(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102016866 A
(43)申请公布日 2011.04.13

(21)申请号 200980115996.8
(22)申请日 2009.03.02
(30)优先权数据
61/033,728 2008.03.04 US
(85)PCT申请进入国家阶段日
2010.11.03
(86)PCT申请的申请数据
PCT/US2009/035755 2009.03.02
(87)PCT申请的公布数据
WO2009/111411 EN 2009.09.11
(71)申请人 苹果公司
地址 美国加利福尼亚
(72)发明人 D·德阿特勒 H·潘塞 M·安德勒尔 S·库铂 M·布劳沃 M·丽达
(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038
代理人 邹姗姗
(51)Int.Cl.
G06F 21/00(2006.01)

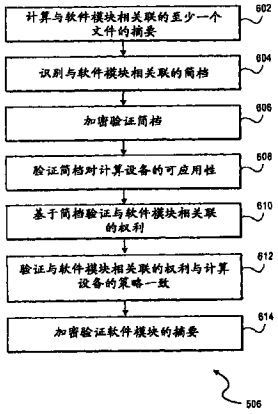
权利要求书 3 页 说明书 14 页 附图 9 页

(54)发明名称

基于授予承载商的权利授权在设备上执行软件代码的系统和方法

(57)摘要

实施例包括用于基于至少一个承载商简档来授权软件代码在安全操作环境中执行或访问性能的系统和方法。承载商简档可由可信实体发出，以将信任扩展到其他实体，从而准许这些其他实体在安全操作环境中，例如在特定计算设备上，提供或控制应用程序的执行。该承载商简档准许实体将软件代码添加到设备，而无需由可信授权机构再次授权每个发布，或者添加到由其他实体控制或授权的有限组设备。



CN 102016866 A

1. 一种授权软件的方法，该方法包括：

在处理器的可信空间中接收用以执行在电子设备上存储的软件模块的请求；

将指示所述软件模块的数据传送到在所述处理器的不可信空间中执行的服务；

通过所述服务认证与设备相关联的服务提供商的至少一个简档；

通过所述服务认证对所述软件模块的至少一个权利，其中，认证所述至少一个权利至少部分基于所述服务提供商的简档；

将指示所述经认证的权利的数据传送到所述可信空间；以及

基于所述权利执行所述软件模块。

2. 根据权利要求 1 所述的方法，其中，所述在所述不可信空间中执行的服务包括以所述服务器的用户处理执行的处理。

3. 根据权利要求 1 所述的方法，其中，所述服务提供商的至少一个简档包括针对所述软件模块不准许的一个或多个权利。

4. 根据权利要求 1 所述的方法，其中，所述软件模块至少包括应用程序或共享库。

5. 根据权利要求 1 所述的方法，其中，所述指示所述软件模块的数据包括对与所述软件模块相关联的可执行指令的至少一部分的引用。

6. 根据权利要求 5 所述的方法，其中，认证至少一个权利包括计算指示所述部分的摘要。

7. 根据权利要求 6 所述的方法，其中，计算指示所述软件模块的至少一部分的摘要包括：生成指示多个摘要值的一个摘要值，所述多个摘要值指示所述软件模块的相应部分。

8. 根据权利要求 6 所述的方法，其中，所述摘要包括指示所述至少一个部分的 SHA-1 散列。

9. 根据权利要求 6 所述的方法，其中，认证所述软件模块的至少一个权利包括：基于与所述软件模块相关联的实体的加密密钥来认证所述摘要的加密签名。

10. 根据权利要求 9 所述的方法，其中，认证所述摘要的加密签名包括：

基于可信实体的公钥来计算所述摘要的加密签名；以及

将所计算的签名与关于至少一个文件存储的签名进行比较。

11. 根据权利要求 9 所述的方法，其中，认证所述软件模块的至少一个权利包括：

识别与所述软件模块相关联的简档，其中所述简档包括指示至少一个设备标识符的数据；

基于所述实体的加密密钥来认证所述简档；

将所述简档的设备标识符与所述电子设备的设备标识符进行比较；以及

基于所述比较来认证所述权利。

12. 根据权利要求 11 所述的方法，其中，所述软件模块的简档还包括指示至少一个权利的数据，并且其中，认证所述软件模块的至少一个权利包括当所述软件模块的权利与所述简档的权利数据一致时认证所述软件模块的权利。

13. 根据权利要求 1 所述的方法，其中，认证所述服务提供商的至少一个简档包括：

识别与所述服务提供商相关联的简档；以及

基于所述服务提供商的加密密钥来认证所述简档。

14. 根据权利要求 1 所述的方法，其中，所述简档包括指示所述服务提供商的至少一个权利的数据，并且其中，认证所述软件模块的至少一个权利包括确定所述软件模块的权利是否与所述服务提供商的简档的权利数据一致。

15. 根据权利要求 1 所述的方法，其中，所述软件模块的权利包括准许调试权利、准许追踪权利、准许访问地址簿数据权利或者准许访问多媒体 API 权利中的至少一个或多个。

16. 一种计算机可读介质，包括指示代码的数据，该代码可由电子设备的至少一个处理器执行以实现包括如下的处理：

在处理器的可信空间中接收用以执行在电子设备上存储的软件模块的请求；

将指示所述软件模块的数据传送到在所述处理器的不可信空间中执行的服务；

通过所述服务认证与设备相关联的服务提供商的至少一个简档；

通过所述服务认证对所述软件模块的至少一个权利，其中，认证所述至少一个权利至少部分基于所述服务提供商的简档；

将指示所述经认证的权利的数据传送到所述可信空间；以及

基于所述权利执行所述软件模块。

17. 一种设备，包括：

存储设备，配置为：

存储用于在电子系统上执行的软件模块；和

存储至少一个简档，该至少一个简档包括与所述软件模块相关联的至少一个权利；以及

至少一个处理器，配置为：

通过在处理器的可信空间中执行的处理来接收用以执行软件模块的请求；

将指示所述软件模块的数据传送到在所述处理器的不可信空间中执行的服务；

通过所述服务认证与设备相关联的服务提供商的至少一个简档；

通过所述服务认证所述软件模块的至少一个权利，其中，认证所述至少一个权利至少部分基于所述服务提供商的简档；

将指示所述经认证的权利的数据传送到可信空间处理；以及

基于所述权利执行所述软件模块。

18. 根据权利要求 17 所述的设备，其中，所述可信空间包括以可信模式在所述设备的处理器上执行的操作系统内核，并且所述在所述不可信空间中执行的服务包括以所述处理器的用户模式处理执行的处理。

19. 根据权利要求 17 所述的设备，其中，所述软件模块至少包括应用程序或共享库。

20. 根据权利要求 17 所述的设备，其中，所述服务提供商的至少一个简档包括针对所述软件模块不准许的一个或多个权利。

21. 根据权利要求 17 所述的设备，其中，所述指示所述软件模块的数据包括对与所述软件模块相关联的可执行指令的至少一部分的引用。

22. 根据权利要求 21 所述的设备，其中，为了认证所述摘要的加密签名，所述处理器还配置为计算指示所述部分的摘要。

23. 根据权利要求 22 所述的设备，其中，为了计算所述摘要，所述处理器配置为生成

指示多个摘要值的一个摘要值，所述多个摘要值指示所述软件模块的相应部分。

24. 根据权利要求 22 所述的设备，其中，所述摘要包括指示所述至少一个部分的 SHA-1 散列。

25. 根据权利要求 22 所述的设备，其中，为了认证所述摘要的加密签名，所述处理器还配置为基于与所述软件模块相关联的实体的加密密钥来认证所述摘要的加密签名。

26. 根据权利要求 25 所述的设备，其中，为了认证所述摘要的加密签名，所述处理器还配置为：

基于可信实体的公钥来计算所述摘要的加密签名；以及

将所计算的签名与关于至少一个文件存储的签名进行比较。

27. 根据权利要求 25 所述的设备，其中，为了认证所述摘要的加密签名，所述处理器还配置为：

识别与所述软件模块相关联的简档，其中所述简档包括指示至少一个设备标识符的数据；

基于所述实体的加密密钥来认证所述简档；

将所述简档的设备标识符与所述电子设备的设备标识符进行比较；以及

基于所述比较的结果来认证所述权利。

28. 根据权利要求 27 所述的设备，其中，所述软件模块的简档还包括指示至少一个权利的数据，并且其中，认证所述软件模块的至少一个权利包括当所述软件模块的权利与所述简档的权利一致时认证所述软件模块的权利。

29. 根据权利要求 17 所述的设备，其中，为了认证所述服务提供商的至少一个简档，所述处理器还配置为：

识别与所述服务提供商相关联的简档；以及

基于所述服务提供商的加密密钥来认证所述简档。

30. 根据权利要求 17 所述的设备，其中，所述简档包括指示所述服务提供商的至少一个权利的数据，并且其中，认证所述软件模块的至少一个权利包括确定所述软件模块的权利是否与所述服务提供商的简档的权利数据一致。

31. 根据权利要求 17 所述的设备，其中，所述软件模块的权利包括准许调试权利、准许追踪权利、准许访问地址簿数据权利或者准许访问多媒体 API 权利中的至少一个或多个。

基于授予承载商的权利授权在设备上执行软件代码的系统和方法

技术领域

[0001] 本申请涉及控制对软件代码的执行。

背景技术

[0002] 不同的网络承载商关于移动计算设备如何可以与它们相应的网络或者它们可以执行的应用程序进行交互通常具有不同的要求。 为了确保移动计算设备正常工作并且符合网络策略，通常对移动计算设备进行准备 (provisioning) 处理，该处理通过固件更新对电话进行配置以在承载商的网络上操作。

[0003] 另外，经常这些计算设备可以被配置为要求在计算机系统上执行的代码由可信方来授权。 例如，这种授权可以用于帮助确保计算设备的完整性不会被恶意或未授权的代码损害。 在一些情况下，计算设备可被配置为要求代码由可信方数字地签名以及验证，用以在计算设备上执行和 / 或控制对访问设备的特定资源或服务的软件的执行。 对数字签名的验证有助于确保底层的应用代码自被可信授权机构 (authority) 数字签名起不再被修改。

[0004] 然而，移动设备通常具有承载商不希望用在它们的网络上的能力。 例如，移动设备可设计具有蓝牙功能，但是承载商可能希望禁止其用户利用该能力。 这些设备上的各种应用程序也可能需要被限制。 不幸的是，在采用如上所述的应用程序签名安全的移动设备上执行这些限制是困难的。

