(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 108293045 B
(45)授权公告日 2021.01.26

(21)申请号 201680066500.2

(22)申请日 2016.11.06

(65)同一申请的已公布的文献号
申请公布号 CN 108293045 A

(43)申请公布日 2018.07.17

(30)优先权数据
14/939,811 2015.11.12 US

(85)PCT国际申请进入国家阶段日
2018.05.14

(86)PCT国际申请的申请数据
PCT/US2016/060746 2016.11.06

(87)PCT国际申请的公布数据
WO2017/083209 EN 2017.05.18

(73)专利权人 微软技术许可有限责任公司
地址 美国华盛顿州

(72)发明人 E·多伊奇 Y·V·安格洛夫
S-V·永 Y·I·劳斯科夫
R·P·亚当斯 A·比布里奥威茨
H·罗玛赫

(74)专利代理机构 北京市金杜律师事务所 11256
代理人 王茂华 姚杰

(51)Int.Cl.
H04L 29/06(2006.01)
G06F 21/41(2006.01)

(56)对比文件
CN 102970292 A,2013.03.13
CN 103930897 A,2014.07.16
CN 104205723 A,2014.12.10
US 6754696 B1,2004.06.22
US 2014373126 A1,2014.12.18
WO 2015116609 A1,2015.08.06
CN 105052105 A,2015.11.11
US 2012096271 A1,2012.04.19
WO 2013071087 A1,2013.05.16
CN 104410604 A,2015.03.11
CN 104468587 A,2015.03.25
weixin_34240520.“windows azure 联合身份验证服务配置(SSO)”.《https://blog.csdn.net/weixin_34240520/article/details/92322610》.2015,
youtube.“WindowsAzureAD:"Windows Azure Active”.《https://www.youtube.com/watch?v=DiVVH3Shvg8 》.2013,

审查员 齐丽静

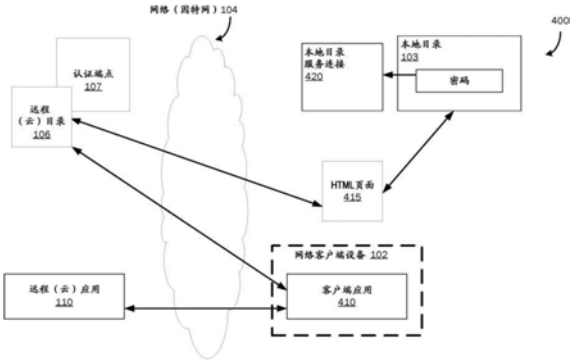
权利要求书3页 说明书15页 附图8页

(54)发明名称

本地和远程系统之间的单点登录身份管理

(57)摘要

提供了本地和基于云的系统之间的单点登录身份管理。远程或基于云的认证端点被注册为用户本地目录服务系统中的本地设备、服务或资源。请求对基于云的资源的访问的本地设备和相关联用户然后将认证端点看作内部(在企业内部)服务器,并且可以提供认证票证,认证票证包括用户的处所登入或登录身份。然后远程或基于云的认证端点可以验证认证票证,并且用户然后可以访问与远程或基于云的认证端点相关联地操作的设备、应用和服务,而无需第二次或分离的登入或登录并且无需在用户的企业网络处对附加的认证设备的使用。



CN 108293045 B

1.一种用于向远程或基于云的计算资源提供单点登录的计算机实现的方法,包括:

向本地目录服务系统将基于云的目录服务系统的基于云的认证端点注册为内联网寻址系统,以用于允许从请求对基于云的资源的访问的本地网络计算机对所述基于云的认证端点的访问;

经由所述本地网络计算机请求对所述基于云的资源的访问;

将针对与所述本地目录服务系统上的用户的身份相对应的服务票证的请求从所述本地网络计算机传递到所述本地目录服务系统,所述服务票证被所述基于云的目录服务系统利用以准许对所述基于云的资源的访问;

将与所述本地目录服务系统上的所述用户的所述身份相对应的所述服务票证从所述本地网络计算机传递到所述基于云的目录服务系统,以用于由所述基于云的目录服务系统验证与进行请求的所述本地网络计算机相关联的所述用户;

从所述基于云的目录服务系统接收所述服务票证已经由所述基于云的目录服务系统验证的指示,其中所述服务票证的所述验证基于从所述服务票证上提取的用户身份信息;以及

响应于接收到所述服务票证已经由所述基于云的目录服务系统验证的所述指示,在进行请求的所述本地网络计算机处接收对访问所请求的所述基于云的资源的授权。

2.根据权利要求1所述的计算机实现的方法,其中从所述基于云的目录服务系统接收由所述基于云的目录服务系统对所述服务票证的验证还包括:接收针对进行请求的用户的标识信息和授权信息,以用于接收对访问所请求的所述基于云的资源的授权。

3.根据权利要求1所述的计算机实现的方法,在将针对与所述基于云的目录服务系统相关联的服务票证的所述请求从所述本地网络计算机传递到本地目录服务系统之前,从所述基于云的目录服务系统接收认证错误,其中所述认证错误指示所述请求不能被认证。

4.根据权利要求1所述的计算机实现的方法,在经由本地网络计算机接收针对基于云的资源的访问的请求之前,在所述本地网络计算机处接收登录。

5.根据权利要求1所述的计算机实现的方法,其中将针对所述访问的所述请求传递到基于云的目录服务系统包括:基于所述基于云的目录服务系统作为由进行请求的所述本地网络计算机经由所述本地网络可访问的本地设备、服务或资源的指定,将所述请求传递到所述基于云的目录服务系统。

6.根据权利要求5所述的计算机实现的方法,其中将所述请求传递到所述基于云的目录服务系统包括:将所述请求传递到基于云的认证端点。

7.根据权利要求6所述的计算机实现的方法,其中将所述服务票证传递到所述基于云的目录服务系统包括:将所述服务票证传递到所述基于云的认证端点。

8.根据权利要求7所述的计算机实现的方法,在经由所述本地网络计算机来接收针对基于云的资源的访问的请求之前,在所述本地目录服务系统中为所述基于云的认证端点创建计算机标识对象。

9.根据权利要求8所述的计算机实现的方法,在将所述服务票证传递到所述基于云的认证端点之前,向所述本地目录服务系统将所述基于云的认证端点注册为本地设备、服务或资源,以用于允许所述服务票证被传递到作为本地端点的所述基于云的认证端点。

10.根据权利要求9所述的计算机实现的方法,还包括:为所述基于云的认证端点创建

用于将所述基于云的认证端点与所述本地目录服务系统相关联的专用标识符，以用于将所述本地目录服务系统和相关联的本地设备、服务或资源与所述基于云的认证端点进行链接。

11.根据权利要求8所述的计算机实现的方法，其中在所述本地目录服务系统中为所述基于云的认证端点创建计算机标识对象包括：

在所述本地目录服务系统中创建所述计算机标识对象，其中所述计算机标识对象表示所述基于云的认证端点；

经由密码或加密标识信息将所述计算机标识对象链接到所述基于云的认证端点；以及

利用所述链接以用于创建所述服务票证，所述服务票证被传递给所述基于云的认证端点以用于由所述基于云的端点对所述服务票证的验证，以用于响应于对所请求的所述基于云的资源的单点登陆尝试来认证由进行请求的用户经由所述本地网络计算机对所请求的所述基于云的资源的访问。

12.根据权利要求10所述的计算机实现的方法，其中创建用于将所述基于云的认证端点与所述本地目录服务系统相关联的专用标识符包括创建所述基于云的认证端点的服务主体名称(SPN)。

13.根据权利要求9所述的计算机实现的方法，其中向所述本地目录服务系统将所述基于云的认证端点注册为本地设备、服务或资源包括向多个本地目录服务系统将所述基于云的认证端点注册为所述多个本地目录服务系统中的每个目录服务系统中的本地设备、服务或资源，以用于允许服务票证从所述多个本地目录服务系统中的每个本地目录服务系统传递到所述基于云的认证端点，以用于针对所述基于云的认证端点来认证与多个本地目录网络服务系统中的每个本地目录网络服务系统相关联的本地网络计算机。

14.根据权利要求13所述的方法，其中所述多个本地目录服务系统中的每个本地目录服务系统与不同的租户相关联。

15.根据权利要求1所述的计算机实现的方法，还包括：

在所述基于云的认证端点处接收来自所述本地网络计算机的、针对对所述基于云的资源的访问的初始请求；

返回认证错误代码，所述认证错误代码指示所述初始请求不能被认证；

响应于所述认证错误代码，在所述基于云的认证端点处接收来自所述本地目录服务系统的、与所述本地目录服务系统上利用所述本地网络计算机的进行请求的用户的所述身份相对应的所述服务票证；以及

在所述基于云的认证端点处，针对对所述基于云的资源的访问，验证所接收的所述服务票证以认证与进行请求的所述本地网络计算机相关联的所述进行请求的用户。

16.一种用于向远程或基于云的计算资源提供单点登录的计算机实现的方法，包括：

向本地目录服务系统将基于云的目录服务系统的基于云的认证端点注册为内联网寻址系统，以用于允许从请求对基于云的资源的访问的本地网络计算机对所述基于云的认证端点的访问；

响应于在所述本地目录服务系统处的、来自所述本地网络计算机的针对与所述本地目录服务系统上的用户的身份相对应的服务票证的请求，在所述基于云的目录服务系统处从所述本地网络计算机接收与所述本地目录服务系统上的所述用户的所述身份相对应的所

述服务票证，以用于由所述基于云的目录服务系统针对对所请求的所述基于云的资源的访问验证与进行请求的所述本地网络计算机相关联的进行请求的用户；

由所述基于云的目录服务系统提供所述服务票证已经被验证的指示，其中所述服务票证的所述验证基于与所述服务票证相关联的、用于针对对所请求的所述基于云的资源的访问认证所述进行请求的用户的用户身份信息；以及

响应于接收到所述服务票证已经由所述基于云的目录服务系统验证的指示，向进行请求的所述本地网络计算机提供对访问所请求的所述基于云的资源的授权。

17.根据权利要求16所述的计算机实现的方法，其中针对对所述基于云的资源的访问认证与本地网络计算机相关联的用户包括：生成针对所述进行请求的用户的授权信息，以用于向由所述进行请求的用户对所请求的基于云的资源的访问提供授权。

18.根据权利要求16所述的计算机实现的方法，其中将基于云的认证端点注册为内联网寻址系统以用于允许从请求对基于云的资源的访问的内联网设备对所述基于云的认证端点的访问包括：将所述基于云的认证端点与所述本地目录服务系统进行链接，以用于允许所述基于云的认证端点从与所述内联网设备相关联的所述本地目录服务系统接收所述服务票证。

19.根据权利要求16所述的计算机实现的方法，其中注册所述基于云的认证端点包括：向多个本地目录服务系统将所述基于云的认证端点注册为本地设备、服务或资源，以用于允许服务票证从所述多个本地目录服务系统中的每个本地目录服务系统被传递到所述基于云的认证端点以用于针对所述基于云的认证端点认证与多个本地目录网络服务系统中的每个目录网络服务系统相关联的本地网络计算机。

20.一种用于向远程或基于云的计算资源提供单点登录的系统，包括：

至少一个处理器；以及

存储器，被耦合到所述至少一个处理器，所述存储器包括计算机可执行指令，所述计算机可执行指令在由所述至少一个处理器执行时执行方法，所述方法包括：

向本地目录服务系统将基于云的目录服务系统的基于云的认证端点注册为内联网寻址系统，以用于允许从请求对基于云的资源的访问的本地网络计算机对所述基于云的认证端点的访问；

经由所述本地网络计算机请求对所述基于云的资源的访问；

将针对与所述本地目录服务系统上的用户的身份相对应的服务票证的请求从所述本地网络计算机传递到所述本地目录服务系统，所述服务票证被所述基于云的目录服务系统利用以准许对所述基于云的资源的访问；

