用于存储保证密钥；其中一虚拟可信平台模块服务使用所述物理可信平台模块来创建用于一虚拟机的虚拟可信平台模块，所述虚拟可信平台模块用于为虚拟机生成虚拟保证密钥，所述虚拟保证密钥至少部分基于所述保证密钥，并且使用用于证实密钥的凭证以及由所述证实密钥签署的用于虚拟保证密钥的认证信息从虚拟化认证授权机构获取用于所述虚拟保证密钥的经签署的保证凭证，生成用于所述虚拟机的虚拟证明书身份密钥，并且使用所述虚拟证明书身份密钥以及用于所述虚拟保证密钥的经签署的保证凭证从保密认证授权机构获取用于所述虚拟证明书身份密钥的身份凭证。

附图说明

[0014] 本发明的特征和优点从所附权利要求书、以下对一个或多个示例实施例的详细描述以及相应的附图中将变得显而易见，附图中：

[0015] 图 1 是描绘了在其中可以实现本发明一个示例实施例的某些方面的合适数据处理环境的框图；

[0016] 图 2 是描绘了根据本发明一个示例实施例的合适虚拟机体系结构的框图；

[0017] 图 3 是示出根据本发明一个示例实施例的用于提供虚拟 TPM 的过程的流程图；以

及

[0018] 图 4 是示出根据本发明一个示例实施例的用于利用虚拟 TPM 的过程的流程图。

具体实施方式

[0019] 虚拟 TPM(vTPM) 是提供类似 TPM 功能的逻辑设备。本公开描述了用于提供虚拟 TPM 的系统、方法和装置的一个或多个示例实施例。

[0020] 图 1 是描绘了在其中可以实现本发明一个示例实施例的某些方面的合适数据处理环境 12 的框图。数据处理环境 12 包括处理系统 20，处理系统 20 包括经由一个或多个系统总线 24 或其他通信路径或介质与各种其他组件通信耦合的一个或多个处理器和中央处理单元 (CPU)22。

[0021] 在此使用的术语“处理系统”和“数据处理系统”旨在广泛地包含单个机器，或者共同操作的通信上耦合的机器或设备的系统。示例性处理系统包括但不限于 ：分布式计算系统、超级计算机、高性能计算系统、计算机集群、大型计算机、小型计算机、客户机—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、图形输入板、电话机、个人数字助理 (PDA)、手持式设备、诸如音频和 / 或视频设备等娱乐设备、以及用于处理或传输信息的其他设备。

[0022] 处理系统 20 可至少部分地通过来自诸如键盘、鼠标等的常规输入设备的输入，和 / 或通过接收自另一台机器的指示、与虚拟现实 (VR) 环境的交互、生物测定反馈、或其他输入源或信号来控制。处理系统 20 可以利用诸如通过网络控制器、调制解调器或其他的通信耦合与一个或多个远程数据处理系统，例如保密认证授权机构 (CA)76、虚拟化认证授权机构 (CA)78 的一个或多个连接。处理系统可以通过诸如局域网 (LAN)、广域网 (WAN)、内联网、因特网之类的物理和 / 或逻辑网络 80 的方式互连。涉及网络 80 的通信可以利用各种有线和 / 或无线近程或远程载体和协议，包括射频 (RF)、卫星、微波、电气和电子工程师协会 (IEEE)802.11、蓝牙、光学、红外线、电缆、激光等等。

[0023] 在处理系统 20 中，CPU 22 可以通信耦合至一个或多个易失性或非易失性数据存储设备，诸如随机存取存储器 (RAM)26、只读存储器 (ROM)、诸如集成驱动器电子电路 (IDE) 硬盘驱动器等大容量存储设备、和 / 或诸如软盘、光学存储、磁带、闪存、记忆棒、数字视频盘、生物学存储等的其他设备或介质。为了本发明的目的，术语“ROM”通常用于指代诸如可擦除可编程 ROM(EPROM)、电可擦除可编程 ROM(EEPROM)、闪速 ROM、闪存等的非易失性存储器设备。CPU22 还可以通信耦合至其它组件，诸如视频控制器、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、诸如键盘和鼠标等输入设备等等。处理系统 20 还可以包括用于与各种系统组件通信耦合的一个或多个桥接器或集线器 27，诸如存储器控制器集线器、输入 / 输出 (I/O) 控制器集线器、PCI 根桥接器等等。

[0024] 诸如网络控制器等某些组件可以被实现为用来与 PCI 总线通信的带接口适配器卡，诸如 PCI 连接器。在一个实施例中，一个或多个设备可以被实现为使用诸如可编程或不可编程逻辑器件或阵列、专用集成电路 (ASIC)、嵌入式计算机、智能卡等等的嵌入式控制器。

[0025] 如图所示，处理系统 20 还包括通信耦合至 CPU 22 的 TPM 30。TPM 30 也可被称为物理 TPM 或硬件 TPM(hwTPM)30。在一个实施例中，TPM 30 被实现为位于处理系统 20 的

系统主板或底板上的嵌入式设备。TPM 30 包括若干存储机制，包括易失性平台配置寄存器(PCR)32 和授权会话，以及持久数据完整性寄存器 (DIR)36、授权摘要以及通用持久存储。这些机制的每一种都可具有相应的存储器内数据结构。

[0026] 本发明可以参考或结合包括指令、函数、过程、数据结构、应用程序等在内的相关联数据来描述，当这些数据被机器访问时，会使该机器执行任务或定义抽象数据类型或低级硬件上下文。该数据可以被存储在易失性和 / 或非易失性数据存储中。

[0027] 例如，RAM 26 可以包括用于提供 TPM 的安全虚拟化的一个或多个指令集。在该示例实施例中，这些指令可以实现部分或全部位于虚拟机监控程序 (VMM)106(参见图 2) 内的虚拟 TPM 服务 104。处理系统 20 可以在引导时将 VMM 106 载入 RAM 26 中以支持处理系统 20 内的一个或多个虚拟机。处理系统 20 例如可以从 ROM 和 / 或从一个或多个本地或远程大容量存储设备中载入实现 VMM 106 的指令。如果有任何附加的指令用于支持 TPM 的安全虚拟化，那么这些指令也从例如 ROM 和 / 或从一个或多个本地或远程大容量存储设备中载入。