附图说明

[0005] 图 1 是例示了计算环境的一个示例的框图，在该计算环境中，软件代码从一个或多个承载商发布到计算设备。

[0006] 图 2 是例示了在如图 1 中所例示的环境中的计算设备的软件部件的一个实施例的框图。

[0007] 图 3 是例示了用于控制在如图 2 中所例示的设备上执行软件的简档的一个实施例的框图。

[0008] 图 4 是例示了在图 2 所例示的计算设备的一个实施例的软件部件之间的数据流的框图。

[0009] 图 5 是例示了基于图 2 所例示的简档而执行软件的方法的一个实施例的流程图。

[0010] 图 6 是更详细地例示了图 5 的方法的部分的流程图。

[0011] 图 7 是例示了如图 2 所例示的计算设备的一个示例的框图。

[0012] 图 8A 和 8B 是例示了如图 2 所例示的计算设备的一个示例的框图。

[0013] 图 9 是例示了如图 8A 和 8B 所例示的移动设备的实施的一个示例的框图。

具体实施方式

[0014] 这里描述的各种实施例提供了用于基于执行的承载商简档控制例如在承载商网络上的计算设备的系统和方法。 在一些情况下，计算设备可以被配置为要求代码的一些或全部由可信方数字地签名并且验证，以在计算设备上执行。 这里所公开的系统和方法允许承载商将它们的简档安装在与其网络相连接的计算设备上。 利用这里所描述的系统和方法，承载商由此能够有效地将简档应用到这些计算设备，以按照可信应用程序还符合承载商的期望策略的方式控制对设备上的工具 (facility) 和资源的访问。

[0015] 在一些实施例中，为了将其简档安装在计算设备上，承载商（或其代表）可以将请求发送到可信授权机构。 该请求可以指定承载商希望设备在其网络上操作时所具有的访问和功能的类型。 可信授权机构可以针对承载商创建承载商简档，该承载商简档反映了针对在承载商的网络上的这些设备的承载商所期望的网络策略，或者允许承载商适当地修改设备。 访问简档和策略处理还可以被提供并且安装到指定的设备以执行其承载商简档。

[0016] 当代码在设备上执行时，策略处理可以检查承载商简档中指定的权利，以确定代码执行请求是否可以被准许。 如果承载商简档包括必要的权利，则代码可以被允许访问所请求的数据和 / 或系统功能。 如果承载商简档不包括必要的权利，则代码访问设备上的特定数据和 / 或功能的能力可以被限制。

[0017] 为了例示本发明的实施例，下面将给出图 1-7。 图 1 例示了实施例可以实施的整体系统图。 图 2-3 示出了软件部件和用于控制软件的执行的示例性简档的实施例。 图 4 示出了软件部件之间的数据流的一个示例。 接着图 5-6 例示了用于基于简档执行软件的处理流程图。 提供图 7 来例示移动计算设备的一个示例。 下面将从参照图 1 开始进一步描述这些附图。

[0018] 图 1 是适于实践这里所描述的各种实施例的环境的示例。 在所示系统中，计算设备 100 可以由可信授权机构 102 提供或者控制，并且可以利用承载商 104 所运营的网络。 下面将进一步描述这些实体和部件。

[0019] 计算设备 100 可以是移动计算设备，例如移动电话、移动智能电话、或者一些其他类型的移动设备。 计算设备 100 可以被配置为运行要求代码执行中的一些或全部由可信授权机构 102 准许的操作系统。 由此，如果在未授权状态下将软件递送到计算设备 100，则设备可能不能完全执行软件中所包括的代码指令，因为它们还没有被授权。

[0020] 尽管本公开涉及移动设备，但是计算设备 100 可以是任意数量的不同类型的计算设备，包括台式计算机、膝上型计算机、手持式计算机、个人数字助理 (PDA) 设备、移动电话设备、媒体播放设备，等等。

[0021] 当用户希望在承载商 104 的网络上操作它们的计算设备 100 时，设备 100 可能需要被准备或激活以使得能够在网络上操作。 在一个或多个实施例中，激活服务 106 用于执行该准备处理。 激活服务 106 可以被实施为网络（例如，因特网）上的一个或多个服务器，其将数据传送到计算设备 100，该数据然后用于配置设备 100 以在承载商 104 的网络上操作。

[0022] 激活服务 106 所传送的数据可以采取可被称为承载商准备简档的形式。 承载商准备简档可以指定设备 100 如何可以利用设备 100 上的工具和 / 或资源以及设备 100 如何可与承载商 104 运营的网络服务交互的策略和权利。

[0023] 可信授权机构 102 可以是能够授权代码以使得其能够在计算设备 100 上运行的任何人或组织。 当然，特定设备 100 可以具有多于一个的可信授权机构 102。 在一些实施例中，可信授权机构 102 可以是通过计算设备 100 的操作系统和安全模型进行控制的组织和 / 或实体。

[0024] 本文所采用的承载商 104 可以是为计算设备 100 提供网络访问的实体或服务提供商。 承载商 104 的广为公知的示例是移动电话服务提供商，例如 Verizon、 AT&T、 T-Mobile、 Sprint 等等。

[0025] 如所提到的，激活服务 106 可以是用于准备设备 100 的系统和处理。 激活服务 106 可以包括在被配置为通过网络传送准备数据的联网计算设备上操作的一个或多个网络应用程序和服务器。

[0026] 在一些实施例中，激活服务 106 可以将准备发送到在个人计算机上运行的本地应用程序。 一个或多个设备 100 可以耦接到个人计算机以通过在个人计算机上的准备应用程序接收准备数据。 另选地，计算设备 100 出货时可以具有如下基本功能，该基本功能允许设备 100 连接到承载商网络以从激活服务 106 接收准备数据。 激活服务 106 还可以例如通过承载商 104 的网络将准备数据直接传送到设备 100。 准备数据还可以从计算机可读介质安装，或者安装到与服务器耦接的存储设备上。

[0027] 图 2 是提供计算设备 100 如何可以被配置为采用承载商简档 208 来执行由除可信授权机构 102 之外的实体（例如，承载商 104 或其指定代表）签名的软件模块 206 的一个示例的框图。

[0028] 软件 106 可以包括存储在设备 100 上或可由设备 100 访问的一个或多个软件模块 206。 在一个实施例中，计算设备 100 的存储设备 209 可以包括计算机可读存储介质（易失性和 / 或非易失性的），其可被配置为存储软件模块 206 和简档 208 中的一个或两者。存储设备 209 还可以被配置为存储操作系统 202 的代码，并且还可以包括设备 100 的通用存储设备。 软件模块 206 可以被暂时存储在设备 100 上或者永久性地存储在设备 100 上。

[0029] 计算设备 100 可以包括操作系统。 操作系统可以是广为公知的操作系统，例如 MacOS、Windows、Linux、Unix、Symbian 等等。 如以上简要地讨论的，操作系统的一部分（例如，操作系统 202 的内核）可以被配置为要求在设备 100 上执行的代码在被允许在设备上执行之前被授权。 该授权可以采取数字地签名软件模块 206 中的一些或全部的可信授权机构 102 的形式。 在一些实施例中，可信授权机构 102 采用代码签名证书，其可以被用于验证经签名的计算机代码的来源和完整性。

[0030] 在一些实施例中，计算设备 100 还可以包括诸如调试、追踪或描绘软件的开发和测试相关的软件，作为安装在计算设备 100 上的标准发布的一部分，作为预先准备处理的一部分，或者在任何其他时间包括该软件。 在一些实施例中，计算设备 100 被预先准备有这种附加的开发相关软件。 在其他实施例中，开发相关软件可以随访问简档或者与之相结合地被安装在设备上。

[0031] 操作系统 202 所采用的存储器的内核空间在概念上可以被认为是可信空间。 信任可以通过对内核的引导时认证来建立。 在一个实施例中，计算设备 100 可以包括用于提供对操作系统 202 及其内容所采用的内核空间的引导时认证的硬件支持。 例如，在一个实施例中，计算设备 100 的引导加载器可以例如采用适合的公钥签名验证来在加载和

引导内核之前认证内核软件的签名。

[0032] 数字签名可以包括摘要，该摘要例如可以通过在软件上执行散列函数以创建消息摘要来创建。在一些实施例中，可以采用递增代码签名。散列值可以是针对软件的全部或特定部分产生的散列值。例如，在一些实施例中，软件被分为诸如一个或多个页面的一个或多个单元。散列值是针对软件的每个单元或页面生成的。在这种实施例中，软件的摘要包括针对每个代码或页面的散列值的阵列或表生成的散列值。然后可以利用与可信授权机构 102 相关联的私用加密密钥来加密消息摘要。在一个实施例中，广为公知的 SHA-1 函数可以用来生成消息摘要。然后可以将加密的消息摘要（也称为签名）附加到一个或多个软件模块 206。

[0033] 在一些实施例中，当在设备上请求执行软件代码时，操作系统 202 可以通过证实数字签名而验证软件代码的来源和完整性来处理请求。如果可信授权机构 102 验证了代码的来源，并且代码的完整性没有被损害，则操作系统 202 可以允许代码在计算设备 100 上运行。

[0034] 计算设备 100 还可以包括设备标识符 204。设备标识符 204 可以采取多种形式。在一个实施例中，设备标识符 204 可以是唯一地标识计算设备 100 的序列号。在其他实施例中，设备标识符 204 可以是操作系统 202 生成的唯一标识符。

[0035] 如上所述，计算设备 100 还可以具有可信授权机构 102 创建的承载商简档 208。开发者访问简档 208 可以包括指示允许特定设备执行没有被可信授权机构 102 签名的软件的一组数据。在一个实施例中，承载商简档 208 允许承载商 104 修改和 / 或提供其自己的软件模块 206，而无需从可信授权机构 102 请求附加的代码签名服务。相反，承载商 104 可以被允许数字地签名其软件模块 206，并且在具有如下承载商简档 208 的计算设备 100 上运行软件，该承载商简档 208 指定承载商 104 签名的代码可以在设备 100 上执行。在一些实施例中，承载商简档还可以指定承载商 104 在执行软件模块 206 中可以执行的特定操作。计算设备 100 还可以具有多于一个的承载商简档 208。

[0036] 在一些实施例中，承载商简档 208 可以与策略服务 210 相结合地操作。策略服务 210 可以采取在操作系统的用户（不可信）存储器空间中运行的守护 (daemon) 或其他处理的形式。策略服务 210 可以被进一步配置为执行承载商简档 208 中指定的策略。

[0037] 策略服务 210 可以是由操作系统 202 初始启动的，操作系统 202 可以在加载服务 210 之前验证该服务的加密保护的摘要。操作系统 202 可以经由处理间通信或类似的适合端口来保持对服务 210 的引用。由此，当简档服务 210 在不可信或用户模式的空间中执行时，简档服务 210 的代码可以在执行时被验证为由可信授权机构签名。

[0038] 图 3 是承载商简档 208 的更详细视图。如上所述，承载商简档 208 可以是存储在设备 100 的存储器中的一组数据，其指示即使在软件没有被可信授权机构 102 签名的情况下设备也被允许执行该软件。承载商简档 208 可以包括设备标识符数据 302、承载商标识符数据 304 以及权利数据 306。

[0039] 设备标识符数据 302 指定承载商简档 208 应用到的一个或多个设备标识符 302。在设备 100 是移动电话设备的实施例中，设备标识符数据 302 可以包括移动电话设备序列号的阵列。

[0040] 承载商简档 208 的设备标识符数据 302 可以包括不同设备的一个或多个设备标识

符 204。在一个实施例中，设备标识符 204 可以是特定设备的特定标识符，其可以被表示为数字或字母数据。在其他实施例中，可以采用更广义的设备标识数据。例如，一些设备销售商和 / 或制造商可以提供具有特定于组织的设备标识符的设备。例如，设备销售商和 / 或制造商可以基于设备递送到的组织来定制与设备相关联的设备标识符 204 的特定方面。

