(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 116134426 A
(43)申请公布日 2023.05.16

(21)申请号 202080104869.4
(22)申请日 2020.07.20
(85)PCT国际申请进入国家阶段日
2023.01.11
(86)PCT国际申请的申请数据
PCT/US2020/042766 2020.07.20
(87)PCT国际申请的公布数据
WO2022/019880 EN 2022.01.27
(71)申请人 惠普发展公司，有限责任合伙企业
地址 美国德克萨斯州
(72)发明人 马文·杜安·纳尔逊
霍恩·李·梅萨
詹妮弗·林恩·梅林
布莱恩·C·迈耶
(74)专利代理机构 北京德琦知识产权代理有限公司 11018
专利代理师 王明轩 康泉
(51)Int.Cl.
G06F 11/30(2006.01)

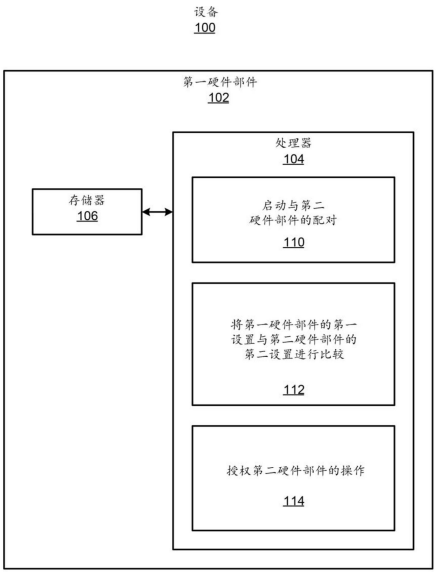
权利要求书3页 说明书8页 附图4页

(54)发明名称

配对硬件部件以授权操作

(57)摘要

根据示例，设备可以包括第一硬件部件，第一硬件部件包括第一存储器和第一处理器。第一处理器可以启动第一硬件部件与第二硬件部件之间的配对，以在第一硬件部件与第二硬件部件之间建立信任关系。响应于第一硬件部件与第二硬件部件之间成功配对，处理器可以将第一硬件部件的第一设置与第二硬件部件的第二设置进行比较。响应于确定第二设置与第一设置相对应，处理器可以授权第二硬件部件的操作。



CN 116134426 A

1.一种设备,包括:

第一硬件部件,包括:

第一存储器;以及

第一处理器,用于:

启动所述第一硬件部件与第二硬件部件之间的配对,以在所述第一硬件部件与第二硬件部件之间建立信任关系;

响应于所述第一硬件部件与所述第二硬件部件之间成功配对,将所述第一硬件部件的第一设置与所述第二硬件部件的第二设置进行比较;以及

响应于确定所述第二设置与所述第一设置相对应,授权所述第二硬件部件的操作。

2.根据权利要求1所述的设备,包括:

所述第二硬件部件,所述第二硬件部件包括:

第二存储器;以及

第二处理器,用于:

响应于与所述第一硬件部件成功配对,将所述第二硬件部件的所述第二设置与所述第一硬件部件的所述第一设置进行比较;以及

响应于确定所述第一设置与所述第二设置相对应,授权所述第一硬件部件的操作;

响应于确定配对不成功或所述第一设置与所述第二设置不同,防止所述第一硬件部件的操作;以及

确定所述第一硬件部件是新的硬件部件,请求云服务授权所述新的硬件部件,并且基于来自所述云服务的所述新的硬件部件的授权,授权新的信任关系和所述新的硬件部件的操作。

3.根据权利要求1所述的设备,其中,所述第一处理器用于:

响应于与所述第二硬件部件配对不成功,或者响应于确定所述第二设置与所述第一设置不对应,防止所述第二硬件部件的操作。

4.根据权利要求1所述的设备,其中,为启动所述配对,所述第一处理器用于:

将与所述第一硬件部件相关联的第一装置身份发送到所述第二硬件部件,所述第一装置身份唯一地标识所述第一硬件部件;

响应于在所述第二硬件部件处的所述第一装置身份的验证,接收与所述第二硬件部件相关联的第二装置身份,所述第二装置身份唯一地标识所述第二硬件部件;

启动验证以证明所接收的第二装置身份与所述第二硬件部件相关联;以及

响应于所述第二装置身份的成功验证,在所述第一硬件部件与所述第二硬件部件之间建立所述信任关系。

5.根据权利要求4所述的设备,其中,所述第一处理器用于:

基于认证密钥启动验证,以证明所接收的第二装置身份与所述第二硬件部件相关联,所述认证密钥被生成为包括与第三硬件部件相关联的唯一认证密钥、与所述第一硬件部件相关联的第一凭证以及与所述第二硬件部件相关联的第二凭证。

6.根据权利要求1所述的设备,其中,所述第一处理器进一步用于:

在所述第一硬件部件与云服务之间建立信任关系;以及

基于所述第一硬件部件与所述第二硬件部件之间的所述信任关系以及所述第一硬件

部件与所述云服务之间的所述信任关系，使得信任关系能够在所述第二硬件部件与所述云服务之间被继承。

7.根据权利要求1所述的设备，其中，所述第一处理器进一步用于：

确定所述第二硬件部件是新的硬件部件；

请求云服务授权所述新的硬件部件；以及

基于来自所述云服务的授权，授权所述新的硬件部件的操作。

8.一种方法，包括：

由处理器启动第一硬件部件与第二硬件部件的配对，所述配对建立所述第一硬件部件与所述第二硬件部件之间的信任关系；

响应于所述第一硬件部件与所述第二硬件部件之间成功配对，由所述处理器确定与在所述第一硬件部件中启用的第一功能相关联的第一设置和与在所述第二硬件部件中启用的第二功能相关联的第二设置相匹配，所述第一功能与所述第二功能相同；以及

基于确定所述第一设置与所述第二设置相匹配，

由所述第一硬件部件授权所述第二硬件部件的操作，以及

由所述第二硬件部件授权所述第一硬件部件的操作。

9.根据权利要求8所述的方法，进一步包括：

响应于所述第一硬件部件与所述第二硬件部件之间配对不成功，或者响应于确定所述第一设置与所述第二设置不匹配，由所述第一硬件部件防止所述第二硬件部件的操作和/或由所述第二硬件部件防止所述第一硬件部件的操作。