[0028] 图 2 是描绘了涉及处理系统 20 内的 VMM 106 的一个示例虚拟机体系结构的框图。在最底层的是 TPM 30 以及其他硬件组件，诸如处理器 24、集线器 27 等 (共同被标识为处理器和芯片组 23)。在操作中，处理系统 20 还包括通过诸如微内核 100 和服务 OS 102 之类的软件或固件组件的执行而实现的 VMM 106。微内核 100 可以包括用于诸如指令调度等系统管理任务的小型指令核心程序。服务 OS 102 可以包括用于创建和维护虚拟机的设备驱动程序和环境虚拟化软件。

[0029] 在该示例实施例中，VMM 106 还包括用于创建和维护 vTPM 的虚拟 TPM 服务 104。虚拟 TPM 服务 104 还可以为虚拟机提供对各自的 vTPM 的访问。虽然诸如虚拟 TPM 服务 104 之类的软件模块在该典型实施例中位于 VMM 106 之内，但是这些模块在替换实施例中可以位于固件或任何其他受保护的环境内。

[0030] 可以为各种各样的 VMM 体系结构提供虚拟 TPM 服务。在某些实施例中，无需将虚拟 TPM 服务嵌入到 VMM 中。此外，在某些实施例中，虚拟 TPM 服务可以根本无需是 VMM 的一部分。

[0031] 在该示例实施例中，虚拟 TPM 服务 104 位于受保护的主机存储器内。例如，处理系统 20 可以使用诸如在美国专利第 6,507,904 号、第 6,633,963 号以及第 6,678,825 号中描述的技术将虚拟 TPM 服务 104 从受硬件保护的存储器的孤立区中载入并执行 TPM 服务 104。在该示例实施例中，受保护的存储器可以确保软件 / 指令在不受干扰或观察的情况下运行。在替换实施例中，可以使用其他技术来提供受保护的存储器。例如，一种环境可以包括提供受保护的存储器的系统管理模式 (SMM)，或者可以使用防篡改软件编译器来创建受保护的执行环境。其他组件 (例如，VMM 106、微内核 100、虚拟 TPM 120A 和 120B 等等) 也可以位于受保护的存储器内。

[0032] 在该示例实施例中，VMM 106 支持多个虚拟机 110A 和 110B，它们都运行它们自己的独立客 OS 以及它们自己的独立可信软件栈或 TCG 软件栈 (TSS)108A、108B 上。在该示例实施例中，TSS 108A 和 108B 符合 TCG 标准。

[0033] 如下将更详细地描述的，虚拟 TPM 服务 104 可以使用 TPM 30 来提供分别用于虚拟机 110A 和 110B 的不同的虚拟 TPM 120A 和 120B。

[0034] 图 2 中的粗箭头表示虚拟化事件 (VE)。例如，左上箭头表示涉及从 VM 110A 至服务 OS 102 的控制转移的 VE。右上箭头表示当 VM 110A 试图访问 TPM 时所触发的 VE。如图所示，虚拟 TPM 服务 104 截取该 VE，以便如最下箭头所示地通过参考 vTPM 120A 来处理该事件。在该示例实施例中，虽然 VM 110A 除了 vTPM120A 之外不知道任何 TPM，但是虚拟 TPM 服务 104 可以使用 hwTPM 30 来支持 vTPM 120A。

[0035] 在该示例实施例中，每个 vTPM 都有其自己的 TPM 结构，包括保证密钥 (EK)、存储根密钥 (SRK)、保证凭证 (EK 凭证)、用户密钥层级、平台配置寄存器 (PCR)、单调计数器、内部持久存储、数据完整性寄存器 (DIR) 等等。再次参见图 1，如右下角的图例所示，存储密钥被示为空心椭圆，证明书身份密钥 (AIK) 被示为内部填充水平线的椭圆、签署密钥被示为内部填充点图案的椭圆。此外，粗线椭圆表示被绑定到 TPM 30 的 PCR 32 的密钥。各密钥之间的线指示各密钥之间的父 / 子关系。例如，这些线指示 SRK 50 是 TPM 30 内某些硬件密钥以及每个 vTPM 内某些虚拟密钥的父密钥。各凭证由平行四边形表示。

[0036] vTPM 内的虚拟密钥以及其他结构或对象可以具有与硬件 TPM 密钥或对象相同的结构，但是虚拟 TPM 内的虚拟对象并不仅仅参考 TPM 30 内诸如 EK 52、SRK50 和 PCR 32 等标准对象。而是将如以下详述的那样，每个虚拟 TPM 获取其自己的不同对象，诸如虚拟 EK(vEK)64、虚拟 SRK(vSRK)66、虚拟 PCR(vPCR)92、以及虚拟 DIR(vDIR)94。这些虚拟对象是以硬件 TPM 的对象为基础或从中导出的。例如，在该示例实施例中，虚拟 SRK 和虚拟 EK 是硬件 SRK 的子密钥，或者在嵌套 vTPM 的情况下，虚拟 SRK 最终以硬件 SRK 为基础。通过允许 vTPM 密钥作为 vSRK 中的根，该模型就允许 vTPM 嵌套。

[0037] 诸如 vEK 64、vSRK 66、和 vPCR 92 等虚拟 TPM 对象进而可以用作 vTPM 120A 内诸如虚拟签署密钥 (vSig)68、虚拟 AIK(vAIK)70、以及虚拟存储 / 加密密钥 (vEnc)72 等附加虚拟对象的基础。在该示例实施例中，每个 vTPM 都用相同的应用程序接口 (API) 提供由硬件 TPM(hwTPM) 提供的全部功能。例如，vTPM 120A 可以包括其自己的 vDIR 94、vPCR 92、vAIK 70 等等。因此，每个 VM 内的客 OS 都可能完全不知道相应的 vTPM 不是 hwTPM。于是，VM 可使用传统的 OS 码。此外，根据该示例实施例，带常规 hwTPM 的处理系统可被配置成提供 vTPM 而无需对 hwTPM 的任何修改。