[0041] 设备标识符数据 302 可以包括设备标识符的范围，而非列出每单个设备标识符值。在又一些实施例中，可以采用位掩码 (bit mask) 或通配字符来指定承载商简档应用到具有指定标识符特性的所有设备。在又一些实施例中，设备标识符数据 302 可以指定承载商简档 208 应用于所有设备。例如，在一个这种实施例中，由承载商标识符数据 302 中标识的一个或多个承载商签名的软件可以被授权以在安装了承载商简档 208 的任何设备 100 上运行。

[0042] 如上所述，承载商简档 208 可以进一步包括承载商标识符数据 304，该承载商标识符数据 304 指定承载商简档 208 所应用到的承载商 104。承载商标识符数据 304 可以采取多种形式。在一些实施例中，承载商标识符数据 304 可以是与由承载商简档 208 覆盖的承载商 104 相关联的公钥。还可以采用其他类型的标识符。在一些实施例中，承载商标识符数据 304 可以存储在阵列数据结构中，该阵列数据结构存储在承载商简档内。当然，可以采用任何适合的数据结构。

[0043] 此外，承载商简档 208 可以包括权利数据 306。权利数据 306 可以包括如下数据，该数据指示针对由承载商标识符数据 304 标识的承载商签名的软件模块 206 在设备标识符数据 302 中指定的设备 100 上允许的操作的类型。特定的承载商简档 208 可以指定多于一个的承载商 104 为被授权，以数字地签名由承载商简档 208 授权的代码。

[0044] 权利数据 306 可以指定关于在设备标识符数据 302 中标识的设备 100 针对由承载商标识符数据 304 中标识的承载商 104 所签名的应用程序所允许的访问的类型。权利数据 306 可以采取键值对的形式。该值例如可以包括数字、布尔或字母数据。在一个实施例中，权利数据 306 可以包括指示各种指定权利的预定布尔变量的阵列或其他数据结构。

[0045] 在一个实施例中，权利数据 306 可以包括被执行的能力。其他权利可以控制对具有安全或私密暗示（例如，地址簿数据）的设备 100 的联网资源、数据、库或应用程序的访问。另外，其他权利可以控制对特定承载商 API（包括通话、联网、地址或电话存储、或多媒体 API）的访问。

[0046] 图 4 是例示了在系统接收到并且处理请求时在一个实施例的计算设备 100 的软件部件之间发生的事件之间的关系的框图。如图所示，在事件 1 中，可包括可信空间的操作系统 202 可以接收请求（响应于执行特定软件模块 206 的用户请求，或者响应于请求设备 100 上的另一软件部件执行特定软件模块 206）以执行标识的软件模块 206。在一个实施例中，该请求可以包括对存储设备 209 的目录或文件的引用，存储设备 209 存储软件模块 206 的可执行指令代码。

[0047] 在事件 2 中，操作系统 202 可以将认证软件模块 206 的请求传送给策略服务 210。在一个实施例中，认证请求可以包括对与软件模块 206 相关联的存储设备 209 中的存储位置的引用。操作系统 202 还可以将软件模块 206 的至少一部分的摘要提供给策略服务 210。另选地或者另外地，策略服务 210 可以生成软件模块 206 的全部或部分的摘

要。 在一个实施例中，摘要可以基于针对与软件模块 206 相关联的每个代码页面或每个文件所确定的摘要值。 在一个实施例中，对策略服务 210 的请求可以包括诸如要被执行的特定权利的其他数据。

[0048] 例如，操作系统 202 可以指定，权利可以是执行或者访问指定的系统资源的权利。 操作系统 202 或者设备 100 的操作系统的另一部分可以被配置为请求访问特定网络（例如，移动电话网络、蓝牙堆栈）或者设备 100 的特定能力（例如，访问设备 100 的传声器、扬声器、照相机或者其他 I/O 接口）的权利授权。

[0049] 在事件 5 中，策略服务 210 可以访问与执行软件模块 206 相关联的一个或多个简档 208。 在一个实施例中，简档是从存储设备 209 访问的。 在一个实施例中，简档 208 包括与承载商 104 相关联的特定简档。 可以认识到，尽管这里是针对承载商 104 而非可信授权机构 102 描述了简档，但是还可以利用这里描述的系统和方法来控制对由可信授权机构 102（例如，设备或操作系统开发者）提供的软件模块的访问。

[0050] 在事件 5 中，策略服务 210 可以基于摘要和 / 或简档 208 验证软件模块 206 的执行权限。 例如，策略服务 210 可以被配置为接收与软件模块 206 的摘要相关联的签名，并且加密验证所述摘要。 在一个实施例中，策略服务 210 可以采用与特定承载商 104 相关联的并且可以被包括作为简档 208 的一部分的公钥，来验证摘要的签名。

[0051] 在一个实施例中，为了确保简档和承载商密钥是可信的，策略服务 210 加密地验证简档可由可信授权机构 102 信任。 在该实施例中，策略服务 210 可以通过采用可存储在设备 100 上或者例如经由数据网络以其他方式由设备 100 访问的可信授权机构 102 的公钥而验证简档（及其内容）的摘要或其他签名来验证简档。

[0052] 策略服务 210 可以被进一步配置为验证可针对特定设备 100 授权软件模块 206。例如，在一个实施例中，简档 208 可以包括用于匹配设备标识符（例如，用于匹配特定组设备 100 的掩码或通配符）的一个或多个设备标识符或数据。

[0053] 策略服务 210 可以将标识符与设备 100 所安全保持的标识符进行比较，并且当策略 208 的标识符数据与设备 100 的标识符数据匹配时授权软件模块。 设备标识符可以包括存储在设备上可用于标识的任何数据，包括制造商序号、诸如集成电路卡 ID(ICCID) 的移动电话设备的设备或用户标识符、当前插入到设备 100 上的 SIM 卡的国际移动用户标识符 (IMSI)、设备上编码的国际移动设备标识符 (IMEI)、电子序号 (ESN)、或者任何其他适于标识特定软件模块 206 针对其被授权的设备 100 的数据。

[0054] 策略服务 210 可以被配置为基于简档 208 所指定的进一步的权利或其他能力来授权软件模块 206。 可执行或不可执行可以被认为是权利的一个示例。 其他权利可以指定特定软件模块 206 是否可以基于一个或多个简档 208 并基于策略服务 210 可配置为执行的任何其他策略来执行或访问服务。

[0055] 策略服务 210 可以被配置为在用户空间执行，使得其中执行的策略和简档可以是任意复杂并进行更新的而不会增加内核或其他受保护的存储器空间的尺寸，并且更容易被开发和修改而没有一般与内核编程相关联的困难。

[0056] 应当认识到，尽管图 5 例示了操作系统 202 确定特定软件模块 206 是否具有要被执行的权利的示例，但是这里描述的方法和系统可以用于授权对设备硬件能力、内核的其他服务、其他操作系统服务、或者另一软件模块 208 的服务的访问。

[0057] 可以通过与设备相关联的一个或多个策略来执行权利。例如，用于执行权利的策略可以包括将简档中的权利数据处理为白名单 (whitelist)，例如，当简档 208 可以包括指示存在针对特定软件模块 206 和 / 或特定设备 100 的权利的数据时，可以针对特定这种权利认证软件模块 206。另一策略可以基于黑名单 (blacklist) 执行权利，例如，软件模块 206 可以针对特定这种权利被认证，除非简档 208 或可应用的策略可以包括否定针对特定软件模块 206 和 / 或特定设备 100 的权利的数据。在另一实施例中，设备 100 可以被配置具有如下策略，该策略使得一些权利可以被配置为通过白名单执行，而其他权利被配置为通过黑名单执行。

[0058] 可以包括其他策略以更精细地控制特定权利或解决冲突的简档数据。例如，在一个实施例中，移动服务提供商可以在其网络中使用的设备中包括特定承载商简档 208，该简档进一步指定对例如语音网络或拨号盘访问的特定设备能力的权利，其可能与针对特定软件模块 206 的承载商简档 208 相冲突。在这种事件中，设备 100 的策略可以指定一个简档的权利指定来控制。

[0059] 针对配置采用承载商的网络的设备，当设备 100 被承载商 104 激活或准备时，来自承载商 104 的简档 208 可以被接收并存储在设备 100 上。在一个实施例中，承载商简档 208 可以由承载商的 SIM 卡提供，或者响应于插入 SIM 卡而下载到设备 100。在一个实施例中，承载商简档 208 可以包括撤销或限制以其他方式针对一些或全部软件模块 206 提供的权利的权利黑名单。承载商简档 208 可以包括指示 SIM 卡的数据，使得如果设备 100 的 SIM 卡改变而不能与所指示的数据匹配，则不能认证承载商简档。在一个实施例中，服务提供商或承载商简档 208 可以由承载商 104 的数字签名来签名，承载商 104 的数字签名继而可以由可信授权机构 102 的数字信号签名。

[0060] 策略服务 210 可以包括解决服务提供商、制造商以及软件模块简档和权利之间的冲突的规则引擎或其他逻辑器。在一个实施例中，承载商简档 208 可以撤销软件模块简档，该软件模块简档继而可以撤销或扩展制造商简档。由此，例如，制造商简档可以允许软件模块 206 访问诸如网络堆栈的服务。特定软件模块 206 可以进一步被认证以访问网络堆栈。然而，承载商简档 208 可以包括针对指定承载商简档或者针对所有承载商简档指示列黑名单或者以其他方式拒绝对网络堆栈的访问的数据。策略服务 210 可以解决在用户空间处理中的这些复杂性，以最小化操作系统 202 的内核中的这种逻辑器。

[0061] 在事件 6 中，当策略服务 210 可以验证软件模块 240 的权利和 / 或其他执行权限时，策略服务 210 向操作系统 202 或策略服务 210 的其他客户端提供指示软件模块 206 的权利和 / 或认证请求所针对的权利的数据。在事件 7 中，操作系统 202 然后可以根据从策略服务 210 接收到的权利数据来执行软件模块 206。

[0062] 图 5 是例示了在设备 100 中验证软件模块 206 的权利的方法 500 的一个实施例的流程图。该方法可以在块 502 处开始，在块 502 中操作系统 202 的可信空间接收执行特定软件模块 206 的请求。在一个实施例中，可信空间可以在通过设备 100 的引导加载器（其在加载操作系统 202 前对其进行加密验证）启动设备时建立。

[0063] 在块 504 中，可信空间处理将指示软件模块 206 的数据传送到在不可信空间中执行的策略服务 210，但是该不可信空间在初始执行策略服务 210 时已被授予信任。数据可以包括对软件模块 206 的存储位置的引用，并且可选地包括指示特定权利被认证的数

据。

[0064] 接下去在块 506 处，策略服务 210 认证软件模块 206。 在一个实施例中，策略服务 210 基于加密认证来认证软件模块 206。 例如，策略服务 210 可以通过采用诸如非对称 / 公钥加密的适合加密技术验证软件模块 206 的数字签名来认证软件模块 206。 此外，可以利用类似的加密技术来认证与软件模块 206 相关联的一个或多个权利。 参照图 6 将给出块 506 的更多细节。

[0065] 前进到块 508，策略服务 210 将指示软件模块的执行权限的数据传送到操作系统 202 的内核。 该数据可以包括布尔认证响应、指示软件模块 206 的一个或多个权利的数据、软件模块 206 的经验证摘要或者与请求相关的任何其他适合数据。

