(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 105659557 B
(45)授权公告日 2019.11.01

(21)申请号 201480057574.0
(22)申请日 2014.09.22
(65)同一申请的已公布的文献号
申请公布号 CN 105659557 A
(43)申请公布日 2016.06.08
(30)优先权数据
61/880,800 2013.09.20 US
(85)PCT国际申请进入国家阶段日
2016.04.20
(86)PCT国际申请的申请数据
PCT/US2014/056835 2014.09.22
(87)PCT国际申请的公布数据
WO2015/042547 EN 2015.03.26
(73)专利权人 甲骨文国际公司
地址 美国加利福尼亚
(72)发明人 M·B·曼扎 M·阿奇尔
S·W·科恩维尔 S·S·卡啪啦
(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 李晓芳
(51)Int.Cl.
H04L 29/06(2006.01)
G06F 21/41(2006.01)
(56)对比文件
US 2012011578 A1,2012.01.12,
US 2011138453 A1,2011.06.09,
CN 102638454 A,2012.08.15,
US 2013014230 A1,2013.01.10,
CN 102790712 A,2012.11.21,
审查员 周天豪

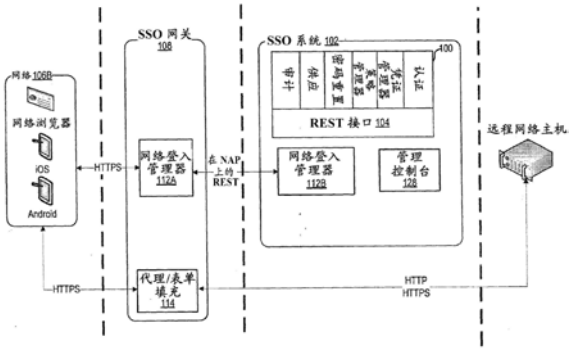
权利要求书3页 说明书29页 附图17页

(54)发明名称

用于单点登录的基于网络的接口集成的方法和系统

(57)摘要

基于网络的单点登录可以使得用户能够(诸如通过网络浏览器或瘦客户端)登入单个接口,并随后向用户提供针对一个或多个网络应用的SSO服务。基于网络的SSO系统可以被扩展以支持一个或多个不同的访问控制方法,诸如表单填充、联合的(OIF)、SSO受保护的(OAM)以及其它策略。基于网络的SSO系统可以包括用户接口,用户通过所述用户接口可以访问不同的网络应用、系统等,并管理他们的凭证。每个SSO服务可以与网络接口相关联,所述网络接口允许通过网络来访问SSO服务。所述网络接口可以为每个SSO服务提供CRUD(创建、读取、更新、删除)功能。为了支持不同的访问策略类型,基于网络的SSO系统可以包括可扩展的数据管理器,其可以透明地管理对不同类型的库的数据访问。



CN 105659557 B

1.一种用于单点登录的方法,包括:

从客户端设备接收对单点登录服务的请求,其中:

所述请求是经由与所请求的单点登录服务相关联的网络接口在计算机系统处被接收的,所述计算机系统被配置为执行多个单点登录服务,所述多个单点登录服务中的一个是所请求的单点登录服务,

所述计算机系统针对使用存储在多个数据的库中的多个单点登录数据的多个单点登录访问控制类型提供所述多个单点登录服务,

所述请求用于管理策略或凭证,以及

每个单点登录服务被配置为由不同的网络接口访问;

基于用于管理所述策略或所述凭证的请求从所述计算机系统向数据管理器发送数据请求,其中所述数据管理器透明地管理对所述多个数据的库的数据访问并且所述多个数据的库包括不同类型的数据的库;以及

经由所述相关联的网络接口返回响应到所述客户端设备;

其中所述请求是代理以第一协议在所述计算机系统处接收的,所述代理将所述请求从所述第一协议转换到第二协议,并将转换后的请求转发到所述单点登录服务。

2.如权利要求1所述的方法,其中,所述响应是所述代理以所述第二协议接收的,并且其中,所述代理将所述响应从所述第二协议转换到所述第一协议,并将转换后的响应返回给网关处的第二代理。

3.如权利要求1所述的方法,其中,所述对所述单点登录服务的请求是策略管理请求,并且所述方法还包括:

向策略管理器发送所述策略管理请求,其中,所述策略管理请求包括一个或多个策略管理操作;以及

基于所述一个或多个策略管理操作来生成数据请求。

4.如权利要求3所述的方法,其中,所述策略管理请求是针对第一接口格式化的,并且其中,所述策略管理器识别与所述策略管理请求相关联的策略管理插件,并基于所识别的策略管理插件将所述策略管理请求转换为针对第二接口的格式。

5.如权利要求1所述的方法,其中,对所述单点登录服务的所述请求是凭证管理请求,并且所述方法还包括:

向凭证管理器发送所述凭证管理请求,其中,所述凭证管理请求包括一个或多个凭证管理操作;以及

基于所述一个或多个凭证管理操作来生成数据请求。

6.如权利要求5所述的方法,其中,所述凭证管理请求是针对第一接口格式化的,并且其中,所述凭证管理器识别与所述凭证管理请求相关联的子管理器,并基于所识别的子管理器将所述凭证管理请求转换为针对第二接口的格式。

7.一种用于单点登录的系统,包括:

计算机,其包括计算机可读介质和处理器;

存储多个单点登录数据的多个数据的库,所述多个数据的库包括不同类型的数据的库;

在所述计算机上执行的多个单点登录服务,其中,每个单点登录服务与不同的网络接

口相关联，所述多个单点登录服务针对使用所述多个单点登录数据的多个单点登录访问控制类型，并且所述多个单点登录服务中的每一个被配置为：

经由单点登录服务的相关联的网络接口从客户端设备接收用于管理策略或凭证的请求，

基于接收到的用于管理所述策略或凭证的针对所述单点登录服务的请求从所述计算机向数据管理器发送数据请求，其中所述数据管理器透明地管理对所述多个数据的库的数据访问，以及

经由相关联的网络接口向所述客户端设备返回响应；

其中，所述请求是第一隧道代理以第一协议在所述计算机处接收的，所述第一隧道代理将所述请求从所述第一协议转换到第二协议，并将转换后的请求转发到所述单点登录服务。

8.如权利要求7所述的系统，其中所述第一隧道代理以所述第二协议接收所述响应，并且其中，所述第一隧道代理将所述响应从所述第二协议转换到所述第一协议，并将转换后的响应返回给网关处的第二隧道代理。

9.如权利要求7所述的系统，其中，所述请求是策略管理请求，并且其中，所述多个单点登录服务中的每一个还被配置为：

向策略管理器发送所述策略管理请求，其中，所述策略管理请求包括一个或多个策略管理操作；以及

基于所述一个或多个策略管理操作来生成数据请求。

10.如权利要求9所述的系统，其中，所述策略管理请求是针对第一接口格式化的，并且其中，所述策略管理器识别与所述策略管理请求相关联的策略管理插件，并基于所识别的策略管理插件将所述策略管理请求转换到针对第二接口的格式。

11.如权利要求7所述的系统，其中，所述请求是凭证管理请求，并且其中，所述多个单点登录服务中的每一个还被配置为：

向凭证管理器发送所述凭证管理请求，其中，所述凭证管理请求包括一个或多个凭证管理操作；以及

基于所述一个或多个凭证管理操作来生成数据请求。

12.如权利要求11所述的系统，其中，所述凭证管理请求是针对第一接口格式化的，并且其中，所述凭证管理器识别与所述凭证管理请求相关联的子管理器，并基于所识别的子管理器将所述凭证管理请求转换到针对第二接口的格式。

