(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 119483991 A
(43)申请公布日 2025.02.18

(21)申请号 202311360054.4
(22)申请日 2018.05.28
(30)优先权数据
15/649,085 2017.07.13 US
(62)分案原申请数据
201880046669.0 2018.05.28
(71)申请人 微软技术许可有限责任公司
地址 美国华盛顿州
(72)发明人 S·辛哈 V·W·黑勒
(74)专利代理机构 永新专利商标代理有限公司 72002
专利代理师 赵腾飞
(51)Int.Cl.
H04L 9/40(2022.01)
H04L 9/00(2022.01)
H04L 9/08(2006.01)
H04L 9/32(2006.01)

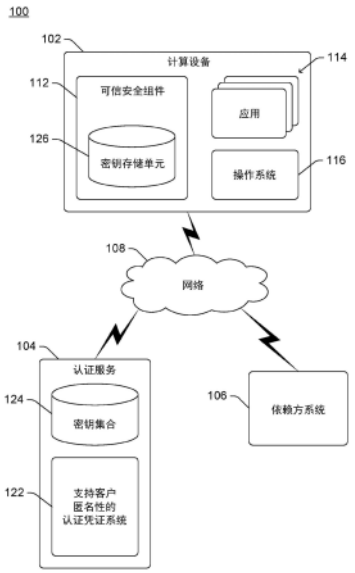
权利要求书3页 说明书14页 附图6页

(54)发明名称

提供设备匿名性的密钥认证声明生成

(57)摘要

一种计算系统,其向认证服务发送针对认证凭证的请求,以及与设备的硬件和/或软件相关的信息。认证服务处理该请求并且验证从所述设备接收的信息。在验证了该信息之后,认证服务从可重复使用的公钥/私钥对集合中选择公钥/私钥对,并且针对所述设备和公钥/私钥对中的公钥来生成认证凭证。该认证凭证由认证服务数字签名,并且被返回至该设备。所选择的公钥/私钥对中的私钥也被加密至该设备的可信安全组件,以确保该密钥不会被恶意软件偷取且在另一设备上重复使用,并且该密钥被返回至该设备。该设备使用该认证凭证来访问依赖方,并且可选地生成另外的公钥/私钥对和认证凭证。



CN 119483991 A

1.一种系统,包括:

处理器;以及

存储器,其被通信地耦合到所述处理器并且存储计算机可执行指令,所述计算机可执行指令当被运行时执行包括以下的操作:

向认证服务发送与设备相对应的认证凭证请求,所述认证凭证请求包括描述所述设备的硬件或软件中的至少一项的信息;

从所述认证服务接收第一公钥/私钥对和认证凭证,所述认证凭证将所述第一公钥/私钥对与所述设备的可信安全组件相关联;

将所述第一公钥/私钥对的私钥存储在所述可信安全组件的安全存储部中;以及

生成第二公钥/私钥对和第二认证凭证,所述第二认证凭证链接到所述认证服务。

2.根据权利要求1所述的系统,其中,所述第一公钥/私钥对是与由所述认证服务提供给多个其他设备的相同的公钥/私钥对。

3.根据权利要求1所述的系统,其中,所述计算机可执行指令执行还包括以下的操作:

针对由在所述设备上运行的网络浏览器访问的每个网站来生成一个或多个另外的公钥/私钥对和一个或多个另外的认证凭证。

4.根据权利要求1所述的系统,其中,所述计算机可执行指令执行还包括以下的操作:

针对由所述设备访问的多个不同的依赖方系统中的每个依赖方系统来生成一个或多个另外的公钥/私钥对和一个或多个另外的认证凭证。

5.根据权利要求1所述的系统,其中,所述计算机可执行指令执行还包括以下的操作:

使用所述可信安全组件的私钥来解密从所述认证服务接收的所述第一公钥/私钥对。

6.根据权利要求1所述的系统,其中,所述可信安全组件包括可信平台模块。

7.一种在其上记录有程序指令的计算机可读存储设备,所述程序指令当由计算设备运行时执行包括以下操作的方法:

向认证服务发送与所述计算设备相对应的认证凭证请求,所述认证凭证请求包括描述设备硬件和/或软件的信息;

从所述认证服务接收包括私钥的公钥/私钥对和认证凭证,所述认证凭证将所述公钥/私钥对与设备可信安全组件相关联;

将所述私钥存储在所述设备可信安全组件的安全存储部中;以及

在所述存储之后并且在所述计算设备处,基于从所述认证服务接收的所述公钥/私钥对来生成一个或多个另外的公钥/私钥对和一个或多个另外的认证凭证,所述另外的认证凭证中的每个认证凭证链接到所述认证服务。

8.根据权利要求7所述的计算机可读存储设备,其中,所接收的公钥/私钥对是与由所述认证服务向多个其他设备提供的相同的公钥/私钥对。

9.根据权利要求7所述的计算机可读存储设备,其中,所述方法还包括:针对由在所述计算设备上运行的网络浏览器访问的每个网站来生成以下中的一项:所述一个或多个另外的公钥/私钥对和一个或多个另外的认证凭证。

10.根据权利要求7所述的计算机可读存储设备,其中,所述方法还包括:针对由所述计算设备访问的多个不同的依赖方系统中的每个依赖方系统来生成以下中的一项:所述一个或多个另外的公钥/私钥对和一个或多个另外的认证凭证。

11.根据权利要求7所述的计算机可读存储设备,其中,所述方法还包括:使用所述设备可信安全组件的私钥来解密从所述认证服务接收的所述公钥/私钥对。

12.根据权利要求7所述的计算机可读存储设备,其中,所述设备可信安全组件包括可信平台模块。

13.根据权利要求7所述的计算机可读存储设备,其中,所述方法还包括:将所生成的一个或多个另外的公钥/私钥对的另外的私钥存储在所述设备可信安全组件的所述安全存储部中。

14.一种在其上记录有程序指令的计算机可读存储设备,所述程序指令当由至少一个处理器运行时执行认证服务中的方法,所述方法包括:

从第一计算设备接收与所述第一计算设备相对应的第一认证凭证请求,所述第一认证凭证请求包括描述第一计算设备硬件和/或软件的信息;

验证所接收的信息;

从非对称密钥对集合中选择非对称密钥对,所选择的非对称密钥对也同时与多个另外的计算设备中的每个计算设备相关联,所述多个另外的计算设备被提供有所选择的非对称密钥对中被加密的私钥;

生成第一认证凭证,所述第一认证凭证与所述第一计算设备相对应并且将所选择的非对称密钥对的公钥与所述第一认证凭证相关联;

对专用于所述第一计算设备的所述私钥进行加密;以及

将经加密的私钥和所述第一认证凭证返回到所述第一计算设备。

15.根据权利要求14所述的计算机可读存储设备,其中,在所述方法中,对专用于所述第一计算设备的所述私钥进行加密包括:使用第一计算设备可信安全组件的公钥/私钥对的公钥来加密所选择的非对称密钥对的所述私钥。

16.根据权利要求14所述的计算机可读存储设备,其中,在所述方法中,选择所述非对称密钥对包括:从所述非对称密钥对集合中随机地或者伪随机地选择所述非对称密钥对。

17.根据权利要求14所述的计算机可读存储设备,其中,所述方法还包括:在接收到所述第一认证凭证请求之前,在所述非对称密钥对集合中生成非对称密钥对。

18.根据权利要求14所述的计算机可读存储设备,其中,所述方法还包括:以一个或多个间隔改变所述非对称密钥对集合中的非对称密钥对。

19.根据权利要求14所述的计算机可读存储设备,其中,所述方法还包括:

从第二计算设备接收与所述第二计算设备相对应的第二认证凭证请求,所述第二认证凭证请求包括描述第二计算设备硬件和/或软件的另外的信息;

验证所接收的另外的信息;

从所述非对称密钥对集合中选择先前针对所述第一计算设备选择的所述非对称密钥对;

生成与所述第二计算设备相对应并且将所述公钥与所述第二认证凭证相关联的第二认证凭证;

对专用于生成另外的加密私钥的所述第二计算设备的所述私钥进行加密;以及

向所述第二计算设备返回所述另外的加密私钥和所述第二认证凭证。

20.根据权利要求14所述的计算机可读存储设备,其中,所述第一认证凭证不具有所述

第一计算设备的名称或标识符。

提供设备匿名性的密钥认证声明生成

[0001] 本申请是2018年05月25日提交的申请号为201880046669.0、名称为“提供设备匿名性的密钥认证声明生成”的发明专利申请的分案申请。

背景技术

[0002] 计算设备之间的互连变得越来越紧密,这使得为这些设备的用户提供大量信息和/或功能的服务对这些设备可用。所述信息和功能的可用性对用户是有帮助的,但也存在一些问题。一个这样的问题是,用户通常也希望保持其隐私。然而,访问这些服务可能涉及对用户和/或用户的设备的至少一些识别,如果这些识别传播到其他服务或与其他服务共享,则会降低用户具有的隐私性。这可能会导致用户对他们的设备和/或他们所访问的服务不满意。

发明内容

[0003] 提供了该发明内容以用简化形式引入对在以下的具体实施方式中进一步描述的概念的选择。该发明内容不旨在标识所要求保护的主题的关键特征或必要特征,也不旨在用来帮助确定所要求保护的主题的范围。

[0004] 根据一个或多个方面,在认证服务中,从计算设备接收针对计算设备的认证凭证的请求。该请求包括描述计算设备的硬件和/或软件的信息。对所接收的信息进行验证,并且从非对称密钥对集合中选择非对称密钥对,所选择的密钥对也被选择用于多个另外的计算设备。生成计算设备的认证凭证,该认证凭证将所选择的密钥对中的公钥与该认证凭证相关联。所选择的密钥对中的私钥是针对第一计算设备而被加密的。将所选择的密钥对中的经加密的私钥以及认证凭证返回至该第一计算设备。