[0038] 诸如 vPCR 92 等虚拟 PCR 没有 hwTPM 的资源约束，而是可能具有数目可配置的 PCR 供其使用。在该示例实施例中，vPCR 92 被存储在 vTPM 120A 的存储器空间内，而 vTPM 120A 则在 vPCR 92 上仿真标准 PCR 操作。

[0039] 在该示例实施例中，vTPM 120A 使用软件来提供模拟的、持久的单调计数器。计数器的数目基本不受限制。在该示例实施例中，vTPM 120A 至少提供 hwTPM 期望的四个计数器。这些 vTPM 计数器不要求与硬件 TPM 计数器的任何直接链接。

[0040] 虚拟机体系结构可以充分利用硬件 TPM 来保护虚拟密钥和相关数据。在一个实施例中，vTPM 密钥层级和相关数据可以在标准 hwTPM 内受到保护。例如，虚拟 TPM 可以被存储在硬件 TPM 中并且从不从中释放，除非该数据如下所述首先由 vTPM 120A 加密。因此，如果虚拟 TPM 被泄密，则相关联的 vTPM 密钥的公共部分则很可能遭受未经授权的使用，但也仅限于泄密期间。在该示例实施例中，所有的密钥都将保留在硬件 TPM 之内，因此一旦泄密终止就无法偷取或使用私钥。

[0041] 根据本发明的处理系统还可提供允许 vTPM 提供传统 TPM 证明书服务的证明书协

议体系结构。不知道虚拟 TPM 的远程质询器可以完全地参与到证明书进程中。此外，知道 vTPM 的远程质询器能在无需附加协议的情况下将 hwTPM 与 vTPM 进行区分，并在随后决定是否信任主存 vTPM 的平台。

[0042] 在该示例实施例中，当虚拟 TPM(vTPM) 不可操作时，用于该 vTPM 的持久数据结构被存储在磁盘上并用父 SRK 密封到 vTPM 服务的 PCR。于是，即使在 vTPM 未运行时，TPM 30 仍保护着 vTPM。

[0043] 在此示例实施例中，vTPM 120A 能够在单用户授权会话下透明地提供来自它本身和来自 hwTPM 双方的 TPM 功能。vTPM 120A 通过维护与用户和 hwTPM 双方的分开的授权会话来实现这一目标。即，用户将如同 vTPM 是 hwTPM 那样用 vTPM 120A 来创建授权会话。vTPM 120A 可以基于 hwTPM 会进行的这一会话来实现所有相同的授权检查。如果 vTPM 120A 可以直接提供所请求的功能，则 vTPM120A 就可以简单地更新会话现时值并做出回复。如果 vTPM 120A 需要硬件 TPM 提供该服务，则 vTPM 120A 将用该 hwTPM 创建授权会话或重新使用现有的授权会话来做出该请求。一旦 vTPM 120A 使用完 hwTPM，vTPM 120A 就可更新用户会话的现时值并做出回复。

[0044] 图 3 是示出了根据本发明一个实施例用于提供虚拟 TPM 的过程的流程图。图 3 的过程在处理系统 20 内激活了 TPM 30 之后开始，使得如同常规的 TPM 一样，TPM 30 包括如图 1 所示的 SRK 50、EK 52 以及诸如 EK 凭证 54 等标准凭证。在框 210 至 214 处，VMM 106 执行几个操作以初始化虚拟 TPM 服务 104 来为支持虚拟 TPM 做准备。例如，在框 210 处，VMM 106 创建被称为证实密钥 (CK)56 的 AIK。VMM 106 可以使用用于创建 AIK 的标准过程来创建 CK 56。虚拟 TPM 服务 104 随后可以在证实诸如 vEK64 等虚拟保证密钥时使用 CK 56。在框 412 处，虚拟 TPM 服务 104 从诸如保密认证授权机构 (CA)76 之类的第三方或可信第三方 (TTP) 获取针对 CK 56 的 CK 凭证 58。CK 凭证 58 由保密 CA 76 签署并且通过指示 CK 56 受到有效 TPM 的保护来担保 CK 56。

[0045] 在框 214 处，VMM 106 创建被称为绑定密钥 (BK)57 的 AIK。BK 57 在随后 vTPM 数据从 vTPM 服务 104 中释放时用于保护这些数据。例如，在该示例实施例中，vTPM 120A 用与 hwTPM 存储持久密钥和寄存器相类似的方式保存持久数据。然而，为保护释放的数据，vTPM 120A 将以下各项与 BK 57 绑定：由 vEK 64 包装的密钥块 (blob)、由 vSRK 66 包装的密钥块、用于 vEK 64 的授权数据、用于 vSRK 66 的授权数据、vDIR 94 以及用于装载的持久密钥的包装的密钥块。

[0046] 对于 vTPM 120A，用来实现局部性的总线控制器的逻辑等效物是 VMM 106。于是，vTPM 120A 将在 VMM 106 指示它操作的任何局部进行操作。若有需要，VMM 106 可以使用任何合适的技术来改变 vTPM 120A 的当前局部性。

[0047] 一旦 VMM 106 已经初始化了虚拟 TPM 服务 104，虚拟 TPM 服务 104 就能在需要时创建虚拟 TPM。

[0048] 在该示例实施例中，每个虚拟 TPM 一旦被初始化就能够操作并支持诸如证明书等传统功能，如同该虚拟 TPM 就是硬件 TPM 一样。为允许虚拟 TPM 以这一方式操作，向虚拟 TPM 提供硬件 TPM 期望拥有的相同种类的凭证。例如，如随后将详述的那样，在一个实施例中，虚拟 TPM 服务 104 针对每个新的 vTPM 创建或获取新的 vEK、新的虚拟 SRK(vSRK) 以及用于该 vEK 的凭证。这一 vEK 凭证指示该 vEK 是依据 TPM 规范安全存储的。此外，平台凭证