10.根据权利要求8所述的方法，进一步包括：

在每次所述第一硬件部件和/或所述第二硬件部件上电时，在所述第一硬件部件与所述第二硬件部件之间共享所述第一硬件部件的身份和所述第二硬件部件的身份；

启动验证以证明所述第一硬件部件的所述身份和所述第二硬件部件的所述身份；以及

基于确定所述第一硬件部件的所述身份和所述第二硬件部件的所述身份被验证，在所述第一硬件部件与所述第二硬件部件之间建立所述信任关系。

11.根据权利要求10所述的方法，进一步包括：

生成验证所述第一硬件部件和所述第二硬件部件的认证密钥，所述认证密钥包括与第三硬件部件相关联的唯一认证密钥、与所述第一硬件部件相关联的第一凭证以及与所述第二硬件部件相关联的第二凭证。

12.根据权利要求8所述的方法，进一步包括：

基于所述第一硬件部件与云服务之间的配对过程，在所述第一硬件部件与所述云服务之间建立信任关系；以及

基于所述第一硬件部件与所述第二硬件部件之间的所述信任关系以及所述第一硬件部件与所述云服务之间的所述信任关系，建立要在所述第二硬件部件与所述云服务之间被继承的信任关系，

其中，所述第二硬件部件与所述云服务之间的所述信任关系被建立，而无需所述第二硬件部件与所述云服务之间的配对过程。

13.根据权利要求8所述的方法，进一步包括：

确定所述第一硬件部件或所述第二硬件部件是新的硬件部件；

请求云服务授权所述新的硬件部件的安装;以及

基于来自所述云服务的授权,在所述新的硬件部件与所述第一硬件部件和所述第二硬件部件中剩余的一个之间建立配对。

14.一种非暂时性计算机可读介质,所述非暂时性计算机可读介质上存储有计算机可读指令,当执行所述计算机可读指令时,使计算装置的处理器:

在第一硬件部件与第二硬件部件之间共享识别信息;

验证所述识别信息,以在所述第一硬件部件与第二硬件部件之间建立信任关系;

响应于确定在所述第一硬件部件与所述第二硬件部件之间已经建立所述信任关系,验证所述第一硬件部件的与第一授权的功能相关联的第一设置和所述第二硬件部件的与第二授权的功能相关联的第二设置;以及

响应于所述第一设置和所述第二设置的成功验证,授权所述第一硬件部件和/或所述第二硬件部件的操作。

15.根据权利要求14所述的非暂时性计算机可读介质,其中,所述指令进一步使所述处理器:

响应于所述第一硬件部件与所述第二硬件部件之间配对不成功,或者响应于确定所述第一设置和所述第二设置彼此不对应,防止所述第一硬件部件和/或所述第二硬件部件的操作。

配对硬件部件以授权操作

背景技术

[0001] 电子装置(包括计算装置)可以由多种不同的硬件部件组成。这些硬件部件可以在电子装置中被替换。

附图说明

[0002] 本公开的特征以示例的方式图示,并且不限于以下附图,其中,相同的数字表示相同的元件,在附图中:

[0003] 图1描绘了可以包括第一硬件部件的示例设备的框图,第一硬件部件可以启动与第二硬件部件的配对,以建立信任关系并授权第二硬件部件的操作;

[0004] 图2示出了可以包括在图1所描绘的示例设备的示例系统的框图;

[0005] 图3示出了用于启动第一硬件部件与第二硬件部件之间的配对以建立信任关系以及用于授权第一硬件部件和/或第二硬件部件的操作的示例方法的流程图;

[0006] 图4描绘了示例性非暂时性计算机可读介质的框图,该非暂时性计算机可读介质具有存储在其上的可以存储授权第一硬件部件和/或第二硬件部件的操作的计算机可读指令。

具体实施方式

[0007] 为了简单和说明的目的,本公开主要通过参照示例来描述。在以下描述中,提出了多种具体细节,以提供对本公开的透彻理解。然而,显而易见的是,本公开可以在不限于这些具体细节的情况下实践。在其他实例中,没有详细描述一些方法和结构,以免不必要地混淆本公开。

[0008] 在本公开全文中,术语“一”旨在表示具体元件中的至少一个。如在本文中所使用的,术语“包括”表示包括但不限于。术语“基于”表示至少部分地基于。

[0009] 在本文中公开了可以在硬件部件之间建立信任关系并基于所建立的信任关系授权硬件部件的操作的设备、系统、方法和计算机可读介质。诸如打印机、个人计算机等的电子装置可以由多种不同的硬件部件组成。硬件部件可以包括各种类型的控制板(诸如数字控制板或模拟控制板)、打印墨盒、定影器和/或扫描仪等。这些硬件部件中的多种硬件部件可以具有启用与具体电子装置相关联的硬件部件的授权的功能的设置,例如,和与具体电子装置相关联的业务逻辑相对应的功能。

[0010] 作为具体示例并且出于说明的目的,电子装置可以具有多个硬件部件,并且可以维护硬件部件的业务逻辑设置。例如,业务可以开发以多种配置销售的产品,并且不同的配置中的一些配置可以与特定产品的不同业务逻辑(例如,授权的功能和/或许可特征等)相关联。在这一点上,例如,与以较低价格点销售的产品相比,以较高价格点销售的产品可以具有启用的附加的和/或不同的功能。

[0011] 与这种产品相关联的问题可能是,低价格产品可能被以未授权的方式被购买和修改,例如,通过替换设备中的硬件部件来覆盖与所购买的产品相关联的业务逻辑。本公开的

示例设备、系统、方法和计算机可读介质可以使得能够跨多个更高性能(并且因此相对更昂贵)的硬件部件安全地维护业务逻辑,这可以防止例如购买较低性能的模型,然后通过替换硬件部件将其转换为较高性能的模型。

[0012] 在一些示例中,设备可以包括第一硬件部件,该第一硬件部件包括第一存储器和第一处理器。第一处理器可以启动第一硬件部件与第二硬件部件之间的配对,以在第一硬件部件与第二硬件部件之间建立信任关系。响应于第一硬件部件与第二硬件部件之间成功配对,处理器可以将第一硬件部件的第一设置与第二硬件部件的第二设置进行比较。在这一点上,响应于确定第二设置与第一设置相对应,处理器可以授权第二硬件部件的操作。