将与所述本地目录服务系统上的所述用户的所述身份相对应的所述服务票证从所述本地网络计算机传递到所述基于云的目录服务系统，以用于由所述基于云的目录服务系统验证与进行请求的所述本地网络计算机相关联的所述用户；

从所述基于云的目录服务系统接收所述服务票证已经由所述基于云的目录服务系统验证的指示，其中所述服务票证的所述验证基于从所述服务票证上提取的用户身份信息；以及

响应于接收到所述服务票证已经由所述基于云的目录服务系统验证的指示，在进行请求的所述本地网络计算机处接收对访问所请求的所述基于云的资源的授权。

本地和远程系统之间的单点登录身份管理

背景技术

[0001] 在联网目录服务系统中，各种组件被用于认证用户并被用于生成用于控制对网络资源的访问的授权数据，以提供授权用户对网络数据的安全网络访问，并且该授权数据拒绝未授权用户的访问。在典型的公司或其他企业网络中，计算设备、应用和服务在企业网络内得被维护和保护，并且通常仅向授权的企业人员提供对这些系统的访问。然而，随着用户经由诸如因特网(也称为基于云的系统)的分布式计算网络可访问的位于远程的计算设备、应用和服务变得越来越可用，存在用于提供对在用户的企业网络之外运行和维护的应用和服务的访问的增长的需要。为了准许对这种远程维护的应用和服务的访问，类似地存在以下增长的需要：使用现有的本地设备和/或用户身份来访问基于远程的应用和服务，使得用户对这些设备、应用和服务的访问并不困难、耗时或繁琐。

[0002] 在典型的身份管理系统中，用户可能被要求登入或登录到她的本地企业目录服务系统用于访问企业设备、应用和服务，随后进行第二次登入或登录到基于云的目录服务系统，用于访问基于远程的设备、应用或服务。备选地，用户的基于企业的目录服务系统的操作员可以安装和维护附加的本地转换设备/服务器(例如，联合服务器)，其将用户的登入或登录身份(例如，诸如用户名和密码的证书)转换为令牌，该令牌可以由远程或基于云的目录服务系统消耗以认证用户对远程设备、应用和服务的访问。首先，必须进行两次登录操作，第二次必须维护附加设备。因此，需要单点登录(SSO)身份管理，其允许用户访问远程或基于云的设备、应用和服务，从而节省时间、处理资源和设备资源，并使登录处理对用户更加高效和令人愉快。

发明内容

[0003] 提供本发明内容是为了以简化的形式介绍将在以下具体实施方式部分中进一步描述的一些概念。本发明内容不旨在标识要求保护的主题的关键特征或必要特征，也不旨作为确定所要求保护的主题的范围的辅助手段。

[0004] 本公开的各方面提供了本地系统和基于云的系统之间的单点登录身份管理。根据各方面，远程或基于云的认证端点被注册为用户本地目录服务系统中的本地地址，使得本地目录环境中的客户端应用可以在没有用户交互的情况下对端点执行认证。根据示例实现，端点可以被注册为用户本地目录中的内部网地址。由于认证端点已被注册到本地目录服务系统以被视为内部设备、服务或资源，因此请求访问基于云的资源的本地设备、应用或服务会将认证端点视为内部(在企业内部的)客户端，并且可以提供认证票证，认证票证包括用户的处所登入或登录身份。然后远程或基于云的认证端点可以验证认证票证，并且用户然后可以访问与远程或基于云的认证端点相关联地操作的设备、应用和服务，而无需第二次或分离的登入或登录并且无需在用户的企业网络处对附加的认证设备的使用。

[0005] 示例被实现为计算机过程、计算系统或者诸如计算机程序产品或计算机可读介质的制品。根据一个方面，该计算机程序产品是计算机存储介质，计算机存储介质由计算机系统可读并且对用于执行计算机处理的指令的计算机程序进行编码。

[0006] 在下面的附图和描述中阐述了一个或多个方面的细节。通过以下详细描述的阅读和相关联的附图的查看，其他特征和优点将显而易见。应当理解，下面的详细描述仅是解释性的，并不限制权利要求。

附图说明

[0007] 附图图示了各个方面，该附图被并入并且构成本公开的一部分。

[0008] 图1是用于从本地计算设备或系统利用远程或基于云的计算资源的系统的简化框图。

[0009] 图2是用于向本地目录服务系统注册远程认证端点的系统的简化框图。

[0010] 图3是图示了用于向本地目录服务系统注册远程认证端点的示例方法中涉及的一般阶段的流程图。

[0011] 图4是用于针对远程或基于云的认证端点的本地客户端设备、应用或服务的运行时认证的系统的简化框图。

[0012] 图5是示出了用于针对远程或基于云的认证端点的本地客户端设备、应用或服务的运行时认证的示例方法中涉及的一般阶段的流程图。

[0013] 图6是图示了计算设备的示例物理组件的框图。

[0014] 图7A和7B是移动计算设备的简化框图。

具体实施方式

[0015] 以下详细描述参考了附图。只要可能，在附图中使用相同的附图标记，在以下描述中指代相同或相似的元件。尽管示例可以被描述，但是修改、自适应和其他实现是可能的。例如，可以对附图中图示的元件进行替换、添加或修改，并且可以通过对所公开的方法进行替代、重新排序或添加阶段来修改本文描述的方法。因此，以下详细描述不是限制性的，而是适当的范围由所附权利要求限定。示例可以采取硬件实现，或者完全软件实现，或者结合软件和硬件方面的实现的形式。因此，下面的详细描述不应被认为是限制性的。

[0016] 本公开的方面提供了在两个或多个计算系统之间的单点登录身份管理，例如在相互之间远程操作的两个或更多个本地系统之间或本地和远程或基于云的系统之间的单点登录身份管理。根据各方面，远程或基于云的认证端点在客户端设备/服务或本地目录服务系统处向客户端设备、应用或服务注册。根据一个方面，当本地设备/服务(或其用户)试图使用设备/应用/服务时，认证端点被注册(如下所述)用于允许客户端设备/服务针对端点执行认证，经由端点针对设备/应用/服务的认证是需要的。根据一个示例操作，当本地认证请求应用是因特网浏览应用时，认证端点可以在本地客户端设备/应用/服务或用户的本地目录服务系统中被注册为内联网安全原则。在注册到进行请求的用户的本地目录服务系统的情况下，可以在本地目录服务系统中执行注册以便将认证端点标记为针对本地网络设备的设置集合(例如，在针对本地网络设备/应用/服务的组策略对象(GPO)中)中的本地设备、服务或资源(例如，内联网地址)，以便于允许远程认证端点被本地目录视为本地设备。

[0017] 如下面进一步详细描述的，当将认证端点注册到本地目录服务系统时，用于认证端点的计算机对象被添加到本地目录服务系统以用于认证端点。根据本公开的各方面，为注册认证端点创建专用标识符(例如，服务主体名称(SPN))，用于将端点与本地目录服务系

统以及与该本地目录服务系统相关联的设备、应用和服务进行关联或链接，本地目录服务系统可能需要对端点进行认证。当接收到访问远程或基于云的设备、应用或服务的请求时，其中进行请求的客户端试图对远程端点进行认证用于访问所请求的设备/应用/服务，远程认证端点针对进行请求的设备/应用/服务对象要求来自本地目录服务系统的服务票证，该进行请求的设备/应用/服务对象具有与远程或基于云的认证端点(即，请求的目标)相关联的专用标识符(例如，SPN)。

[0018] 根据一个示例方面，所添加的计算机对象使用离线域加入供应过程与本地目录服务系统相关联，其中加入域的客户端设备、应用或服务将认证端点视为内部(在企业内部)客户端并且能够提供认证票证(例如，Kerberos票证)，认证票证包括用户的处所登入或登录身份。应当理解，认证端点的注册过程可以通过以下而被执行：首先向本地目录服务系统添加计算机对象(具有相关联的专用标识符(例如，SPN))，该计算机对象表示远程或基于云的目录服务系统(和相关联的认证端点)，随后配置(“通知”或“告知”)将请求访问远程或基于云的资源的应用(例如，浏览器应用)以接受端点地址(例如，URL)作为适当的地址，以便进行请求的应用被允许从本地目录服务系统为进行请求的用户请求服务票证，然后可以在没有用户交互的情况下将其发送到认证端点。添加计算机对象可以在本地目录服务系统中全局地完成一次，以使得进行请求的客户端能够要求本地目录服务系统发布包含进行请求的用户身份的、针对给定计算机对象的服务票证。例如，配置应用以接受端点地址作为适当地址的过程可以经由本地网络设备/应用/服务的设置集合(例如，如上所述在组策略对象(GPO)中)被自动地供应，或者该注册/配置处理可以针对每个设备/应用/服务和相关联的用户手动地执行。

[0019] 根据请求，远程或基于云的认证端点可以使用秘密元数据(例如，诸如计算机名称或其它计算机标识和密码的加密的标识信息，以及针对给定设备、应用或服务的其他加密标识信息)来对认证票证进行验证，秘密元数据是在对象供应过程中为计算机对象创建的，用于消耗用户的身份。也就是说，如上所述，当新的计算机对象被添加到本地目录服务系统以用于远程或基于云的目录服务系统和相关联的认证端点时，为新计算机对象创建密码。密码(以及对象的计算机名称和相关联的本地目录服务系统域的标识)用于认证将为计算机对象发出的服务票证。根据一个示例性实现，虽然可以使用密码、计算机名称和域标识，但只有密码才足以进行验证。一旦由基于云的认证端点对用户进行认证，则用户然后可以访问与远程或基于云的认证端点相关联地运行的设备、应用和服务，而无需第二次或分离的登入或登录，也无需在用户企业处使用附加的认证设备。

[0020] 例如，用户可以在诸如她的工作场所的公司网络、学校网络、家庭网络等的本地处所企业环境中操作计算设备。用户对她本地企业的设备、应用和服务的访问可以通过在处所设备处的用户证书(例如，用户名、密码、指纹扫描、视网膜扫描、语音识别等)的输入来获得。在用户那一天的各种时间点，用户可能期望使用远离用户本地网络的基于云的设备、应用或服务或非基于云的设备、应用或服务。例如，用户的雇主可以利用基于云的生产力应用套件(例如，MICROSOFT OFFICE 365)，并且用户可以不时地希望针对她的工作或休闲利用基于云的应用中的一个或多个。同样，用户可能希望访问远程或基于云的数据库、数据中心或其他远程或基于云的数据存储装置或数据访问点，以在各种时间点处存储、取回或以其他方式使用数据。其他基于云的设备、应用或服务还可以包括各种通信服务，诸如电子邮件

和消息传送服务等。非基于云的设备、应用或服务可驻留在远离用户本地网络运行的一个或多个本地网络上。

[0021] 根据本公开的各方面，并且如上面简要描述的，远程或基于云的认证端点被注册到在客户端设备/应用/服务上或在本地目录服务系统处的用户的本地设备、应用或服务，以允许客户端对端点执行认证。当用户随后希望从其处所计算机或其他设备访问基于云的资源时，认证票证可以由她的客户端设备/应用/服务或她的处所目录服务系统发布以供客户端用于认证访问期望的远程或基于云的资源。根据这个方面，客户端设备/应用/服务或处所目录服务系统不知道发布的票证用于访问远程或基于云的资源。客户端或本地目录服务系统假定为作为本地设备/应用/服务域或网络的一部分的本地设备/应用/服务发布票证。因此，如本文所述，启用单点登录是因为客户端或本地目录服务系统不知道它启用对远程或基于云的资源的访问。

[0022] 图1是用于从本地计算设备或系统利用远程或基于云的计算资源的系统100的简化框图。如上面简要描述的，在典型的环境中，用户利用经由本地企业(例如他们的工作场所、教育场所、休闲场所等)运行的各种设备和相关联的应用和服务的计算资源，其中一个或多个设备和相关联的应用和服务可以经由本地网络联网在一起。在这样的本地网络中，个体用户对各种设备、应用和服务的访问可以在本地企业内部被监控和授权。