和一致性凭证可由虚拟 TPM 软件厂商提供。

[0049] 在该示例实施例中，框 216 至 222 表示用于为虚拟机初始化虚拟 TPM 的操作。例如，虚拟 TPM 服务 104 响应于创建虚拟机 110A 的请求，可如在框 216 处所示的使用 TPM 30 来创建被称为 vEK 64 的存储密钥。此外，虚拟 TPM 服务 104 可使用 TPM 30 将 vEK 64 绑定至用于虚拟 TPM 服务 104 和虚拟 TPM 服务 104 所在的引导环境的 PCR 值。还可以在 vTPM 120A 内创建并存储用于 vEK 64 的初始授权数据。

[0050] 在框 218 处，虚拟 TPM 服务 104 使用 CK 56 来证实 vEK 64。例如，虚拟 TPM 服务 104 可使用 TPM 30 的 TPM_CertifyKey 函数来证实 vEK 64 并为 vEK 64 获取诸如 TPM_CERTIFY_INFO 结构等认证信息。在该示例实施例中，用于 vEK 64 的这一认证信息由 CK 56 签署，并且包含 vEK 64 所绑定到的 PCR 信息（例如，用于 PCR 32 的信息）。该过程可以保证 vEK 64 被存储在经保密 CA 76 批准的硬件 TPM 中。在此示例实施例中，因为保密 CA 76 已签署了 CK 凭证 58，所以 CK 56 对 vEK 64 的 PCR 绑定的认证会受到信任，如同保密 CA 76 已经指示 vEK 64 处于依据 TCG 标准可认为良好的 hwTPM 中那样。

[0051] 在框 220 处，虚拟 TPM 服务 104 可以将 vTPM 的 EK 凭证请求发送给被称为虚拟化 CA 78 的第三方或 TTP。该凭证请求可以包括 CK 凭证 58 以及由 CK 56 签署的用于 vEK 64 的认证信息。

[0052] 虚拟化 CA 78 可以是受到保密 CA 信任的认证授权机构。通常可以将虚拟化 CA 78 示为 TPM 的另一个生产商。在该示例实施例中，虚拟化 CA 78 是知道 vTPM 的，并且能够将经批准的或“安全”的虚拟 TPM 环境与未经批准的或“不安全”的虚拟 TPM 环境区分。在一个实施例中，虚拟化 CA 78 是处理系统 20 外为进行有效的 TPM 虚拟化而必须知道 TPM 虚拟化的存在的唯一实体。

[0053] 在虚拟化 CA 78 评价了 CK 凭证 58 以及针对 vEK 64 的包括 PCR 绑定在内的认证信息之后，如果请求被批准，则虚拟化 CA 78 将经签署的 vEK 凭证返还给处理系统 20。在此示例实施例中，vEK 凭证 60 包括带有指示 vEK 64 与在可标识环境内运行的虚拟 TPM 相关联的数据的模型字段。在框 222 处，虚拟 TPM 服务 104 可接收经签署的 vEK 凭证 60。

[0054] 上述过程于是就可以建立下列信任链：CK 凭证 58 是由保密 CA 76 签署的凭证以指示 CK 56 是合法 TPM 内的合法 AIK。用于 vEK 64 的认证信息指示根据 CK56，vEK 64 是绑定到一组特定 PCR 并位于同一合法 TPM 内的密钥。因为保密 CA76 创建了 CK 凭证 58，所以虚拟化 CA 78 就信任由 CK 56 创建的用于 vEK 64 的认证信息。如果虚拟化 CA 78 批准了 EK 所绑定到的 vTPM 环境，则因而乐于产生用于 vEK 64 的保证凭证以指示 vEK 64 表示一个有效 TPM。此外，在 vEK 凭证 60 中，虚拟化 CA 78 可以包括指示该 TPM 是虚拟的并且在证明期间能被远程质询器自行信任的模型信息。

[0055] 框 224 至 226 表示用于初始化 vTPM 的附加操作。在一个实施例中，虚拟 TPM 服务 104 为执行这些操作，使用标准函数来初始化 vTPM 120A，如同 vTPM 120A 是 hwTPM 那样。例如，虚拟 TPM 服务 104 可以分别如框 224 和 226 处所描绘的那样，调用 TPM_Get_PUBEK 以获取 vEK 64 的公共部分，并且可以调用 TPM_TakeOwnership 以创建 vSRK 66。在该示例实施例中，虚拟 TPM 服务 104 将 vSRK 绑定到与 vEK 64 相同的 PCR（例如，PCR 32）上。虚拟 TPM 服务 104 能以用 vEK 64 的公共部分加密的形式为 vTPM 120A 提供授权。这些授权随后由 vTPM 120A 用 vEK 64 解密。在该示例实施例中，因为这些授权不是 TPM_BOUND_DATA，所以

使用传统的密钥 vEK 64 来解密这些授权。

[0056] 在该示例实施例中，用于 vEK 64 的授权数据从 vEK 64 创建期间被存储在 vTPM 120A 内的数据改为在 TPM_TakeOwnership 调用中提供的数据。

[0057] 如在框 228 处所述以及如下将参考图 4 详述的，VM 110A 随后使用 vTPM120A，如同 vTPM 120A 是 hwTPM 一样。如框 240 处所示，虚拟 TPM 服务 104 随后确定是否正在创建要求新 vTPM 的新 VM。如果是，则该过程返回到框 216，其中执行操作以用例如为该新 VM 创建的新 vEK 等来实例化上述新 vTPM。如果没有创建新的 VM，则虚拟 TPM 服务 104 可以继续使用 TPM 30 来为 VM 110A 提供 vTPM 120A。

[0058] 图 4 是示出利用诸如 vTPM 120A 之类的虚拟 TPM 的一过程的示例实施例的流程图。示出的过程提供了关于图 3 中框 228 处概括的某些操作的更多细节。例如，框 310 至 314 描述了用于为 VM 110A 创建 vAIK 的操作，其中 VM 110A 如同 vTPM120A 是 hwTPM 一样来使用 vTPM 120A。虚拟 vTPM 120A 可以在 TPM 30 中创建 vAIK 70，并且可以创建硬件 TPM 通常会为 AIK 创建的常规文档。