[0066] 在块 510 中，操作系统 202 或其他可信处理可以执行软件模块 206，或者可以基于经认证的权利执行针对软件模块 206 的服务。

[0067] 图 6 是更详细地例示了图 5 的方法中的块 506 的流程图。 在块 602 处，策略服务 210 可以计算与软件模块 206 的可执行代码相关联的至少一个文件或其他数据结构的摘要。 摘要可以利用例如包括 SHA-1 的任何适合散列算法来计算。

[0068] 在块 604 中，策略服务 210 可以识别与软件模块 206 和 / 或设备 100 相关联的一个或多个简档 208。 在一个实施例中，简档 208 可以各自包括签名密钥和指示软件模块 206 的权利的数据。 例如，权利可以包括诸如表 1 中例示的表格形式的数据结构。

[0069] 表 1 示例简档数据

[0070]

开发者签名密钥	123555
设备 ID1	123FFF
设备 ID2	123FFF
可执行的	真
可调试的	假
可访问网络	真
代码摘要	AAFF1144BB

[0071] 软件模块 206 可以经由识别软件模块 206 的摘要（例如，表 1 中所例示的“代码摘要”）的简档的键值对而与简档 208 相关联。 简档 208 还可以包括数字签名，例如通过例如可信授权机构 102 加密签名的简档的摘要。 接下去在块 606 处，策略服务 210 例如通过验证简档 208 的摘要的加密签名是正确的来加密验证简档 208。

[0072] 移至块 608，策略服务 210 验证可以应用到特定设备 100 的简档 208。 在一个实施例中，该验证可以包括将特定设备 100 的设备标识符 204 与签名简档 208 中列出的设备标识符进行比较。 在块 606 处的先前签名验证可以确保简档 208 中识别的设备没有在未

授权的情况下被改变或修改。

[0073] 接下去在块 610 处，策略服务 210 可以基于简档 208 识别与软件模块 206 相关联的执行权限。 在一个实施例中，该识别可以包括访问每个简档的权利。

[0074] 在块 612 中，策略服务 210 可以验证针对软件模块 206 要被验证的权利与计算设备 100 的策略一致。 在一个实施例中，该验证可以包括确定所请求的权利是否可以被包括在与软件模块 206 和设备 100 的策略相关联的简档 208 中。

[0075] 前进到块 614，策略服务 210 然后可以将在块 602 处计算出的摘要值与软件模块 206 的签名摘要进行比较，并且验证摘要的加密签名。应当认识到，取决于实施例，这里描述的任何方法的特定动作或事件可以按照不同的顺序来执行，可以被添加、合并或者一起省去（例如，并非所有所描述的动作或事件对于实践方法都是必要的）。 此外，在特定实施例中，动作或事件可以例如通过多线程处理、中断处理或者多个处理器同时地而非顺序地执行。

[0076] 图 7 是例示了实现为移动设备的一个设备 100 的示例的框图。 设备 100 可以包括与存储器 704 通信的处理器 702。 网络接口 706 可以包括被配置为根据一个或多个适合的数据和 / 或语音通信系统经由信号进行通信的接收器 724 和发送器 726。 例如，网络接口 708 可以是可通信的，以通过诸如 GSM、CDMA、CDMA2000、EDGE 或者 UMTS 的移动电话网络传送语音和 / 或数据。 网络接口 706 还可以包括用于其他数据网络（例如包括诸如 WiFi 或蓝牙的任何 IEEE 802.x 网络）的接收器 / 发送器。

[0077] 设备 100 还可以包括以下中的一个或多个：显示器 710；诸如按键、触摸屏或者其他适合的触知型输入设备的用户输入设备 712；扬声器 714，包括适于基于通过通信链路 106 接收到的信号提供听觉输出的换能器；和 / 或传声器 716，包括适于提供可通过通信链路 106 和 108 中的一个或两者发送的信号的听觉输入的换能器。

[0078] 在一个实施例中，输入设备 712 可以包括加速计或被配置为检测设备的移动的其他设备。 设备 100 可选地可包括电池 731 来为设备 100 的一个或多个部件提供电力。设备 100 可以包括移动手持机、个人数字助理、膝上型计算机、头戴式耳机、车载免提设备或者任何其他电子设备中的至少一个。 例如，这里教习的一个或多个方面可以并入到电话（例如，移动电话）、个人数据助理（“PDA”）、娱乐设备（例如，音乐或视频设备）、头戴式耳机（例如，头戴式受话器、听筒等等）、传声器或者任何其他电子设备。如下面将进一步描述的，在一些实施例中，设备 100 被实施为移动设备。

[0079] 图 8A 例示了示例移动设备 2500。 移动设备 2500 例如可以是手持式计算机、个人数字助理、蜂窝式电话、网络仪器、照相机、智能电话、增强通用分组无线电服务 (EGPRS) 移动电话、网络基站、媒体播放器、导航设备、电子邮件设备、游戏控制台，或者这些数据处理设备或其他数据处理设备中的任何两个或更多个的组合。

[0080] 移动设备概览

[0081] 在一些实施中，移动设备 2500 包括触摸敏感显示器 2502。触摸敏感显示器 2502 可以利用液晶显示 (LCD) 技术、发光聚合物显示 (LPD) 技术或者一些其他显示技术来实施。 触摸敏感显示器 2502 可以对与用户的触觉和 / 或触知接触敏感。

[0082] 在一些实施中，触摸敏感显示器 2502 可以包括多触摸敏感显示器 2502。 多触摸敏感显示器 2502 例如可以处理多个同时触摸点，包括处理与每个触摸点的压力、角度和

/ 或位置相关的数据。 这种处理便于利用多个手指的姿态和交互、配合 (chording) 以及其他交互。 还可以采用其他触摸敏感显示技术，例如采用触笔或其他指向设备进行接触的显示器。 多触摸敏感显示技术的一些示例在美国专利第 6,323,846 号、第 6,570,557 号、第 6,677,932 号以及第 6,888,536 号中进行了描述，上述专利中的每一个的全部内容通过引用被并入于此。

[0083] 在一些实施例中，移动设备 2500 可以在触摸敏感显示器 2502 上显示一个或多个图形用户界面，用于向用户提供对各种系统对象的访问以及用于向用户传递信息。 在一些实施中，图形用户界面可以包括一个或多个显示对象 2504、2506。 在所示的示例中，显示对象 2504、2506 是系统对象的图形表示。 系统对象的一些示例包括设备功能、应用、窗口、文件、告警、事件或者其他可识别系统对象。

[0084] 示例移动设备功能

[0085] 在一些实施中，移动设备 2500 可以实施多个设备功能，例如，如由电话对象 2510 指示的电话设备 ；如由邮件对象 2512 指示的电子邮件设备 ；如由地图对象 2514 指示的地图设备 ；Wi-Fi 基站设备 (未示出) ；以及如由网络视频对象 2516 指示的网络视频发送和显示设备。 在一些实施中，可以在菜单栏 2518 中显示特定显示对象 2504，例如电话对象 2510、邮件对象 2512、地图对象 2514 以及网络视频对象 2516。 在一些实施中，可以从顶层 (top-level) 的图形用户界面 (例如，图 8A 中所例示的图形用户界面) 来访问设备功能。 触摸对象 2510、2512、2514 或 2516 中的一个例如可以调用对应的功能。

[0086] 在一些实施中，移动设备 2500 可以实现网络发布功能。 例如，该功能可以使得用户能够在旅行中带上移动设备 2500 并提供对其相关联的网络的访问。 特别地，移动设备 2500 可以将因特网访问 (例如， Wi-Fi) 扩展到附近的其他无线设备。 例如，移动设备 2500 可以被配置为一个或多个设备的基站。 因此，移动设备 2500 可以准许或拒绝对其他无线设备的网络访问。

[0087] 在一些实施中，在调用设备功能时，移动设备 2500 的图形用户界面改变，或者增加有或替代以另一用户界面或者用户界面元素，以便于用户访问与对应的设备功能相关联的特定功能。 例如，响应于用户触摸电话对象 2510，触摸敏感显示器 2502 的图形用户界面可以呈现与各种电话功能相关的显示对象 ；同样，触摸邮件对象 2512 可以使得图形用户界面呈现与各种电子邮件功能相关的显示对象 ；触摸地图对象 2514 可以使用图形用户界面呈现与各种地图功能相关的显示对象 ；以及触摸网络视频对象 2516 可以使得图形用户界面呈现与各种网络视频功能相关的显示对象。

[0088] 在一些实施中，可以通过按压位于移动设备 2500 的底部附近的按钮 2520 来恢复图 8A 的顶层图形用户界面环境或状态。 在一些实施中，各个对应的设备功能可以使得对应的 “始位” 显示对象显示在触摸敏感显示器 2502 上，并且可以通过按压 “始位” 显示对象来恢复图 8A 的图形用户界面环境。

[0089] 在一些实施中，顶层图形用户界面可以包括附加显示对象 2506，例如短消息传送服务 (SMS) 对象 2530、日历对象 2532、照片对象 2534、照相机对象 2536、计算器对象 2538、股票对象 2540、地址簿对象 2542、媒体对象 2544、网络对象 2546、视频对象 2548、设置对象 2550 以及备忘录对象 (未示出) 。 触摸 SMS 显示对象 2530 例如可以调用 SMS 消息传送环境和支持功能 ；同样，对显示对象 2532、2534、2536、2538、2540、

2542、2544、2546、2548 和 2550 的每个选择可以调用对应的对象环境和功能。

[0090] 在图 8A 的图形用户界面上还可以显示附加和 / 或不同的显示对象。例如，如果设备 2500 用作其他设备的基站，则在图形用户界面上可以出现一个或多个“连接”对象以指示连接。在一些实施中，显示对象 2506 可以被用户配置，例如用户可以指定显示哪些显示对象 2506，并且 / 或者可以下载附加应用程序或提供其他功能和对应显示对象的其他软件。

[0091] 在一些实施中，移动设备 2500 可以包括一个或多个输入 / 输出 (I/O) 设备和 / 或传感器设备。例如，可以包括扬声器 2560 和传声器 2562 来便于语音使能功能，例如电话和语音邮件功能。在一些实施中，可以包括用于扬声器 2560 和传声器 2562 的音量控制的上 / 下按钮 2584。移动设备 2500 还可以包括用于进入的电话呼叫的铃声指示符的开 / 关按钮 2582。在一些实施中，可以包括扬声器 2564 来便于免提语音功能，例如扬声器电话功能。还可以包括用于头戴式受话器和 / 或传声器的音频插孔 2566。

[0092] 在一些实施中，还可以包括接近传感器 2568 来便于检测用户将移动设备 2500 定位在用户耳边，并且响应地脱开触摸敏感显示器 2502 以防止意外的功能调用。在一些实施中，当移动设备 2500 在用户耳边时，触摸敏感显示器 2502 可以关闭以保存额外电力。