[0023] 如图1所示，图示了本地网络101包括一个或多个客户端设备102a-g(统称为设备102)。如本领域技术人员所理解的，网络设备102可以形成处所内联网，处所内联网可以在单个位置或设施处运行或可以跨给定企业的一个或多个分布式位置或设施运行。根据本公开的各方面，可以允许一个或多个设备102经由分布式网络104例如因特网访问在一个或多个远程或基于云的设备(例如，应用服务器108)处运行的各种远程的基于云的应用和/或服务110。非网络设备102h图示了远离本地网络101定位的计算设备，其可以与本地网络101的系统进行通信，包括经由本地网络101访问远程资源。如以下参照图2、3、4、5详细描述的，本地目录服务系统103维护设备102和关联用户的身份信息并管理本地设备102和其他设备102之间的交互，以及与基于云的目录服务系统106的交互，其用于认证对远程或基于云的设备、应用110和服务108的访问，并管理远程或基于云的设备、应用110和服务108的使用。

[0024] 如上面简要描述的，当设备102的用户期望访问在用户的本地企业网络101之外操作的设备102、应用110或服务108时，用户对远程或基于云的资源的访问必须被认证，并且根据本公开的各方面，期望用户对远程或基于云的资源的访问经由用户的单点登录而被准许，使得用户对远程或基于云的资源的访问和使用对于用户是无缝的，并且使得用户对她的处所计算设备102的单点登录用作对期望的远程或基于云的资源的登录。例如，如果用户期望使用在基于云的应用服务器108处维护和操作的文字处理应用110，则期望用户接收对所请求的文字处理应用110的认证访问作为用户对她的本地设备102的认证访问的一部分。

[0025] 图2是用于将本地计算资源注册到远程或基于云的目录服务系统的系统200的简化框图。如上面简要描述的，根据本公开的各方面，当处所计算设备102被安装在本地企业网络101中供处所企业中的一个或多个用户使用时，计算机对象(具有关联的专用标识符(例如，SPN))被添加到代表远程或基于云的目录服务系统(和相关联的认证端点)的本地目录服务系统中，随后配置(“通知”或“告知”)应用(例如，浏览器应用)，其将请求访问来自安装的设备的远程或基于云的资源，以接受端点地址(例如，URL)作为适当的地址，使得进行

请求的应用被允许为进行请求的用户从本地目录服务系统请求服务票证，服务票证然后可以在没有用户交互的情况下被发送到认证端点。如下所述，该安装/注册处理允许经由认证端点对需要认证的资源的单点登录访问，而无需附加登录要求或者无需本地企业网络101处的附加认证设备、系统和资源。即，根据此方面，由于与端点相关联的本地地址，处所设备102可对远程或基于云的认证端点执行自动认证。

[0026] 参考图2，安装工具2101图示了用于向本地目录服务系统103注册远程或基于云的目录服务系统(以及相关联的认证端点)以及用于将本地设备安装元数据和加密的认证数据(密钥)传递到远程或基于云的目录服务系统106的软件应用、模块、组件或计算机硬件组件。根据示例性方面，安装工具210用于建立本地目录服务系统103和远程或基于云的目录服务系统106之间的信任关系，使得认证端点107被视为本地目录中的另一个设备/应用/服务，使得针对给定的本地设备102的、包含相关联的用户标识信息的认证服务票证被发布，用于允许经由身份认证端点来对远程或基于云的资源进行单点登录访问。

[0027] 本地目录服务系统103图示了维护每个设备、应用或服务或其本地处所网络101中的用户的身份信息用于为所有设备102分配和实施安全策略的服务或系统，包括由一个或多个处所用户对这些设备102的认证使用、软件安装和更新等。例如，当用户登入到作为设备域的一部分的给定设备102时，设备域包括作为本地网络101的一部分图示的设备和系统102，可以查询本地目录服务系统103以确定用户名和密码或由登入用户提供的其他认证证书是可信的，以允许登入用户访问本地网络101中的期望设备、应用或服务。应当理解，设备102在其中操作的域可以跨经由分布式计算网络104连接在一起的多个物理本地网络101扩展。在一个方面，本地目录服务系统103将网络资源和设备102的名称映射到相应的网络地址，以允许网络资源和设备102之间的通信。本地目录103的一个示例是来自微软公司的活动目录(“ACTIVE DIRECTORY”)。在一些方面，本地目录服务系统103可以包括域控制器，域控制器认证并授权本地网络101内的用户和计算机根据需要彼此通信。

[0028] 在图2中所图示的系统的基于远程云端的一侧，基于云的目录服务系统106图示了基于云的目录服务系统，其可以充当基于多租户的基于云的目录和标识管理服务。根据本公开的各方面，如本文所述，基于云的目录服务系统106可将处所身份扩展到云中以提供对基于云的设备、应用和服务的访问。基于云的目录服务系统106的示例是来自微软公司的AZURE活动目录。

[0029] 认证端点107图示了允许系统之间的自动认证连接的认证服务。根据本公开的各方面，端点107可操作以接收由本地目录服务系统发布的认证票证。然后，端点107可以认证接收到的票证，用于允许代表进行请求的客户端设备/应用102、410来访问远程或基于云的资源。认证服务的示例包括来自微软公司的WINDOWS集成认证(WIA)，该WINDOWS集成认证(WIA)使用Windows操作系统的安全特征，用于提供对安全设备、应用和服务的认证访问。认证票证的示例是根据Kerberos协议的Kerberos票证。

[0030] 图2中所图示的安装数据220图示了可以从本地网络101从安装工具210传递到基于云的目录服务系统106的用于向本地目录服务系统注册远程认证端点的认证数据和标识数据。根据一个示例，安装数据220可以包括为计算机对象创建的秘密元数据(例如，加密的标识信息，诸如计算机名称和密码，以及用于给定设备、应用或服务的其他加密标识信息)，计算机对象被添加用于对象供应过程中注册的远程认证端点以消耗用户的身份。如上所

述，当针对远程或基于云的目录服务系统和相关联的认证端点的新计算机对象被添加到本地目录服务系统时，为新计算机对象创建密码。密码(以及对象的计算机名称和相关联的本地目录服务系统域的标识)用于认证将为计算机对象发布的服务票证。应当理解，这些数据可以作为加密和未加密的元数据和/或密钥传递。

[0031] 注册过程可以用于将认证端点标记为用于本地目录服务系统103的本地设备、服务或资源，使得当本地目录服务系统103被要求发布用于使用远程认证端点认证本地客户端设备102的服务票证时，本地目录服务系统103将认证端点视为另一本地设备102。如上所述，如果进行请求的本地认证请求应用是因特网浏览应用，则认证端点可以被注册为在本地客户端设备/应用/服务上或在用户的本地目录服务系统103中的用于允许对基于云的资源的单点登录访问的内联网安全原则，如本文所述。

[0032] 根据另一示例方面，注册过程可以手动执行。如上所述，注册过程的目的是在本地目录服务系统103和远程或基于云的目录服务系统106之间创建信任关系。因此，可以创建具有相关安装数据的计算机对象(例如，标识和认证数据)，并且管理人员可以手动地向远程或基于云的目录服务系统106提供安装数据。对于自动或手动注册过程，安装数据可能需要随时地更新、刷新或重新加密，以保护安装数据免受未经授权的使用。

[0033] 仍然参考图2，安装数据刷新机制215图示了不时地更新安装数据的软件模块或设备，包括更新的用户证书的重新加密和收集，并且将更新的数据经由安装工具210传递到基于云的目录服务系统106并传递到本地目录服务系统103。根据一个示例实现，安装数据220的更新或刷新可能不是必需的，但可以出于安全目的或当基础数据发生变化时而周期性地执行。例如，安装数据的更新或刷新可以包括经由本地目录服务系统103来创建新密码，随后将新密码安全地发送到远程或基于云的目录服务系统106，以便于延长或更新在向本地系统注册远程系统期间在远程或基于云的目录服务系统106和本地目录服务系统103之间建立的信任关系。

[0034] 根据各方面，密码更新也可以作为备选信任机制的一部分来执行。例如，如果用户以允许将处所身份扩展到云中以提供对基于云的设备、应用和服务(例如前述的AZURE活动目录)的访问的方式利用基于云的目录服务系统106，其中系统106启用密码回写，密码回写允许用户在基于云的目录服务系统106中重置他们的密码，使得重置密码被传播到本地目录服务系统103，那么这样的密码回写特征可以用于重置或更新远程端点计算机对象的密码。

[0035] 图3是示出了示例方法300中涉及的一般阶段的流程图，示例方法300用于当与本地目录服务系统相关联的设备、应用或服务需要访问远程或基于云的资源时，向本地目录服务系统注册远程或基于云的认证端点，使得远程或基于云的端点将作为本地设备呈现给本地目录服务系统，其中这种访问需要经由远程或基于云的认证端点进行认证。如本文所描述的，为了允许从本地网络设备102对远程或基于云的资源进行单点登录访问，远程或基于云的认证端点必须被向进行请求的本地网络设备102或向其中本地设备进行操作的本地网络目录服务系统103注册，使得在本地设备或目录服务系统与远程或基于云的目录服务系统之间建立信任关系，使得当进行请求的本地设备经由远程或基于云的认证端点请求访问远程或基于云的资源时，远程或基于云的认证端点被本地目录服务系统视为另一本地设备。

[0036] 图3中示出的方法300图示了安装和注册过程，通过该安装和注册过程，远程基于云的认证端点相对于被添加到本地网络101的、将被用于请求访问远程或基于云的资源计算机对象被注册到本地目录服务系统，如本文所述。作为在远程或基于云的认证端点与本地目录服务系统103之间创建信任关系的一部分，新的计算机对象被添加到针对远程认证端点的网络或域中，如本文所述。根据一个方面，该过程不是每当新的对象被在本地目录服务系统中创建时运行，而是发生一次，然后被更新或扩展以便于在远程和本地目录之间建立信任。

[0037] 方法300在开始操作305处开始并且前进到操作310，其中用于远程认证端点的计算机对象被添加到本地目录服务系统103，用于允许远程端点作为本地地址链接到本地目录服务系统103，使得本地设备、应用和服务可以对作为本地地址的远程端点进行认证。根据本公开的一个方面，计算机对象被添加到本地目录服务系统103以表示远程或基于云的目录服务系统106(和相关联的认证端点)。添加计算机对象可以在本地目录服务系统103中全局地完成一次，以使得进行请求的客户端能够请求本地目录服务系统103发布包含进行请求的用户身份的、针对给定计算机对象的服务票证。

[0038] 应当理解，添加到本地目录服务系统103的计算机对象可以包括用于所添加的计算机的各种标识信息，包括针对所添加的计算机的序列号、针对所添加的计算机的网络地址、针对所添加的计算机(例如，计算机、外围设备等)的类型、以及与所添加的计算机的用户相关联的证书。

[0039] 根据一个方面，使用离线域加入供应过程将新计算机对象添加到本地目录服务系统103，但是应当理解的是，计算机对象可以经由任意其他合适的机制被添加到本地目录服务系统，该其他合适的机制将允许当从所添加的计算机接收到针对远程或基于云的服务的请求时，本地目录服务系统代表所添加的计算机对象来向远程或基于云的认证端点发布认证票证。根据本公开的示例实现，如上面详细描述的，使用离线域加入过程，以便于添加表示远程或基于云的目录和相关联的认证端点的计算机对象。