[0059] 例如，在框 310 处，VM 110A 通过调用 TPM MakeIdentity 在 vTPM 120A 内创建 vAIK。vTPM 120A 响应该调用，指示 TPM 30 在 TPM 30 内创建新的 TCG-SIGNING_KEY 密钥。这一将用作新的虚拟证明书身份密钥的签署密钥在图 1 中被描述为 vAIK 70。这样，从 hwTPM 的观点来看，虚拟 AIK 不是“AIK”类型的密钥，而可以是签署密钥。但在 hwTPM 外的其他地方，该虚拟 AIK 仍然用作并看似“AIK”类型的密钥。

[0060] 用于 vAIK 70 的 TCG_IDENTITY_CONTENTS 随后由 vTPM 120A 和 TSS108A 创建。TSS 108A 随后可以执行 TSS_CollateIdentityRequest 来创建 TCG_IDENTITY_REQ。除非使用的 EK 凭证是 vEK 凭证 60 而非针对 hwTPM 的 EK 凭证，否则就可以照常做出上述调用。

[0061] 如框 312 处所描述的那样，在 VM 110A 内运行的 TSS 108A 随后将包括诸如 vAIK 70 和 vEK 凭证 60 等文档在内的请求发送给保密 CA 76。保密 CA 76 随后检验这些文档。此外，保密 CA 76 可能不知道 TPM 的虚拟化，并且信任来自虚拟化 CA 78 的 vEK 保证凭证 60 就如同它是任何其他 TPM 厂商的凭证那样。在验证了这些文档之后，保密 CA 76 将为 vAIK 70 创建一新的身份凭证 62，签署该凭证，并将其发送到处理系统 20。因此，TSS 108A 可如框 314 中所示地接收来自保密 CA 76 的 vAIK 身份凭证 62。

[0062] 接着，框 320 至 324 描述用于处理证明书请求的操作。在框 320 处，vTPM 120A 确定接收到的命令是否要求关于 VM 110A 的可信赖性的证明书。当接收到这一请求时，TSS 108A 可以使用 vTPM 120A 来引证 vPCR 92，并且可以如框 322 处所示使用 vAIK 70 来签署 PCR 的引证。如框 324 处示出的那样，当 VM 110A 受到远程实体的质询时，TSS 108A 可以如同 vAIK 70 在 hwTPM 内一样将 vAIK 凭证 62 发送给该远程实体。

[0063] 根据一个实施例，如果质询器知道 vTPM，则它就能够考虑模型信息，发现由 VM 110A 使用的 TPM 是 vTPM，并且决定是否应该信任该底层平台。上述模型信息可以唯一地标识该底层平台配置。

[0064] 如果质询器信任该底层平台，质询器就会获知保密 CA 76 做出了如下声明：vTPM 是硬件 TPM 中的根，vTPM 仅在该硬件 TPM 中可用。如果质询器不信任该 vTPM 的这一特定配置，则质询器能够选择拒绝该事务。此外，如果质询器是不知道 vTPM 的传统应用程序，则质询器就能够仅仅基于对保密 CA 76 的签名的信任确定，使用标准 TPM 协议来推断证明书。

[0065] 用类似的方式，vTPM 120A 可以为 VM 提供常规硬件 TPM 能够为单片系统提供的全部其他功能。

[0066] 所公开的一个或多个实施例因而允许多个 VM 使用 TPM 功能，而无需多个专用硬件 TPM，无需修改 VM 内的软件，并且无需修改与目标系统交互的远程实体。根据本公开内容，虚拟 TPM 可以度量 VM 内的 OS 和应用程序以向远程实体提供证明书。此外，即使硬件 TPM 和质询器仅能利用在当前 TPM 规范（诸如，以上参考的 TPM1.2 版设计规范）中描述的功能，虚拟 TPM 仍可以为硬件 TPM 质询器证明虚拟机的状态。虚拟机内的客 OS 可以保持不知道硬件 TPM 被共享，并且在一系统内的 VM 之间不需要信任关系。

[0067] 如图 1 所示，可以为每个 vTPM 创建零个或更多的 vSig 68、零个或更多的 vAIK70 和零个或更多的 vEnc 72。如上所述，在一个实施例中，诸如 vSig 68 和 vEnc 72 之类的虚拟密钥可以被创建并存储在 hwTPM 中。因此，vTPM 能够以使对虚拟 TPM 的泄密无法永久性地泄密存储在 vTPM 内的密钥的方式存储并创建它的密钥。

[0068] 可选地，为增加灵活性和 / 或性能，虚拟密钥可由 vTPM 软件创建并使用。例如，这些虚拟密钥可以不由 hwTPM 储存或者直接保护。属于虚拟 TPM 或由其生成的私钥可以不由硬件 TPM 操作，因为该硬件 TPM 可以不使用这些私钥来执行密码操作。相反，虚拟 TPM 可以使用主机处理器和密码软件来以其私钥执行密码操作。为此，虚拟 TPM 服务可以在受保护的主机存储器内存储其私钥。尽管如此，虽然没有使用该私钥，但是虚拟 TPM 服务可以使用硬件 TPM 特征来将该密钥包装到其软件配置中。

[0069] 这些选项可以允许 vTPM 以比硬件 TPM 所提供的性能的更为优越的性能来对 vTPM 软件内的对象进行加密、解密、签署和验证。于是，这些选项对于例如批量加密或性能敏感服务器环境中的使用是首选。然而，为添加性能仍需权衡的是如果 vTPM 被泄密，则泄密密钥也会被永久地泄密。

[0070] 鉴于在此描述并示出的原理和示例实施例，应该认识到，可以在不背离上述原则的情况下对所示的实施例的安排和细节做出修改。例如，虚拟 TPM 是结合虚拟机来描述的，但是替换实施例也可包括与其他类型的系统细分，诸如与一个服务器或与共享硬件 TPM 的一组服务器内的分区结合使用的 vTPM。例如，虚拟 TPM 可以在被划分成两个逻辑双处理器系统的四处理器系统内使用。此处的教示还可用于将逻辑 TPM 提供给一个或多个服务协处理器，或者提供给硬件平台上一个或多个其他类型的独立处理元件。