[0005] 根据一个或多个方面,在计算设备中,针对计算设备的认证凭证的请求被发送至认证服务,该请求包括描述计算设备的硬件和/或软件的信息。从认证服务接收公钥/私钥对以及将该公钥/私钥对与计算设备的可信安全组件相关联的认证凭证。公钥/私钥对中的私钥被存储在可信安全组件的安全存储部中。在不访问认证服务的情况下,生成一个或多个另外的公钥/私钥对和一个或多个另外的认证凭证,其中每个另外的认证凭证都向上链接至认证服务。

附图说明

[0006] 参考附图描述了具体实施方式。在附图中,附图标记中最左边的数字标识了该附图标记第一次出现的图。在描述和图中的不同实例中所使用的相同的附图标记可以指示相似或相同的项。在图中所表示的实体可以指示一个或多个实体,并且因此,以下讨论中的实体的单数或复数形式是以可互换的方式来引用的。

[0007] 图1示出了根据一个或多个实施例的、实现提供设备匿名性的密钥认证声明生成的示例系统。

[0008] 图2示出了根据一个或多个实施例的示例认证服务。

[0009] 图3示出了根据一个或多个实施例的示例可信安全组件。

[0010] 图4是示出了根据一个或多个实施例的、用于实现提供设备匿名性的密钥认证声明生成的示例过程的流程图。

[0011] 图5是示出了根据一个或多个实施例的、用于实现提供设备匿名性的密钥认证声明生成的另一示例过程的流程图。

[0012] 图6示出了包括示例计算设备的示例系统,该示例计算设备代表可以实现在本文中所描述的各种技术的一个或多个系统和/或设备。

具体实施方式

[0013] 在本文中讨论了提供设备匿名性的密钥认证声明生成。为了让计算设备访问需要该计算设备是其所声称的设备的证明的系统,计算设备从可信的第三方获得认证凭证。该可信的第三方也被称为认证服务或凭证机构。计算设备向认证服务发送针对认证凭证的请求,以及与该计算设备的硬件和可选地在计算设备上运行的软件相关的信息。该信息来自计算设备的可信安全组件,并且因此能够由该认证服务信任。计算设备还将加密密钥中的公钥发送至该认证服务。该加密密钥是驻留在计算设备的可信安全组件中的非对称密钥对,这确保加密密钥中的私钥不能够被来自计算设备和在其他地方使用的恶意软件所获得。

[0014] 认证服务处理认证凭证请求并验证从计算设备所接收的信息。该验证可以包括各种动作,例如验证计算设备包括特定的硬件,验证特定的软件正在计算设备上运行,等等。在认证服务验证了认证凭证请求的硬件和/或软件属性之后,认证服务确保所述属性是真实的,因此其可以通过以下归纳来验证:如果真实的属性证明了属于可信安全组件的加密密钥的存在,则加密至加密密钥中的公钥的任何内容仅能够由该可信安全组件来解密。

[0015] 认证服务保存可重用的公钥/私钥对集合。在验证了从计算设备所接收的信息之后,认证服务从可重用的所述公钥/私钥对集合中选择公钥/私钥对,并且针对计算设备和公钥/私钥对中的公钥而生成认证凭证。该认证凭证由认证服务进行数字签名,以保证所选择的公钥/私钥对中的公钥与计算设备的可信安全组件相关联。因此,该认证凭证也被称为认证声明或密钥认证声明。

[0016] 认证服务将认证凭证连同所选择的公钥/私钥对中的私钥一起返回至计算设备。私钥是利用绑定到计算设备的可信安全组件的密钥来加密的,这允许将私钥安全地传输至计算设备的可信安全组件。所述可信安全组件接收并存储该认证凭证以及该公钥/私钥对。

[0017] 当随后与期望该计算设备是其声称的实体的证明的依赖方进行通信时,可信安全组件向该依赖方提供拥有认证凭证和公钥/私钥对的证明。该证明可以以各种方式来提供,例如通过使用公钥/私钥对中的私钥来对由依赖方提供至可信安全组件的数据值(例如,随机数(nonce)进行数字签名。

[0018] 认证服务可以并且确实从公钥/私钥对集合中为请求认证凭证的多个不同计算设备选择了相同的公钥/私钥对。由此,多个不同的计算设备将同时使用相同的公钥/私钥对。允许多个不同的计算设备具有相同的公钥/私钥对防止不同的依赖方相互勾结并且确定特定计算设备的身份。例如,如果两个不同的依赖方由使用相同的公钥/私钥对和认证凭证的一个或多个计算设备来访问,则这两个不同的依赖方无法知道是相同的计算设备访问他们

两者还是两个不同的计算设备被给予了相同的公钥/私钥对。这为计算设备提供了匿名性，因为依赖方不能够串通和共享与特定计算设备相关的信息，这是由于依赖方不能够确保它们在与同一计算设备进行通信。

[0019] 另外地，可信安全组件可以可选地使用从认证服务所接收的公钥/私钥对来生成其自己的公钥/私钥对和向上链接至认证服务的认证凭证。这允许可信安全组件生成新的公钥/私钥对和认证凭证，以供不同的依赖方使用。此外，这些新的公钥/私钥对中的每一个公钥/私钥对向上链接至认证服务中之前被提供至多个不同的计算设备的密钥，因此这允许可信安全组件快速地生成新的公钥/私钥对(而无需访问认证服务)，同时仍然提供为不同的计算设备选择同一公钥/私钥对的匿名性。

[0020] 在本文中引用了对称密钥加密、公钥加密、和公钥/私钥对。尽管这样的密钥加密对于本领域技术人员而言是公知的，但在这里包括对这样的加密的简要概述以帮助读者。在公钥加密(也被称为非对称公钥/私钥对加密)中，实体(例如，用户、硬件或软件组件、设备、域等等)将公钥/私钥对与之相关联。该公钥/私钥对也被称为非对称密钥对。公钥可以被使得公开可获得，但是实体将私钥保密。没有私钥，在计算上难以将使用公钥加密的数据解密。因此，数据能够由任何实体利用公钥来加密，并且仅能够由实体利用对应的私钥来解密。另外地，可以通过使用数据和私钥来生成该数据的数字签名。在没有私钥的情况下，在计算上难以创建能够使用公钥来验证的签名。具有公钥的任何实体可以通过以下操作来使用该公钥验证该数字签名:对该公钥、签名、和被签名的数据执行合适的数字签名验证算法。

[0021] 另一方面，在对称密钥加密中，共享的密钥(也被称为对称密钥)为两个实体所知道和保密。具有共享的密钥的任何实体通常都能够解密利用该共享的密钥加密的数据。没有该共享的密钥，在计算上难以解密利用该共享的密钥加密的数据。因此，如果两个实体都知道该共享的密钥，则每个实体都可以加密能够由另一个实体解密的数据，但是其他实体在其不知道该共享的密钥的情况下则不能够解密该数据。类似地，具有共享的密钥的实体能够加密能够由该同一实体解密的数据，但其他实体在其不知道该共享的密钥的情况下则不能够解密该数据。另外地，可以基于对称密钥加密来生成数字签名，例如使用密钥散列(keyed-hash)消息验证码机制。具有共享的密钥的任何实体都可以生成和验证数字签名。例如，可信的第三方可以基于特定实体的身份来生成对称密钥，并且接着可以生成且验证该特定实体的数字签名(例如，通过使用对称密钥来对数据进行加密或解密)。

[0022] 图1示出了根据一个或多个实施例的、实现提供设备匿名性的密钥认证声明生成的示例系统100。系统100包括计算设备102，其可以经由网络108与认证服务104和依赖方系统106进行通信。网络108可以是多种不同的网络，包括互联网、局域网(LAN)、电话网络、内联网、其他公共和/或专用网络、其组合，等等。

[0023] 计算设备102可以是多种不同类型的设备。例如，计算设备102可以是台式计算机、服务器计算机、膝上型或上网本计算机、移动设备(例如，平板计算机或平板电话设备、蜂窝或其他无线电话(例如，智能电话)、笔记本计算机、移动站)、可穿戴设备(例如，眼镜、头戴显示器、手表、手环、增强现实(AR)设备、虚拟现实(VR)设备)、娱乐设备(例如，娱乐家电、与显示设备可通信地耦合的机顶盒、游戏机)、物联网设备(例如，带有允许与其他设备通信的软件、固件、和/或硬件的对象或事物)、电视机或其他显示设备、汽车计算机等。因此，计算

设备102的范围可以从具有大量存储器和处理器资源的满资源设备(例如,个人计算机、游戏机)到具有有限存储器和/或处理资源的低资源设备(例如,传统机顶盒、手持游戏机)。

[0024] 认证服务104是由相同或不同类型的一个或多个计算设备实现的服务或系统。与对计算设备102的讨论类似,认证服务104可以由多种不同类型的设备实现,所述设备的范围从具有大量存储器和处理器资源的满资源设备到具有有限存储器和/或处理资源的低资源设备。

[0025] 依赖方系统106是由相同或不同类型的一个或多个计算设备实现的。与对计算设备102的讨论类似,依赖方系统106可以由多种不同类型的设备实现,所述设备的范围从具有大量存储器和处理器资源的满资源设备到具有有限存储器和/或处理资源的低资源设备。

[0026] 图1示出了示例系统100,其具有单个计算设备102、单个认证服务104、和单个依赖方系统106。然而,应当注意的是,系统100可以包括多个计算设备102、多个认证服务104、和/或多个依赖方系统106。

[0027] 计算设备102包括可信安全组件112、一个或多个应用114、和操作系统116。可信安全组件112是认证服务104认为可信的组件。可信安全组件112将在下文更加详细地被讨论,并且其可以包括特定的硬件组件、特定的软件组件、以特定的方式或顺序对计算设备102的加载或启动,等等。

[0028] 操作系统116包括向计算设备102提供各种功能的一个或多个程序,所述功能包括促进与计算设备102的硬件组件的通信。可以在操作系统116上运行一个或多个应用114,例如娱乐应用、教育应用、生产力应用等等。操作系统116和/或应用114的程序可以访问依赖方系统106。尽管被示出为与可信安全组件112是分开的,但一个或多个应用114可以被包括在可信安全组件112中,和/或操作系统116的至少一部分可以被包括在可信安全组件112中。