[0040] 在操作315处，根据一个示例方面，被添加到本地目录服务系统的、为其注册认证端点的每个对象(例如，设备、应用或服务)可以被分配一个或多个专用标识符(例如，一个或多个服务主体名称(SPN))或可以与一个或多个唯一标识符(例如，一个或多个服务主体名称(SPN))相关联。因此，当接收到访问远程或基于云的资源的请求时，其中进行请求的客户端试图对远程认证端点进行认证以访问所请求资源，当请求客户端尝试对端点进行认证时，客户端从本地目录服务系统请求针对具有专用标识符(例如，SPN)的、与远程或基于云的认证端点相关联的的对象的服务票证。

[0041] 在操作320处，远程或基于云的认证端点107被向与新添加的计算机对象相关联的本地目录服务系统103注册，以便经由网络本地目录服务系统创建认证端点与新添加的计算机对象之间的链接。在远程或基于云的认证端点与针对端点的新添加的计算机对象之间的链接或关联通过将远程或基于云的认证端点与新添加的计算机对象经由为新添加的计算机对象创建的专用标识符(例如，SPN)进行链接和关联来执行。根据各方面，将认证端点链接到在本地目录服务系统处为认证端点创建的计算机标识对象通过安装数据220(例如，密码或其他秘密数据项)来完成，如下面参考操作330所描述。根据一个示例实现，注册认证端点包括配置(“通知”或“告知”)应用(例如，浏览器应用)，其将请求访问远程或基于云的

资源以接受端点地址(例如,URL)作为适当的地址,使得进行请求的应用被允许从本地目录服务系统为进行请求的用户请求服务票证,该服务票证然后可以在没有用户交互的情况下被发送到认证端点。例如,该注册/配置过程可以经由本地网络设备/应用/服务的设置集合(例如,如上所述在组策略对象(GPO)中)被自动地供应,或者该注册/配置处理可以针对每个设备/应用/服务和相关用户被手动地执行。

[0042] 在操作325,作为向本地目录服务系统注册远程或基于云的认证端点的一部分,远程或基于云的认证端点被标记或指定为本地设备或端点(本地于本地目录服务系统),使得当本地目录服务系统随后针对进行请求的客户端发布认证票证以用于认证注册的远程或基于云的认证端点时,本地或处所目录服务系统将不会意识到发出的票证用于远程或基于云端的设备(端点)。也就是说,本地或处所目录服务系统将假定票证被发布用于作为本地域或网络一部分的本地设备、应用或服务。根据一个示例方面,如本文所述,远程或基于云的认证端点被视为本地设备用于允许其他本地设备对端点进行认证以访问远程或基于云的资源。根据备选示例性方面,远程或基于云的认证端点可被标记、指定或被视为在本地目录服务系统处的内联网地址,以允许因特网浏览应用对远程或基于云的认证端点作为内部网站点进行认证。

[0043] 根据一个示例性方面,端点可因此被指定或标记为本地目录服务系统处的设置集合中的本地设备、服务或资源,该设置定义本地网络101将包括关于设备、应用和服务的哪些内容以及设备、应用和服务中的每一个如何相互作用。通过将基于云的目录认证端点107标记为在该设置集合中的本地设备、服务或资源,基于云的目录服务系统对于本地网络101中的加入计算机和其他设备、应用和服务将显现为另一个本地设备、应用或服务。这种设置集合的示例是组策略对象(GPO),并且这样的设置集合可以与在本地目录服务系统103处维护的诸如站点、域、组织单元等的组织信息容器相关联。

[0044] 在操作330处,在远程或基于云的端点的安装过程期间创建的所有相关安装数据220被传递到基于云的目录服务系统106和相关联的认证端点107。根据一个示例方面,安装数据220可以被传递到并存储在可以被基于云的目录服务系统106和相关联的认证端点访问的数据库中。安装数据220可以包括加入计算机对象(用于认证端点)的标识信息以及诸如用户名、密码、指纹扫描、视网膜扫描、语音识别标识等的认证信息,被利用用于访问加入计算机对象并且用于安装加入计算机对象并用于将加入计算机对象与基于云的目录服务系统106相关联,如本文所述。应当理解,针对加入的计算机对象被传递到远程或基于云的目录服务系统106的元数据和其他信息可以经由任意合适的安全方法来发送,其中信息可以被加密成一个或多个密码密钥、散列值等,用于安全地将信息传递到远程目的地。

[0045] 根据一个示例实现,当远程或基于云的目录服务系统最初被创建时,创建信息技术(IT)管理账户。为了使远程或基于云的目录服务系统接受本地目录安装数据220(使得远程目录将接受由本地目录发布的令牌),远程目录和本地目录之间的链接可以在远程目录IT管理员的授权下发生。如上所述,当将信息传递到远程目的地时,执行或监视本文描述的安装过程的企业IT管理人员使用管理人员或远程或基于云的目录的设备向远程或基于云的目录服务系统标识他/她自己,以确保本地和远程目录之间的链接值得信赖。

[0046] 在操作340处,在加入计算机设备102的初始安装之后,可以执行定期维护以根据需要不时地更新计算机对象安装数据,并且将更新的信息传递到基于云的目录服务系统

106，如上所述。例如，如果加入的计算机设备102被移动到不同的网络地址，如果与加入的计算机相关联的组件或外围设备改变等，则用于一个或多个安装数据项的加密密钥过期，更新的计算机对象信息可以被生成并传递到基于云的目录服务系统106以继续从加入的计算机访问基于云的资源。方法300在操作395处结束。

[0047] 根据本公开的各方面，可以针对多个不同的本地网络或域101执行上述远程或基于云的认证端点的注册。即，一个认证端点可以同时向多个本地目录服务系统103注册。根据这个方面，远程或基于云的目录服务系统是多租户系统，并且认证端点可以处理来自属于不同企业的不同网络的客户端的多个认证请求。根据示例方面，远程或基于云的目录服务系统和相关联的认证端点可以被启用以在单个远程或云计算资源上用租户隔离来执行服务票证验证。也就是说，可以在单个资源上执行验证，而无需逐租户地在远程或基于云的目录中使用专用设备或专用虚拟机(VM)。

[0048] 图4是一个示例系统400的简化框图，该示例系统400用于针对远程或基于云的认证端点运行时认证本地客户端设备、应用或服务，用于允许本地客户端设备、应用或服务经由处所单点登录来访问远程或基于云的资源。在远程或基于云的认证端点已经向本地目录服务系统103注册之后，如以上参考图2和图3所图示的和所述的，所添加的计算机设备102可以参与运行时操作，包括用于访问基于云的资源108、110，如以上参考图1所述。参考图4所图示的和所描述的系统仅是用于本地客户端设备的运行时认证的系统的一个示例。例如，其他系统结构和布局可以被用于其他类型的进行请求的客户端应用(例如，当地应用和其他非浏览器客户端应用)，这些请求客户端应用可以利用本地目录和远程目录之间的信任关系来认证本地客户端应用经由本地设备对远程资源的访问。

[0049] 然后参照图4，客户端应用410被图示为与客户端设备102相关联，用户可以用客户端设备102来访问基于云的设备、应用110和服务108。根据一个示例，客户端应用410可以包括因特网浏览器应用，用于允许用户经由针对期望的基于云的应用或服务的浏览操作来访问基于因特网的应用110和服务108。应当理解，客户端应用410可以包括其他类型的应用，包括生产力应用、电子邮件应用、日历应用、笔记应用等，其可操作用于在对远程或基于云端的认证端点进行认证之后访问基于云的应用和服务。例如，客户端应用410可以包括可操作用于访问基于网络的系统的电子邮件或消息传送应用，电子邮件/通信系统可以通过基于网络的系统被操作。

[0050] HTML页面415图示了页面，该页面由本地目录服务系统103用于将认证服务票证自动传递到基于云的目录服务系统106和相关联的认证服务系统，用于认证由给定设备102对所请求的远程或基于云的资源的访问。经由HTML页面415自动地向基于云的认证服务端点107发布认证服务票证避免向用户提示与第二次登录相关联的认证证书。根据各方面，可以根据任意合适的通信协议来执行去往和来自本地目录服务系统103和基于云的目录服务系统106的信息通信，包括通过将认证信息发布到与Java脚本相关联的Java馈送。根据替代方面，对于非浏览应用，HTML页面415可以不被利用，但是进行请求的应用可以实现某种其他通信方法，以通过利用本地和远程目录之间的信任关系来对远程或基于云的目录自动地进行认证，用于代表登录用户来针对服务票证请求本地目录。

[0051] 目录服务连接系统420图示了软件应用、模块、设备或其他组件，其可操作用于将针对本地客户端应用和设备410、102的用户和设备认证信息对应于基于云的认证端点107，

用于允许对端点107的认证以及设备和用户对基于云的资源的访问，如本文所述。以上参考图2描述了远程或基于云的目录服务系统106和远程或基于云的认证端点107。

[0052] 图5是示出了示例方法500中涉及的一般阶段的流程图，该方法用于向远程或基于云的认证端点运行时认证本地客户端设备、应用或服务，用于允许本地客户端设备、应用或服务经由处所单点登录来访问远程或基于云的资源。为了描述图5的目的，例如考虑用户期望从她的本地计算机设备102访问基于云的应用110，例如，基于云的文字处理应用，用于准备和/或编辑或查看文档。

[0053] 方法500在开始操作501处开始并且前进到操作505，其中进行请求的用户在本地计算机设备102处登入用于访问基于云的应用。例如，在设备102处的登入可以包括输入用户名和密码或其他认证信息作为用户的正常日常或定期登入到她的企业计算机的一部分。根据各方面，用户的登入证书(例如，用户名和密码)被传递到本地目录服务系统103。如本领域技术人员所理解的，用户对她本地网络的访问因此被认证(即，用户是她说她是的她)，然后用户被授权访问网络资源(即用户具有访问特权)。在操作510处，在登入到她的本地网络之后，期望访问基于云的应用110的用户可以启动应用，例如因特网浏览器应用410，利用该应用用户可以尝试访问期望的基于云的应用110。

[0054] 在操作515处，进行请求的应用(例如，客户端浏览器应用410)联系基于云的目录服务系统106以访问所请求的远程或基于云的资源。响应于该请求，远程或基于云的目录服务系统106向进行请求的应用返回认证错误，例如有www认证头部的401状态码，用于使进行请求的客户端应用请求服务票证，它可以用服务票证向远程或基于云的认证端点107进行认证。

[0055] 在操作520，响应于从基于云的目录服务系统106(和相关联的端点107)接收到的错误代码，进行请求的应用410向本地目录服务系统103发出用于获得服务票证的请求，该服务票证可以由进行请求的应用410使用用于向远程或基于云的端点107进行认证以获得进行请求的用户以及相关联的设备和应用102、410用于访问所请求的基于云的应用110的认证。也就是说，进行请求的应用410尝试访问认证端点107并获得具有www认证头部的401错误代码。应用知道它正在具有用户登录会话的进行请求的设备102上运行，因此，进行请求的应用向本地目录(其自身)发出请求以便接收服务票证，以便它可以用接收到的服务票证来向认证端点107重新发布请求。根据替代方面，一个或多个服务票证可能先前已经被生成并被高速缓存，并且客户端应用410可以从高速缓存而不是从本地目录服务系统103请求服务票证。

[0056] 在操作525处，目录服务连接系统420生成需要用于向基于云的认证服务端点107认证进行请求的设备/应用所需的端点服务票证。如以上参考图2和3所述，当进行请求的设备102被首先安装时，认证端点107被指定并标记为本地企业网络101内的本地设备、服务或资源。另外，如上所述，提供针对认证端点的专用标识符(例如，SPN)用于将认证服务端点107标识为进行请求的本地设备可以与其通信的组件，就像本地设备将与在本地企业网络101内部操作的任意其他设备或服务进行通信一样。

[0057] 因此，与目录服务连接系统420相关联的本地目录服务系统103生成端点服务票证，用于允许进行请求的应用和设备以与生成服务票证相同的方式与认证端点107连接，用于允许进行请求的设备与本地企业网络101内部的任意其他设备或服务连接。所生成的服