13.一种包括在其上存储的指令的非暂时性计算机可读存储介质，当所述指令被计算机系统的处理器执行时，所述指令使得所述处理器执行包括以下操作的方法：

从客户端设备接收对单点登录服务的请求，其中：

所述请求是经由与所述单点登录服务相关联的网络接口在所述计算机系统处被接收的，

所述单点登录服务是来自多个单点登录服务当中的单点登录服务，

所述计算机系统针对使用存储在多个数据的库中的多个单点登录数据的多个单点登录访问控制类型提供所述多个单点登录服务，

所述请求用于管理策略或凭证，以及

每个单点登录服务被配置为由不同的网络接口访问；

基于用于管理所述策略或所述凭证的请求从所述计算机系统向数据管理器发送数据请求，其中所述数据管理器透明地管理对所述多个数据的库的数据访问并且所述多个数据的库包括不同类型的数据的库；以及

经由所述相关联的接口返回响应到所述客户端设备；

其中，所述请求是代理以第一协议在所述计算机系统处接收的，所述代理将所述请求从所述第一协议转换到第二协议，并将转换后的请求转发到所述单点登录服务。

14.如权利要求13所述的非暂时性计算机可读存储介质，其中，所述响应是所述代理以所述第二协议接收的，并且其中，所述代理将所述响应从所述第二协议转换到所述第一协议，并将转换后的响应返回给网关处的第二代理。

15.如权利要求13所述的非暂时性计算机可读存储介质，其中，所述对单点登录服务的请求是策略管理请求，并且其中，所述多个单点登录服务中的每一个还被配置为：

向策略管理器发送所述策略管理请求，其中，所述策略管理请求包括一个或多个策略管理操作；以及

基于所述一个或多个策略管理操作来生成数据请求；

其中，所述策略管理请求是针对第一接口格式化的，并且其中，所述策略管理器识别与所述策略管理请求相关联的策略管理插件，并基于所识别的策略管理插件将所述策略管理请求转换到针对第二接口的格式。

16.如权利要求13所述的非暂时性计算机可读存储介质，其中，所述对单点登录服务的请求是凭证管理请求，并且其中，所述多个单点登录服务中的每一个还被配置为：

向凭证管理器发送所述凭证管理请求，其中，所述凭证管理请求包括一个或多个凭证管理操作；以及

基于所述一个或多个凭证管理操作来生成数据请求。

17.如权利要求16所述的非暂时性计算机可读存储介质，其中，所述凭证管理请求是针对第一接口格式化的，并且其中，所述凭证管理器识别与所述凭证管理请求相关联的子管理器，并基于所识别的子管理器将所述凭证管理请求转换到针对第二接口的格式。

用于单点登录的基于网络的接口集成的方法和系统

[0001] 相关申请的交叉引用

[0002] 本申请要求在2013年9月20日提交的、名称为“SYSTEMS AND METHODS FOR WEB-BASED SINGLE SIGN-ON”的美国临时专利申请No.61/880,800[代理案号为88325-887051(143801US)]的优先权，该临时专利申请的公开内容通过引用的方式全部并入本文以用于所有目的。

背景技术

[0003] 在企业中，用户(例如，雇员)通常可以有权访问一个或多个不同的系统和应用。这些系统和应用中的每一个可以利用不同的访问控制策略并且要求不同的凭证(例如，用户名和密码)。这可能需要用户对用于他们常常使用的系统和应用的许多不同凭证进行管理，这带来了密码疲劳、输入和重新输入凭证所浪费的时间、以及用于恢复和/ 或重置丢失的凭证的额外的IT资源。单点登录(SSO)可以给用户提供在初始登入(log-in)之后对多个系统和应用的访问。例如，当用户登入他们的工作计算机时，用户随后也可以有权访问一个或多个其它系统和应用。

[0004] 先前的SSO方案是基于桌面的，包括在用户的计算机上本地执行的桌面客户端，其允许用户管理他们的凭证并提供其它SSO服务和管理。这需要桌面型计算机或膝上型计算机执行客户端并访问用户的系统和应用。本地执行的客户端可以监视用户的活动以便提供单点登录服务。然而，用户正越来越多地使用可能无法执行完全桌面SSO客户端的智能电话和平板来访问基于网络的服务。附加地，这些先前的 SSO系统通常可以提供对利用相同访问控制类型的系统的单点登录，而并不集成使用不同访问控制类型的应用。结果是，SSO可以提供对用户的应用中的几个应用的单点登录，而可能仍然要求用户手动登入其它系统或应用。

发明内容

[0005] 根据一个实施例，基于网络的单点登录可以使得用户能够(诸如通过网络浏览器或瘦客户端)登入单个接口，并随后向用户提供针对一个或多个网络应用、系统和其它服务的SSO服务。基于网络的SSO 系统可以扩展以便支持一个或多个不同的访问控制方法，诸如表单填充、联合的(OIF)、SSO受保护的(OAM)、享有特权的/共享的 (OPAM)、Oauth以及其它策略。基于网络的SSO系统可以包括用户接口，通过该用户接口，用户可以访问不同的网络应用、系统等，并管理他们的凭证。每个SSO服务可以与网络接口(诸如REST接口) 相关联，该网络接口使得能够使用任何网络使能的设备通过网络访问 SSO服务，例如通过浏览器，而不需要将功能完全的客户端部署到用户的设备。该网络接口可以为每个SSO服务提供CRUD(创建、读取、更新、删除)功能性。为了支持不同的访问策略类型，基于网络的SSO 系统可以包括可扩展的数据管理器，该数据管理器可以透明地管理对不同类型的库的数据访问。

[0006] 传统地，SSO服务是(例如，通过在本地机器或本地网络上执行的SSO服务)在本地

提供的，并且被配置为使用提供策略和凭证信息的安全传输的协议来进行通信。然而，从远程的基于网络的或基于云的SSO系统访问这些相同的服务，同时维持后向兼容，存在复杂的通信挑战。客户端通常被配置为通过HTTP或HTTPS发送网络请求和接收网络响应，而SSO服务请求和响应通常使用访问协议(诸如网络访问协议或Oracle访问协议)。在本发明的一些实施例中，通过访问协议可以将请求和响应从客户端隧道化传输到访问管理器服务器。在一些实施例中，通过使用一个或多个网络接口(诸如REST接口)可以将对单点登录服务(包括凭证管理和策略管理)的访问与基于网络的或基于云的SSO系统集成在一起。

[0007] 在一些实施例中，一种方法可以包括：接收对单点登录服务的请求。可以经由与单点登录服务相关联的网络接口来接收请求。该方法还可以包括基于请求向数据管理器发送数据请求，以及经由相关联的网络接口返回响应。该请求可以包括响应于该请求的策略或凭证信息，该策略或凭证信息被客户端设备用来自动地登入应用。例如，策略信息可以包括模板，该模板可以被客户端设备用来将接收到的网络响应 (例如，进入的网页)与要通过所述进入的网页提交的凭证进行匹配，以便使用户登入应用。

[0008] 在一些实施例中，代理可以以第一协议接收请求，该代理将该请求从第一协议转换到第二协议，并将转换后的请求转发到单点登录服务。在一些实施例中，代理以第二协议接收响应，并且其中，代理将该响应从第二协议转换到第一协议，并返回转换后的响应。

[0009] 在一些实施例中，对单点登录服务的请求是策略管理请求，并且该方法还可以包括：向策略管理器发送策略管理请求。策略管理请求可以包括一个或多个策略管理操作。该方法还可以包括：基于该一个或多个策略管理请求来生成数据请求。在一些实施例中，策略管理请求可以是针对第一接口格式化的，并且策略管理器可以识别与策略管理请求相关联的策略管理插件，并基于所识别的策略管理插件将策略管理请求转换到针对第二接口的格式。

[0010] 在一些实施例中，对单点登录服务的请求可以是凭证管理请求，并且该方法还可以包括：向凭证管理器发送凭证管理请求。凭证管理请求可以包括一个或多个凭证管理操作。该方法还可以包括：基于该一个或多个凭证管理操作来生成数据请求。在一些实施例中，凭证管理请求可以是针对第一接口格式化的，并且凭证管理器可以识别与凭证管理请求相关联的子管理器，并基于所识别的子管理器来将凭证管理请求转换到针对第二接口的格式。