[0013] 通过使得硬件部件能够配对以建立信任关系,设备内的硬件部件可以被实现为在产品的整个寿命期间跨多个硬件部件安全地维护设备的预定的功能配置(诸如安全业务逻辑)。本公开的示例设备可以通过使用硬件部件之间的信任关系来防止硬件部件的未授权的替换(通过在每次上电时使得一个硬件部件能够防止另一个未授权的硬件部件的操作)来改善安全性。在这一点上,每个硬件部件可以具有唯一的身份,并且因此硬件部件不能简单地从第一设备中被卸载并被安装在第二设备中以替换第二设备中的相对应的硬件部件。这样,本公开的示例设备可以防止较低性能(例如,较低价格)的模型到较高性能(例如,较高价格)的模型的未授权的转换(例如,通过替换设备的硬件部件)。在一些示例中,新的硬件部件可以在新的硬件部件可以被安装在装置上之前从云服务获得授权,从而防止对硬件部件的未授权的改变。

[0014] 首先参照图1和图2。图1示出了可以包括第一硬件部件102的示例设备100的框图,第一硬件部件102可以启动与第二硬件部件的配对,以建立信任关系并授权第二硬件部件的操作。图2示出了可以包括在图1所描绘的示例设备100的示例系统200的框图。应当理解的是,在图1中所描绘的设备100和/或在图2中所描绘的系统200可以包括附加的特征,并且可以移除和/或修改在本文中所描述的特征中的一些,而不偏离设备100和/或系统200的范围。

[0015] 设备100可以包括第一硬件部件102,第一硬件部件102可以包括第一处理器104和第一存储器106。设备100可以是打印机、多功能设备和/或诸如服务器、网络中的节点(诸如数据中心)、个人计算机、膝上型计算机、平板计算机、智能电话、网关、网络路由器的计算装置和/或诸如物联网(IoT)装置的电子装置等。作为具体示例,设备100的第一硬件部件102可以是打印机的部件,包括例如控制板(诸如数字控制板和/或模拟控制板等)、墨盒、定影器和/或激光扫描仪等。第二硬件部件202也可以是以上列出的部件中的任何一个,并且可以与第一硬件部件102类似或不同。

[0016] 处理器104和204中的每一个可以是基于半导体的微处理器、中央处理单元(CPU)、专用集成电路(ASIC)、现场可编程门阵列(FPGA)和/或其他硬件装置。尽管第一硬件部件102和第二硬件部件202被描绘为分别具有单个处理器104、204,但是应当理解的是,硬件部件102、202和/或设备100可以包括附加的处理器和/或核心,而不偏离硬件部件102、202和/或设备100的范围。在这一点上,对单个处理器104、204以及单个存储器106、206的引用可以被理解为附加地或替代地适用于多个处理器104、204和多个存储器106、206。

[0017] 存储器106、206可以分别是例如非易失性存储器,诸如只读存储器(ROM)、闪存、固态驱动器、随机存取存储器(RAM)、电可擦除可编程只读存储器(EEPROM)、存储装置或光盘

等。举例而言，存储器106、206可以分别是非易失性随机存取存储器(NVRAM)，其可以被实现为通过串行可编程接口(SPI)总线/连接来存储和返回数据。在一些示例中，存储器106、206可以是集成到可以提供增强的安全性的例如片上系统(SoC)和/或安全芯片等中的专用存储器。在一些示例中，存储器106、206可以分别被焊接在位于相应的硬件部件102、202上的芯片上，并且可以用于安全性和安全存储。

[0018] 如在图1中所示出的，处理器104可以执行各种操作110至114以授权第二硬件部件202的操作。操作110至114可以是处理器104可以执行的硬件逻辑块。在其他示例中，操作110至114可以是机器可读指令(例如，非暂时性计算机可读指令)。在其他示例中，设备100可以包括指令和硬件逻辑块的组合，以实现或执行与操作110至114相对应的功能。

[0019] 处理器104可以执行操作110以启动第一硬件部件102与第二硬件部件(诸如在图2中所描绘的第二硬件部件202)之间的配对，以在第一硬件部件102与第二硬件部件202之间建立信任关系。在一些示例中，第二硬件部件202可以与第一硬件部件102一起安装在设备100中，并且可以包括第二处理器204和第二存储器206。第一硬件部件102和第二硬件部件202可以通过总线经由通信协议进行通信。在一些示例中，第一硬件部件102和第二硬件部件202可以彼此分开布置，并且可以通过网络222联接以彼此通信。

[0020] 配对过程可以包括共享识别信息(诸如在图2中所描绘的第一硬件部件102的第一装置身份214)并验证所共享的识别信息，以在第一硬件部件102与第二硬件部件202之间建立信任关系。作为具体示例并且出于说明的目的，处理器104可以将第一硬件部件102相关联的第一装置身份214发送到第二硬件部件202。在一些示例中，第一装置身份214可以包括第一装置标识符216，第一装置标识符216可以唯一地标识第一硬件部件102。第一装置身份214可以包括第一凭证218，第一凭证218可以用于认证第一装置标识符216。在一些示例中，第一凭证218可以包括非对称公钥，该非对称公钥可以内置于第一硬件部件102中，并由第二硬件部件202用于验证第一硬件部件102的第一装置身份214。在这一点上，第一装置标识符216可以是将唯一性和可跟踪性提供到相应硬件部件的标识符。第一凭证218可以是提供真实性和所有权的加密验证的凭证。

[0021] 第二硬件部件202中的第二处理器204可以在第二硬件部件202处验证第一装置身份214。响应于在第二硬件部件202处成功验证第一装置身份214，在第一硬件部件102处的处理器104可以接收与第二硬件部件202相关联的第二装置身份224。第二装置身份224可以唯一地标识第二硬件部件202，并且可以包括与第二硬件部件202相关联的第二装置标识符226和第二凭证228。

[0022] 在一些示例中，处理器104可以启动验证以证明所接收的第二装置身份224与第二硬件部件202相关联。在这一点上，处理器104可以通过第二硬件部件202来认证第二装置身份224的所有权。处理器104可以使用第二装置标识符226和第二凭证228来认证第二装置身份224，第二装置标识符226和第二凭证228可以是第二硬件部件202所独有的。