[0071] 此外，替换实施例包括不对硬件 TPM 进行仿真，但会（例如，通过提供更多的 PCR、更多的存储等）扩展和 / 或放大硬件 TPM 的能力的 vTPM 服务。替换实施例还包括在安全 OS 之上、受管运行时环境 (MRTE) 之上、服务处理器或协处理器内、平台的系统管理模式 (SMM) 内等运行的虚拟 TPM 服务。

[0072] 同样，虽然前述讨论关注了某些特定实施例，但是仍然可以构想其他配置。更具体地，即使在此使用了诸如“在一个实施例中”、“在另一个实施例中”之类的表达，但这些短语一般仅意味着参考实施例的可能性，而不旨在将本发明限于某些特定的实施例配置。如此处所使用的，这些术语可以参考可并入其他实施例的相同或不同的实施例。

[0073] 类似地，虽然已关于以特定顺序执行的特定操作描述了示例过程，但是可以对这些国车杠应用各种修改以导出本发明的多个替换实施例。例如，替换实施例可以包括使用少于全部公开的操作的过程、使用附加操作的过程、使用顺序不同的相同操作的过程以及

其中组合、细分或改变了在此公开的各个操作的过程。

[0074] 本发明的替换实施例还包括用于执行本发明的各操作的机器可访问介质编码指令。这些实施例还可被称为程序产品。这些机器可访问介质包括但不限于存储介质，诸如软盘、硬盘、CD-ROM、ROM 和 RAM ；以及通信介质，诸如天线、电线、光纤、微波、无线电波和其他的电磁或光载波。因此，指令和其他数据能以分组、串行数据、并行数据、传播信号等的形式经由传输环境或网络传播，并能在分布式环境中使用并被本地和 / 或远程存储以供单或多处理器机器访问。

[0075] 应该理解，在此描述的硬件和软件组件表示合理自持以便各自都能被充分彼此独立地设计、构造或更新的功能元件。在替换实施例中，许多组件都可被实现为硬件、软件或硬件和软件的组合以提供在此描述并示出的功能。

[0076] 考虑到能从在此描述的示例实施例中轻易导出的各种有用的变化，该详细描述仅出于示意性的目的，而不应被理解为限制本发明的范围。因此，本发明所要求保护的是落入所附权利要求书的范围和精神内的全部实现以及这些实现的所有等效技术方案。