[0011] 在一些实施例中，可以提供一种系统，该系统包括计算机，该计算机包括计算机可读介质和处理器。该系统还可以包括在计算机上执行的多个单点登录服务。该单点登录服务可以与一个或多个网络接口相关联。该多个单点登录服务可以被配置为：经由相关联的网络接口从客户端接收用于管理策略或凭证的请求；基于用于管理策略或凭证的请求向数据管理器发送数据请求；以及经由相关联的网络接口向客户端返回响应。

[0012] 在一些实施例中，可以提供非暂时性计算机可读存储介质，包括存储于其上的指令，所述指令在被处理器执行时使得处理器执行以下步骤：接收对单点登录服务的请求，其中，该请求是经由与单点登录服务相关联的网络接口接收的；基于用于管理策略或凭证的请求向数据管理器发送数据请求；以及经由相关联的网络接口返回响应。

附图说明

[0013] 下面参考以下附图来详细地描述本发明的示意性实施例：

[0014] 图1示出了根据本发明实施例的基于网络的单点登录系统的概览图。

[0015] 图2示出了根据本发明实施例的表单填充体系架构的方框图。

[0016] 图3描绘了根据本发明实施例的响应于访问资源的请求而注入 SSO代理应用的方法的方框图。

[0017] 图4描绘了根据本发明实施例的表单填充状态图。

[0018] 图5示出了根据本发明实施例的用于在不同环境中可操作地执行的可插式单点登录应用。

[0019] 图6示出了根据本发明实施例的桌面登入管理器接口。

[0020] 图7示出了根据本发明实施例的移动登入管理器接口。

[0021] 图8示出了根据本发明实施例的登入管理器体系架构。

[0022] 图9描绘了根据本发明实施例的通过网络登入接口来访问网络应用的方法的方框图。

[0023] 图10示出了根据本发明实施例的集成了单点登录服务的SSO服务器体系架构。

[0024] 图11A和11B示出了根据本发明实施例的策略管理器体系架构和凭证管理器体系架构。

[0025] 图12描绘了根据本发明实施例的通过基于网络的接口来提供 SSO服务的方法的方框图。

[0026] 图13示出了根据本发明实施例的数据管理器体系架构。

[0027] 图14描绘了根据本发明实施例的对在多个数据存储装置上存储的凭证进行管理的方法的方框图。

[0028] 图15描绘了用于实现实施例之一的分布式系统的简化图。

[0029] 图16是根据本公开的实施例的系统环境的组件的简化方框图，通过该系统环境，实施例系统的组件所提供的服务可以被提供为云服务。

[0030] 图17示出了示例性计算机系统，在该计算机系统中可以实现本发明的各种实施例。

具体实施方式

[0031] 在以下的描述中，为了解释的目的，阐述了特定的细节以便提供对本发明实施例的透彻理解。然而，将显而易见的是，可以在不具有这些特定细节的情况下实施各个实施例。附图和描述并不旨在是限制性的。

[0032] 可以用各种配置提供在一些图中描绘的系统。在一些实施例中，系统可以被配置成分布式系统，在分布式系统中，系统的一个或多个组件分布在云计算系统中的一个或多个网络上。

[0033] 本发明的实施例涉及的是基于网络的单点登录服务，其可以使用户能够(诸如，通过网络浏览器或客户端应用)登入单个接口，并随后向用户提供针对一个或多个网络应用、企业系统和其它服务的单点登录(SSO)服务。基于网络的SSO系统可以扩展以便支持一个或多个不同的访问控制方法，诸如表单填充、联合身份、基于策略的控制、享有特权的/共享的

账户、OAuth以及其它安全系统。基于网络的SSO 系统可以包括用户接口，用户可以通过该用户接口来访问不同的网络应用、系统等，并管理他们的凭证。每个SSO服务可以与网络接口(诸如REST接口)相关联，该网络接口使得能够使用任何网络使能的设备通过网络来访问SSO服务，例如，通过浏览器而不用将功能完全的客户端部署到用户的设备。网络接口可以为每个SSO服务提供CRUD (创建、读取、更新、删除)功能性。为了支持不同的访问策略类型，基于网络的SSO系统可以包括可扩展的数据管理器，其可以透明地管理对不同类型的库的数据访问。

[0034] 图1示出了根据本发明实施例的基于网络的单点登录系统的概览图。如图1所示，可以在SSO服务器102上实现单点登录服务100。SSO服务器102可以使用一个或多个定制的网络接口104来向一个或多个不同的客户端106提供SSO服务100。在一些实施例中，SSO服务器102可以被集成到访问管理器服务器中。这允许一个或多个不同的终端用户客户端106访问并利用来自单个SSO后端的SSO服务。客户端106可以包括已经安装了SSO客户端应用106A的客户端设备，这些可以被称为胖客户端或富客户端，并且可以包括个人计算机、工作站、移动设备和其它客户端设备。附加地或可替换地，SSO服务可以由网络应用106B或浏览器应用(诸如Javascript应用)来管理和提供，从而消除在每个客户端设备上单独地供应和安装独立SSO应用的需要。如本文中使用的那样，SSO应用可以用于指代安装在客户端设备的独立SSO客户端应用或者指代基于浏览器的SSO应用。

[0035] 每个网络接口104定义客户端可以如何访问SSO服务和资源，资源包括凭证(用户名/密码、到联合的或受保护的站点的链路或者其它类型)和策略，该策略定义SSO服务如何使用凭证与应用进行交互。在一些实施例中，每个SSO服务100可以与不同的网络接口104相关联。在一些实施例中，应用可以是本地的或者是远程的，该应用包括网络应用，诸如SaaS或其它基于云的应用和/或服务。因为是基于网络的，因此用户可以使用任何因特网连接的设备来安全地访问他们的应用。虽然在本文中描述了REST(代表性状态转移)接口，但是可以使用任何基于网络的接口。

[0036] 在一些实施例中，SSO应用可以使用存储在SSO服务100中的预定义策略来识别认证事件。通过网络接口，终端用户凭证和策略可以被管理，并被应用于从客户端106A接收的请求。用户可以通过提供凭证(智能卡/邻近卡、令牌、PKI(公钥基础设施)、Windows登入、LDAP(轻量级目录访问协议)登入、生物计量设备等)来在一个客户端106处登入。随后，凭证可以被认证服务分析。在一些实施例中，一个或多个客户端侧的认证插件可以检测不同的认证事件，并收集从用户接收的凭证。每个认证插件可以与不同类型的凭证和/或不同的登入方法相关联。在一些实施例中，每个认证插件可以与一个等级相关联。在一些实施例中，等级可以被分配给凭证类型和请求类型。可以将等级存储成数字值。这使得SSO系统能够根据用户所提供的凭证的等级来改变其对登入请求的响应。例如，如果用户利用与等级1 相关联的凭证进行登入，那么当认证事件被识别出与等级2或更高等级相关联时，可以提示用户提供更高等级的凭证。在一些实施例中，可以将认证信息作为认证跟踪器(cookie)存储在用户的浏览器应用内。在从用户接收到凭证时(例如，在用户通过基于网络的登入页面等登入他们的客户端设备时)，可以从本地的或基于网络的认证服务获得认证cookie。认证cookie可以与去往SSO服务器102的网络请求包括在一起，并且可以在响应于所述请求来提供SSO服务之前验证认证cookie。在一些实施例中，不同的服务可能需要不同的认证水平，

该认证水平可以体现在不同的认证cookie中。如果用户请求服务，但是用户的认证cookie并没有授权对该服务的访问，那么用户可以被重新定向到登入页面以获得新的认证cookie。