[0023] 在一些示例中，除了从第二硬件部件202检索的信息之外，处理器104还可以使用来自第三硬件部件(未示出)的信息来认证第二装置身份224。例如，处理器104可以通过使用多个硬件部件所独有的信息来启动验证，以证明所接收的第二装置身份224与第二硬件部件202相关联。在这一点上，处理器104可以基于认证密钥来证明第二装置身份224的所有权，该认证密钥可以被生成为包括与第三硬件部件相关联的唯一认证密钥、与第一硬件部

件102相关联的第一凭证218和/或与第二硬件部件202相关联的第二凭证228。第三硬件部件可以是安装在设备100中的与第一硬件部件102和/或第二硬件部件202类似的硬件部件，诸如墨盒、定影器和/或激光扫描仪等。

[0024] 响应于来自第二硬件部件202的第二装置身份224的成功验证，处理器104可以在第一硬件部件102与第二硬件部件202之间建立信任关系。在这一点上，设备100中的硬件部件之间的信任关系可以在设备100的整个寿命期间被验证/建立。例如，在每次第一硬件部件102和/或第二硬件部件202上电时，处理器100可以启动配对和验证过程，以在第一硬件部件102与第二硬件部件202之间建立信任关系。

[0025] 在一些示例中，响应于与第二硬件部件202配对不成功，例如基于第二装置身份224的验证或证明不成功，处理器104可以防止第二硬件部件202的操作。在这一点上，第一硬件部件102的处理器104可以扣留操作数据和流程，以使第二硬件部件202不可操作。在一些示例中，第一硬件部件102的处理器104可以拒绝对第二硬件部件202的供电和/或连接等，以防止第二硬件部件202的操作。替代地或附加地，第一硬件部件102的处理器104可能无法提供诸如凭证218的基本密码资料来允许正常操作。

[0026] 在一些示例中，硬件部件可以利用与一个硬件部件形成的信任关系来建立与另一个硬件部件的信任关系。作为具体示例，除了与第二硬件部件202的信任关系之外，第一硬件部件102还可以具有与云服务212的信任关系。云服务212可以是将服务提供到设备100的服务器、计算装置和/或一组计算装置。在这一点上，处理器104可以基于第一硬件部件102与第二硬件部件202之间的信任关系以及第一硬件部件102与云服务212之间的信任关系，使得信任关系能够在第二硬件部件202与云服务212之间被继承。在一些示例中，处理器104可以使得第二硬件部件202与云服务212之间的信任关系能够被继承，而无需通过利用已知的信任关系来执行先前描述的配对和证明过程。

[0027] 在一些示例中，第二硬件部件202可以建立与云服务212的信任关系，而无需从第一硬件部件102继承对云服务212的信任关系。在这一点上，第二硬件部件202可以启动与云服务212的配对，包括共享和验证装置身份以及证明所共享的装置身份，如先前参照与第一硬件部件102的配对所描述的。应当理解的是，第二硬件部件202可以与实现在设备100中的多个硬件部件建立信任关系，或者替代地或附加地，第二硬件部件202可以通过网络222与实现在网络222上的其他装置中的硬件部件建立信任关系。

[0028] 响应于第一硬件部件102与第二硬件部件202之间成功配对，处理器104可以执行操作112，以将第一硬件部件102的第一设置220与第二硬件部件202的第二设置230进行比较。在一些示例中，第一设置220可以限定第一硬件部件102的功能，并且第二设置230可以限定第二硬件部件202的功能。第一设置220和第二设置230可以是彼此的镜像副本，并且可以被写入位于相应的硬件部件上的安全存储器(诸如第一存储器106和第二存储器206)。

[0029] 作为具体示例并且出于说明的目的，第一设置220可以被实现为控制位，控制位可以被写入第一硬件部件102的安全存储器。在一些示例中，第一设置220可以包括允许替换的硬件部件与其他硬件部件配对的设置，或者锁定第一硬件部件102的第一设置220的设置。在这一点上，第一硬件部件102可以防止与未识别的硬件部件配对和/或防止硬件部件的未授权的替换或安装。

[0030] 在一些示例中，第一设置220可以包括限定设备100的授权的功能(例如，与设备

100的预期业务逻辑相关联的功能)的设置。作为具体示例,在第二硬件部件202在设备100中被替换并且与第一硬件部件102成功配对的情况下,处理器104可以验证第二设置230,并且可以基于确定授权的功能已经被改变来防止新的硬件部件的操作,例如,在第二设置230和与授权的功能相关联的第一设置220不匹配的情况下。

[0031] 在一些示例中,处理器104可以在设备100的引导过程期间对照第二设置230来验证第一设置220。基于确定第一设置220与第二设置230不对应,处理器104可以防止第二硬件部件202的操作。在这一点上,响应于确定第二设置230与第一设置220相对应,处理器104可以执行操作114,以授权第二硬件部件202的操作。

[0032] 在一些示例中,如先前所描述,第二硬件部件202可以采用与第一硬件部件102类似的方式来授权第一硬件部件102的操作。例如,第二处理器204可以基于由第二处理器204确定的信任关系以及第一设置220和第二设置230的验证来授权第一硬件部件102的操作。例如,响应于与第一硬件部件102成功配对,第二处理器204可以将第二硬件部件202的第二设置230与第一硬件部件102的第一设置220进行比较。

[0033] 在这种情况下,响应于确定第一设置220与第二设置230相对应,第二处理器204可以授权第一硬件部件102的操作,并且响应于确定配对不成功或第一设置220与第二设置230不同,第二处理器204可以防止第一硬件部件102的操作。在一些示例中,第二处理器204可以确定第一硬件部件102是新的硬件部件,并且可以请求云服务212授权新的硬件部件。在这一点上,基于来自云服务212的新的硬件部件的授权,第二处理器204可以授权新的硬件部件的操作。在一些示例中,云服务212可以包括先验信息,该先验信息向云服务212提供信息以做出确定,从而授权或拒绝硬件部件的重新配对请求。存储在云服务212中的信息可以允许云服务212跟踪硬件部件102、202,包括修改、替换、操作和/或状态信息等,并且可以确保硬件部件102、202的合适操作。