[0029] 依赖方系统106可以是向计算设备102提供信息或功能的多种不同系统中的任何一种。这些可以例如是允许计算设备102访问各种不同类型的娱乐内容(例如,音频和/或视频内容)的系统,允许计算设备102运行各种教育或生产力应用的系统,允许计算设备102访问安全或机密信息的系统,等等。

[0030] 为了访问依赖方系统106,可信安全组件112从认证服务104获得认证凭证。在一个或多个实施例中,在本文中所讨论的认证凭证是根据X.509凭证标准(例如,针对评论的网络工作组请求1422(1993年2月))的X.509凭证。可信安全组件112向认证服务104发送认证凭证请求,其包括描述计算设备102的信息,该信息包括描述可信安全组件112的信息。

[0031] 认证服务104包括支持客户端匿名性的认证凭证系统122和密钥集合124。密钥集合124是多个公钥/私钥对集合。密钥集合124可以以多种不同的方式被保存,例如在存储设备(例如,磁驱动器、固态驱动器)中或在其他存储器(例如,随机存取存储器(RAM))中。支持客户端匿名性的认证凭证系统122从可信安全组件112接收认证凭证请求,并且验证作为该认证凭证请求的一部分所接收的信息。该验证将在下文更加详细地被讨论,并且可以包括各种动作,例如验证计算设备包括特定的硬件、验证特定的软件正在计算设备上运行等等。基于可信安全组件112被实现的方式,验证被执行的方式可以有所不同。

[0032] 如果支持客户端匿名性的认证凭证系统122不能够验证作为认证凭证请求的一部

分所接收的信息,则支持客户端匿名性的认证凭证系统122就不向计算设备102发出认证凭证。然而,如果支持客户端匿名性的认证凭证系统122验证了作为认证凭证请求的一部分所接收的信息,则支持客户端匿名性的认证凭证系统122从密钥集合124中选择公钥/私钥对并且为计算设备102生成认证凭证。该认证凭证将可信安全组件112与所选择的公钥/私钥对相关联,并且由支持客户端匿名性的认证凭证系统122进行数字签名。

[0033] 支持客户端匿名性的认证凭证系统122将该认证凭证连同所选择的公钥/私钥对中的私钥一起返回至计算设备102。支持客户端匿名性的认证凭证系统122利用绑定到可信安全组件112的密钥(例如,可信安全组件112的公钥/私钥对中的公钥)来对私钥进行加密,以允许所选择的公钥/私钥对中的私钥被安全地传输至可信安全组件112。可信安全组件112接收认证凭证和公钥/私钥对并将其存储在密钥存储单元126中。

[0034] 计算设备102可以通过向依赖方系统106提供已由认证服务104向可信安全组件112发布了认证凭证的证明来使用依赖方系统106。已知为计算设备102选择的认证凭证和公钥/私钥对,该证明可以以各种不同的方式被提供至依赖方系统106。例如,依赖方系统106可以向可信安全组件112提供随机数,并且可信安全组件112使用从认证服务104所接收的公钥/私钥对中的私钥来对该随机数进行数字签名。认证凭证上的认证服务104的数字签名可以由依赖方系统106使用认证服务104的公钥来验证。该随机数上的数字签名也可以由依赖方系统106使用包括在认证凭证中的公钥来验证,由此向依赖方系统106证明:认证凭证(和该认证凭证所引用的公钥)是由认证服务104提供至计算设备102的。

[0035] 依赖方系统106可选地包括各种另外的检查或验证,以便允许计算设备102使用依赖方系统106。例如,依赖方系统106可以施加以下约束:计算设备102的可信安全组件112必须至少是特定的版本号。

[0036] 图2示出了根据一个或多个实施例的示例认证服务104。认证服务104包括支持客户端匿名性的认证凭证系统122和密钥集合124。支持客户端匿名性的认证凭证系统122包括通信模块202、验证模块204、密钥选择模块206、和认证凭证生成模块208。

[0037] 通信模块202从图1的计算设备102接收针对认证凭证的请求。尽管参考图1中的计算设备102进行了讨论,但应当注意的是,认证服务104可以并且通常也确实从多个不同计算设备102接收针对认证凭证的请求。如上文所讨论的,该请求包括描述计算设备102的信息。

[0038] 验证模块204验证描述计算设备102的信息。从计算设备102所接收的具体信息可以有所不同,并且验证模块204验证描述计算设备102的信息的方式也至少部分地基于可信安全组件112被实现方式而有所不同。

[0039] 返回图1,通常实现可信安全组件112以使得可信安全组件112包括允许计算设备102在认证服务104信任的状态下运行的硬件和/或软件。认证服务104信任的状态是针对可能攻击计算设备102的恶意软件得到保护的状态,其允许认证服务104确保认证服务104与计算设备102(或计算设备102的可信安全组件112)而不是冒充计算设备102和/或可信安全组件112等的另一设备进行通信。

[0040] 在一个或多个实施例中,可信安全组件112包括作为可信平台模块(TPM)的安全加密处理器。TPM包括各种功能,例如密钥生成、加密、解密、安全存储(例如,平台配置寄存器)等。在一个或多个实施例中,TPM符合可信计算组可信平台模块规范版本2.0,其是作为可信

平台模块库规范、系列“2.0”、级别00、修订01.16(2014年10月30日)、第1-4部分发布的。尽管在本文中对TPM进行了引用,但可信安全组件112可以可替代地使用提供类似于TPM的功能的一个或多个其他加密处理器。

[0041] 可信安全组件112具有相关联的公钥/私钥对。这允许其他设备或组件使用可信安全组件的公钥/私钥对中的公钥来加密数据,以使得只有可信安全组件112能够解密该数据。在一个或多个实施例中,可信安全组件112只有在计算设备102已经引导到特定模式中或以特定顺序引导了加载软件的情况下,才能够从TPM获取其相关联的公钥/私钥对。这为可信安全组件112提供了另外的保护,以允许可信安全组件112仅在计算设备已经引导到特定的已知模式(例如,安全或可信模式)中或引导有特定的软件(例如,没有恶意软件)的情况下,才能够访问其相关联的公钥/私钥对。

[0042] 在一个或多个实施例中,伴随针对认证凭证的请求的描述计算设备102的信息指示计算设备102的健康(或健康认证)。可以以多种方式来指定计算设备的健康102,例如,对哪个模块在引导计算设备102时被加载的指示,对特定的模块或功能是否在引导计算设备102时被加载的指示,对计算设备102是否在特定的模式中(例如,在安全引导模式中)被引导的指示,对特定的安全特性是打开的还是关闭的指示,对虚拟安全模式(VSM)是否在计算设备102中运行(例如,作为可信安全组件112的一部分)的指示,等等。

[0043] 另外地或可替代地,伴随针对认证凭证的请求的描述计算设备102的信息指示可信安全组件112是受认证服务104(也被称为密钥认证)信任的组件(例如,硬件组件)。可信安全组件112可以具有公钥/私钥对,并且该公钥/私钥对中的公钥可以是认证服务104已知的。因此,可信安全组件112可以通过使用可信安全组件112的公钥/私钥对中的私钥来对一个值(例如,随机数)进行数字签名从而提供其的确是可信安全组件112的指示。

[0044] 返回图2,验证模块204验证伴随针对认证凭证的请求的描述计算设备102的信息。例如,针对健康认证,验证模块204可以验证从计算设备102所接收的信息指示:特定的模块在引导计算设备102时被加载,计算设备102在特定的模式中(例如,在安全引导模式中)被加载,特定的安全特性是打开的还是关闭的,等等。作为另一示例,针对密钥认证,验证模块204可以验证由可信安全组件112数字签名的值(例如,随机数)上的数字签名。

[0045] 如果验证模块204没有验证从计算设备102所接收的信息,则没有为计算设备102选择密钥并且没有为计算设备102生成认证凭证。然而,如果验证模块204确实验证了从计算设备102所接收的信息,则密钥选择模块206从密钥集合124中选择非对称密钥对(公钥/私钥对)。该选择可以是随机地、伪随机地、或者是根据其他各种规则或标准被执行的。

[0046] 密钥集合124可以具有任何数量的非对称密钥对,例如数十、数百、数千、或更多。密钥集合124中的非对称密钥对可以是先前生成(例如,在从计算设备102接收到针对认证凭证的请求之前由密钥选择模块206或认证服务104的另一模块生成)的,并且被保存在密钥集合124中,接着当密钥选择模块206期望时从中选择。在密钥集合124中包括的非对称密钥对的数量可以基于各种不同的因素而不同。在一个或多个实施例中,在密钥集合124中包括的非对称密钥对的数量是通过以下方式来确定的:将计算设备的匿名性针对在密钥受到威胁(例如,被恶意软件发现或潜在地发现)的事件中无效认证凭证的需要进行平衡。例如,较少的非对称密钥对引起计算设备的增加的匿名性,这是因为较多的计算设备得到相同的非对称密钥对,但是也引起对在非对称密钥对受到威胁的事件中无效大量认证凭证的需

要,这是因为大量的计算设备接收了受到威胁的非对称密钥对。

[0047] 还应当注意的是,在密钥集合124中包括的非对称密钥对可以随着时间改变。例如,密钥选择模块206可以生成新的非对称密钥对,以定期或不定期地将其添加至密钥集合124,并且可以定期或不定期地从密钥集合124中删除非对称密钥对。