[0037] 在一些实施例中，可以通过SSO网关108(诸如负载均衡器或其它网络服务器)来接收来自客户端106的请求。SSO网关108可以实现一个或多个访问中介110来平衡来自客户端106的请求。在一些实施例中，用户可以通过在他们的设备上执行的客户端106或者通过网络浏览器来访问SSO用户接口112A，在本文中SSO用户接口被称为登入管理器或仪表板。在一些实施例中，可以在SSO系统实现SSO 用户接口112B。在一些实施例中，SSO用户接口108可以包括用户通常利用的应用的列表。用户可以通过SSO用户接口来管理他们的与应用相关联的凭证和策略。当用户通过用户接口请求访问应用时，SSO 用户接口可以确定该应用的策略类型并基于该策略类型来获取用户的凭证。在一些实施例中，授权模块118可以验证与该请求包括在一起的认证cookie，以确定用户是否被授权获取凭证。如果被授权，那么可以使用该凭证使用户登入应用。可以在不同的库中维持各种凭证和策略。当接收到用于访问、获取、更新、删除或以其它方式与所存储的凭证和/或策略交互的请求时，SSO服务100可以通过数据管理器 122访问相应的库120。在一些实施例中，SSO代理114可以使用户能够直接通过网络浏览器使用SSO服务来访问网络应用116，而不需要首先访问SSO用户接口110或使用在用户的设备上执行的客户端。在一些实施例中，SSO服务100可以访问身份管理器124(诸如，公司目录)来验证用户的身份。

[0038] 在一些实施例中，SSO服务100可以对许可/拒绝对应用的访问进行管理，包括自动登录、应用密码改变和重置、会话管理、应用凭证供应以及会话内部和会话外部的认证。在一些实施例中，SSO系统 102可以为在客户端设备上运行的或从客户端设备访问的Windows、网络、Java和基于主机/终端的应用提供自动的单点登录功能性。登入管理器112A可以监视会话，自动地检测来自应用的登入请求，并根据与该请求相关联的特定登入要求自动地完成登入。

[0039] 在一些实施例中，可以支持各种应用和凭证类型，诸如Oracle 访问管理保护的资源、联合应用/资源和表单填充应用。对于OAM保护的资源，用户请求可以被认证，并且随后被定向到与所请求的资源相关联的URL。对于联合应用，可以提供到联合的伙伴和资源的链路，包括商业对商业(B2B)伙伴应用和SaaS应用。对于表单填充应用，可以使用模板来识别应用网页的字段，可以通过该应用网页的字段来提交凭证。

[0040] 如上面所描述的，可以通过各种客户端应用(包括多个基于浏览器的访问方法)来提供基于网络的SSO服务。如下面进一步讨论的，用户可以通过SSO网关108访问应用并接收SSO服务。一个访问方法使用户能够通过自动地安装在用户浏览器中的嵌入式SSO应用来透明地访问SSO服务。在一些实施例中，用户可以使用他们的浏览器来访问网络登入管理器以便访问应用、管理策略和凭证以及以其它方式消费SSO服务。下面进一步讨论这些以及其它访问方法。

[0041] 利用表单填充代理应用的基于网络的单点登录

[0042] 根据实施例，可以通过SSO代理来传递对网络应用的请求。当 SSO代理接收到来自网络应用的响应时，代理可以用策略信息和其它有效载荷内容来增强该响应、嵌入将SSO处理卸载到客户端设备的 SSO应用、以及根据需要重写该响应的内容。嵌入的应用(在一些实

施例中其可以被实现成Javascript应用)利用客户端设备的处理能力来执行单点登录功能性。通过将大量的SSO处理卸载到客户端设备,这种方案可以容易地调整以适应许多设备。将SSO功能性添加到基于网络的接口还改进了用户体验。

[0043] 图2示出了根据本发明实施例的表单填充体系架构200的方框图。如上面所描述的,可以通过SSO网关108来访问SSO系统102。SSO网关108可以包括表单填充代理,表单填充代理将SSO应用嵌入到客户端的网络浏览器应用中。在一些实施例中,SSO应用可以是Javascript应用,其可以通过SSO网关108与访问管理器服务器102 上的SSO网络服务通信,以管理凭证并获得策略。

[0044] 根据实施例,用户可以通过在客户端设备106B上执行的网络浏览器来访问网络应用202。网络应用202可以是基于网络的电子邮件服务、商业应用或任何其它网络应用。客户端设备106B可以发送用于访问网络应用202的请求204,其被SSO网关108拦截。SSO网关 108可以将该请求转发给网络应用202,并且可以拦截来自网络应用的响应206。在一些实施例中,SSO网关108可以修改该请求,使得来自网络应用202的任何响应都被返回到SSO网关108。在将该响应返回到发出请求的客户端106B之前,SSO网关108可以将该响应206 传递到SSO网关108处的SSO代理114。SSO代理114可以修改该响应以包括额外的数据208,该额外的数据208提供对各种SSO特征的访问。

[0045] 例如,代理可以将诸如Javascript之类的SSO应用代码添加到该响应,该SSO应用代码使得SSO功能能够从浏览器被调用并执行。SSO应用可以在用户设备106B处执行,以识别表单可填充页面和字段、请求来自SSO服务器的策略并管理凭证。如下面进一步描述的,可以通过网络接口向SSO系统102发送凭证和策略请求。例如,SSO 应用可以检测从网络应用接收到的登入页面。SSO应用可以读取针对网络应用的策略并获取凭证。使用该凭证,SSO应用可以使用获取的凭证自动地填充登入页面的适当字段,并提交登入请求。如果登入失败,那么SSO应用可以检测登入失败并执行登入失败流程,该登入失败流程例如使得用户能够重置和/或恢复他们的针对网络应用的凭证,并利用SSO服务器更新他们的凭证。

[0046] 根据实施例,代理可以将额外的内容208添加到从网络应用接收到的响应中。额外的内容208可以包括模板和策略。模板可以被SSO 应用用来识别表单可填充页面和字段,并确定如何将凭证添加到这些字段。通过将SSO应用添加到网络页面响应,从后端系统将大量的 SSO处理卸载下来,并卸载到用户设备上。通过将大量的处理卸载到终端用户,降低了SSO服务器处的处理需求,从而带来了与先前的系统相比更具有可扩展性的SSO方案。

[0047] 图3描绘了根据本发明实施例的响应于访问资源的请求而注入 SSO代理应用的方法300的方框图。在方框302,可以从客户端设备接收用于访问网络应用的请求。如上面所描述的,可以在与SSO系统相关联的SSO网关处接收该请求。在一些实施例中,来自客户端设备的请求可以是对与网络应用相关联的网页的请求(例如HTTP请求)。该请求可以是从客户端设备接收的,其中所述客户端设备不包括在设备上执行的SSO客户端。

[0048] 在方框304,可以将该请求传递到网络应用。在一些实施例中, SSO网关可以记录与该请求有关的信息(时间、日期、网络地址等) 以供后续审计或其它目的。在方框306,接收来自网络应用的响应。该响应可以是网页,该网页包括供用户提供登入信息的字段。在方框 308,该响应可以被增强以包括策略数据和单点登录应用,以创建增强的响应。在一些实施例中,可以重写该响应,以提供该用户的企业系统的类似外观和感觉。例如,可以修改响

应于用户请求的网页的颜色方案和布局，以显得类似于用户的内部内联网的颜色方案和布局。在方框310，将增强的响应返回给客户端设备。

[0049] 在一些实施例中，单点登录应用是Javascript应用。单点登录应用可以在用户的浏览器应用中执行，并且提供SSO服务。例如，SSO 应用可以请求来自SSO系统的策略和模板，并且使用该策略和模板将响应于对网络应用的请求而接收到的页面与对应策略匹配。SSO应用可以自动地将适当的用户凭证注入到网络页面响应的匹配字段中，并将该凭证提交给网络应用。通过这种方式，在不需要在用户的客户端设备上供应并安装单独的SSO客户端应用的情况下，实现了单点登录。

[0050] 在一些实施例中，单点登录应用可以包括与不同的硬件、操作系统、浏览器或它们的组合相关联的可执行脚本。SSO应用可以被配置为：识别与客户端设备相关联的平台，以及将自身配置为执行一个或多个特定于平台的操作。该平台可以指客户端设备类型(桌面、移动设备、工作站或其它硬件配置)、浏览器应用类型和/或操作系统中的一个或多个。