[0093] 还可以采用其他传感器。例如，在一些实施中，可以利用背景光传感器 2570，以便于调整触摸敏感显示器 2502 的亮度。在一些实施中，可以采用加速计 2572 来检测移动设备 2500 的移动，如由方向箭头 2574 所指示的。因此，可以根据检测到的朝向（例如，纵向或横向）来呈现显示对象和 / 或媒体。在一些实施中，移动设备 2500 可以包括用于支持位置确定功能的电路和传感器，例如，由全球定位系统 (GPS) 或其他定位系统（例如，利用 Wi-Fi 接入点、电视信号、蜂窝式网格、统一资源定位符 (URL) 的系统）所提供的功能。在一些实施中，定位系统（例如，GPS 接收器）可以被集成到移动设备 2500 中，或者提供为单独的设备，该单独的设备可以通过提供对基于位置的服务的访问的接口（例如，端口设备 2590）耦接到移动设备 2500。

[0094] 在一些实施中，可以包括例如通用串行总线 (USB) 端口或者对接端口的端口设备 2590 或者一些其他有线端口连接。端口设备 2590 例如可以用于建立到其他计算设备的有线连接，所述其他计算设备例如有其他通信设备 2500、网络访问设备、个人计算机、打印机、显示屏或者能够接收和 / 或发送数据的其他处理设备。在一些实施中，端口设备 2590 允许移动设备 2500 例如利用一个或多个协议（例如，TCP/IP、HTTP、UDP 以及任何其他已知协议）与主机设备同步。

[0095] 移动设备 2500 还可以包括照相机镜头和传感器 2580。在一些实施中，照相机镜头和传感器 2580 可以位于移动设备 2500 的背面。照相机可以捕捉静止图像和 / 或视频。

[0096] 移动设备 2500 还可以包括一个或多个无线通信子系统，例如 802.11b/g 通信设备 2586 和 / 或 Bluetooth™ 通信设备 2588。还可以支持其他通信协议，包括其他 802.x 通信协议（例如，WiMax、Wi-Fi、3G）、码分多址 (CDMA)、全球移动通信系统 (GSM)、增强数据 GSM 环境 (EDGE)，等等。

[0097] 示例可配置的顶层图形用户界面

[0098] 图 8B 例示了设备 2500 的可配置的顶层图形用户界面的另一示例。设备 2500 可

以被配置为显示一组不同的显示对象。

[0099] 在一些实施中，设备 2500 的一个或多个系统对象中的每一个具有一组与之相关联的系统对象属性；以及属性中的一个确定系统对象的显示对象是否将被呈现在顶层图形用户界面中。该属性可由系统自动设置，或者如下所述地由用户通过特定程序或系统功能来设置。图 8B 示出了如何将备忘录对象 2552（在图 8A 中未示出）添加到设备 2500 的顶层图形用户界面并且从设备 2500 的顶层图形用户界面移除网络视频对象 2516 的示例（例如，当修改备忘录系统对象和网络视频系统对象的属性时）。

[0100] 示例移动设备架构

[0101] 图 9 是移动设备（例如，移动设备 2500）的示例实施的框图 3000。移动设备可以包括存储器接口 3002，一个或多个数据处理器、图像处理器和 / 或中央处理单元 3004，以及外设接口 3006。存储器接口 3002、一个或多个处理器 3004 和 / 或外设接口 3006 可以是单独的部件或者可以集成在一个或多个集成电路中。移动设备中的各种部件可以由一个或多个通信总线或信号线来耦接。

[0102] 传感器、设备以及子系统可以耦接到外设接口 3006 以便于实现多个功能。例如，可以将运动传感器 3010、光敏传感器 3012 以及接近传感器 3014 耦接到外设接口 3006 以便于实现关于图 8A 描述的定向、照明以及接近功能。还可以将其他传感器 3016 连接到外设接口 3006，例如定位系统（例如，GPS 接收器）、温度传感器、生物测量传感器或者其他感测设备，以便于实现相关的功能。

[0103] 可以利用照相机子系统 3020 和光学传感器 3022（例如，电荷耦合器件 (CCD) 或互补金属氧化物半导体 (CMOS) 光学传感器）来便于实现照相机功能，例如记录照片和视频剪辑。

[0104] 可以通过可包括射频接收器和发送器以及 / 或者光学（例如，红外）接收器和发送器的一个或多个无线通信子系统 3024 来便于实现通信功能。对通信子系统 3024 的特定设计和实施可以取决于移动设备要通过其操作的通信网络。例如，移动设备可以包括被设计用于在 GSM 网络、GPRS 网络、EDGE 网络、Wi-Fi 或 WiMax 网络以及 Bluetooth™ 网络上操作的通信子系统 3024。特别地，无线通信子系统 3024 可以包括主机协议，使得移动设备可以被配置为用于其他无线设备的基站。

[0105] 音频子系统 3026 可以耦接到扬声器 3028 和传声器 3030，以便于能够实现语音功能，例如语音识别、语音复制、数字记录以及电话功能。

[0106] I/O 子系统 3040 可以包括触摸屏控制器 3042 和 / 或其他输入控制器 3044。触摸屏控制器 3042 可以耦接到触摸屏 3046。触摸屏 3046 和触摸屏控制器 3042 例如可以利用多种触摸敏感技术（包括但不限于电容式、电阻式、红外的以及表面声波技术）中的任一种以及其他接近传感器阵列或用于确定与触摸屏 3046 的一个或多个接触点的其他元件来检测接触以及接触的移动或断开。

[0107] 其他输入控制器 3044 可以耦接到其他输入 / 控制设备 3048，例如一个或多个按钮、摇臂开关、指轮、红外端口、USB 端口以及 / 或者诸如触笔的指向器设备。一个或多个按钮（未示出）可以包括用于扬声器 3028 和 / 或传声器 3030 的音量控制的上 / 下按钮。

[0108] 在一个实施中，按压按钮达第一持续时间可以解除对触摸屏 3046 的锁定；并且

按压按钮达长于第一持续时间的第二持续时间可以对移动设备通电或断电。 用户能够定制一个或多个按钮的功能。 触摸屏 3046 例如还可以用于实现虚拟或软按钮和 / 或键盘。

[0109] 在一些实施中，移动设备可以呈现所记录的音频和 / 或视频文件，例如 MP3、AAC 和 MPEG 文件。 在一些实施中，移动设备可以包括诸如 iPod™ 的 MP3 播放器的功能。 因此，移动设备可以包括与 iPod™ 兼容的 32 针连接器。 还可以采用其他输入 / 输出和控制设备。

[0110] 存储器接口 3002 可以耦接到存储器 3050。存储器 3050 可以包括高速随机存取存储器和 / 或非易失性存储器，例如一个或多个磁盘存储设备、一个或多个光学存储设备以及 / 或者闪速存储器（例如，NAND、NOR）。 存储器 3050 可以存储操作系统 3052，例如 Darwin、RTXC、LINUX、UNIX、OS X、WINDOWS 或者诸如 VxWorks 的嵌入式操作系统。 操作系统 3052 可以包括用于处理基本系统服务的指令以及用于执行依赖于硬件的任务的指令。 在一些实施中，操作系统 3052 可以是内核（例如，UNIX 内核）。

[0111] 存储器 3050 还可以存储便于与一个或多个附加设备、一个或多个计算机以及 / 或者一个或多个服务器进行通信的通信指令 3054。 存储器 3050 可以包括：便于图形用户界面处理的图形用户界面指令 3056；便于传感器相关处理和功能的传感器处理指令 3058；便于电话相关处理和功能的电话指令 3060；便于电子消息传送相关处理和功能的电子消息传送指令 3062；便于网络浏览相关处理和功能的网络浏览指令 3064；便于媒体处理相关处理和功能的媒体处理指令 3066；便于 GPS 和导航相关处理和指令的 GPS/ 导航指令 3068；便于照相机相关处理和功能的照相机指令 3070；以及 / 或者便于其他处理和功能的其他软件指令 3072。 存储器 3050 还可以存储其他软件指令（未示出），例如便于网络视频相关处理和功能的网络视频指令；和 / 或便于网络购物相关处理和功能的网络购物指令。 在一些实施中，媒体处理指令 3066 被分为分别便于音频处理相关处理和功能以及视频处理相关处理和功能的音频处理指令和视频处理指令。 在存储器 3050 中还可以存储激活记录和国际移动设备标识 (IMEI)3074 或类似的硬件标识符。

[0112] 鉴于以上所述，将会认识到实施例克服的问题可以包括实施执行简档以允许开发者在通常由一个或多个其他可信实体提供应用程序的执行环境中开发和测试应用程序。 另外，诸如企业的设备提供商可以被提供以发布自定义开发的应用程序而不会通过可信实体干扰这种应用程序的灵活性。

[0113] 本领域技术人员将认识到，关于这里公开的实施例所描述的各种示例性逻辑块、模块、电路和算法步骤可以被实施为电子硬件、计算机软件或两者的结合。 为了清楚地例示硬件和软件的这种可互换性，以上大体关于其功能描述了各种示例性部件、块、模块、电路和步骤。 这种功能是否实施为硬件或软件取决于特定应用和施加于整体系统的设计限制。 熟练的技术人员可以针对每个特定应用按照不同的方式来实施所描述的功能，但是这种实施决定不应被解释为脱离本发明的范围。

[0114] 关于这里公开的实施例所描述的各种示例性逻辑块、模块和电路可以利用以下来实施或执行：被设计用于执行这里所描述的功能的通用处理器，数字信号处理器 (DSP)，专用集成电路 (ASIC)，现场可编程门阵列 (FPGA)，或者其他可编程逻辑器件、离散门或晶体管逻辑器件、离散硬件部件，或者它们的任意组合。 通用处理器可以是微处理器，但是另选地处理器可以是任何常见处理器、控制器、微控制器或状态机。

处理器还可以实施为计算设备的组合，例如 DSP 和微处理器的组合、多个微处理器、与 DSP 核结合的一个或多个微处理器、或者任何其他这种配置。

[0115] 关于这里所公开的实施例描述的方法或算法的步骤可以直接以硬件实现、以处理器执行的软件模块实现或者以两者的组合来实现。 软件模块可以位于 RAM 存储器、闪速存储器、ROM 存储器、EPROM 存储器、EEPROM 存储器、寄存器、硬盘、可拆除盘、CD-ROM 或本领域公知的任何其他形式的存储介质内。 示例性存储介质耦接到存储器，使得存储器可以从 / 向存储介质读取 / 写入信息。另选地，存储介质可以与处理器是一体的。 处理器和存储介质可以位于 ASIC 内。 ASIC 可以位于用户终端中。 另选地，处理器和存储介质可以作为离散部件位于用户终端中。

[0116] 虽然上面的详细描述已经示出、描述以及指出了本发明在应用于各种实施例时的新颖特征，但应当明白，在不脱离本发明宗旨的情况下，本领域技术人员可以对所示设备或处理的形式和细节进行各种省略、替代以及改变。 如将认识到，本发明可以在不提供这里所阐述的所有特征和优点的形式内实现，因为一些特征可以与其他特征分开使用或实践。 本发明的范围由所附权利要求书而非由以上描述来指示。 落在权利要求书的含义和等同范围内的所有变化都被认为是包含在其范围内。