务票证可以作为基于网络的HTML页面415被自动地传递到认证端点107。根据各方面，服务票证作为HTTP请求中的头部被传递。浏览器应用410生成该请求是由于嵌入在HTML页面415中的Java脚本代码而发生的，但也可以作为例如用于到达客户端应用的不同协议的一部分来执行。

[0058] 在操作530处，进行请求的应用410用包括所发布的端点服务票证的HTTP头部将原始请求重新发送到认证服务端点107。在操作535，认证服务端点107认证所接收的端点服务票证以确定所请求的访问可被认证以允许经由进行请求的应用410访问所请求的基于云的资源。根据一个方面，所接收的端点服务票证的认证是使用在进行请求的设备的安装期间传递给认证端点的安装数据220来执行的，如参照图2和图3所图示的和所描述的。在操作540，认证端点107消耗安装数据220以针对远程或基于云的目录服务系统106向用户授权所请求的资源。也就是说，在操作540处，用户身份信息被从服务票证提取，然后用于在远程或基于云的目录中查找关于进行请求的用户的附加信息。应当理解的是，在一些情况下，接收到的服务票证可以包括足以用于认证过程的身份信息，并且附加信息查找是不必要的。

[0059] 在操作545，用户经由进行请求的设备被准许对所请求的资源的访问。因此，用户用单点登录请求并接收对期望的基于云的资源的访问，而不需要附加的本地设备，例如用于分离地认证用户对基于云的资源的期望访问的联合服务器，而不需要在运行时期间向本地目录服务系统进行通信。方法500在操作595处结束。

[0060] 在多个不同的本地网络(例如，与不同的公司、学校或其他企业相关联的多个不同的本地企业网络101)利用基于云的目录服务系统106和相关联的认证端点107的服务来访问一个或多个远程或基于云的设备、应用或服务的情况下，可能期望发现与进行请求的用户/应用/设备相关联的租户身份。根据一个方面，当用户输入她的用户名用于在与特定本地目录服务系统相关联的基于云的目录服务系统106中标识租户时，可以取回租户身份信息。有利的是，可以由单个基于云的目录服务系统106和相关联的认证端点107来提供对请求访问基于云的资源的多个租户的认证。

[0061] 已经在计算设备和系统组件以及程序模块的一般上下文中描述了实现，程序模块结合在计算机上的操作系统上运行的应用来执行。本领域的技术人员将认识到，这些方面也可以结合其他程序模块来实现。通常，程序模块包括例程、程序、组件、数据结构和执行特定任务或实现特定抽象数据类型的其他类型的结构。

[0062] 本文描述的方面和功能可以经由多种计算系统来操作，包括但不限于台式计算机系统、有线和无线计算系统、移动计算系统(例如移动电话、上网本、平板计算机或平板型计算机、笔记本计算机和膝上型计算机)、手持设备、多处理器系统、基于微处理器或可编程消耗电子产品、小型计算机和大型计算机。

[0063] 另外，根据一个方面，本文描述的方面和功能性在分布式系统(例如，基于云的计算系统)上操作，其中应用功能、存储器、数据存储和取回以及各种处理功能通过诸如因特网或内联网的分布式计算网络彼此远程操作。根据一个方面，各种类型的用户界面和信息经由机载计算设备显示器或经由与一个或多个计算设备相关联的远程显示单元来显示。例如，用户界面和各种类型的信息在墙面上显示和交互，用户界面和各种类型的信息被投影到墙面上。与实施实现的大量计算系统的交互包括按键输入、触摸屏输入、语音或其他音频输入、手势输入等，在手势输入中，相关联的计算设备配备有检测(例如，相机)功能，用于捕

获和解释用于控制计算设备的功能的用户手势。

[0064] 图6、7A和7B以及相关描述提供了在其中实践示例的各种操作环境的讨论。然而，关于图6、7A和7B所图示和讨论的设备和系统仅用于示例和说明的目的，并不限制用于实践本文所描述的方面的大量计算设备配置。

[0065] 图6是图示了实施本公开的示例的计算设备600的物理组件(即，硬件)的框图。在基本配置中，计算设备600包括至少一个处理单元602和系统存储器604。根据一个方面，取决于计算设备的配置和类型，系统存储器604包括但不限于易失性存储装置(例如，随机存取存储器)、非易失性存储装置(例如，只读存储器)、闪存或这些存储器的任意组合。根据一个方面，系统存储器604包括操作系统605和适合于运行软件应用410的一个或多个编程模块606。根据一个方面，系统存储器604包括安装工具210。操作系统605，例如适用于控制计算设备600的操作。此外，各个方面结合图形库、其他操作系统或任意其他应用被实践，并且不限于任意特定应用或系统。该基本配置在图6中由虚线608内的那些组件图示。根据一个方面，计算设备600具有附加特征或功能。根据一个方面，计算设备600包括附加数据存储设备(可移动和/或不可移动)，诸如例如磁盘、光盘或磁带。这种附加存储装置在图6中由可移动存储设备609和不可移动存储设备610图示。

[0066] 如上所述，根据一个方面，多个程序模块和数据文件被存储在系统存储器604中。当在处理单元602上执行时，程序模块606(例如，安装工具210)执行包括但不限于图3和5中所图示的方法300和500的一个或多个阶段的处理。根据一个方面，其他程序模块根据示例被使用并且包括诸如电子邮件和联系人应用、文字处理应用、电子表格应用、数据库应用、幻灯片演示应用、绘图或计算机辅助应用等的应用。

[0067] 根据一个方面，各个方面可以被实施在包括分立电子元件的电路、包含逻辑门的封装或集成电子芯片、利用微处理器的电路、或包含电子元件中或被实施在微处理器的单个芯片上。例如，各方面经由片上系统(SOC)来实施，其中图6中所图示的组件中的每个或多个被集成到单个集成电路上。根据一个方面，这样的SOC设备包括一个或多个处理单元、图形单元、通信单元、系统虚拟化单元和各种应用功能，所有这些处理单元被集成(或“烧”)到芯片衬底上作为单个集成电路。当经由SOC进行操作时，本文描述的功能经由与单个集成电路(芯片)上的计算设备600的其他组件集成的专用逻辑来操作。根据一个方面，本公开的各个方面使用能够执行诸如例如与(AND)、或(OR)和非(NOT)的逻辑运算的其他技术来实施，该其他技术包括但不限于机械、光学、流体和量子技术。另外，各方面在通用计算机或任意其他电路或系统内被实施。

[0068] 根据一个方面，计算设备600具有一个或多个输入设备612，诸如键盘、鼠标、笔、声音输入设备、触摸输入设备等。诸如显示器、扬声器、打印机等的输出设备614也根据一个方面被包括。上述设备是示例，并且可以使用其他设备。根据一个方面，计算设备600包括允许与其他计算设备618进行通信的一个或多个通信连接616。合适的通信连接616的示例包括但不限于射频(RF)发射机、接收机和/或收发器电路；通用串行总线(USB)、并行和/或串行端口。

[0069] 本文使用的术语计算机可读介质包括计算机存储介质。计算机存储介质包括以用于存储诸如计算机可读指令、数据结构或程序模块的信息的任意方法或技术实现的易失性和非易失性、可移动和不可移动介质。系统存储器604、可移动存储设备609和不可移动存储

设备610都是计算机存储介质示例(即存储器存储装置)。根据一个方面,计算机存储介质包括RAM、ROM、电可擦除可编程只读存储器(EEPROM)、闪存或其他存储器技术、CD-ROM、数字多功能盘(DVD)或其他光存储器、磁带盒、磁带、磁盘存储器或其他磁存储设备或可以用于存储信息并且可以由计算设备600访问的任意其他制品。根据一个方面,任意这样的计算机存储介质是计算设备600的一部分。计算机存储介质不包括载波或其他传播的数据信号。

[0070] 根据一个方面,通信介质由计算机可读指令、数据结构、程序模块或诸如载波或其他传输机制的调制数据信号中的其它数据来实施,并且包括任意信息传递介质。根据一个方面,术语“调制数据信号”描述具有以对信号中的信息进行编码的方式设置或改变的一个或多个特性的信号。作为示例而非限制,通信介质包括诸如有线网络或直接有线连接的有线介质,以及诸如声学、射频(RF)、红外线的无线介质以及其他无线介质。

[0071] 图7A和图7B图示了移动计算设备700,例如移动电话、智能电话、平板个人计算机、膝上型计算机等,可以利用其来实施这些方面。参照图7A,图示了用于实现这些方面的移动计算设备700的示例。在基本配置中,移动计算设备700是具有输入元件和输出元件的手持式计算机。移动计算设备700通常包括显示器705和允许用户将信息输入到移动计算设备700中的一个或多个输入按钮710。根据一个方面,移动计算设备700的显示器705用作输入设备(例如,触摸屏显示器)。如果包括,则可选的侧输入元件715允许进一步的用户输入。根据一个方面,侧输入元件715是旋转开关、按钮或任意其他类型的手动输入元件。在备选示例中,移动计算设备700集成更多或更少的输入元件。例如,在一些示例中,显示器705可能不是触摸屏。

[0072] 在替代示例中,移动计算设备700是便携式电话系统,诸如蜂窝电话。根据一个方面,移动计算设备700包括可选小键盘735。根据一个方面,可选小键盘735是物理小键盘。根据另一方面,可选小键盘735是在触摸屏显示器上生成的“软”小键盘。在各个方面,输出元件包括用于示出图形用户界面(GUI)的显示器705、可视指示器720(例如,发光二极管)和/或音频换能器725(例如,扬声器)。在一些示例中,移动计算设备700集成了用于向用户提供触觉反馈的振动换能器。在又一个示例中,移动计算设备700集成了输入和/或输出端口,诸如音频输入(例如麦克风插孔),音频输出(例如,耳机插孔)和视频输出(例如HDMI端口),用于向外部设备发送信号或从外部设备接收信号。在又一示例中,移动计算设备700集成了外围设备端口740,诸如音频输入(例如麦克风插孔)、音频输出(例如耳机插孔)和视频输出(例如HDMI端口),用于向外部设备发送信号或从外部设备接收信号。

[0073] 图7B是示出移动计算设备的一个示例的架构的框图。也就是说,移动计算设备700集成了用于实现一些示例的系统(即,体系结构)702。在一个示例中,系统702被实现为能够运行一个或多个应用(例如,浏览器、电子邮件、日历、联系人管理器、消息传送客户端、游戏和媒体客户端/播放器)的“智能电话”。在一些示例中,系统702被集成为计算设备,诸如集成个人数字助理(PDA)和无线电话。

[0074] 根据一个方面,一个或多个应用410被加载到存储器762中,并且在操作系统764上或者与操作系统764相关联地运行。应用程序的示例包括电话拨号程序、电子邮件程序、个人信息管理(PIM)程序、文字处理程序、电子表格程序、因特网浏览器程序、消息程序等等。根据一个方面,安装工具210被加载到存储器762中。系统702还包括存储器762内的非易失性存储区域768。非易失性存储区域768用于存储如果系统702断电时不应当丢失的持久信

息。应用程序410可以使用信息并将信息存储在非易失性存储区域768中，诸如由电子邮件应用使用的电子邮件或其他消息等。同步应用(未示出)也驻留在系统702上，并被编程为与驻留在主计算机上的对应同步应用交互，以保持存储在非易失性存储区域768中的信息与存储在主计算机中的对应信息同步。应当理解，其他应用可以被加载到存储器762中并且在移动计算设备700上运行。

[0075] 根据一个方面，系统702具有电源770，其被实现为一个或多个电池。根据一个方面，电源770还包括外部电源，诸如对电池进行补充或再充电的AC适配器或供电对接支架。

[0076] 根据一个方面，系统702包括执行发送和接收射频通信的功能的无线电772。无线电772经由通信运营商或服务提供商来促进系统702与“外部世界”之间的无线连接。来自和去往无线电772的传输在操作系统764的控制下进行。换句话说，无线电772接收的通信可以经由操作系统764被传播到应用410，反之亦然。