[0051] 一旦被安装，SSO应用就可以通过用户的浏览器向用户提供SSO 服务，而不需要单独的SSO客户端应用。图4描绘了根据本发明实施例的SSO应用状态图。如图4所示，在方框402，在用户的浏览器中执行的SSO应用可以请求与网络应用相关联的策略。该请求可以是根据SSO系统所提供的网络接口而格式化的网络请求。如果没有返回任何策略，那么SSO应用的执行可以结束，并且可以在用户的浏览器中打开该网络应用，而不提供任何额外的SSO服务(例如，在没有发现针对该网络应用的任何策略的情况下，SSO应用不添加凭证或不会使用户登入该网络应用)。

[0052] 如果返回了至少一个策略，那么在方框404，SSO应用可以将该策略与网络应用所返回的页面进行匹配。例如，一个策略可以与登入页面相对应，而不同的策略可以与密码改变页面相对应。每个策略可以与页面模板相关联。在进入的页面与策略匹配时，该进入的页面与所存储的模板页面进行比较。例如，模板可以定义在给定页面中出现的各种字段和类型、识别内容的位置、标记、标签等。当进入的页面与给定模板匹配时，可以使用与该模板相对应的策略来提供针对该页面的SSO服务。在一些实施例中，策略可以定义针对匹配的页面要采取什么动作(例如，要提供哪些凭证、要如何提供这些凭证等)。如果没有策略相匹配(这指示不存在与进入的页面相匹配的模板)，那么可以向用户呈现进入的页面，而不提供任何进一步的SSO服务。

[0053] 一旦已经匹配了策略，那么在方框406，SSO应用就可以请求来自SSO服务器的凭证。如果返回一个或多个凭证，那么在方框408， SSO应用可以调用登入选择器。在一些实施例中，在方框410，可以在用户的客户端设备上向用户显示登入选择器，从而允许用户从返回的凭证中进行手动选择。一旦用户已经使用登入选择器选择了凭证，在方框412，SSO应用就可以注入所选择的凭证并提交登入请求。

[0054] 在一些实施例中，一旦用户已经做出了选择，就提交所选择的凭证，并且在方框414，SSO应用可以证实登入结果。如果登入被成功地执行了，那么在方框416，SSO应用可以向SSO服务器发送基于用户的选择更新用户的针对该页面的凭证的请求。这样，当用户稍后请求该网络应用时，可以返回所选择的用户凭证而不需要用户从登入选择器手动选择凭证。在一些实施例中，可以在向用户显示登入选择器之前执行自动化的登入选择器过程。例如，如果返回较少数量的凭证，那么SSO应用可以自动地按顺序提交每个返回的凭证，直到

检测到成功登入为止。SSO应用随后可以向SSO服务器发送更新请求以更新用户针对该网络应用的凭证。

[0055] 如果仅仅返回一个凭证，那么处理可以绕过方框410，并去往方框412，在方框412中，可以将该凭证注入到页面中，并提交该凭证，而不需要来自用户的进一步输入。一旦已经提交了凭证，SSO应用就可以监视登入请求的状态。在一些实施例中，如果登入失败了，那么处理可以结束。在一些实施例中，如果登入成功，那么在方框416，可以保存凭证。

[0056] 如果没有返回任何凭证，那么可以在用户的浏览器中向用户显示进入的页面，并且在方框418，SSO应用可以获取用户手动输入的凭证。可以提交用户输入的凭证，并且可以监视登入结果。如果登入是成功的，那么在方框416，对凭证进行保存，并且使用户登入网络应用。如果登入失败，那么可以向用户显示网络应用的登入失败页面。在一些实施例中，SSO应用可以自动地检测登入失败页面，将策略与登入失败页面匹配，并执行与登入失败相对应的流程(诸如密码恢复或重置)。

[0057] 在一些实施例中，用户可以选择在网络应用处执行密码改变 (PWC)。SSO应用可以(例如，使用针对该网络应用定义的PWC 模板)检测PWC页面，并且在方框418可以获取用户提供的凭证。 SSO应用可以监视PWC过程，并且如果成功，那么在方框416可以将新的凭证保存到SSO服务器。如果PWC没有成功，那么可以向用户显示网络应用的PWC失败页面。在一些实施例中，SSO应用可以自动地检测PWC失败页面，将策略与PWC失败页面匹配，并且执行与PWC失败相对应的流程(诸如，重新执行PWC流程以及向用户指示失败的原因)。

[0058] 如图4所示，方框402、406、410和416处的处理(例如，获得策略和凭证、保存凭证以及获得针对登入选择器的用户设置)涉及与 SSO服务器进行通信。然而，其它的处理步骤(包括监视PWC和登入尝试的成功、策略和模板检测、凭证注入等)可以由浏览器中的SSO 应用执行。这减少了SSO服务器所需要的处理资源的量，并使得在不耗尽系统资源的情况下添加额外的用户更加容易。

[0059] 在一些实施例中，SSO服务器可以从单点登录应用接收对与网络应用相关联的策略的请求。SSO服务器随后可以向数据管理器发送对所请求的策略的请求。如果返回一个或多个策略，那么SSO服务器可以向单点登录应用发送包括所述一个或多个策略的响应。如果没有返回任何策略，那么SSO服务器可以向SSO应用返回指示没有与网络应用相关联的策略的响应。

[0060] 在一些实施例中，SSO服务器可以从单点登录应用接收对与用户相关联的用于访问网络应用的凭证的请求。SSO服务器随后可以向数据管理器发送对所述凭证的请求。如果返回一个或多个凭证，那么SSO 服务器可以向单点登录应用发送包括所述一个或多个凭证的响应。 SSO应用随后可以向用户呈现登入选择器，用以从所述一个或多个凭证中进行选择。如果没有返回任何凭证，那么SSO服务器可以向SSO 应用返回指示没有凭证与该用户和该网络应用相关联的响应。

[0061] 在一些实施例中，SSO应用可以包括凭证管理器，该凭证管理器可以搜索并列出凭证、执行自动和手动密码改变(PWC)处理、登入选择器以及登入失败。如上面所描述的，在一些实施例中，可以响应于对网络应用的请求而将SSO应用安装在用户的浏览器中，例如可以将SSO应用添加到发送给用户的增强的响应中。这样，SSO应用可以被初始化为与包括SSO应用的进入的响应网页相对应的状态。

[0062] 在一些实施例中，可以从网络登入管理器(WLM)发起网络应用请求，如下面进一步描述的那样。在这样的实施例中，SSO应用可以(例如，通过检查查询串、会话存储信息或其它信息)从WLM获得凭证信息。使用来自WLM的凭证信息使得SSO应用能够避免从 SSO服务器请求凭证信息，这进一步减少放置在SSO服务器上的负荷。

[0063] 在一些实施例中，自动密码改变(PWC)过程可以由SSO系统来实现。SSO系统可以将PWC页面与模板匹配，从而使得SSO系统能够识别与PWC页面相关联的策略。SSO应用可以发送对与页面模板匹配的凭证的请求。使用该凭证，可以将当前的用户名和密码添加到PWC页面中的适当字段。在自动PWC期间，新的密码可以由SSO 服务器自动地生成，并且可以用新的自动生成的密码来更新用户的凭证。SSO服务器随后可以向SSO应用返回更新的凭证。SSO应用可以将新的密码添加到PWC页面的适当字段，并提交密码改变请求。在方框420，可以证实PWC结果。如果密码被成功地更新，那么在方框416，对改变进行确认并存储更新的凭证。如果密码没有被成功地更新，那么可以使用户返回到PWC页面。

[0064] 在一些实施例中，也可以提供手动的PWC过程。在手动的PWC 期间，与在自动PWC中一样，PWC页面被匹配，并且基于该匹配来识别凭证。SSO应用可以接收凭证，并将凭证注入到PWC页面中的适当字段中。对于手动的PWC，策略可以禁用自动提交，从而防止 SSO应用自动地提交凭证。SSO应用随后可以监视PWC页面以获取用户手动输入的新的密码凭证。随后可以使用用户所提供的密码来更新所存储的凭证。在一些实施例中，SSO服务器可以确认用户所提供的密码满足密码标准(由网络应用或SSO服务器设置的那些标准)，诸如字符数量、字符类型等等。