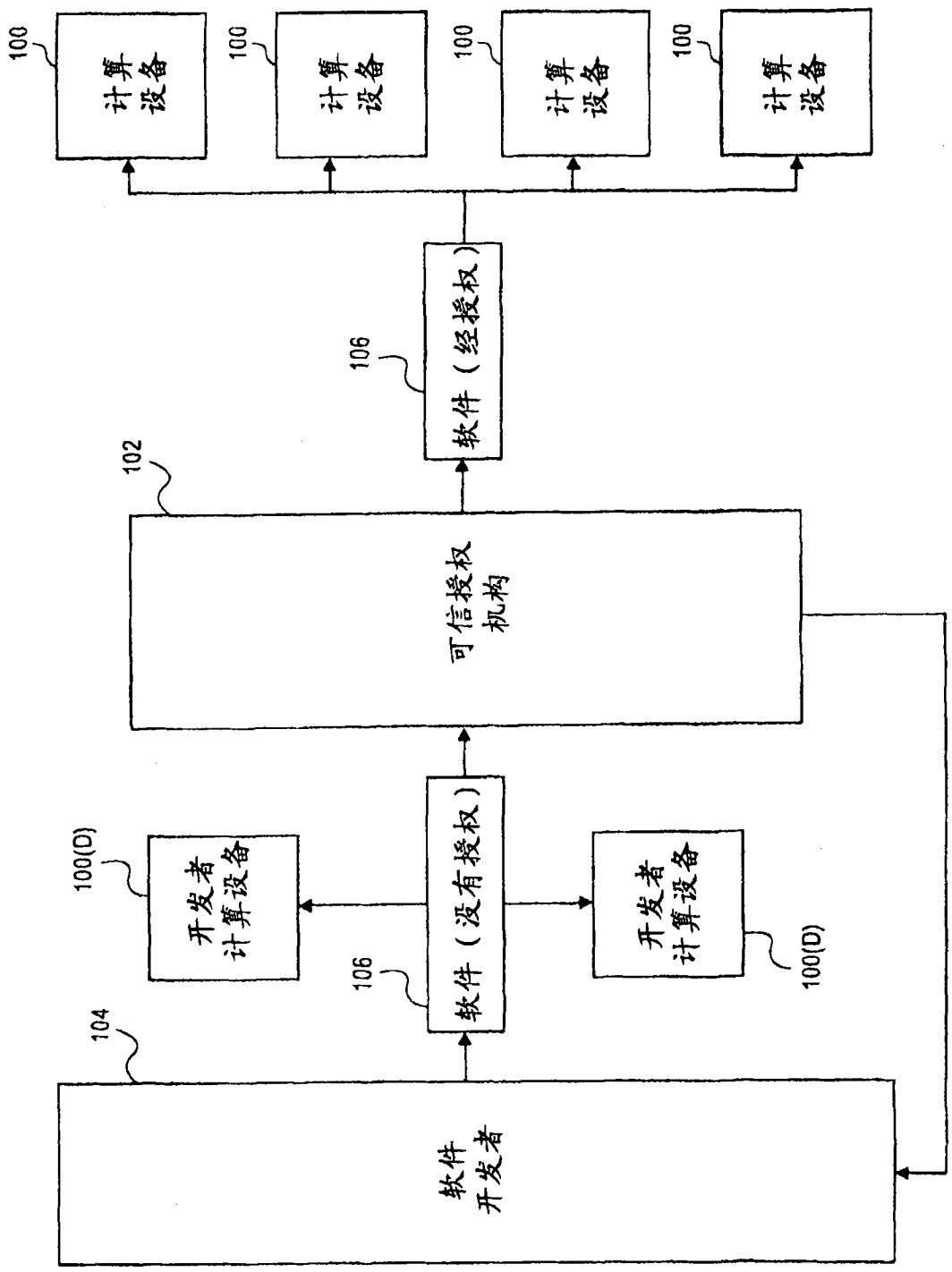

100
计算设备
100
计算设备
100
计算设备
100
计算设备
106
软件（经授权）
102
可信授权机构
100(D)
开发者计算设备
106
软件（没有授权）
开发者计算设备
100(D)
104
软件开发者

图 1

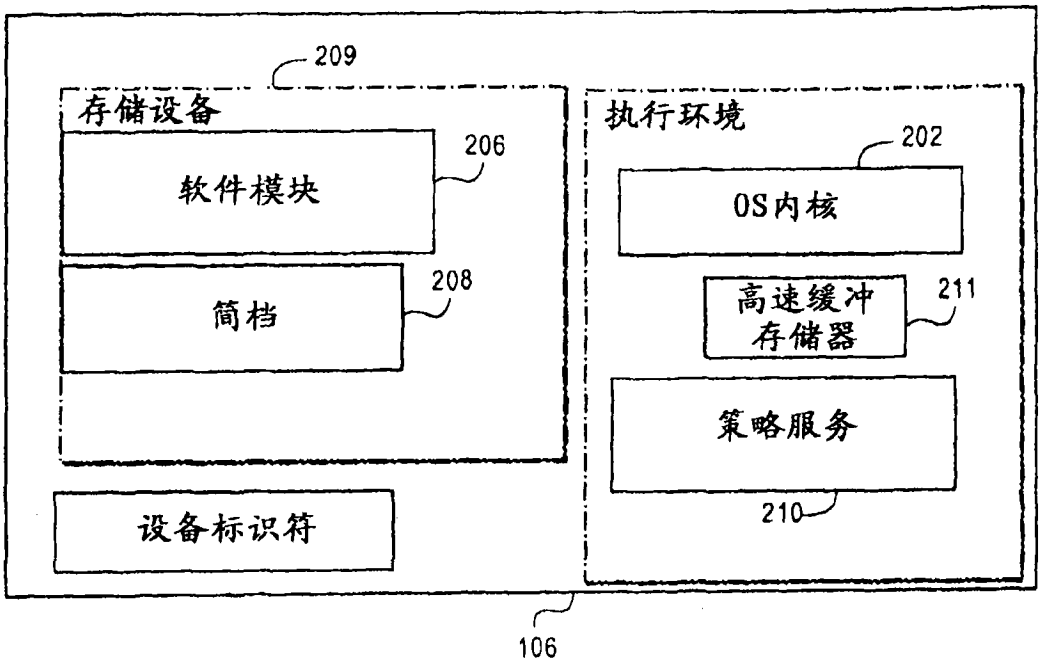

209
存储设备
206
软件模块
208
简档
设备标识符
执行环境
202
OS内核
211
高速缓冲存储器
策略服务
210
106

图 2

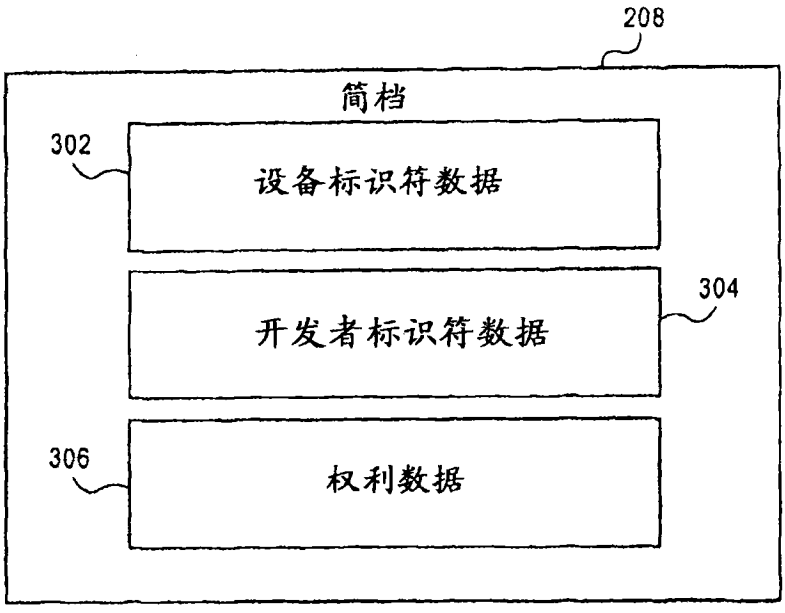

208
简档
302
设备标识符数据
304
开发者标识符数据
306
权利数据

图 3

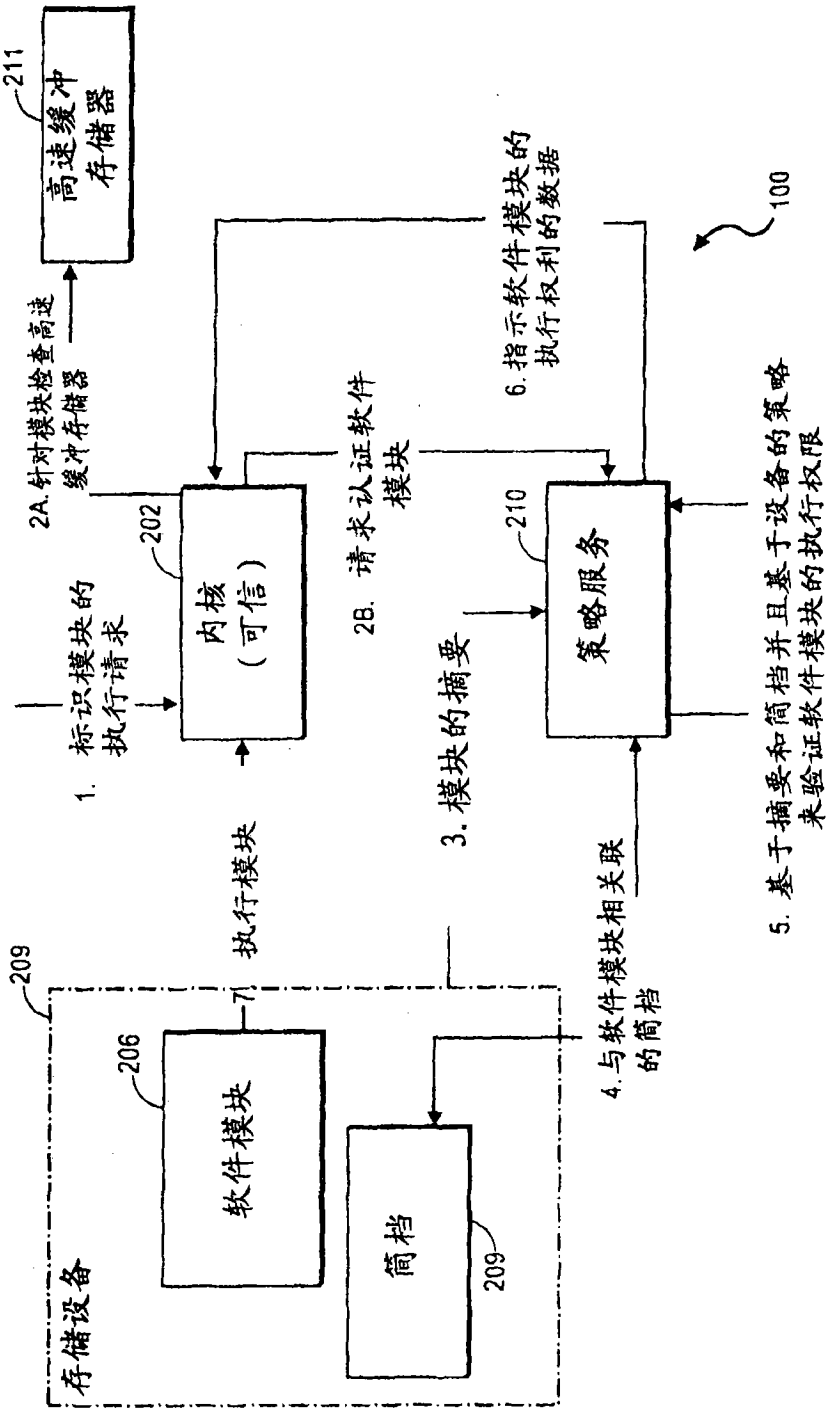

211
高速缓冲存储器
2A. 针对模块检查高速缓冲存储器
1. 标识模块的执行请求
202
内核（可信）
2B. 请求认证软件模块
6. 指示软件模块的执行权利的数据
100
3. 模块的摘要
210
策略服务
5. 基于摘要和简档并且基于设备的策略来验证软件模块的执行权限
执行模块
4. 与软件模块相关联的简档
209
存储设备
206
软件模块
简档
209