[0048] 认证凭证生成模块208生成这样的凭证,其将该凭证与所选择的公钥/私钥对中的公钥相关联。认证凭证还将可信安全组件112(和/或计算设备102)与所选择的公钥/私钥对中的公钥相关联。该关联例如是通过以下方式执行的:认证包括所选择的公钥/私钥对中的公钥,以及所选择的公钥/私钥对中的私钥被安全地提供至可信安全组件112(例如,使用可信安全组件112的密钥加密的)。为了保持可信安全组件112(和/或计算设备102)的匿名性,不需要将可信安全组件112和/或计算设备102的名称或其他标识符包括在所生成的凭证中。认证凭证生成模块208使用认证服务104的公钥/私钥对中的公钥来对凭证进行数字签名,以创建这样的认证凭证,该认证凭证允许依赖方知道认证服务104验证了可信安全组件112,并且给予了可信安全组件112所选择的公钥/私钥对。

[0049] 通信模块202将认证凭证以及由密钥选择模块206所选择的公钥/私钥对中的私钥返回至可信安全组件112。所选择的公钥/私钥对中的私钥被加密(例如,使用可信安全组件112的公钥/私钥对中的公钥),以使得私钥被安全地传输至可信安全组件112,并且不能够由任何窃听或其他中间设备读取。认证凭证也可以但不需要被加密,以便被安全地传输至可信安全组件112。

[0050] 因此,由认证凭证生成模块208生成的认证凭证包括所选择的公钥/私钥对中的公钥。认证凭证由认证凭证生成模块208进行数字签名,以证明所选择的公钥/私钥对中的公钥是与该认证凭证一起被给出的。接着,将所选择的公钥/私钥对中的私钥安全地提供至可信安全组件112。当计算设备102随后期望访问依赖方104时,依赖方104可以向计算设备的可信安全组件112提供随机数。可信安全组件112使用所选择的公钥/私钥对中的私钥来对随机数进行数字签名,并且将经签名的随机数以及认证凭证发送至依赖方104。依赖方104使用认证服务104的公钥来验证认证凭证生成模块208确实对认证凭证进行了数字签名(并且因此给出该认证凭证)。此外,依赖方104可以使用认证凭证中的公钥来验证随机数被认证服务104所信任的可信安全组件进行了数字签名(因为可信安全组件112将仅具有私钥,该私钥是与认证中的公钥相同的公钥/私钥对的一部分,如果认证服务信任可信安全组件112并且将私钥给予可信安全组件112的话)。因此,依赖方104可以验证可信安全组件112受到认证服务104的信任,但是依赖方104所依赖的凭证不需要具有特定的可信安全组件112和/或计算设备102的名称或其他标识符。

[0051] 图3示出了根据一个或多个实施例的示例可信安全组件112。可信安全组件112包括密钥存储单元126、认证凭证获取模块302、认证凭证生成模块304、密钥生成模块306、和凭证存储单元308。

[0052] 认证凭证获取模块302与认证服务104进行通信,以发送针对认证凭证的请求,并且从认证服务104接收认证凭证和经加密的私钥。从认证服务104所接收的公钥/私钥对(或至少是公钥/私钥对中的私钥)被存储在密钥存储单元126中。从认证服务104所收的认证凭证也被存储在凭证存储单元308中。密钥存储单元126是仅能够由可信安全组件112的模块访问的安全存储部。凭证存储单元308可以但不一定是安全存储部。另外地或可替代地,认

证凭证可以被存储在可信安全组件112的外部。

[0053] 可信安全组件112受到认证服务104的信任,并且因此,认证凭证生成模块304也可以生成认证凭证。密钥生成模块306使用多种公共或专用技术中的任何一种来生成公钥/私钥对。认证凭证生成模块304生成这样的凭证,其将该凭证与新生成的公钥/私钥对中的公钥相关联。认证凭证还可以将可信安全组件112(和/或计算设备102)与由密钥生成模块306新生成的公钥/私钥对中的公钥相关联。例如,该关联是通过以下方式执行的:认证包括新生成的公钥/私钥对中的公钥,并且新生成的公钥/私钥对中的私钥由可信安全组件112安全地保存(例如,存储在密钥存储单元126中)。为了保持可信安全组件112(和/或计算设备102)的匿名性,在新生成的凭证中不需要包括可信安全组件112和/或计算设备102的名称或其他标识符。认证凭证生成模块304使用从认证服务104所接收的公钥/私钥对中的公钥来对凭证进行数字签名以创建认证凭证,该认证凭证向上链接至认证服务104并且因此允许依赖方知道认证服务104验证了可信安全组件112。此外,因为由认证凭证生成模块304所生成的认证凭证是使用从认证服务104所接收的公钥/私钥对中的公钥进行数字签名的并且基于该公钥而链接至认证服务104,并且多个不同的计算设备将接收该相同的公钥并且基于该相同的公钥生成认证凭证,尽管计算设备102生成了其自己的认证凭证,但仍然保持了计算设备102的匿名性。

[0054] 由密钥生成模块306所生成的公钥/私钥对(或至少是公钥/私钥对中的私钥)被存储在密钥存储单元126中。由认证凭证生成模块304所生成的认证凭证被存储在凭证存储单元308中。

[0055] 认证凭证生成模块304和密钥生成模块306可以根据需要生成新的密钥和认证凭证。这允许在不针对每个新的密钥和认证凭证访问网络108和认证服务104的情况下生成新的密钥和认证凭证,以减少获得新的密钥和认证凭证所需的时间量。作为示例,可以为由计算设备102所访问的每个新的依赖方系统106、为由在计算设备102上运行的网络浏览器所访问的每个新的网站等来生成新的公钥/私钥对和认证凭证。

[0056] 图4是示出了根据一个或多个实施例的、用于实现提供设备匿名性的密钥认证声明生成的示例过程400的流程图。过程400是由认证服务(例如,图1或图2的认证服务104)实行的,并且可以在软件、固件、硬件或其组合中被实现。过程400被示出为一组动作,并且不限于用于执行各种动作的操作所示出的顺序。过程400是用于实现提供设备匿名性的密钥认证声明生成的示例过程;在本文中参考不同的附图而包括对实现提供设备匿名性的密钥认证声明生成的另外的讨论。

[0057] 在过程400中,接收针对计算设备的认证凭证的请求(动作402)。该请求包括描述计算设备的软件和/或硬件的信息。所述信息可以指示计算设备的健康和/或指示可信安全组件是受到如上所述的认证服务信任的组件。

[0058] 验证所接收的信息(动作404)。认证服务验证信息的方式至少部分地基于上文讨论的所接收的信息而不同。

[0059] 从非对称密钥的集合中选择非对称密钥对(动作406)。密钥的集合中的每个非对称密钥都是公钥/私钥对,并且所述密钥对中的一个密钥对是以上文所讨论的各种方式被选择的,例如随机地或伪随机地。

[0060] 生成计算设备的认证凭证和所选择的密钥对(动作408)。该认证凭证将所选择的

密钥对中的公钥与认证凭证相关联。

[0061] 也针对计算设备来对所选择的密钥对中的私钥进行加密(动作410)。可以加密所选的非对称密钥对,或者只加密所选择的非对称密钥对中的私钥。所选择的密钥对中的私钥是使用计算设备的可信安全组件的公钥/私钥对中的公钥来加密的。可信安全组件的公钥可以被包括在在动作402中所接收的描述计算设备的信息中,或者可以通过其他方式获得。

[0062] 将所选择的密钥对中的经加密的私钥和认证凭证返回至计算设备(动作412)。所选择的密钥对中的经加密的私钥和认证凭证可以以各种方式被返回,例如经由网络被传输至计算设备。

[0063] 图5是示出了根据一个或多个实施例的、用于实现提供设备匿名性的密钥认证声明生成的另一示例过程500的流程图。过程500可以由计算设备(例如,图1中的计算设备102)实行,并且可以在软件、固件、硬件或其组合中被实现。过程500被示出为一组动作,并且不限于用于执行各种动作的操作所示出的顺序。过程500是用于实现提供设备匿名性的密钥认证声明生成的示例过程;在本文中参考不同的附图而包括对实现提供设备匿名性的密钥认证声明生成的另外的讨论。

[0064] 在过程500中,将针对计算设备的认证凭证的请求发送至认证服务(动作502)。该请求包括描述计算设备的软件和/或硬件的信息。所述信息可以指示计算设备的健康和/或指示可信安全组件是受到如上所述的认证服务信任的组件。

[0065] 响应于该请求,从认证服务接收公钥/私钥对和认证凭证(动作504)。如果在动作502中发送至认证服务的计算设备的信息被认证服务验证,则接收公钥/私钥对和认证凭证。认证凭证将所接收的公钥/私钥对中的公钥与计算设备(和/或该计算设备的可信安全组件)相关联。该关联例如是通过以下方式执行的:认证凭证包括所选择的公钥/私钥对中的公钥,并且所选择的公钥/私钥对中的私钥被安全地提供至该计算设备(例如,使用该计算设备的可信安全组件的密钥加密的)。

[0066] 存储所接收的公钥/私钥对和认证凭证(动作506)。所接收的公钥/私钥对中的私钥被存储在计算设备的可信安全组件的安全存储部中。所接收的公钥/私钥对中的公钥以及认证凭证可以被存储在安全存储部中或可替代地被存储其他地方。

[0067] 生成向上链接至认证服务的一个或多个另外的公钥/私钥对和认证凭证(动作508)。所述另外的公钥/私钥对和认证凭证是由可信安全组件在不访问认证服务的情况下生成的。

[0068] 尽管参考特定的模块在本文中讨论的特定的功能,但应当注意的是,在本文中所讨论的个体模块的功能可以被分成多个模块,和/或多个模块的至少一些功能可以被组合成单个模块。额外地,在本文中被讨论为执行动作的特定模块包括执行该动作的该特定模块本身,或者可替代地,调用或者以其他方式访问执行该动作(或者结合该特定模块执行该动作)的另一组件或模块的该特定模块。因此,执行动作的特定模块包括执行该动作的该特定模块本身,和/或由执行该动作的该特定模块调用或者以其他方式访问的另一模块。

[0069] 图6在600处一般地示出了示例系统,其包括代表可以用于实现在本文中所描述的各种技术的一个或多个系统和/或设备的示例计算设备602。计算设备602可以是例如服务提供商的服务器、与客户端相关联的设备(例如,客户端设备)、片上系统、和/或任何其他合