[0065] 图5示出了根据本发明实施例的用于在不同环境中可操作地执行的可插式单点登录应用。如上面所描述的，代理对来自网络应用的响应进行增强，以便包括SSO应用，该SSO应用在用户的浏览器中执行并且可以与SSO服务器进行通信以提供SSO服务，诸如策略和凭证管理。由于每个用户设备、客户端和浏览器可能具有不同的要求和能力，因此SSO应用可以是可插式的，以便支持不同的环境。例如，可以设置环境变量500来定义所使用的客户端(例如，其是独立客户端或浏览器)和浏览器(诸如Internet Explorer、Chrome、Firefox等)。每个所支持的客户端可以与特定于浏览器以及特定于平台的功能502相关联。可以通过创建特定于平台或特定于浏览器的用于SSO 应用的插件来添加对新的平台和浏览器的支持。

[0066] 可以在SSO应用被安装时对SSO应用进行配置或者可以由SSO 服务器提供特定于平台的SSO应用。在一些实施例中，一旦被安装， SSO应用就可以调用特定于平台的功能来执行SSO服务。在一些实施例中，除了特定于平台的功能之外，还可以在多个平台上提供一组共享的功能。例如，可以在多个平台上共享被调用以与SSO服务器通信的功能，同时还可以提供用于注入并获取来自网页的凭证的特定于平台的功能。

[0067] 如上面所描述的，SSO应用可以安装在用户的浏览器应用中，并透明地向用户提供SSO服务。附加地，SSO应用可以利用用户的客户端设备的处理能力来减少SSO服务器102所需要的处理的量。例如，可以在客户端侧处理模板匹配、凭证注入以及其它SSO处理。在一些实施例中，用户可以通过基于网络的登入管理器接口来访问额外的应用并执行额外的SSO管理。

[0068] 在一些实施例中，客户端可以通过网络向在远程服务器上执行的网络应用发送请

求。该请求可以被SSO代理接收，并被转发到网络应用。在一些实施例中，SSO代理可以修改该请求，使得网络应用向SSO 代理而不是请求的客户端返回响应。网络应用可以接收该请求(例如，对网页的网络请求)并返回响应(例如，网络响应，其包括可以被在客户端上执行的浏览器呈现到所请求的网页的数据)。SSO代理可以接收来自远程服务器的响应并修改该响应。在一些实施例中，SSO代理可以添加(例如增强)该响应以包括与该响应有关的策略和/或凭证信息。例如，SSO代理可以向SSO服务器发送请求以获得与网络应用相关联的策略信息(诸如一个或多个模板，如上面描述的)和/或凭证信息(诸如与用户和网络应用相关联的一个或多个用户名和一个或多个密码)。除了策略信息和/或凭证信息以外，SSO代理还可以将SSO 应用添加到响应中。SSO应用可以是被配置为在客户端上执行的浏览器应用内执行的Javascript应用或其它应用。SSO代理随后可以向客户端返回增强的响应。当客户端接收到该响应时，SSO应用可以被自动地安装在浏览器应用中，并且策略信息和/或凭证信息可以被存储在客户端上。如上面所描述的，SSO应用随后可以将SSO服务提供给请求和响应，并且它们被发送和接收。

[0069] 基于网络的单点登录的登入管理器

[0070] 现有的登入管理器通常可能仅仅协调对使用相同登入方法的应用的访问。例如，无法将表单填充应用与使用不同登入方法的其它应用一起进行管理。本发明的实施例提供了终端用户应用仪表板，其提供中心位置，终端用户可以通过该中心位置来访问他们的应用。该仪表板为具有不同登入要求的多个应用提供统一的启动点。例如，表单填充应用、联合应用和其它访问受控和未受保护的应用。应用可以向仪表板进行注册并指定如何访问该应用。可以基于如何访问应用而在注册之后针对这些应用定义策略。仪表板是可扩展的，使得可以支持新的登入类型。仪表板为用户的应用中的全部提供简单的、统一的访问点，而不管这些应用如何被访问。

[0071] 图6示出了根据本发明的实施例的桌面登入管理器接口。如图6 中所示，登入管理器接口600可以提供一个或多个应用图标602的统一视图，每个应用图标代表用户可以访问的网络应用、服务和/或系统。可以在终端用户应用目录或仪表板中显示用户的应用图标，并且每个应用可以与不同的访问要求相关联。可以在用户登入系统之后显示仪表板。在一些实施例中，用户可以登入到他们的客户端设备来访问网络登入管理器。在一些实施例中，用户可以在访问网络登入管理器时首先进行登入。在仪表板上显示的一些应用可能是未受保护的，并且访问这些应用不需要凭证，而其它应用可以是表单填充应用、联合应用或其它访问类型。因此，仪表板可以显示应用，而不管访问类型，从而向用户呈现统一的应用视图和单个访问点。

[0072] 在仪表板中示出的每个应用图标可以与一个或多个策略以及一个或多个凭证相关联。策略定义应用可以如何被访问，并且凭证提供可以用于认证访问应用的用户的信息。在一些实施例中，可以对用户的仪表板进行供应。例如，公司的新雇员可以对仪表板进行设置，使其具有该雇员将利用的若干应用图标，诸如电子邮件应用和商业应用的图标。一旦应用被设置并且在用户的仪表板中可见，每个应用的策略类型/凭证类型就是对用户隐藏的。用户可以简单地选择应用并访问它，而不必对访问特定应用的细节进行管理。

[0073] 在一些实施例中，网络登入管理器可以显示用户可用的应用的不同视图，使得用户能够诸如通过改变在仪表板中显示哪些应用以及改变应用如何被组织，从而对他们的仪

表板的布局进行定制。例如，网络登入管理器可以提供搜索功能604，使得用户能够(例如通过名称、类型或其它特性)搜索特定应用，并且网络登入管理器随后可以显示包括匹配的应用的搜索视图。在一些实施例中，用户可以选择查看全部606图标，以将全部可用的应用显示在仪表板上。用户还可以选择沿着不同维度(例如，最频繁访问、添加的时间、字母顺序等)对应用进行排序。在一些实施例中，用户可以将特定应用指定为最喜欢的，并且选择最喜欢图标608来仅仅查看已经被这样指定的那些应用。在一些实施例中，用户可以通过选择最近图标610来查看最近增加的应用。

[0074] 在一些实施例中，用户可以将新的应用手动添加612到网络登入管理器。例如，用户可以通过添加或删除相应的策略和凭证来添加和移除应用。在一些实施例中，用户可以通过登入管理器来更新他们的凭证。在一些实施例中，可以显示编辑视图614，这允许用户指定最喜欢的应用616并对每个应用进行配置。例如，用户可以选择设置618 来手动更新与应用有关的设置(例如，更新凭证或策略)。从仪表板，用户可以通过在应用名称上进行选择(例如，点击或轻敲)来启动应用。

[0075] 在一些实施例中，用户可以通过从目录中选择可用的应用并提供适当的凭证来将应用添加到他们的仪表板。可用的应用中的每个都可以使用不同类型的凭证。根据所选择的应用，网络登入管理器可以确定所选择的应用所使用的凭证的类型，并且向要求适当凭证的用户显示消息。在一些实施例中，用户可以提供针对应用的定制的显示名称、描述或其它细节。在一些实施例中，显示名称可以是针对用户预先填充的。用户具有根据需要修改它们的选项。在一些实施例中，可以为相同的网络应用提供多个凭证(例如，与电子商务应用的多个账户相对应)。每一个可以由仪表板中其自身的应用图标来表示，并且可以用附加的数字或其它指示符来自动地命名，以在每个凭证之间进行区分。在一些实施例中，附加地或可替换地，可以为应用设置多个登入凭证。例如，登入管理器可以监视网络应用处的用户活动，并获取用户所提供的附加凭证。