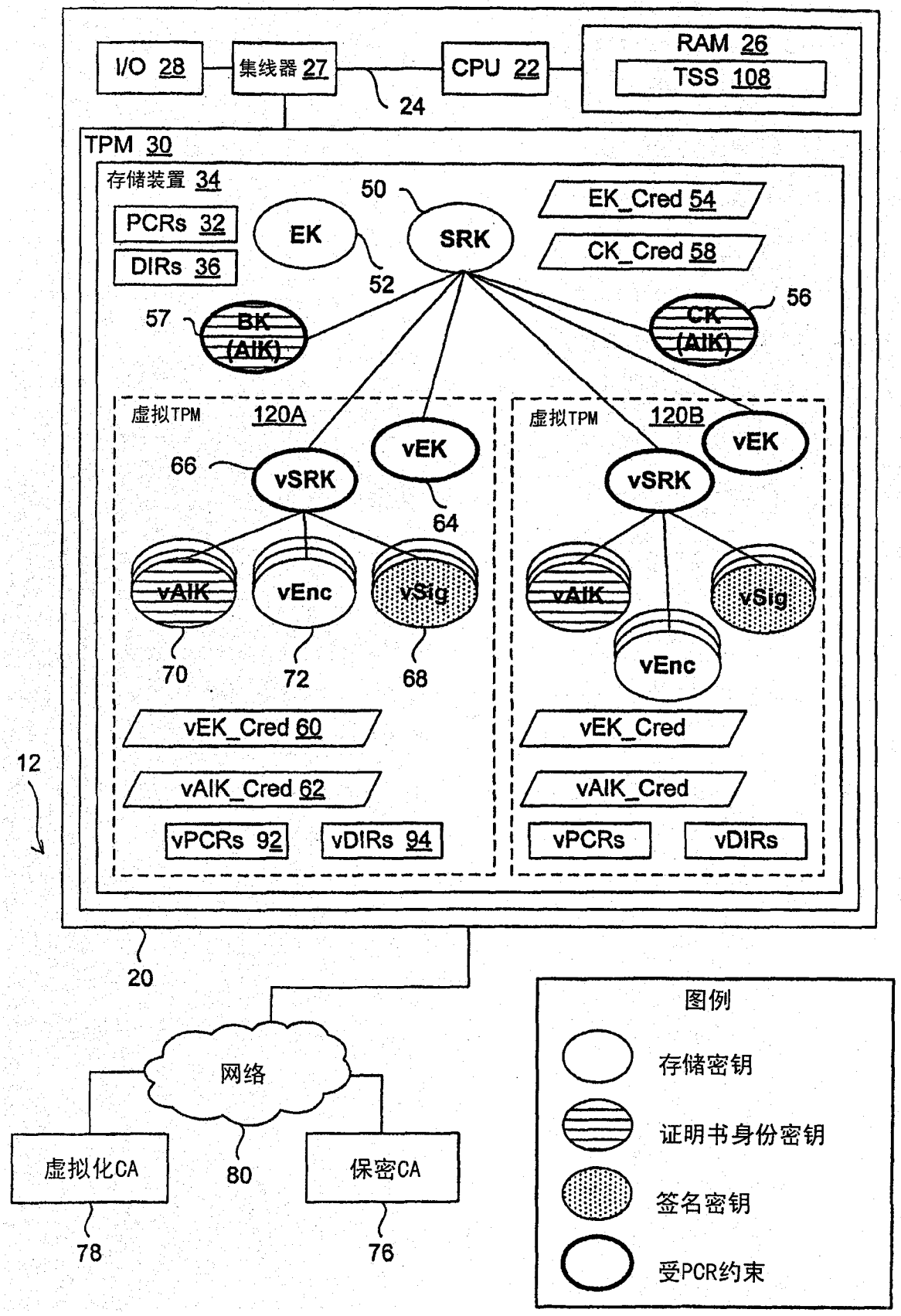

I/O 28
集线器 27
24
CPU 22
RAM 26
TSS 108
TPM 30
存储装置 34
PCRs 32
DIRs 36
EK
50
SRK
52
EK_Cred 54
CK_Cred 58
57
BK (AIK)
CK (AIK)
56
虚拟TPM 120A
虚拟TPM 120B
66
vSRK
vEK
64
vAIK
vEnc
vSig
70
72
68
vEK_Cred 60
vAIK_Cred 62
vPCRs 92
vDIRs 94
vEK_Cred
vAIK_Cred
vPCRs
vDIRs
12
20
网络
虚拟化CA
80
保密CA
78
76
图例
存储密钥
证明书身份密钥
签名密钥
受PCR约束

图 1

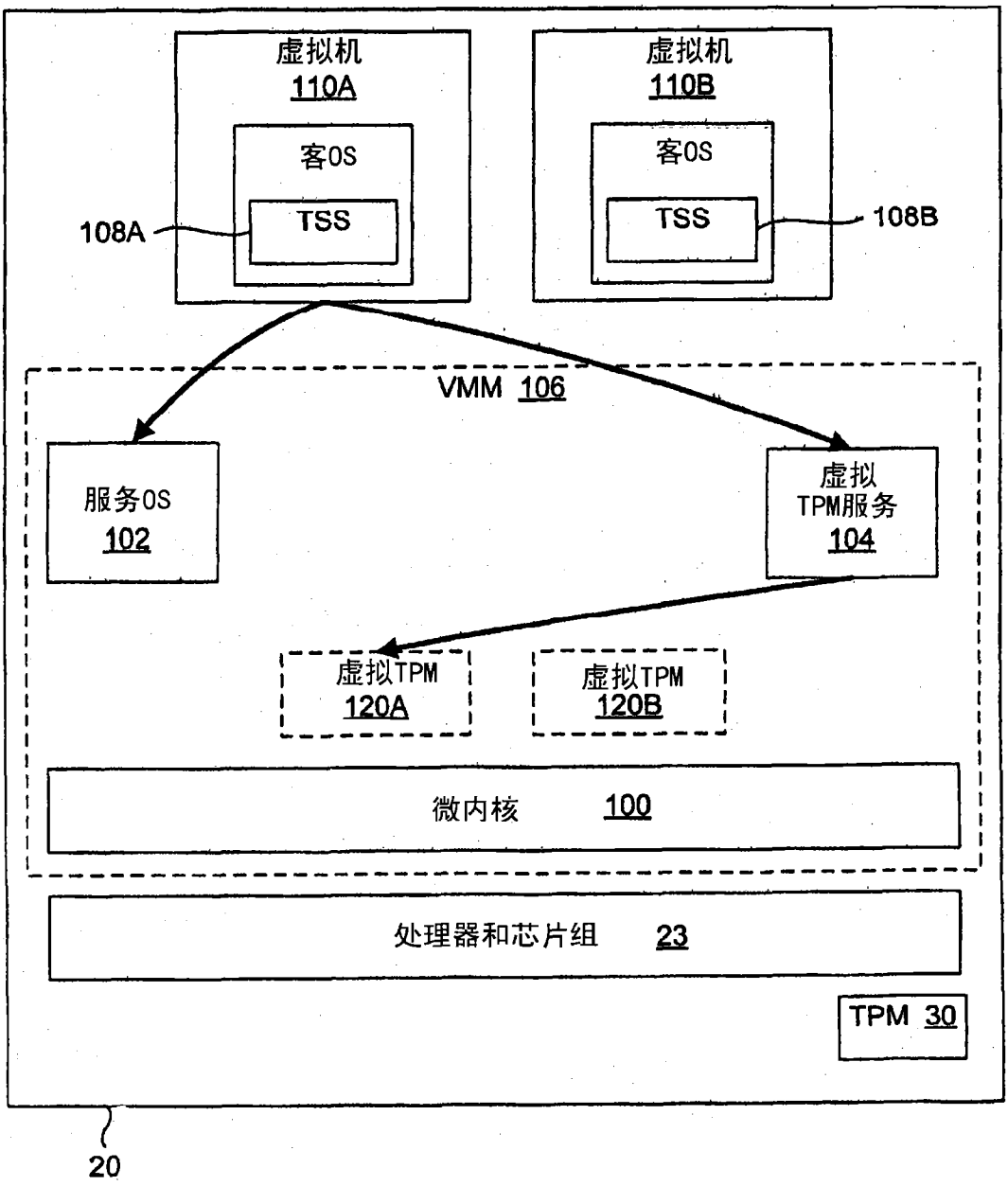

虚拟机
110A
客OS
TSS
108A
虚拟机
110B
客OS
TSS
108B
VMM 106
服务OS
102
虚拟
TPM服务
104
虚拟TPM
120A
虚拟TPM
120B
微内核 100
处理器和芯片组 23
TPM 30
20