适的计算设备或计算系统。

[0070] 如图所示的示例计算设备602包括彼此通信地耦合的处理系统604、一个或多个计算机可读介质606、以及一个或多个I/O接口608。尽管未示出,但计算设备602还可以包括将各种组件彼此耦合的系统总线或其他数据和命令传输系统。系统总线可以包括不同的总线结构中的任何一个或组合,所述不同的总线结构例如存储器总线或存储器控制器、外围总线、通用串行总线、和/或使用多种总线架构中的任何一种的处理器或本地总线。还可以构想多种其他示例,例如,控制和数据线路。

[0071] 处理系统604代表用于使用硬件来执行一个或多个操作的功能。从而,处理系统604被示出为包括可以被配置为处理器、功能块等的硬件元件610。这可以包括以硬件来作为专用集成电路或者使用一个或多个半导体形成的其他逻辑设备的实现。硬件元件610不由形成其的材料或者其中所采用的处理机制来限制。例如,处理器可以由半导体和/或晶体管(例如,电子集成电路(IC))构成。在这样的上下文中,处理器可执行指令可以是电子可执行指令。

[0072] 计算机可读介质606被示出为包括存储器/存储设备612。存储器/存储设备612表示与一个或多个计算机可读介质相关联的存储器/存储设备容量。存储器/存储设备612可以包括易失性介质(例如,随机存取存储器(RAM))和/或非易失性介质(例如,只读存储器(ROM)、阻抗性RAM(ReRAM)、闪速存储器、光盘、磁盘等)。存储器/存储设备612可以包括固定的介质(例如,RAM、ROM、固定的硬盘驱动器等)以及可移动介质(例如,闪速存储器、可移动硬盘驱动器、光盘等)。存储器/存储设备612可以包括例如从加州Santa Clara市的Intel公司或者从Idaho州Boise市的美光科技公司可获得的诸如3D Xpoint存储器之类的存储级存储器(SCM)。计算机可读介质606可以以如在下文中所进一步描述的多种其他的方式来配置。

[0073] 所述输入/输出接口608代表用于允许用户向计算设备602输入命令和信息,并且还允许利用各种输入/输出设备向用户和/或其他组件或设备呈现该信息的功能。输入设备的示例包括键盘、光标控制设备(例如,鼠标)、麦克风(例如,用于语音输入)、扫描仪、触摸功能(例如,被配置以对物理接触进行检测的电容或其他传感器)、相机(例如,可以采用可见或非可见波长(例如,红外频率)来检测运动不包含作为手势的触摸的)等。输出设备的示例包括显示设备(例如,监视器或投影仪)、扬声器、打印机、网络卡、触觉反应设备等。因此,计算设备602可以用如在下文中所进一步描述的多种方式被配置以支持用户交互。

[0074] 在一个或多个实施例中,计算设备602是图1的计算设备102,并且包括可信安全组件614。可信安全组件614从认证服务获得认证凭证,并且也生成向上链接至认证服务的另外的公钥/私钥对和认证凭证。可信安全组件614可以实现例如图1或图3的可信安全组件112。

[0075] 可替代地,计算设备602是实现图1或图2的认证服务104的至少一部分的计算设备。在这样的情况下,计算设备602不需要包括可信安全组件614。相反,计算设备602包括支持客户端匿名性的认证凭证系统,例如图1或图2的支持客户端匿名性的认证凭证系统122。

[0076] 可以在本文中在软件、硬件元件、或程序模块的一般性的上下文中描述各种技术。通常而言,这样的技术包括执行特定的任务或实现特定的抽象数据类型的例程、程序、对象、元件、组件、数据结构等。如在本文中所使用的术语“模块”、“功能”、和“组件”通常表示

软件、固件、硬件、或其组合。在本文中所描述的技术的特征是与平台无关的,意思是可以在具有多种处理器的多种计算平台上实现这些技术。

[0077] 所描述的模块和技术的实现可以存储在一些形式的计算机可读介质上或者跨一些形式的计算机可读介质传输。计算机可读介质可以包括可以由计算设备602访问的多种介质。作为示例而非限制,计算机可读介质可以包括“计算机可读存储介质”和“计算机可读信号介质”。

[0078] “计算机可读存储介质”指的是与仅仅是信号传输、载波、或信号本身相对的支持信息的持久存储的介质和/或设备,和/或有形的存储。因此,计算机可读存储介质是指非信号承载介质。计算机可读存储介质包括以适合于存储信息(例如,计算机可读指令、数据结构、程序模块、逻辑元件/电路、或其他数据)的方法或技术实现的硬件,例如易失性和非易失性、可移动和不可移动介质和/或存储设备。计算机可读存储介质的示例可以包括但不限于,RAM、ROM、EEPROM、闪速存储器、或者其他存储器技术、CD-ROM、数字通用盘(DVD)或其他光存储、硬盘、盒式磁带、磁带、磁盘存储或其他磁存储设备、或者其他存储设备、有形的介质、或者适合于存储期望的信息并且可以由计算机访问的制品。

[0079] “计算机可读信号介质”指的是被配置以将指令传输(例如,经由网络)至计算机设备602的硬件的信号承载介质。通信介质通常可以实施计算机可读指令、数据结构、程序模块、或经调制的数据信号中的其他数据,例如,载波、数据信号、或其他传输机制。信号介质还包括任何信息传递介质。术语“经调制的数据信号”意指将其特征中的一个或多个以将信息编码在信号中的方式来设置或改变的信号。作为示例而非限制,通信介质包括有线介质(例如,有线网络或直接连接)和无线介质(例如,声学、射频(RF)、红外、和其他无线介质)。

[0080] 如前所述,硬件元件611和计算机可读介质606代表以硬件形式实现的指令、模块、可编程设备逻辑和/或固定的设备逻辑,其可以在一些实施例中被采用以实现在本文中所描述的技术中的至少一些方面。硬件元件可以包括集成电路或片上系统的组件、专用集成电路(ASIC)、现场可编程门阵列(FPGA)、复杂可编程逻辑设备(CPLD)、以及硅或其他硬件设备中的其他实现。在该上下文中,硬件元件可以运行为执行由指令、模块、和/或逻辑所定义的程序任务的处理设备,所述指令、模块和/或逻辑由被使用以存储指令以用于执行的硬件元件以及硬件设备(例如,之前所描述的计算机可读存储介质)来实施。

[0081] 也可以采用上述的组合来实现在本文中所描述的各种技术和模块。从而,软件、硬件、或程序模块和其他程序模块可以被实现为在某种形式的计算机可读存储介质上实施和/或由一个或多个硬件元件610实施的一个或多个指令和/或逻辑。计算设备602可以被配置以实现对应于软件和/或硬件模块的特定的指令和/或功能。从而,能够由计算设备602作为软件执行的模块作为模块的实现可以至少部分地以硬件(例如,通过对处理系统的计算机可读存储介质和/或硬件元件610的使用)来完成。指令和/或功能可以由制品(例如,一个或多个计算设备602和/或处理系统604)执行/操作以实现在本文中所描述的技术、模块、和示例。

[0082] 如在图6中进一步示出的,当在个人计算机(PC)、电视设备、和/或移动设备上运行应用时,示例系统600支持针对无缝的用户体验的普遍的环境。对于当在使用应用程序、玩可视游戏、观看视频等的过程中从一个设备转移到下一个时的普通的用户体验而言,服务和应用在所有三种环境中大体相似地运行。

[0083] 在示例系统600中,多个设备通过中央计算设备被互连。中央计算设备可以对于多个设备来说是本地的或者可以远程于多个设备。在一个或多个实施例中,中央计算设备可以是通过网络、互联网、或其他数据通信链路连接至多个设备的一个或多个服务器计算机的云。

[0084] 在一个或多个实施例中,该互连架构支持待跨多个设备而被传递以向多个设备的用户提供共同和无缝的体验的功能。多个设备中的每个都可以具有不同的物理要求和能力,并且中央计算设备使用平台以使能够将既针对该设备定制并且还对所有设备共同的体验传递至设备。在一个或多个实施例中,创建了一类目标设备,并且针对一般类型的设备来定制体验。可以由设备的物理特征、使用类型、或者其他共同的特性来定义设备的类。

[0085] 在各种实现中,计算设备602可以假设多种不同的配置,例如,以供计算机616、移动618、以及电视620使用。这些配置中的每个都包括可以具有一般不同结构和能力的设备,并且因此计算设备602可以根据不同的设备类中的一个或多个而被配置。例如,计算设备602可以被实现为设备的计算机616类,该类包括个人计算机、台式计算机、多屏幕计算机、膝上型计算机、上网本等。

[0086] 计算设备602还可以被实现为设备的移动618类,该类包括移动设备,例如,移动电话、便携式音乐播放机、便携式游戏设备、平板计算机、多屏幕计算机等。计算设备602还可以被实现为设备的电视620类,其包括具有或连接至随意查看环境中的通常较大的屏幕的设备的。这些设备包括电视、机顶盒、游戏控制器等。

[0087] 在本文中所描述的技术可以由计算设备602的这些各种配置支持,并且不限于在本文中所描述的技术的具体的示例。该功能还可以全部或部分地通过对分布式系统的使用(例如,如在下文中所描述的通过经由平台624的“云”622)而被实现。

[0088] 云622包括和/或代表资源626的平台624。平台624提取了云622的硬件(例如,服务器)和软件资源的基础功能。资源626可以包括当在远程于计算设备602的服务器上执行计算机处理时可以被使用的应用和/或数据。资源626还可以包括通过互联网和/或通过订阅者网络(例如,蜂窝或Wi-Fi网络)提供的服务。

[0089] 平台624可以提取资源和功能以将计算设备602与其他计算设备进行连接。平台624还可以用来提取资源的放缩,以对针对经由平台624所实现的资源626的所遇到的需求而提供对应的放缩等级。从而,在经互连的设备实施例中,在本文中所描述的功能的实现可以遍布系统600而分布。例如,功能可以被部分地在计算设备602上被实现,以及经由提取云622的功能的平台624而被实现。