[0034] 在一些示例中,当设备100中的硬件部件被替换时,硬件部件的处理器可以确定哪个硬件部件是现有的硬件部件以及哪个是新的硬件部件。例如,处理器104可以基于信息(诸如第一装置身份214和第二装置身份224)交换来确定第二硬件部件202是新的硬件部件。在这一点上,新的硬件部件可以被安装在设备100中,并且与第一硬件部件102成功配对。响应于识别新的硬件部件,处理器104可以请求云服务212授权设备100中的新的硬件部件,并且基于来自云服务212的授权,处理器104可以授权新的硬件部件的操作,例如,可以授权设备100使用新添加的硬件部件进行打印。

[0035] 作为具体示例并且出于说明的目的,处理器104可以基于第二设置230来确定第二硬件部件202是新的硬件部件。在这一点上,第二设置230可以包括锁定设置,该锁定设置可以启用存储在第二存储器206中的配对信息的锁定状态。当启用第二硬件部件202中的配对信息的锁定状态的第二设置230被设置时,处理器104可以从云服务212获得授权,用于将被确定为新的硬件部件的第二硬件部件202重新配对到第一硬件部件102。

[0036] 尽管设备100被描绘为具有两个硬件部件(特别是第一硬件部件102和第二硬件部件202),但是应当理解的是,可以在设备100中设置附加的硬件部件,而不偏离硬件部件102、202和/或设备100的范围。在这一点上,多个硬件部件可以建立配对的硬件部件的网络。在该实例中,如先前所描述的,第一硬件部件102可以与多个硬件部件中的每一个建立多个配对和/或继承与具体硬件部件的信任关系。

[0037] 相对于在图3中所描绘的方法300，其中处理器104、204可以操作的各种方式被更详细地讨论。图3描绘了用于启动第一硬件部件102与第二硬件部件202之间的配对以建立信任关系以及用于授权第一硬件部件102和/或第二硬件部件202的操作的示例方法300的流程图。应当理解的是，在图3中所描绘的方法300可以包括附加操作，并且可以移除和/或修改其中描述的操作中的一些，而不偏离方法300的范围。出于说明的目的，参照在图1和图2中所描绘的特征对方法300进行描述。

[0038] 在框302处，处理器104可以启动第一硬件部件102与第二硬件部件202的配对。在这一点上，配对可以在第一硬件部件102于第二硬件部件202之间建立信任关系。

[0039] 在一些示例中，处理器104、204可以在第一硬件部件102与第二硬件部件202之间共享第一硬件部件102的身份和第二硬件部件202的身份。第一硬件部件102的身份(诸如在图2中所描绘的第一装置身份214)可以包括第一装置标识符216和第一凭证218。同样地，第二硬件部件202的身份(诸如第二装置身份224)可以包括第二装置标识符226和第二凭证228。在这一点上，第一装置标识符216和第二装置标识符226可以是将唯一性和可跟踪性提供到相应的硬件部件的标识符。第一凭证218和第二凭证228可以是提供真实性和所有权的加密验证的凭证。处理器104、204可以启动验证来证明第一硬件部件102的身份和第二硬件部件202的身份。基于确定第一硬件部件102的身份和第二硬件部件202的身份被验证，处理器104、204可以在第一硬件部件102与第二硬件部件202之间建立信任关系。这样，每个硬件部件可以具有可以被验证的唯一身份，并且因此硬件部件不能简单地从第一设备(诸如设备100)中被取出并被安装在与第一设备不同的第二设备中以替换第二设备中的相应的硬件部件。

[0040] 在一些示例中，处理器104、204可以生成认证密钥以验证第一硬件部件102和第二硬件部件202。在这一点上，处理器104、204可以生成认证密钥，以包括与第三硬件部件相关联的唯一认证密钥。在一些示例中，认证密钥可以包括来自第三硬件部件的唯一认证密钥、与第一硬件部件102相关联的第一凭证218以及与第二硬件部件202相关联的第二凭证228。

[0041] 在框304处，响应于在框302中的第一硬件部件102与第二硬件部件202之间成功配对，处理器104可以确定与在第一硬件部件102中启用的第一功能相关联的第一设置220与第二设置230相匹配，第二设置230与在第二硬件部件202中启用的第二功能相关联。在这一点上，第一功能可以与第二功能相同。在一些示例中，第一设置220可以包括与第二设置230相同的设置集合，并且当设置集合中的每个设置彼此匹配时，第一设置220可以与第二设置230相匹配。

[0042] 在框306处，基于确定第一设置220与第二设置230相匹配，第一硬件部件102的处理器104可以授权第二硬件部件202的操作。此外，在框308处，第二硬件部件202的第二处理器204可以授权第一硬件部件102的操作。

[0043] 在一些示例中，设备100中的硬件部件之间的信任关系可以在设备100的整个寿命期间被验证/建立。例如，在每次第一硬件部件102和/或第二硬件部件202上电时，处理器100可以启动配对和验证过程，以在第一硬件部件102与第二硬件部件202之间建立信任关系。

[0044] 在一些示例中，响应于第一硬件部件102与第二硬件部件202之间配对不成功，或者响应于确定第一设置220与第二设置230不匹配，处理器104可以防止第二硬件部件202的

操作。附加地或替代地，第二处理器204可以防止第一硬件部件102的操作。

[0045] 在一些示例中，处理器104可以通过例如执行第一硬件部件102与云服务212之间的配对过程来使第一硬件部件102与云服务212之间的信任关系被建立。此外，处理器104可以基于第一硬件部件102与第二硬件部件202之间的信任关系以及第一硬件部件102与云服务212之间的信任关系，建立要在第二硬件部件202与云服务212之间被继承的信任关系。在一些示例中，处理器104可以在第二硬件部件202与云服务212之间建立信任关系，而无需通过使用其他已知的信任关系在第二硬件部件202与云服务212之间执行配对过程。

[0046] 在一些示例中，处理器104、204中的一个可以确定第一硬件部件102或第二硬件部件202是新的硬件部件。在这一点上，处理器104、204可以请求云服务212授权新的硬件部件的安装，并且基于来自云服务212的授权，可以在新的硬件部件与第一硬件部件102和第二硬件部件202中剩余的一个之间建立配对。

[0047] 在方法300中所提出的一些或所有操作可以作为实用程序、程序或子程序被包括在任何期望的计算机可访问介质中。此外，方法300可以由计算机程序来实施，计算机程序可以以各种活动和非活动两者的形式存在。例如，它们可以作为计算机可读指令(包括源代码、目标代码、可执行代码或其他格式)存在。以上的任何一个都可以被实施在非暂时性计算机可读存储介质上。