图 4

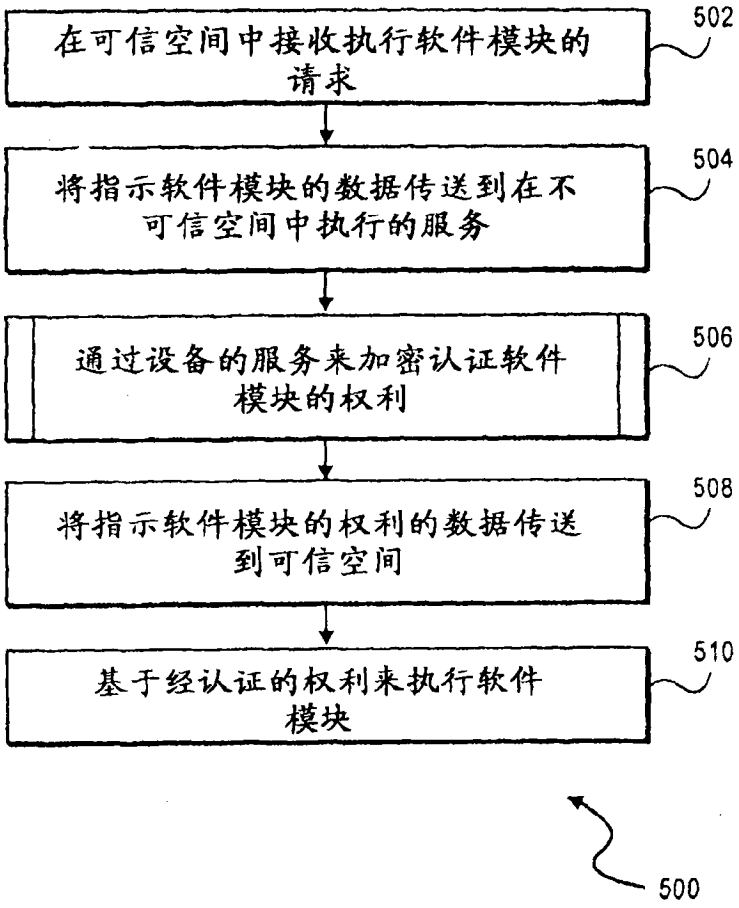

在可信空间中接收执行软件模块的请求
502
将指示软件模块的数据传送到在不可信空间中执行的服务
504
通过设备的服务来加密认证软件模块的权利
506
将指示软件模块的权利的数据传送到可信空间
508
基于经认证的权利来执行软件模块
510
500

图 5

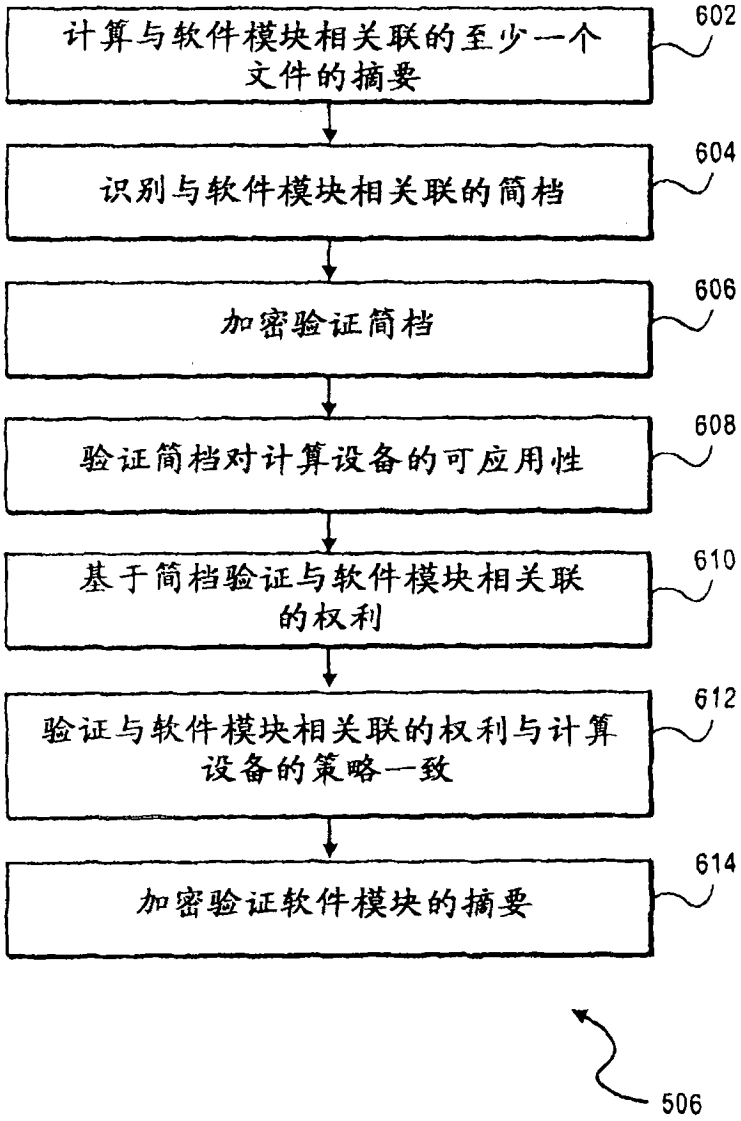

计算与软件模块相关联的至少一个文件的摘要
602
识别与软件模块相关联的简档
604
加密验证简档
606
验证简档对计算设备的可应用性
608
基于简档验证与软件模块相关联的权利
610
验证与软件模块相关联的权利与计算设备的策略一致
612
加密验证软件模块的摘要
614
506