[0090] 在本文的讨论中,描述了各种不同的实施例。应当领会和理解的是,在本文中所描述的每个实施例可以自己使用,或者结合在本文中所描述的一个或多个实施例来使用。在本文中所讨论的另外的方面涉及以下实施例中的一个或多个。

[0091] 一种在认证服务中实现的方法,所述方法包括:从第一计算设备接收针对所述第一计算设备的认证凭证的第一请求,所述请求包括描述所述第一计算设备的硬件和/或软件的信息;验证所接收的信息;从非对称密钥对集合中选择非对称密钥对,所选择的密钥对也是针对多个另外的计算设备选择的;生成所述第一计算设备的所述认证凭证,所述认证凭证将所选择的密钥对中的公钥与所述认证凭证相关联;针对所述第一计算设备来对所选择的密钥对中的私钥进行加密;以及将所选择的密钥对中的经加密的私钥和所述认证凭证

返回至所述第一计算设备。

[0092] 对于在本文中所描述的方法、系统、或计算设备可替代地或另外地,以下项中的任何一项或组合:其中,针对所述第一计算设备来对所选择的密钥对中的所述私钥进行加密包括使用所述第一计算设备的可信安全组件的公钥/私钥对中的公钥来对所选择的密钥对中的所述私钥进行加密;其中,选择所述非对称密钥对包括从所述非对称密钥对集合中随机地或者伪随机地选择所述非对称密钥对;还包括在接收到所述第一请求之前,在所述非对称密钥对集合中生成所述非对称密钥对;还包括在一个或多个间隔处改变所述非对称密钥对集合中的所述非对称密钥对;还包括:从第二计算设备接收针对所述第二计算设备的认证凭证的第二请求,所述第二请求包括描述所述第二计算设备的硬件和/软件的信息,验证所接收的描述所述第二计算设备的所述硬件和/软件的信息,从所述非对称密钥对集合中选择与针对所述第一计算设备所选择的密钥对相同的密钥对,生成所述第二计算设备的所述认证凭证,所述认证凭证将所选择的密钥对中的所述公钥与所述第二计算设备的所述认证凭证相关联,对所述第二计算设备的所选择的密钥对中的所述私钥进行加密,以及将所选择的密钥对中的经加密的私钥和所述第二计算设备的所述认证凭证返回至所述第二计算设备;所述认证凭证不具有所述第一计算设备的名称或标识符。

[0093] 一种在计算设备中实现的方法,所述方法包括:向认证服务发送针对所述计算设备的认证凭证的请求,所述请求包括描述所述计算设备的硬件和/或软件的信息;从所述认证服务接收公钥/私钥对以及所述认证凭证,所述认证凭证将所述公钥/私钥对与所述计算设备的可信安全组件相关联;将所述公钥/私钥对中的私钥存储在所述可信安全组件的安全存储部中;在不访问所述认证服务的情况下,生成一个或多个另外的私钥/公钥对以及一个或多个另外的认证凭证,每个另外的认证凭证向上链接至所述认证服务。

[0094] 对于在本文中所描述的方法、系统、或计算设备可替代地或另外地,以下项中的任何一项或组合:所接收的公钥/私钥对是与由所述认证服务提供至多个其他计算设备的公钥/私钥对相同的公钥/私钥对;还包括针对所述计算设备的网络浏览器所访问的每个网站来生成所述一个或多个另外的公钥/私钥对中的一个公钥/私钥对和一个或多个另外的认证凭证;还包括针对所述计算设备所访问的多个不同的依赖方系统中的每个依赖方系统来生成所述一个或多个另外的公钥/私钥对中的一个公钥/私钥对和一个或多个另外的认证凭证;还包括使用所述可信安全组件的私钥来对从所述认证服务所接收的公钥私钥对进行解密;所述可信安全组件包括可信平台模块。

[0095] 一种系统,包括:一个或多个处理器;以及具有存储在其上的多个指令的计算机可读存储介质,所述指令响应于由所述一个或多个处理器执行,使得所述一个或多个处理器进行以下操作:从第一计算设备接收针对所述第一计算设备的认证凭证的第一请求,所述请求包括描述所述第一计算设备的硬件和/或软件的信息;验证所接收的信息;从非对称密钥对集合中选择非对称密钥对,所选择的密钥对也是针对多个另外的计算设备选择的;生成所述第一计算设备的所述认证凭证,所述认证凭证将所选择的密钥对中的公钥与所述认证凭证相关联;针对所述第一计算设备来对所选择的密钥对中的私钥进行加密;以及将所选择的密钥对中的经加密的私钥和所述认证凭证返回至所述第一计算设备。

[0096] 对于在本文中所描述的方法、系统、或计算设备可替代地或另外地,以下项中的任何一项或组合:其中,针对所述第一计算设备来对所选择的密钥对中的所述私钥进行加密

包括使用所述第一计算设备的可信安全组件的公钥/私钥对中的公钥来对所选择的密钥对中的所述私钥进行加密,所述可信安全组件包括可信平台模块;其中,选择所述非对称密钥对包括从所述非对称密钥对集合中随机地或者伪随机地选择所述非对称密钥对;所述多个指令还使得所述一个或多个处理器在一个或多个间隔处改变所述非对称密钥对集合中的所述非对称密钥对;所述多个指令还使得从第二计算设备接收针对所述第二计算设备的认证凭证的第二请求,所述第二请求包括描述所述第二计算设备的硬件和/软件的信息,验证所接收的描述所述第二计算设备的所述硬件和/软件的信息,从所述非对称密钥对集合中选择与针对所述第一计算设备所选择的密钥对相同的密钥对,生成所述第二计算设备的所述认证凭证,所述认证凭证将所选择的密钥对中的所述公钥与所述第二计算设备的所述认证凭证相关联,对所述第二计算设备的所选择的密钥对中的所述私钥进行加密,以及将所选择的密钥对中的经加密的私钥和所述第二计算设备的所述认证凭证返回至所述第二计算设备;所述认证凭证不具有所述第一计算设备的名称或标识符。

[0097] 一种计算设备,包括:一个或多个处理器;以及具有存储在其上的多个指令的计算机可读存储介质,所述指令响应于由所述一个或多个处理器执行,使得所述一个或多个处理器进行以下操作:向认证服务发送针对所述计算设备的认证凭证的请求,所述请求包括描述所述计算设备的硬件和/或软件的信息;从所述认证服务接收公钥/私钥对以及所述认证凭证,所述认证凭证将所述公钥/私钥对与所述计算设备的可信安全组件相关联;将所述公钥/私钥对中的私钥存储在所述可信安全组件的安全存储部中;在不访问所述认证服务的情况下,生成一个或多个另外的私钥/公钥对以及一个或多个另外的认证凭证,每个另外的认证凭证向上链接至所述认证服务。

[0098] 尽管用特定于结构特征和/或方法动作的语言描述了实施例,但是应当理解的是,所附权利要求中定义的实施例不一定限于所描述的特定特征或动作。相反,特定特征和动作是作为实现所要求保护的实施例的示例形式公开的。

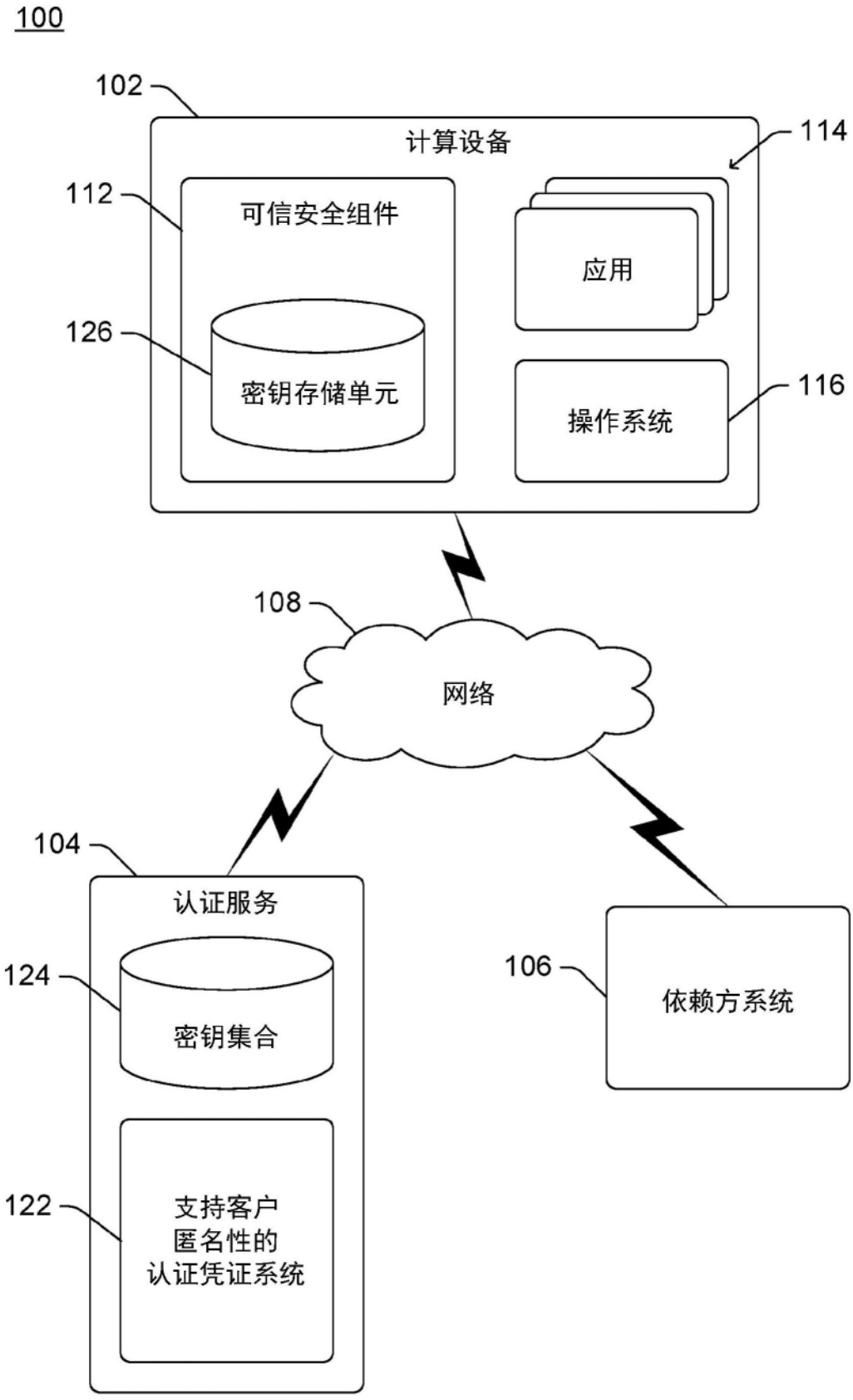

100
102
计算设备
114
112
可信安全组件
应用
126
密钥存储单元
操作系统
116
108
网络
104
认证服务
124
密钥集合
106
依赖方系统
122
支持客户
匿名性的
认证凭证系统