[0048] 非暂时性计算机可读存储介质的示例包括计算机系统RAM、ROM、EPROM、EEPROM以及磁盘或光盘或磁带。因此，应当理解的是，能够执行以上描述的功能的任何电子装置都可以执行以上列举的那些功能。

[0049] 现在参照图4，示出了非暂时性计算机可读介质400的框图，介质400具有存储在其上的授权第一硬件部件102和/或第二硬件部件202的操作的计算机可读指令。应当理解的是，在图4中所描绘的计算机可读介质400可以包括附加的指令，并且可以移除和/或修改在本文中所描述的指令中的一些，而不偏离在本文中所公开的计算机可读介质400的范围。计算机可读介质400可以是非暂时性的计算机可读介质。术语“非暂时性”不包括暂时性传播信号。

[0050] 计算机可读介质400可以具有存储在其上的计算机可读指令402至408，处理器(诸如在图1至图2中所描绘的处理器104、204)可以执行计算机可读指令402至408。计算机可读介质400可以是包含或存储可执行指令的电子、磁性、光学或其他物理存储装置。计算机可读介质400可以是例如随机存取存储器(RAM)、电可擦除可编程只读存储器(EEPROM)、存储装置或光盘等。

[0051] 处理器可以取得、解码并执行指令402，以在第一硬件部件102与第二硬件部件202之间共享识别信息。所共享的识别信息可以包括装置身份214、224，装置身份214、224可以包括装置标识符216、226和凭证218、228，以唯一地标识相应的硬件部件102、202。

[0052] 处理器可以取得、解码并执行指令404，以验证识别信息，从而在第一硬件部件102与第二硬件部件202之间建立信任关系。响应于确定在第一硬件部件102与第二硬件部件202之间已经建立了信任关系，处理器可以取得、解码并执行指令406，以验证第一硬件部件102的与第一授权的功能相关联的第一设置220和第二硬件部件202与第二授权的功能相关联的第二设置230。

[0053] 在一些示例中，与第一硬件部件102相关联的第一设置220和与第二硬件部件202

相关联的第二设置230可以是相同的。处理器可以将第一设置220与第二设置230进行比较，以验证第一设置220和第二设置230已经被保持。

[0054] 响应于第一设置220和第二设置230的成功验证，处理器可以取得、解码并执行指令408，以授权第一硬件部件102和/或第二硬件部件202的操作。在一些示例中，响应于第一硬件部件102与第二硬件部件202之间配对不成功，或者响应于确定第一设置220和第二设置230彼此不对应，处理器可以防止第一硬件部件102和/或第二硬件部件202的操作。

[0055] 尽管在整个本公开中具体描述了本公开的代表性示例，但是本公开的代表性示例具有广泛的应用，并且以上讨论并不旨在并且不应当被解释为限制，而是作为本公开的各方面的说明性讨论而被提供。

[0056] 在本文中已经描述和图示的是本公开及其一些变型的示例。在本文中所使用的术语、描述和附图是通过说明的方式提出的，而不表示限制。在本公开的范围内，多种变型都是可能的，本公开旨在由所附权利要求及其等同物来限定，其中所有术语都表示其最广泛的合理意义，除非另有说明。

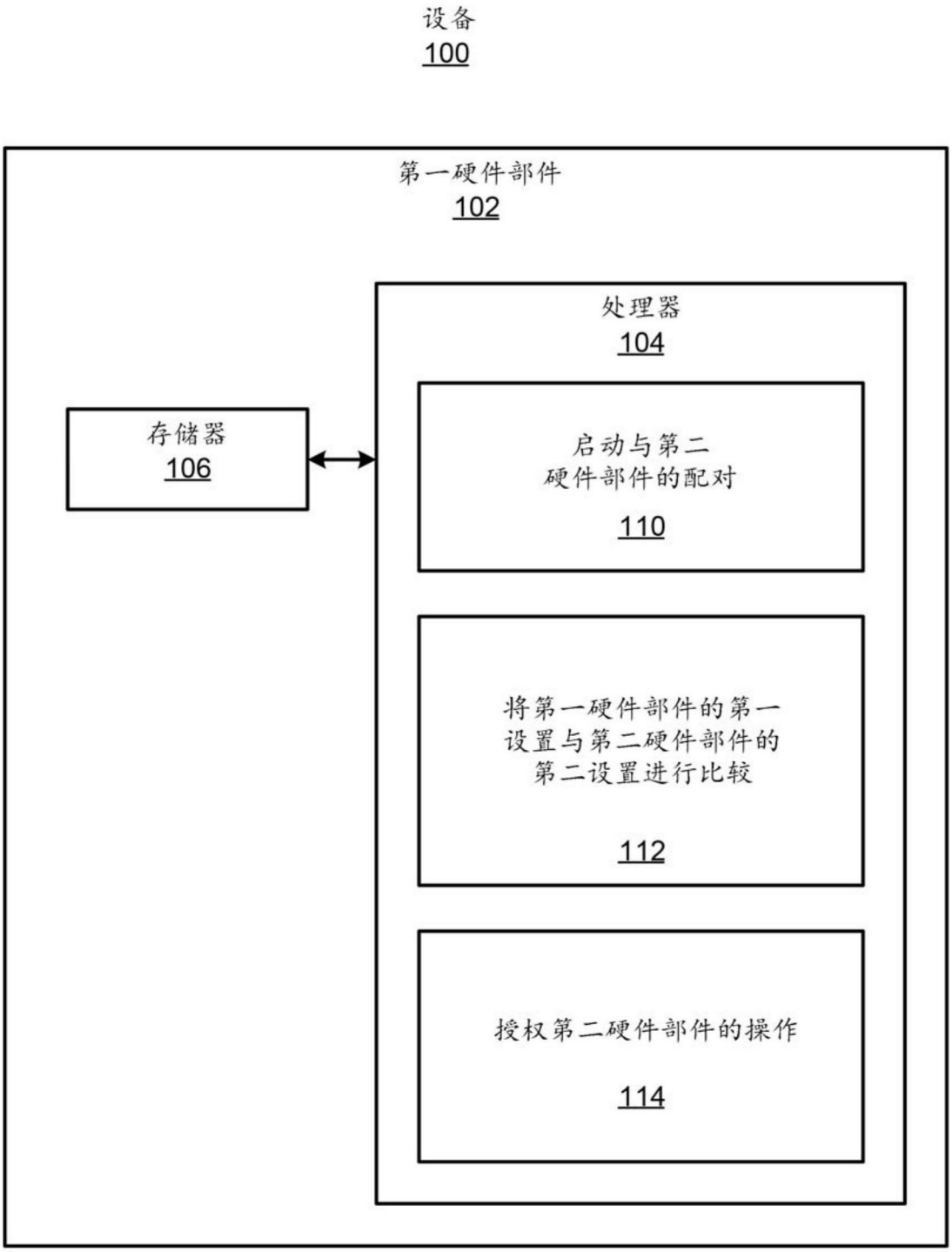

设备
100
第一硬件部件
102
处理器
104
存储器
106
启动与第二
硬件部件的配对
110
将第一硬件部件的第一
设置与第二硬件部件的
第二设置进行比较
112
授权第二硬件部件的操作
114