[0077] 根据一个方面，可视指示器720用于提供可视通知和/或音频接口774用于经由音频换能器725来产生可听通知。在所图示的示例中，可视指示器720是发光二极管(LED)并且音频换能器725是扬声器。这些设备可以直接耦合到电源770，使得当被激活时，即使处理器760和其他组件可能关闭用于保存电池电力，它们仍然保持开启由通知机构指示的持续时间。LED可被编程为无限期地保持开启，直到用户采取行动指示设备的开机状态。音频接口774被用于向用户提供可听信号并从用户接收可听信号。例如，除了耦合到音频换能器725之外，音频接口774还可以耦合到麦克风以接收可听输入，诸如促进电话对话。根据一个方面，系统702还包括视频接口776，其使得板载相机730的操作能够记录静止图像、视频流等。

[0078] 根据一个方面，实现系统702的移动计算设备700具有附加特征或功能。例如，移动计算设备700包括附加的数据存储设备(可移除的和/或不可移除的)，诸如磁盘、光盘或磁带。这种附加存储在图7B中由非易失性存储区域768示出。

[0079] 根据一个方面，如上所述，由移动计算设备700生成或捕获并经由系统702存储的数据/信息被本地存储在移动计算设备700上。根据另一方面，数据被存储在由设备经由无线电772或经由移动计算设备700和与移动计算设备700相关联的分离计算设备(例如诸如因特网的分布式计算网络中的服务器计算机)之间的有线连接可访问的任意数量的存储介质上。应当理解，这种数据/信息可以经由无线电772或经由分布式计算网络经由移动计算设备700访问。类似地，根据一个方面，根据众所周知的数据/信息传送和存储部件(包括电子邮件和协作数据/信息共享系统)，这些数据/信息容易在计算设备之间传送以用于存储和使用。

[0080] 例如，以上参照根据各方面的方法、系统和计算机程序产品的框图和/或操作说明来描述实现。框中记录的功能/动作可以不按如在任意流程图中所示的顺序发生。例如，取决于所涉及的功能/动作，连续示出的两个框实际上可以基本上同时执行，或者框有时可以以相反的顺序执行。

[0081] 本申请中提供的一个或多个示例的描述和说明并不旨在以任意方式限制或约束要求保护的范围。本申请中提供的方面、示例和细节被认为足以传达所有权并使其他人能够制作和使用最佳模式。实现不应当被解释为限于本申请中提供的任意方面、示例或细节。无论是组合还是分离地示出和描述，各种特征(结构和方法两者)都旨在被选择性地包括或省略以产生具有特定特征集合的示例。在被提供有本申请的描述和说明之后，本领域技术

人员可以想到落入本申请中实施的总体发明构思的更广泛方面的精神内的、不脱离该更宽泛的范围的变体、修改和备选示例。

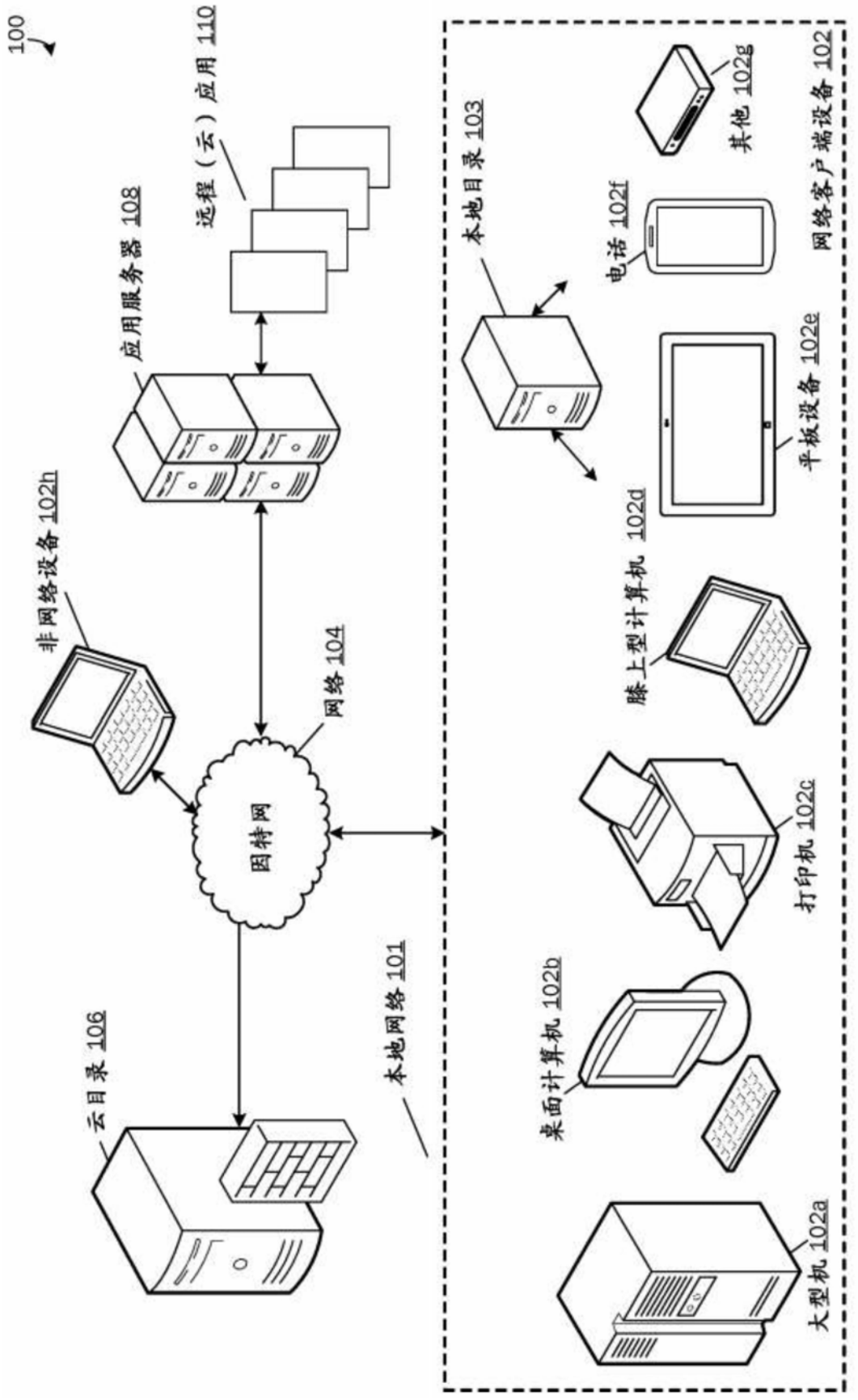

100
远程（云）应用 110
应用服务器 108
非网络设备 102h
网络 104
因特网
云目录 106
本地网络 101
本地目录 103
网络客户端设备 102
其他 102g
电话 102f
平板设备 102e
膝上型计算机 102d
打印机 102c
桌面计算机 102b
大型机 102a

图1

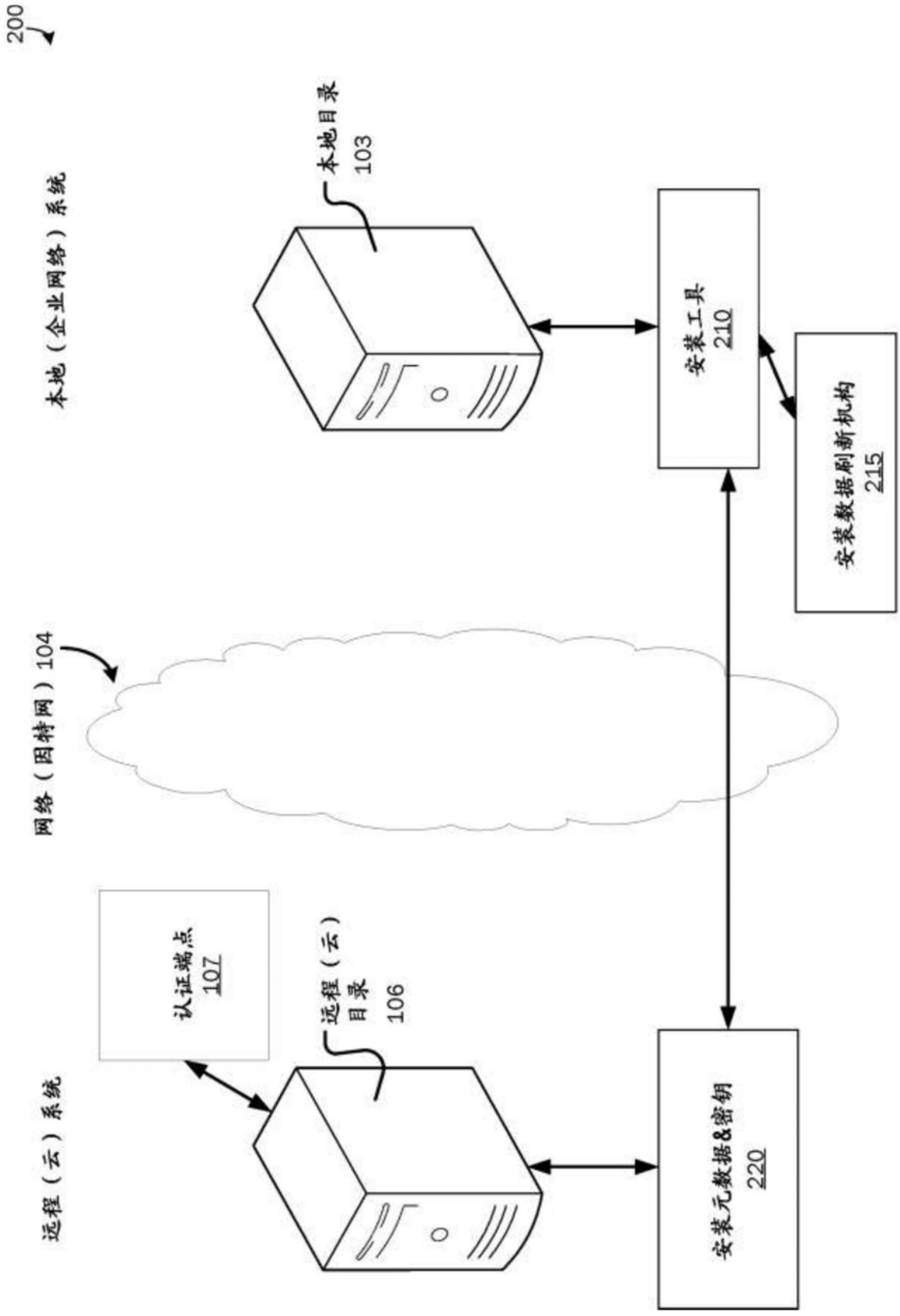

200
本地（企业网络）系统
本地目录
103
安装工具
210
安装数据刷新机构
215
网络（因特网）104
认证端点
107
远程（云）
目录
106
远程（云）系统
安装元数据&密钥
220