[0076] 在一些实施例中，用户可以移除与给定应用相关联的凭证。一旦凭证已经被移除，就可以从用户的仪表板自动地移除应用。在一些实施例中，如果用户已经指定了该应用作为最喜欢的，那么该应用仍然可以显示在用户的仪表板的最喜欢视图中。用户可以后续为该应用添加新凭证，并将该应用返回到用户的仪表板。在一些实施例中，如果已经为给定应用存储了多个凭证，那么用户可以单独地移除每个凭证。在一些实施例中，用户可以请求对与给定应用相关联的全部凭证进行移除。

[0077] 在一些实施例中，用户可以将他们的凭证共享或委托(delegate) 给另一用户。仪表板可以为那些可以共享的应用显示“共享”图标。应用开发者和/或管理者可以对应用进行配置以供共享。在一些实施例中，可以以每个应用为基础禁用共享。当用户选择共享他们的凭证时，可以显示提示，该提示请求用户提供将与之共享凭证的用户的用户信息。在一些实施例中，该提示可以包括用户列表(例如，由企业用户数据库填充的)。当凭证已经被委托时，可以防止受委托者与额外的用户共享凭证。在一些实施例中，可以与之共享凭证的用户的数量可以被限制为最大数量。

[0078] 用户可以在任意给定时间通过选择“撤回”图标来撤回委托。在与另外的用户共享凭证时可以显示撤回图标。在一些实施例中，当用户委托凭证时，用户可以设置委托时间段，在该时间段之后凭证被自动撤回。

[0079] 在一些实施例中，网络登入管理器可以包括密码改变(PWC) 向导。如上面所描述的，PWC向导可以包括手动模式和自动模式，在手动模式中，用户指定新密码，在自动模式中，PWC向导代表用户自动选择新密码。

[0080] 图7示出了根据本发明实施例的登入管理器接口700。在用户从移动设备(诸如智能电话或平板)访问登入管理器时，该接口可以自动适应用户的设备的大小和尺寸要求。移动登入管理器接口700可以提供与上面关于图6描述的全屏或桌面接口类似的特征。每个应用图标(诸如图标702和704)可以被调整大小，并被显示在可滚动列表中。用户可以选择靠近应用的显示名称的图标704来查看该应用的细节。在一些实施例中，在详细查看时，可以给用户呈现(例如，通过更新与应用相关联的凭证和/或策略)编辑该应用的选项。在一些实施例中，图标704在被选择时可以启动该应用。

[0081] 图8示出了根据本发明实施例的登入管理器体系架构。在图6和图7中所示的每个图标可以表示不同的应用，诸如网络应用、本地应用和远程应用。如上面所描述的，每个图标可以与策略和凭证相关联，该策略定义SSO系统如何与该应用交互，该凭证向用户提供对该应用的访问。如图8所示，用户可以通过在用户设备106B上执行的SSO 客户端106来访问登入管理器。在一些实施例中，客户端可以是独立的客户端或基于浏览器的客户端。

[0082] 在一些实施例中，用户可以通过访问与网络登入管理器相关联的 URL，通过客户端设备上的浏览器来访问登入管理器。在一些实施例中，网络登入管理器可以分布在SSO网关108和SSO系统102上。前端网络登入组件112A可以在SSO网关108上执行，并且可以提供图形用户接口(GUI)，通过该图形用户接口可以接收来自客户端106 的请求。在一些实施例中，可以提示用户直接向登入管理器提供凭证 (例如，用户名和密码)，或者可以重新定向用户和提示用户登入SSO 系统102。一旦登入，就可以向用户的浏览器添加cookie或其它标识符，用以指示用户被登入并且可以访问登入管理器以及查看他们的仪表板。在一些实施例中，当用户登入他们的设备(诸如平板、膝上型计算机或智能电话)时，用户随后可以访问登入管理器，而无需提供额外的凭证。一旦被登入，用户就可以请求访问在他们的仪表板上显示的应用，而没有进一步的登入要求。

[0083] 在一些实施例中，例如在用户选择在仪表板中显示的应用时，网络登入管理器112A可以接收访问仪表板中的应用的请求。通过 HTTP/HTTPS在前端网络登入组件112A处可以接收请求，并且前端网络登入组件112A可以将请求转换为访问协议(诸如Oracle访问协议，可从加州红木海岸的Oracle国际公司获得)，并且可以将请求转发给后端网络登入组件112B。转换后的请求可以包括对与应用相关联的策略和/或对与用户相关联的凭证的请求，该请求针对网络接口被格式化。后端网络登入组件112B可以提取策略和/或凭证请求，并通过网络接口104将它们发送到SSO服务100。通过网络接口104可以将策略和/或凭证返回给后端网络登入组件112B。网络登入组件112B可以生成包括策略和/或凭证的响应消息，并通过访问协议将该消息发送到网络登入组件112A。网络登入管理器112A可以例如通过发送对与应用相关联的URL的HTTP请求来启动应用。使用与应用相关联的一个或多个策略，网络登入管理器112A可以将策略与从应用接收到的响应进行匹配。网络登入管理器112A可以自动地根据一个或多个策略向应用提供用户凭证。

[0084] 图9描绘了根据本发明的实施例的通过网络登入接口访问网络应用的方法900的方框图。在方框902，可以通过网络登入管理器用户接口接收访问应用的请求。在一些实施

例中，可以通过在用户的客户端设备(诸如桌面或移动计算设备)上执行的浏览器应用，通过基于网络的接口来接收请求。在一些实施例中，用户可以通过在浏览器应用中输入与网络登入管理器用户接口相对应的URL来导航到网络登入管理器用户接口。在一些实施例中，在通过浏览器应用发送对网页或网络应用的请求时，用户可以自动地被重新定向到网络登入管理器用户接口。网络登入管理器用户接口可以请求来自用户的用于访问用户接口的凭证。

[0085] 在方框904，可以识别与应用相关联的策略。策略可以定义与应用相关联的访问要求。例如，策略可以定义访问应用所需要的凭证的类型，并且可以定义凭证将如何被提供给应用(例如，哪些字段应当接收凭证)。在一些实施例中，通过生成策略请求消息并通过网络接口向SSO系统发送策略请求消息，可以由网络登入管理器识别策略。在方框906，可以基于应用要求来识别用户凭证。在一些实施例中，网络登入管理器可以基于接收到的策略来识别凭证。通过生成凭证请求消息并通过网络接口向SSO系统发送凭证请求消息，网络登入管理器可以获取凭证。

[0086] 在方框908，一旦已经接收到适当的策略和凭证，网络登入管理器就可以自动地向应用提供用户凭证。在一些实施例中，当从应用接收到进入的网页响应时，网络登入管理器可以使用策略来识别网页响应中的字段，以便注入凭证并将该凭证提交给网络应用。在一些实施例中，当网络登入管理器响应于策略请求而接收表单填充策略时，网络登入管理器可以自动地用用户凭证填充与应用相关联的图形用户接口中的字段，并通过图形用户接口将用户凭证提交给应用。在登入时，网络登入管理器可以验证登入是成功的，并将响应网页返回给用户。

[0087] 在一些实施例中，用户或管理员可以向登入管理器添加新的应用。例如，当新的雇员被雇用时，可以向新雇员的仪表板供应若干公司标准的且常用的应用。添加新的应用可以包括接收向登入管理器添加新的应用的请求，该请求可以包括针对用户的策略和凭证。网络登入管理器可以通过网络接口向数据管理器发送存储策略和凭证的请求。一旦数据管理器确认策略和凭证已经被成功地存储，登入管理器就可以向登入管理器添加与新应用相对应的应用图标，使得图标被显示在登入管理器中。在一些实施例中，可以一次批量地添加多个应用。这样的请求可以包括接收为用户供应多个应用的请求，该请求包括针对每个应用的策略和凭证。网络登入管理器随后可以向数据管理器发送针对每个应用存储策略和凭证的多个请求(或单个的批量请求)。一旦接收到对成功存储的确认，网络登入管理器就可以向登入管理器添加与多个应用中的每一个相对应的图标，使得在用户登入登入管理器时这些图标被显示。