图1

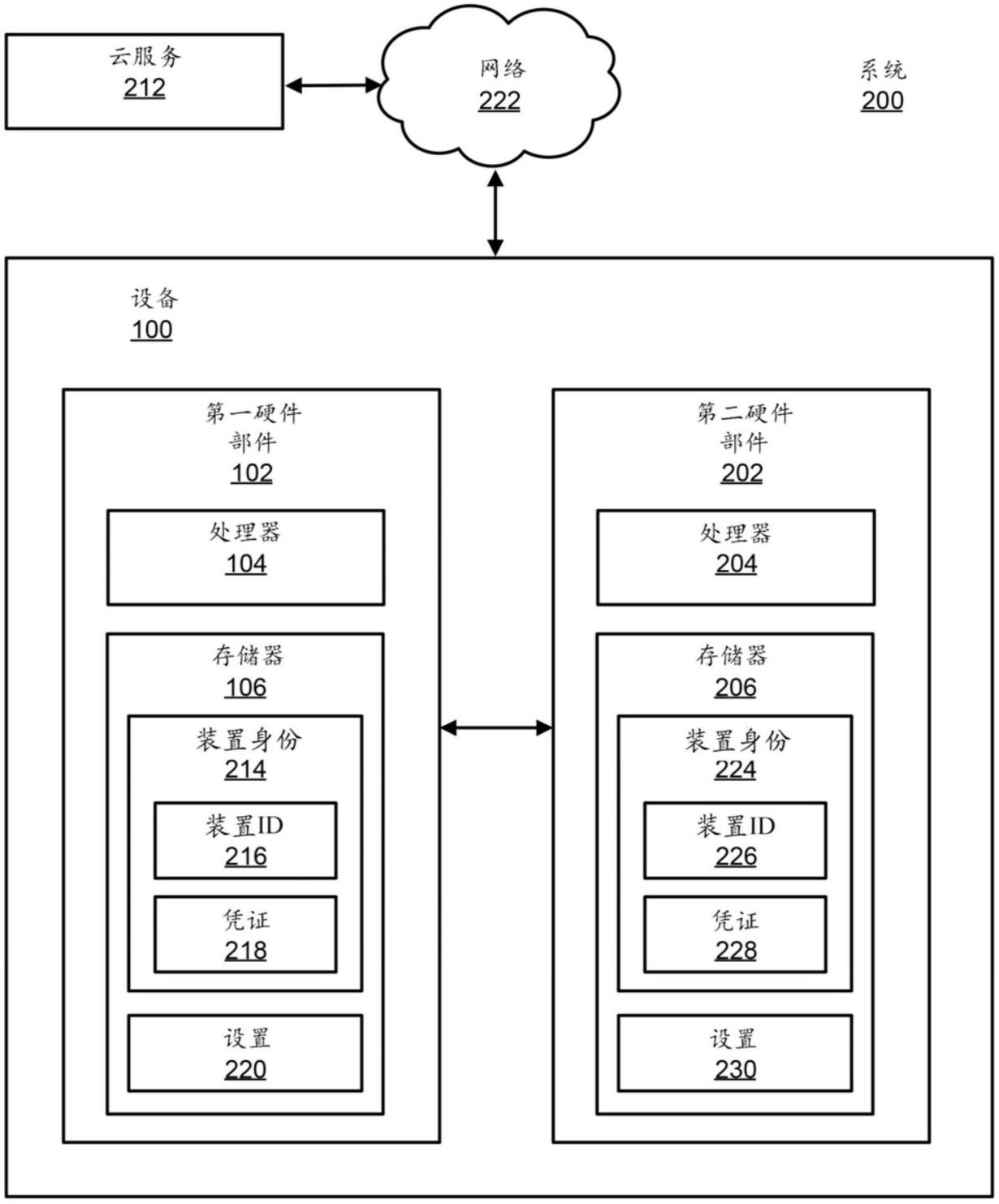

云服务
212
网络
222
系统
200
设备
100
第一硬件
部件
102
处理器
104
存储器
106
装置身份
214
装置ID
216
凭证
218
设置
220
第二硬件
部件
202
处理器
204
存储器
206
装置身份
224
装置ID
226
凭证
228
设置
230