图 2

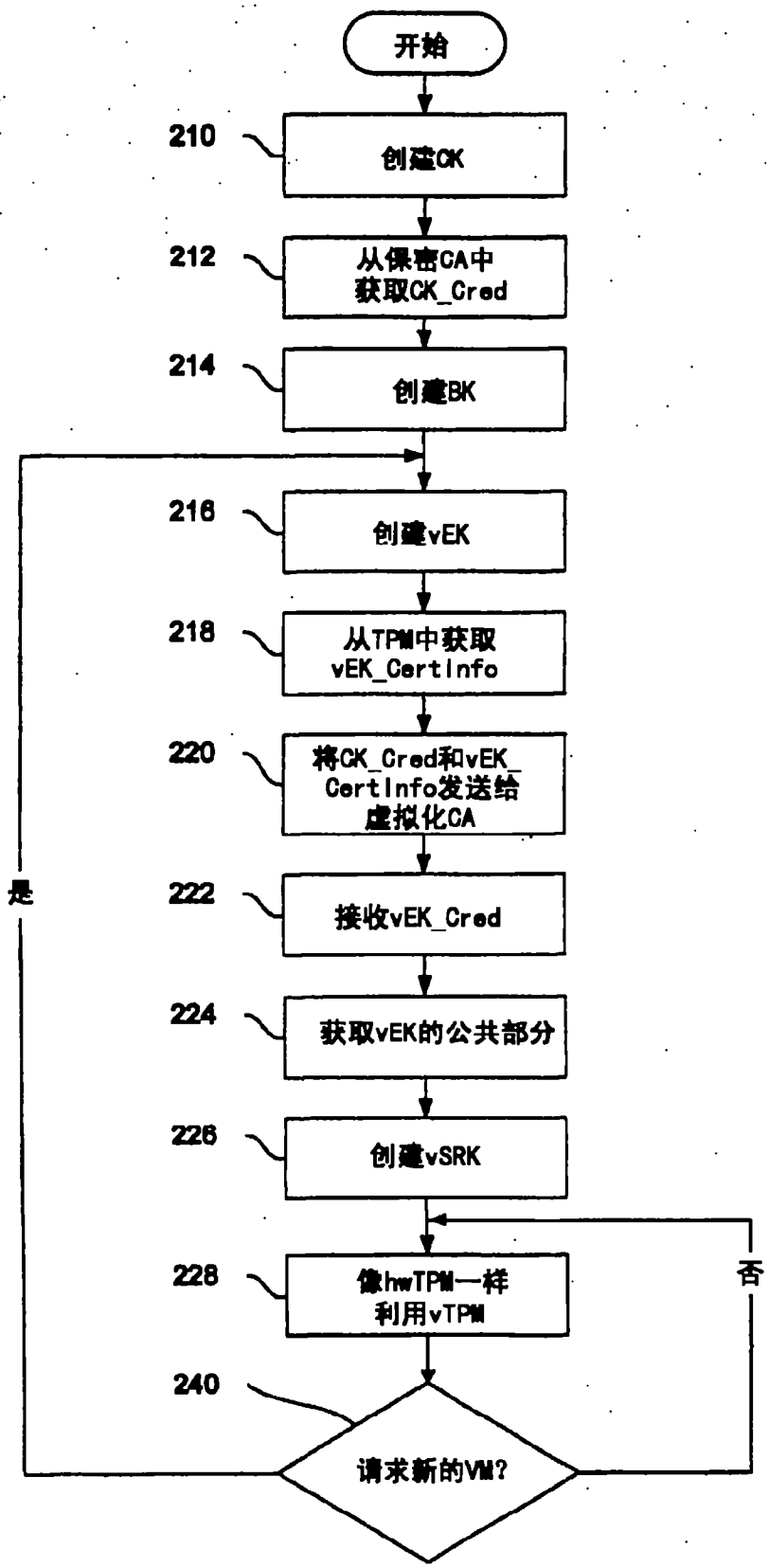

开始
210
创建CK
212
从保密CA中
获取CK_Cred
214
创建BK
216
创建vEK
218
从TPM中获取
vEK_CertInfo
220
将CK_Cred和vEK_
CertInfo发送给
虚拟化CA
222
接收vEK_Cred
224
获取vEK的公共部分
226
创建vSRK
228
像hwTPM一样
利用vTPM
240
请求新的VM?
是
否

图 3

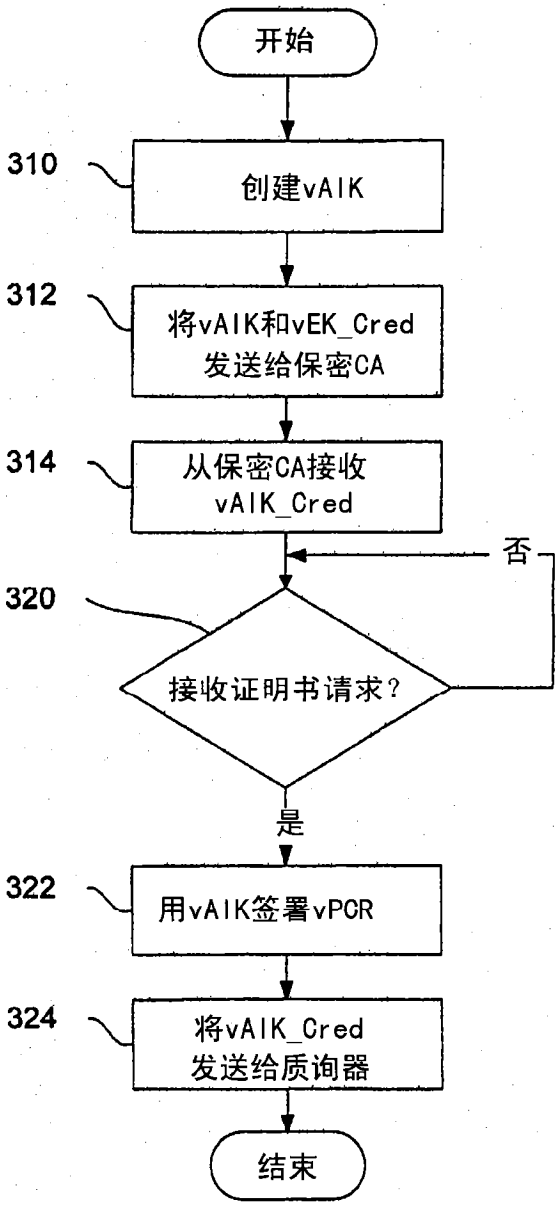

开始
310
创建vAIK
312
将vAIK和vEK_Cred
发送给保密CA
314
从保密CA接收
vAIK_Cred
否
320
接收证明书请求？
是
322
用vAIK签署vPCR
324
将vAIK_Cred
发送给质询器
结束

图 4