图2

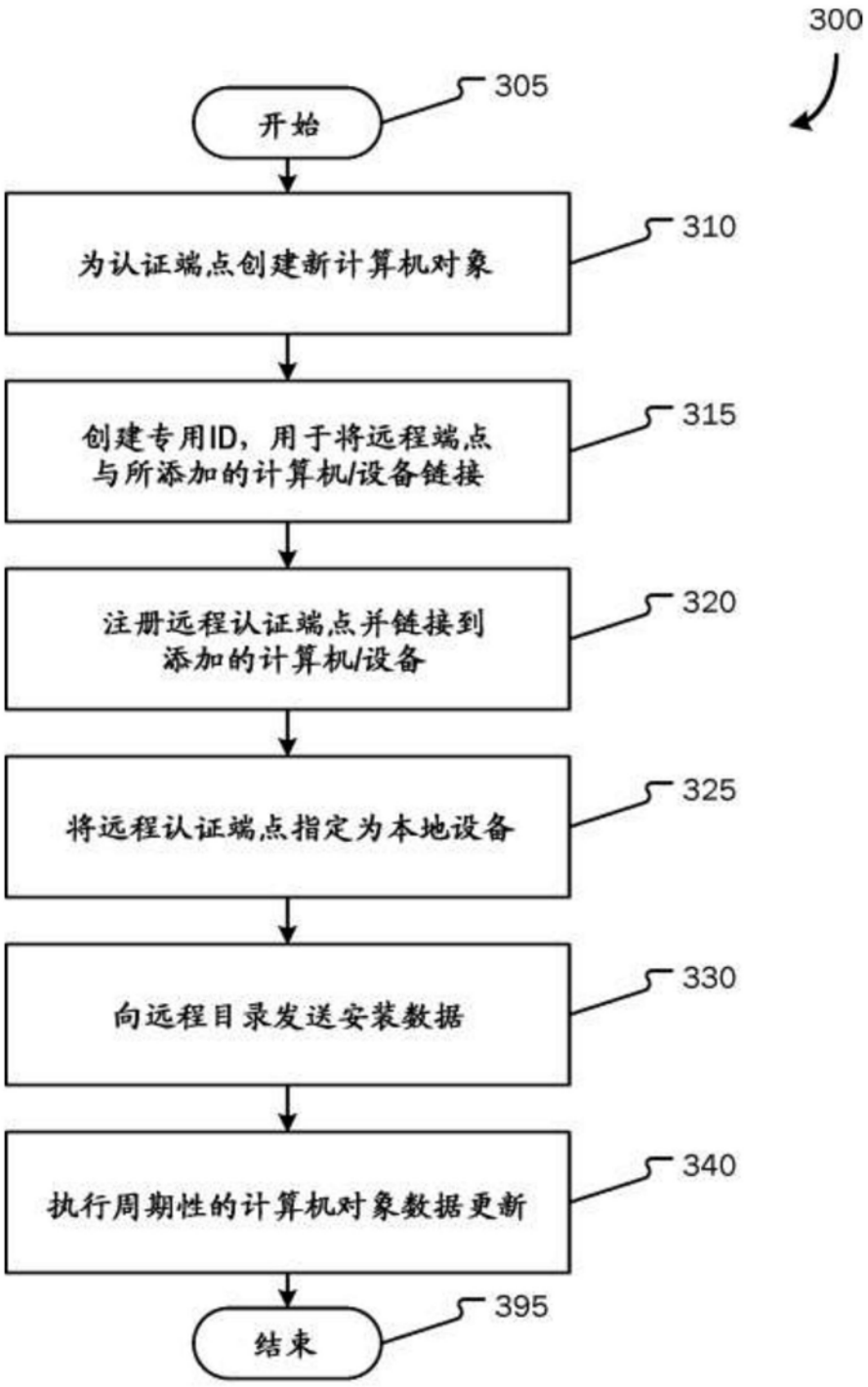

300
305
开始
310
为认证端点创建新计算机对象
315
创建专用ID，用于将远程端点
与所添加的计算机/设备链接
320
注册远程认证端点并链接到
添加的计算机/设备
325
将远程认证端点指定为本地设备
330
向远程目录发送安装数据
340
执行周期性的计算机对象数据更新
395
结束

图3

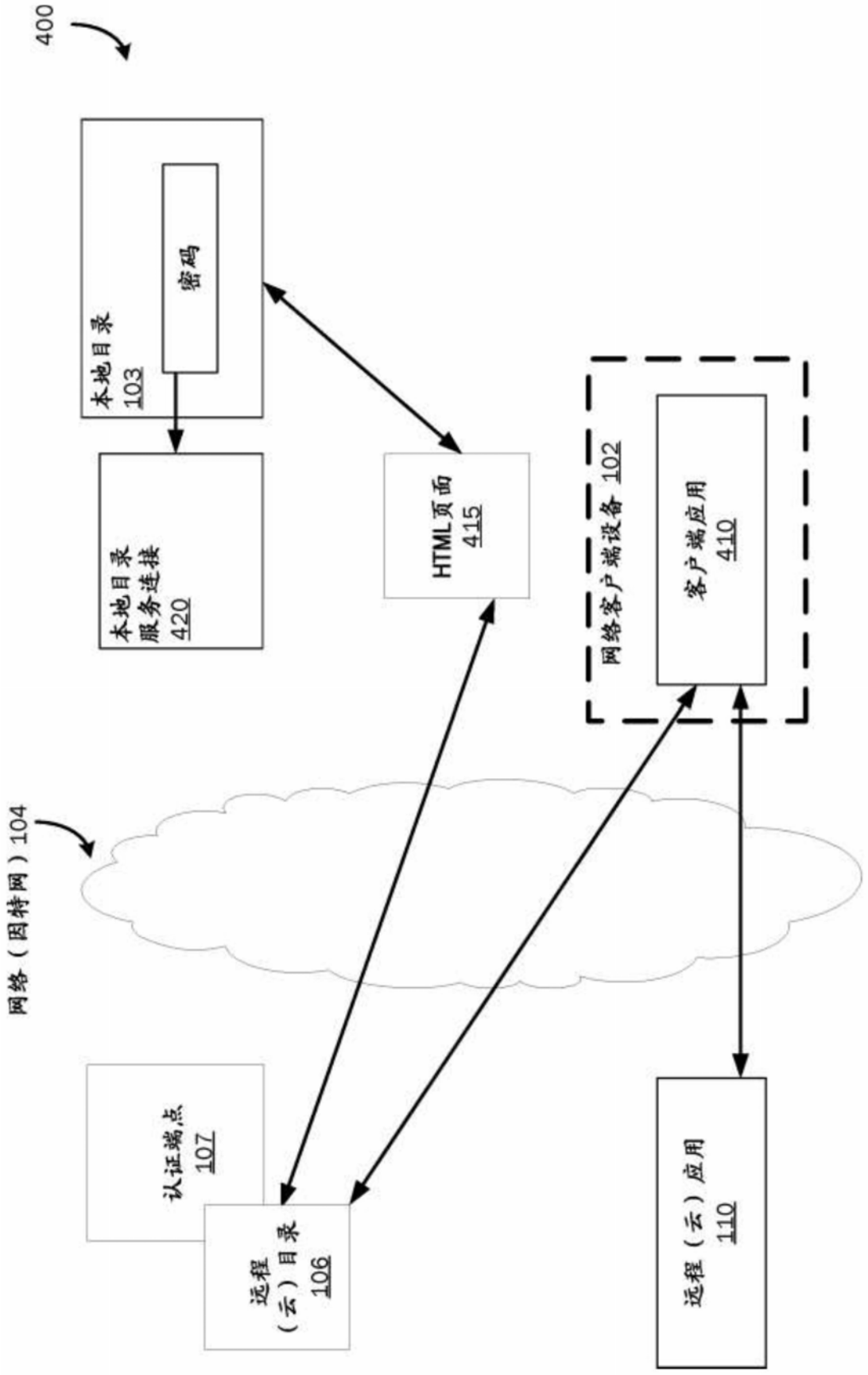

400
本地目录
103
密码
本地目录
服务连接
420
HTML页面
415
网络客户端设备 102
客户端应用
410
网络（因特网）104
认证端点
107
远程
（云）目录
106
远程（云）应用
110

图4

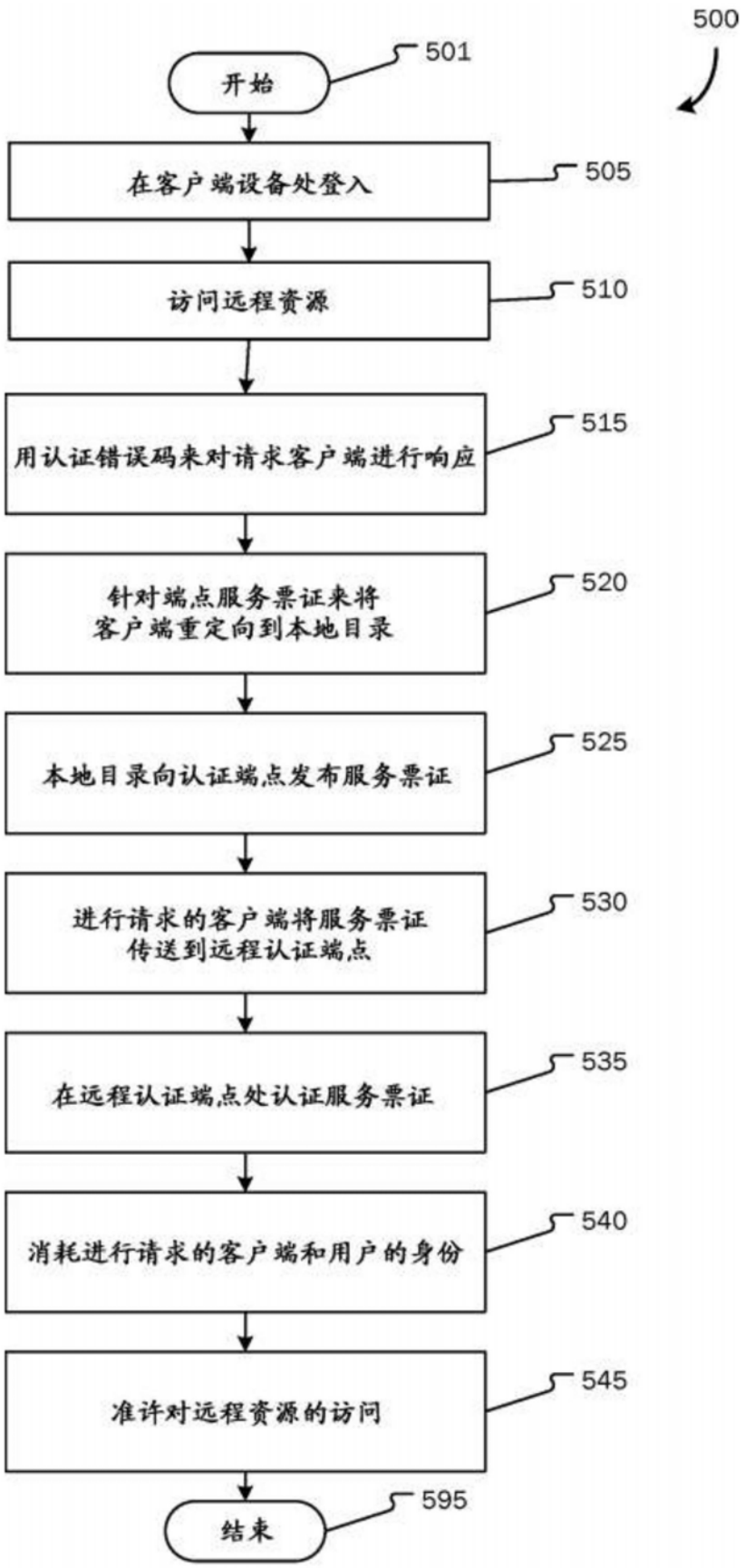

500
501
开始
505
在客户端设备处登入
510
访问远程资源
515
用认证错误码来对请求客户端进行响应
520
针对端点服务票证来将
客户端重定向到本地目录
525
本地目录向认证端点发布服务票证
530
进行请求的客户端将服务票证
传送到远程认证端点
535
在远程认证端点处认证服务票证
540
消耗进行请求的客户端和用户的身份
545
准许对远程资源的访问
595
结束