图2

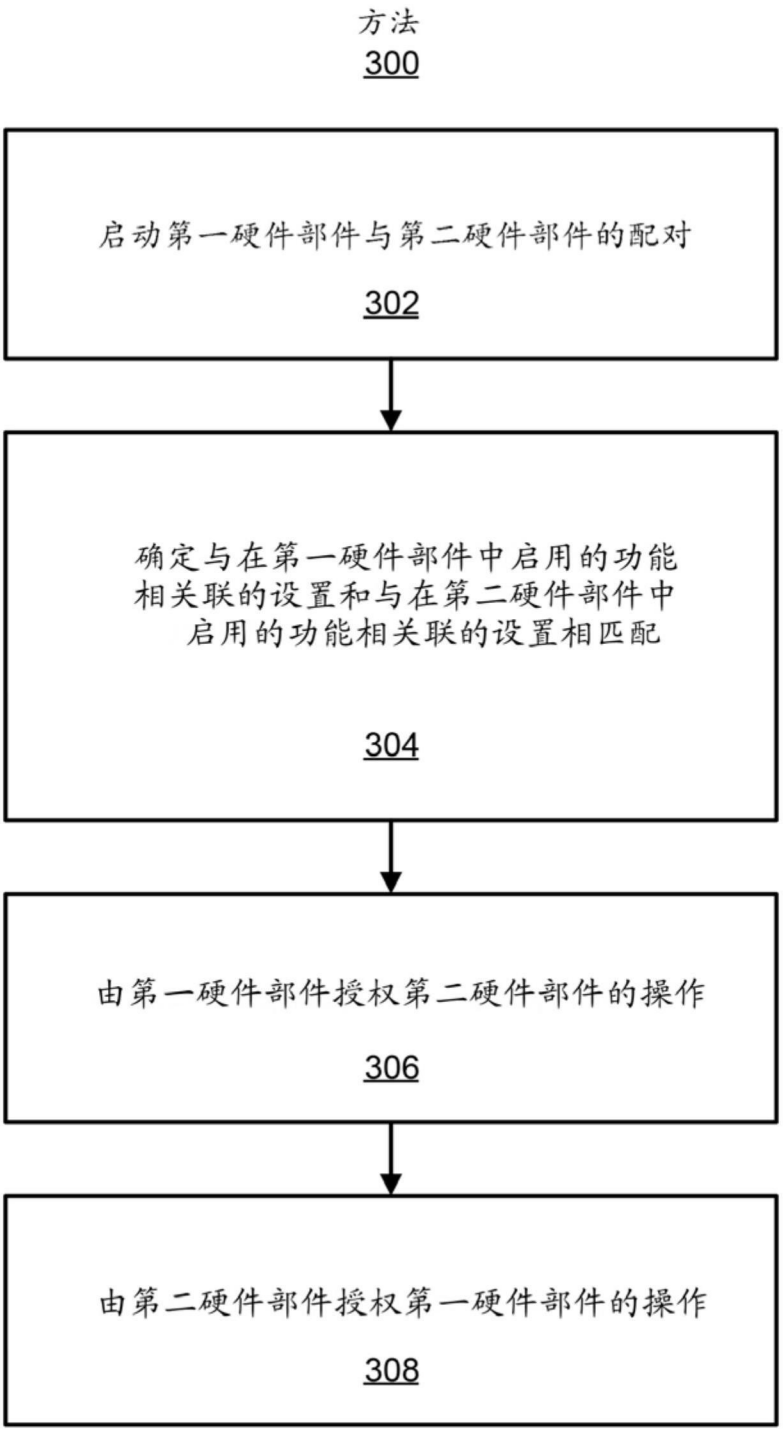

方法
300
启动第一硬件部件与第二硬件部件的配对
302
确定与在第一硬件部件中启用的功能相关联的设置和与在第二硬件部件中启用的功能相关联的设置相匹配
304
由第一硬件部件授权第二硬件部件的操作
306
由第二硬件部件授权第一硬件部件的操作
308

图3

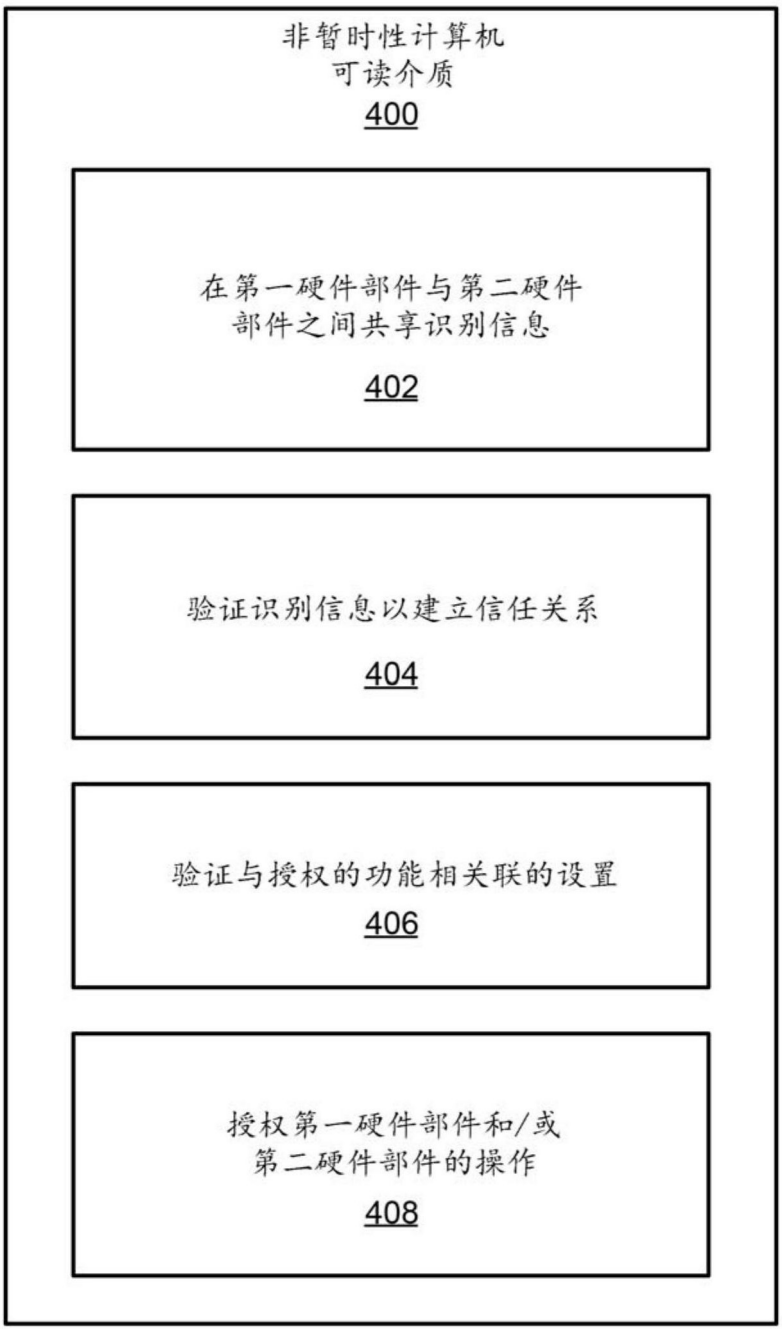

非暂时性计算机
可读介质
400
在第一硬件部件与第二硬件
部件之间共享识别信息
402
验证识别信息以建立信任关系
404
验证与授权的功能相关联的设置
406
授权第一硬件部件和/或
第二硬件部件的操作
408

图4