图1

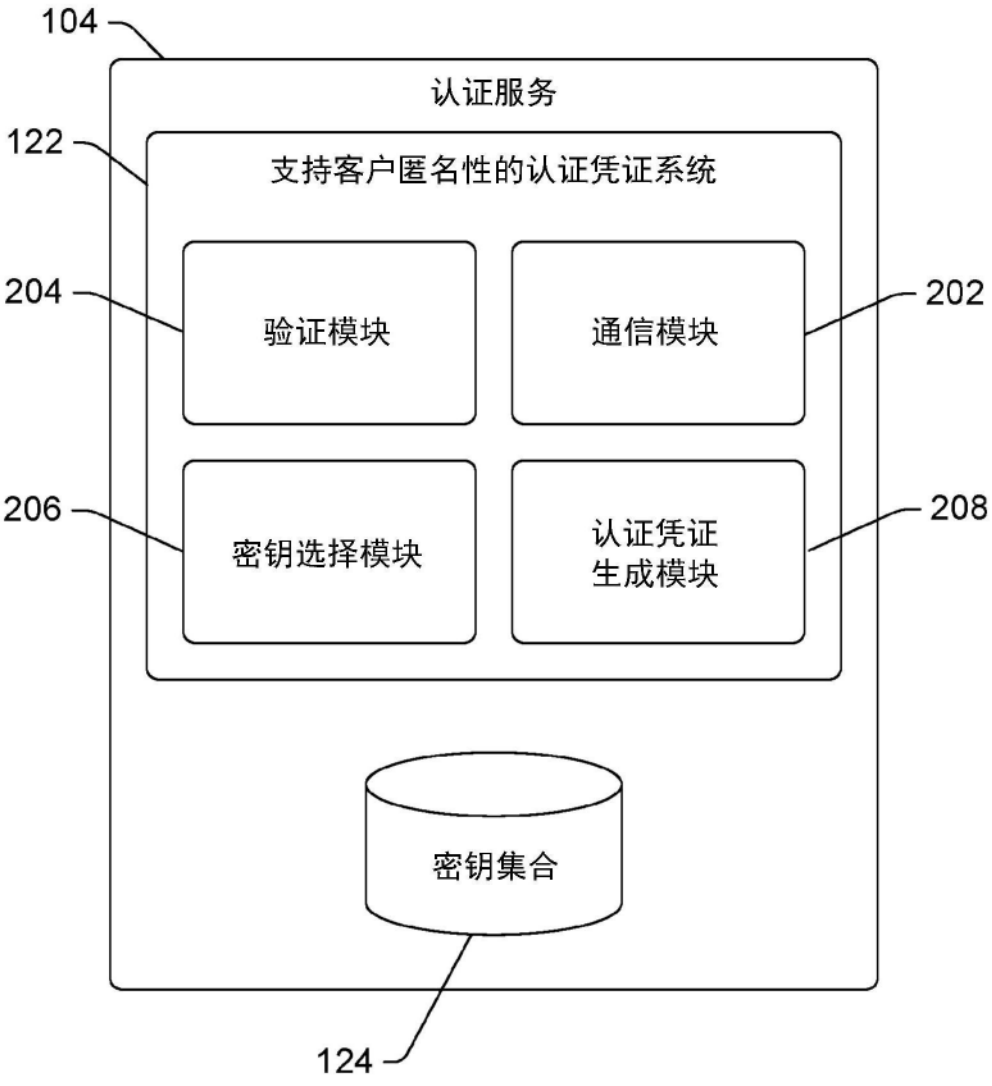

104
认证服务
122
支持客户匿名性的认证凭证系统
204
验证模块
通信模块
202
206
密钥选择模块
认证凭证
生成模块
208
密钥集合
124

图2

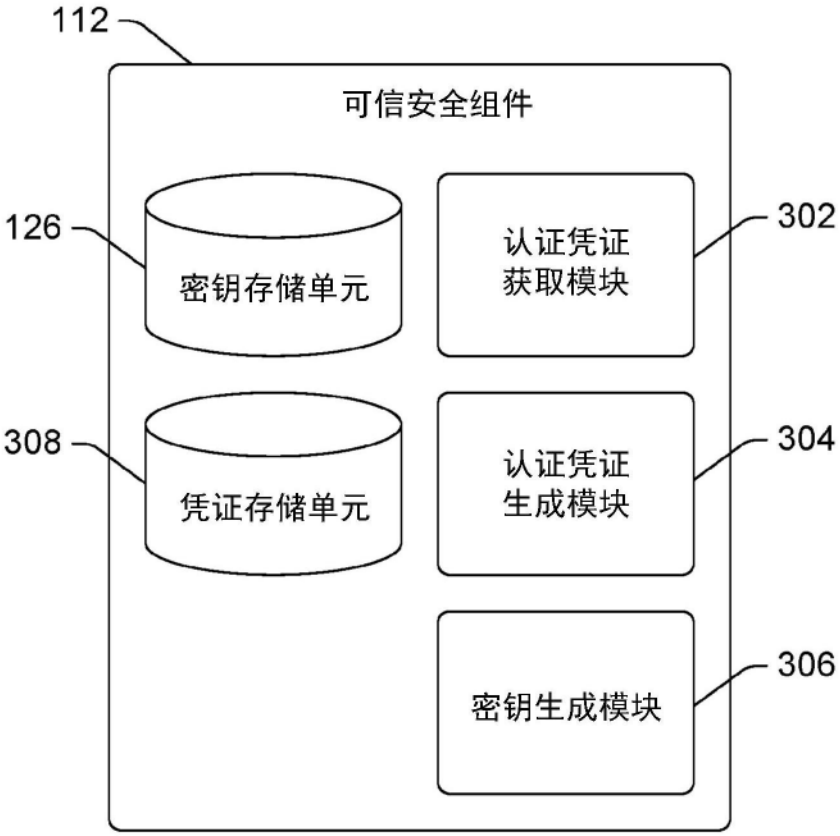

112
可信安全组件
126
密钥存储单元
302
认证凭证
获取模块
308
凭证存储单元
304
认证凭证
生成模块
306
密钥生成模块

图3

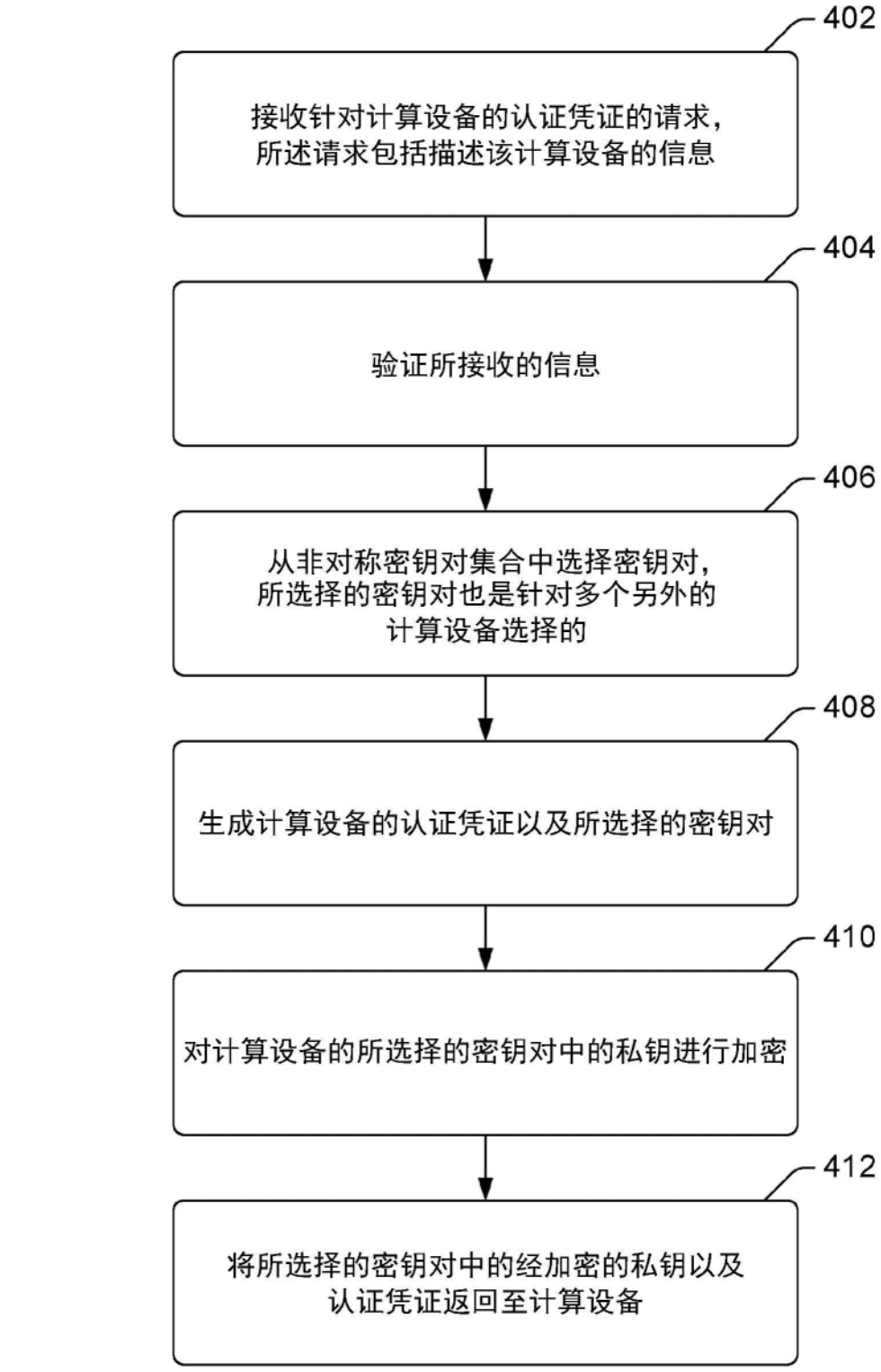

400
402
接收针对计算设备的认证凭证的请求，所述请求包括描述该计算设备的信息
404
验证所接收的信息
406
从非对称密钥对集合中选择密钥对，所选择的密钥对也是针对多个另外的计算设备选择的
408
生成计算设备的认证凭证以及所选择的密钥对
410
对计算设备的所选择的密钥对中的私钥进行加密