图5

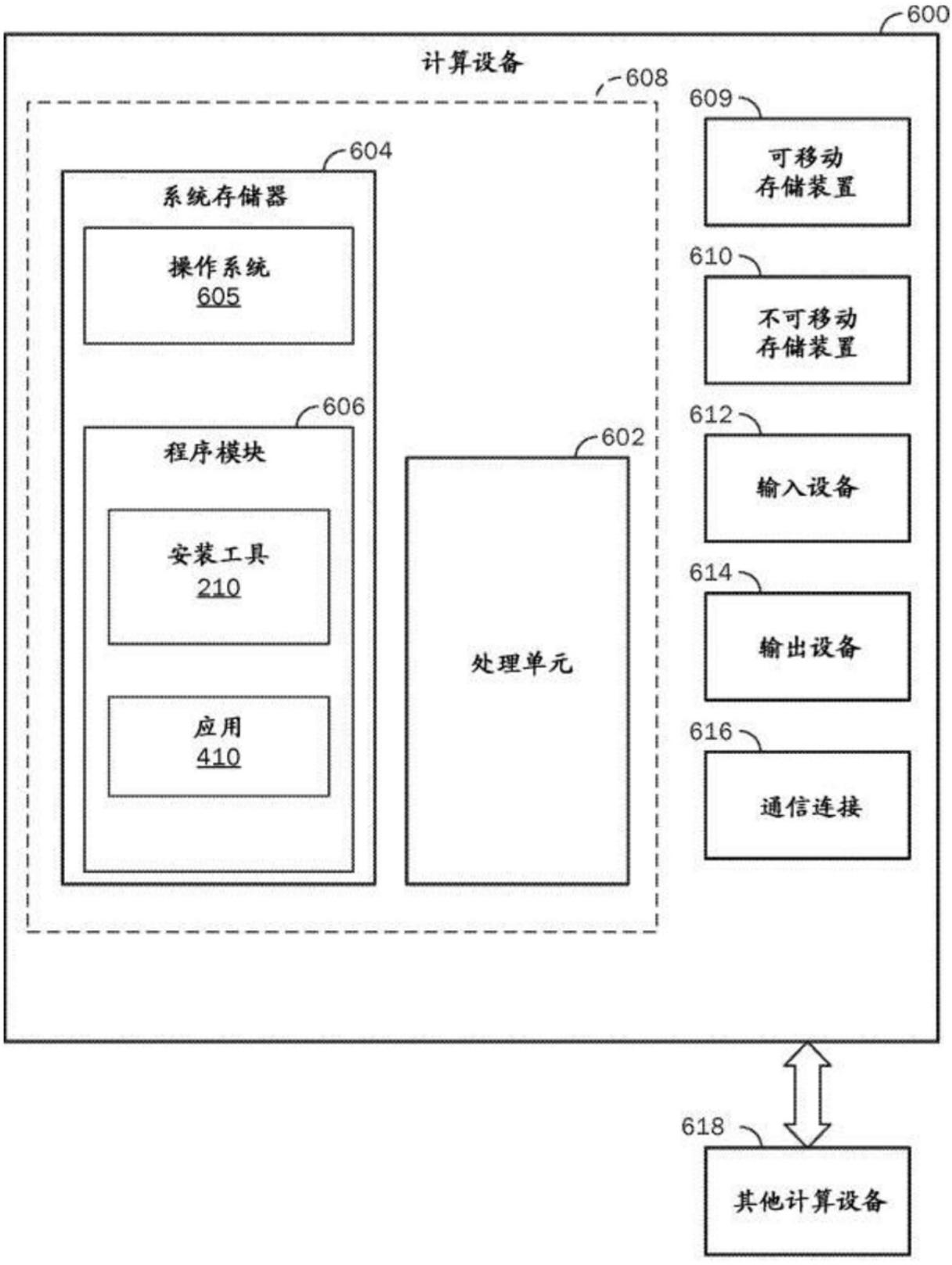

600
计算设备
608
609
可移动
存储装置
604
系统存储器
操作系统
605
610
不可移动
存储装置
606
612
程序模块
602
输入设备
安装工具
210
614
处理单元
输出设备
应用
410
616
通信连接
618
其他计算设备

图6

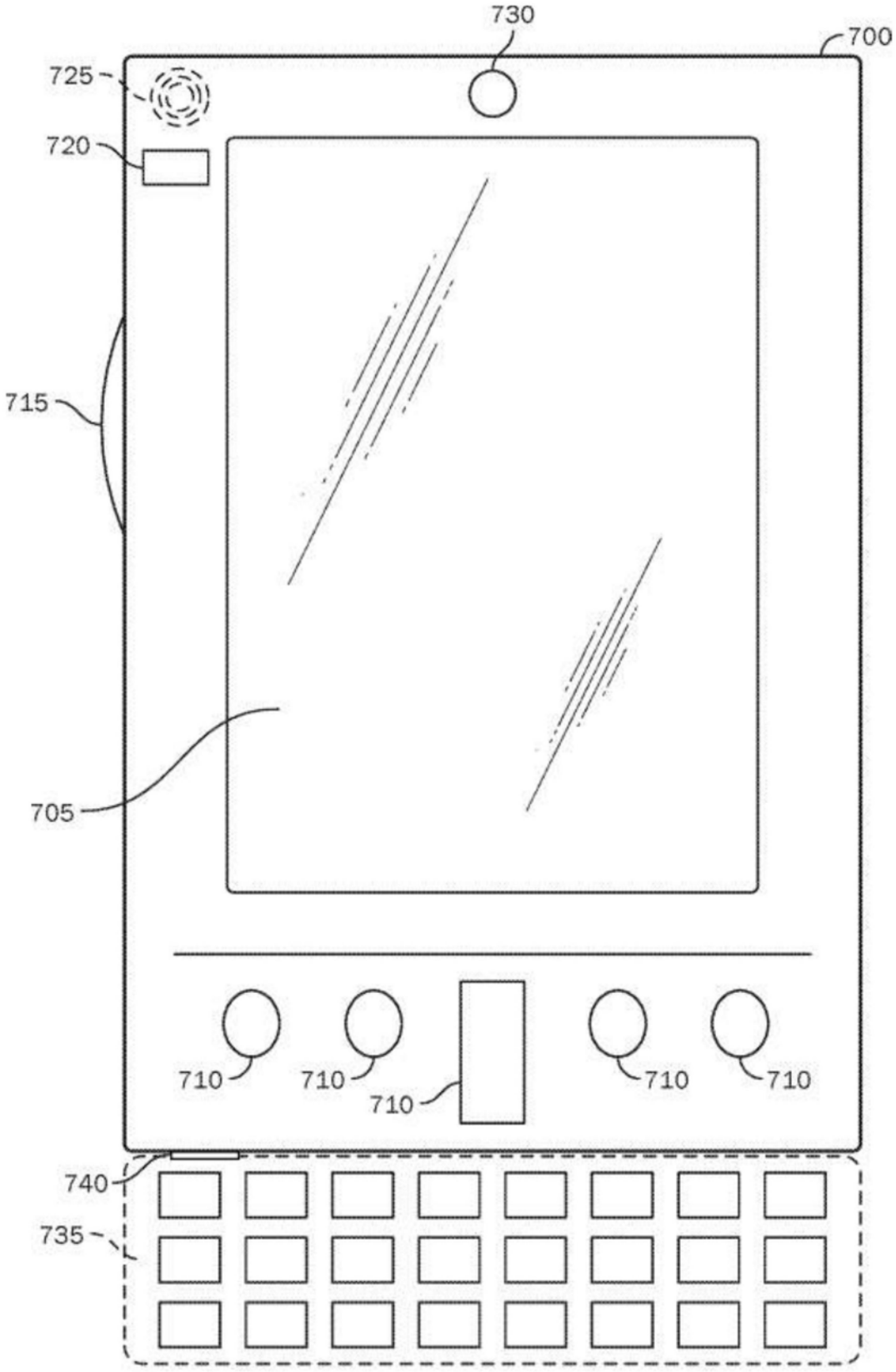


图7A

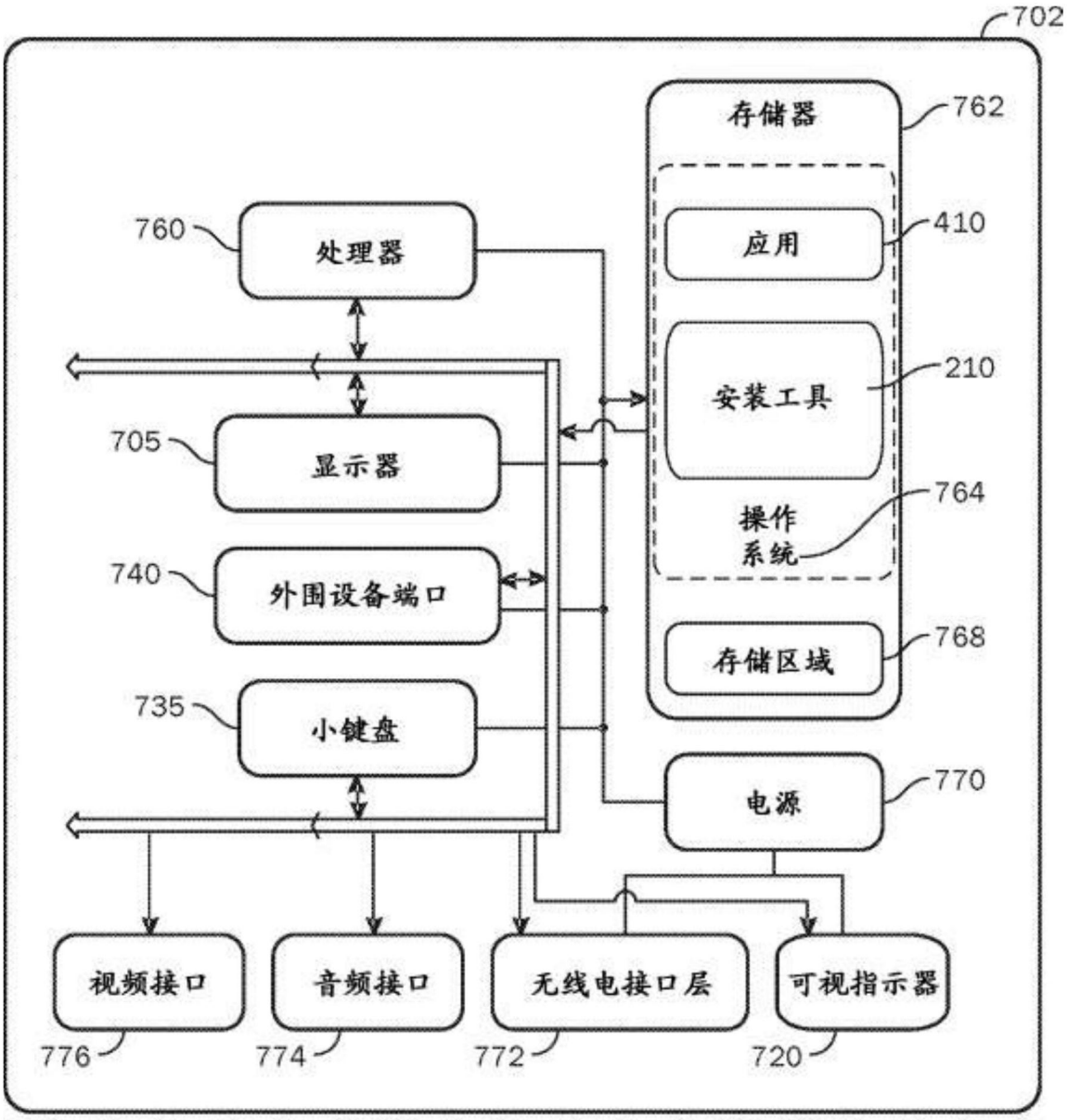

702
存储器
762
760
处理器
应用
410
安装工具
210
705
显示器
764
操作
系统
740
外围设备端口
存储区域
768
735
小键盘
电源
770
视频接口
音频接口
无线电接口层
可视指示器
776
774
772
720

图7B