图 6

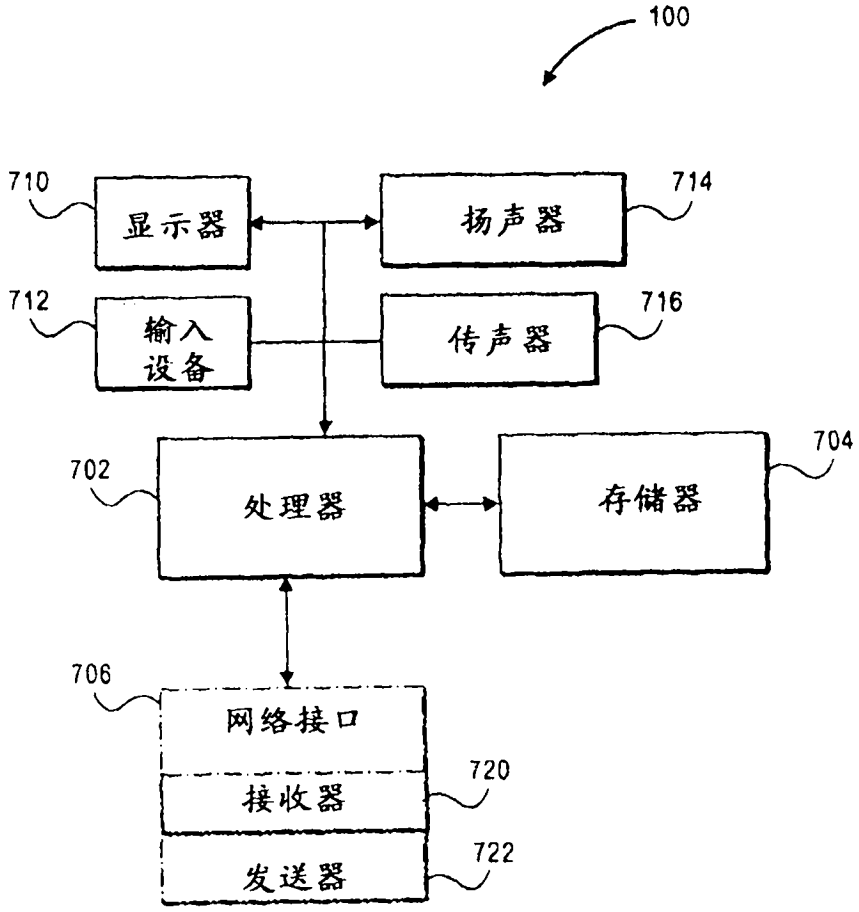

100
710
显示器
714
扬声器
712
输入设备
716
传声器
702
处理器
704
存储器
706
网络接口
720
接收器
722
发送器

图 7

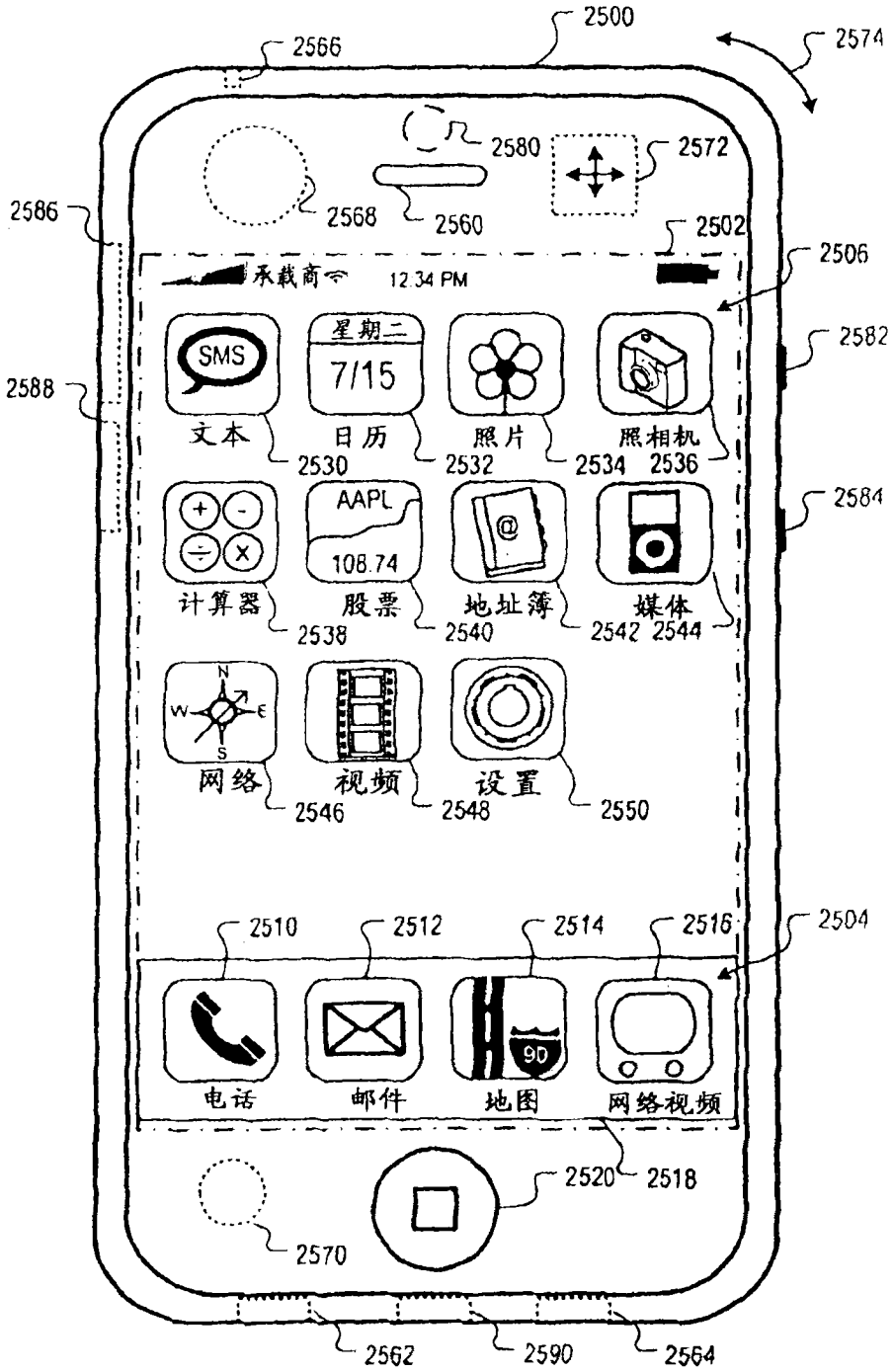

2500
2566
2574
2580
2572
2568
2560
2586
2502
2506
承载商
12:34 PM
2582
2588
SMS
星期二
7/15
文本
日历
照片
照相机
2530
2532
2534
2536
2584
AAPL
108.74
计算器
股票
地址簿
媒体
2538
2540
2542
2544
网络
视频
设置
2546
2548
2550
2504
2510
2512
2514
2516
电话
邮件
地图
网络视频
2520
2518
2570
2562
2590
2564

图 8A

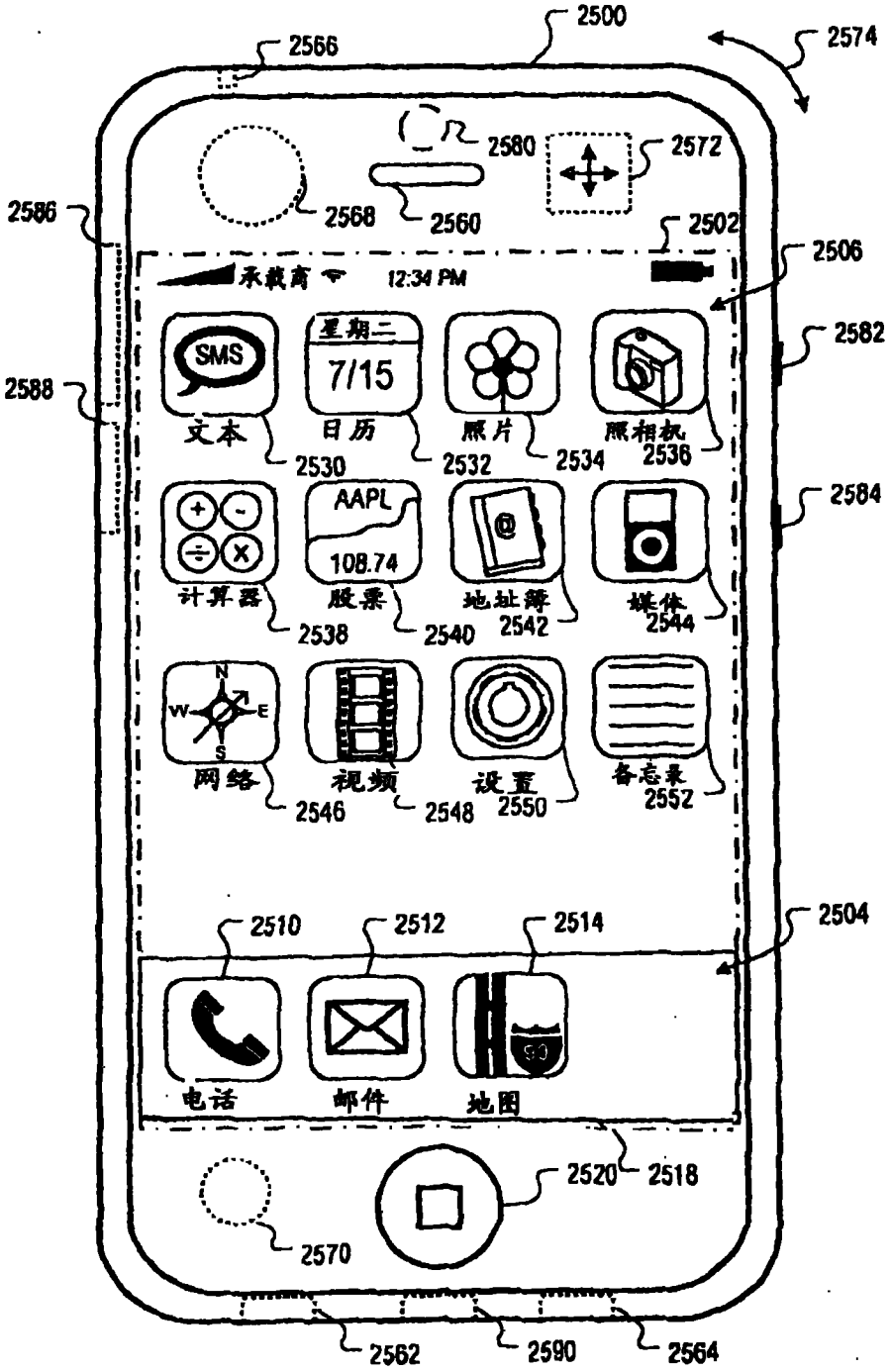

2500
2566
2574
2580
2572
2586
2568
2560
2502
2506
承载商
12:34 PM
2582
2588
SMS
星期二
7/15
文本
日历
照片
照相机
2530
2532
2534
2536
2584
AAPL
108.74
计算器
股票
地址簿
媒体
2538
2540
2542
2544
网络
视频
设置
备忘录
2546
2548
2550
2552
2504
2510
2512
2514
电话
邮件
地图
2520
2518
2570
2562
2590
2564

图 8B

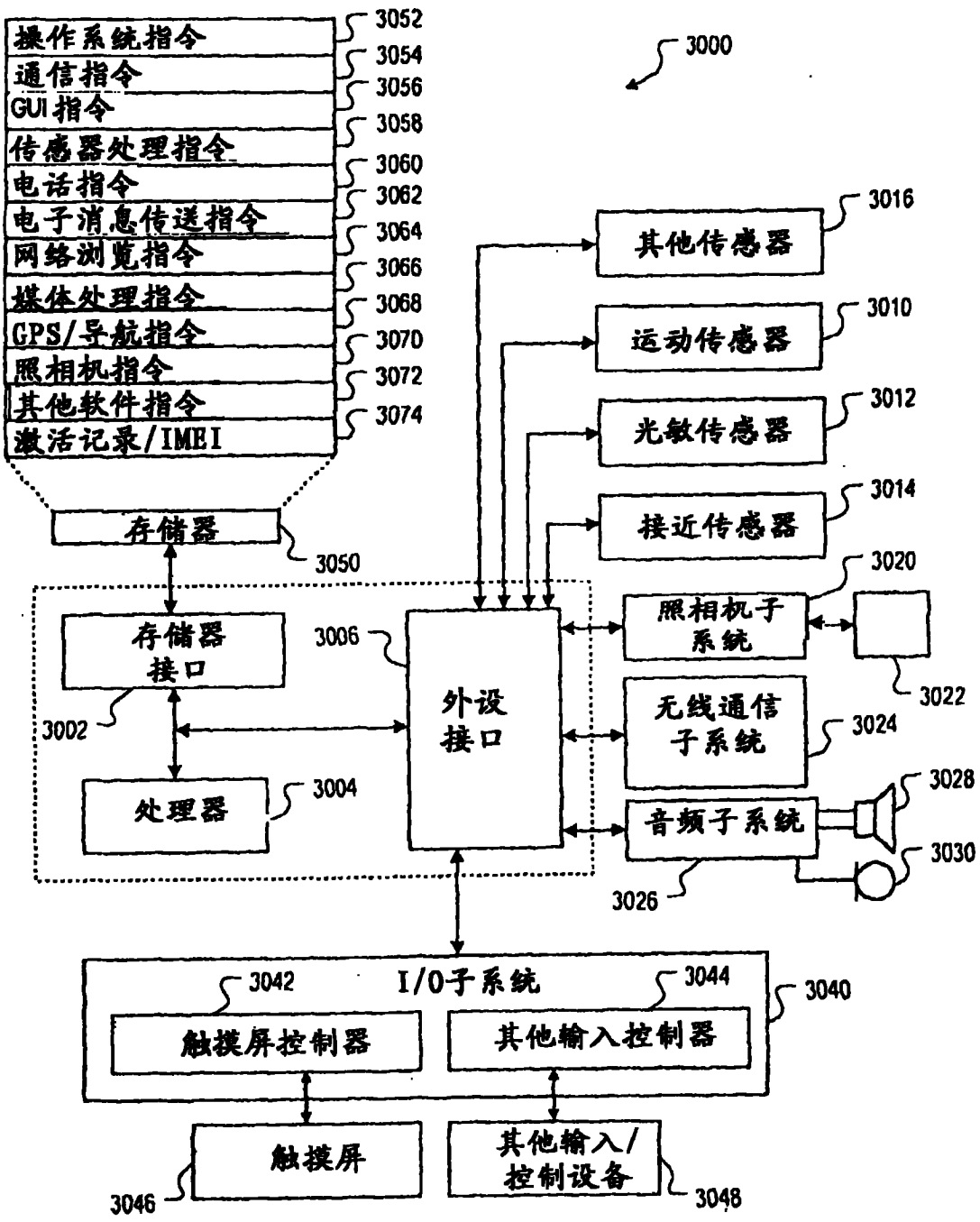

操作系统指令
通信指令
GUI指令
传感器处理指令
电话指令
电子消息传送指令
网络浏览指令
媒体处理指令
GPS/导航指令
照相机指令
其他软件指令
激活记录/IMEI
3052
3054
3056
3058
3060
3062
3064
3066
3068
3070
3072
3074
3000
存储器
3050
其他传感器
3016
运动传感器
3010
光敏传感器
3012
接近传感器
3014
照相机子系统
3020
3022
存储器接口
3002
3006
外设接口
无线通信子系统
3024
处理器
3004
音频子系统
3028
3030
3026
I/O子系统
3042
3044
3040
触摸屏控制器
其他输入控制器
触摸屏
3046
其他输入/控制设备
3048

图 9