412
将所选择的密钥对中的经加密的私钥以及认证凭证返回至计算设备

图4

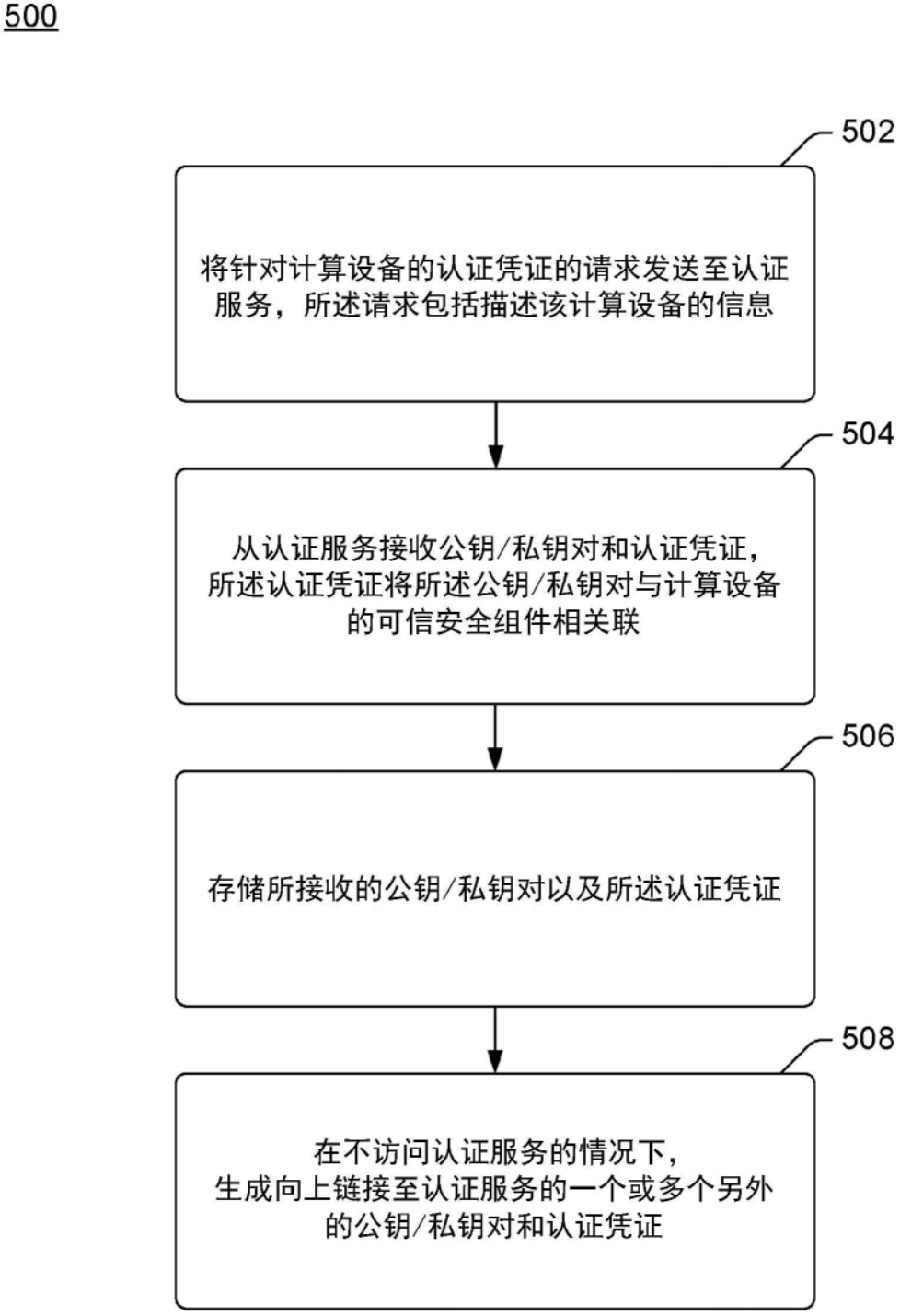

500
502
将针对计算设备的认证凭证的请求发送至认证服务，所述请求包括描述该计算设备的信息
504
从认证服务接收公钥/私钥对和认证凭证，所述认证凭证将所述公钥/私钥对与计算设备的可信安全组件相关联
506
存储所接收的公钥/私钥对以及所述认证凭证
508
在不访问认证服务的情况下，生成向上链接至认证服务的一个或多个另外的公钥/私钥对和认证凭证

图5

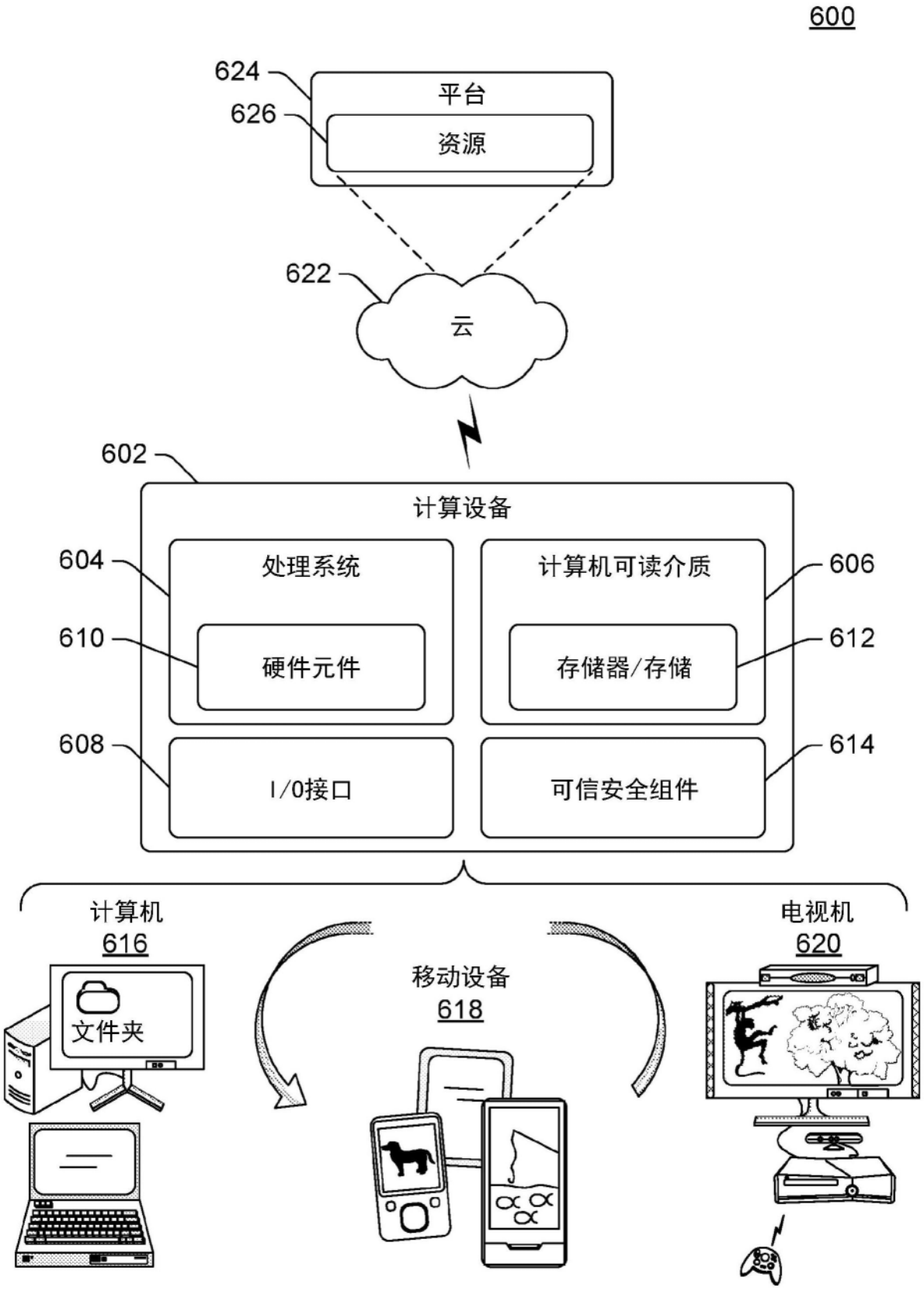

600
624
平台
626
资源
622
云
602
计算设备
604
处理系统
610
硬件元件
608
I/O接口
计算机可读介质
606
存储器/存储
612
可信安全组件
614
计算机
616
文件夹
移动设备
618
电视机
620

图6