[0088] 在一些实施例中，登入管理器接口呈现与不同类型的凭证相关联的应用的统一视图。例如，在用户的仪表板上示出的每个应用图标可以被一起聚合地显示。一旦给定的应用被选择以启动相对应的应用，网络登入管理器就可以与SSO系统进行通信，以使用适当的凭证启动该应用。在一些实施例中，可以对用户的仪表板进行排序，以基于凭证类型来显示应用，或者显示多个视图，其中给定的视图示出与一个凭证类型相关联的应用。

[0089] 如上面所描述的，SSO服务可以通过各种途径(例如，通过安装在用户的浏览器中的SSO应用、通过网络登入管理器、或通过其它途径)被用户访问以及被提供给用户。请求可以通过一个或多个网络接口被传送给SSO服务器102，该一个或多个网络接口提供用于提供

SSO服务的标准的、客户端不可知的方式。

[0090] 用于单点登录的基于网络的接口集成

[0091] 根据实施例，可以通过一个或多个网络接口将单点登录服务(包括凭证管理和策略管理)与基于网络的或基于云的SSO系统集成。由 SSO系统所提供的每个SSO服务可以通过网络经由一个或多个网络接口(诸如REST接口)被客户端访问。传统上，SSO服务是在本地提供的(例如，通过在本地机器或本地网络上执行的SSO服务)，并且被配置为使用提供策略和凭证信息的安全传输的协议来进行通信。然而，为了从远程的基于网络的或基于云的SSO系统访问这些相同的服务，同时维持后向兼容，存在复杂的通信挑战。客户端通常被配置为通过HTTP或HTTPS发送网络请求和接收网络响应，而SSO服务请求和响应通常使用访问协议(诸如网络访问协议或Oracle访问协议)。本发明的实施例有助于请求的隧道化，并且可以通过NAP将响应从客户端隧道化传输到访问管理器服务器。

[0092] 图10示出了根据本发明的实施例的集成单点登录服务的SSO服务器体系架构1000。单点登录，不管是基于网络的还是基于桌面的，均需要策略管理服务和凭证管理服务。如上面所描述的，策略定义单点登录系统如何与应用交互，并且凭证被用于认证用户以获得对应用的访问。本发明的实施例涉及的是提供基于网络的单点登录。可以使用网络接口104(诸如REST接口)来公开每个单点登录服务100。如上面所描述的，通过使用网络接口，不同类型的客户端106可以访问单点登录服务100，并且可以容易地添加新的客户端。在一些实施例中，每个SSO服务100可以与不同的网络接口相关联。网络接口提供了用于创建、读取、更新以及删除(CRUD)策略和凭证的简单方式。

[0093] 客户端106可以通过SSO网关108向SSO系统102发送对单点登录服务的请求，例如对策略或凭证的请求。如图10所示，来自客户端106的请求可以通过访问中介110、网络登入管理器接口112A和/ 或SSO应用114而被SSO网关108接收。该请求可以是例如通过访问协议(诸如NAP或OAP)隧道化传输的REST请求。在一些实施例中，可以使用单个网络接口来访问单点登录服务。在一些实施例中，每个单点登录服务可以与特定于服务的网络接口相关联。

[0094] 在一些实施例中，当通过访问中介、登入管理器或代理对SSO 服务做出请求时，可以从客户端接收请求作为HTTP或HTTPS请求。SSO网关108可以包括隧道代理1002A，该隧道代理1002A可以通过 NAP(网络访问协议)或OAP(Oracle访问协议)将HTTP请求隧道化传输到SSO服务器102。可以在SSO网关108与SSO服务器102 处的NAP/OAP端点1004之间开启NAP连接或OAP连接。在一些实施例中，NAP/OAP端点1004可以是通过指定的URL访问的网络接口。SSO服务器102处的隧道代理1002B随后可以将请求转换回HTTP 或HTTPS，并将转换后的请求发送到SSO服务器102处的适当SSO 服务100。在一些实施例中，服务可以向隧道代理1002B注册以便通过该隧道代理接收隧道化传输的请求以及发送隧道化传输的响应。从SSO服务器102到发出请求的客户端的响应可以类似地被隧道化传回 (例如，请求的服务100所生成的HTTP或HTTPS响应可以被隧道代理1002B接收，隧道代理1002B可以将该请求转换成NAP/OAP，并且隧道化传输的响应随后可以通过网络接口1004被发送到隧道代理1002A)。

[0095] 例如，可以对从SSO网关108隧道化传输到SSO服务器102的 URL进行配置。在一些实施例中，可以将URL映射到SSO服务器102 处的与SSO服务100对应的小服务程序(servlet)或JSP页面。当 HTTP/S请求被发送到URL时，HTTP/S请求被转换成NAP/OAP请求，

并通过NAP/OAP连接被转发到SSO服务器102。SSO服务器102 的端点1004接收NAP/OAP请求，并将该请求传递到隧道代理1002B。隧道代理1002B可以将NAP/OAP请求转换成HTTP/S请求，并将该请求发送到适当的服务。例如，隧道代理可以将NAP/OAP请求转换成HTTPServletRequest，并调用适当的小服务程序(诸如，在JSP 的情况下，来自JSP文件的编译的小服务器程序)。响应可以被隧道代理1002B转换回NAP/OAP，并被传递回NAP/OAP端点1004。随后NAP/OAP请求被返回给SSO网关，在SSO网关处，隧道代理1002A 可以将NAP/OAP响应转换回HTTP/HTTPS响应，该HTTP/HTTPS 响应被返回给客户端，诸如用户的浏览器。

[0096] 在一些实施例中，可以分析通过网络接口层1004(诸如REST 层)接收到的对资源的请求(诸如对应用、凭证、策略或其它数据的访问)，以确定所请求的资源是否受保护以及是否存在与该请求包括在一起的认证cookie。如果没有提供认证cookie或者认证cookie已经到期并且所请求的资源是受保护的，那么可以将该请求重新定向到认证服务，诸如可从加州红木海岸的Oracle国际公司获得的Oracle认证管理器。认证服务可以请求来自用户的凭证(例如，用户名和密码)。当认证服务接收到凭证时，认证服务可以证实该凭证，并且如果有效，则向用户的浏览器返回认证cookie。随后可以将资源请求重新定向到网络接口层，其中，认证cookie提供对所请求的资源的访问。在一些实施例中，当用户通过超时或肯定性的退出而结束他们的会话时，网络接口层可以破坏会话信息并使用户返回到登入屏幕。

[0097] 图11A和11B示出了根据本发明的实施例的策略管理器体系架构1100和凭证管理器体系架构1102。如图11A所示，策略管理器1104 可以提供对SSO策略管理服务1106的集中式访问，诸如在多个策略库/系统上存储并获取策略。策略管理器1104可以与网络接口104(例如REST接口)相关联，使得策略管理器可以通过网络接收请求并发送响应。这使得策略管理器平台是独立的，因为它可操作地与可以发送并接收基于网络的消息的任何客户端进行交互。在一些实施例中，策略管理器1104可以用于管理用户和管理性策略。策略管理器1104 可以被配置为使用插件1106来支持不同的访问控制类型。每个插件可以包括一个或多个方法，以用于创建、读取、更新和删除特定于与插件相对应的策略类型的策略。为了添加对新访问控制类型的支持，可以向策略管理器提供新的插件。

[0098] 在一些实施例中，策略管理器1104可以根据特定的策略类型提供抽象层，例如，客户端仅仅需要知道如何通过网络接口104与策略管理器1104通信，而不需要与每个底层的策略类型通信。当策略管理器1104接收到请求时，策略管理器可以确定与该请求相关联的策略类型，并使用相应的插件1106来生成特定于策略类型的请求。策略管理器1104可以将特定于策略类型的请求发送给数据管理器122。如下面进一步描述的那样，数据管理器122给各种数据源提供抽象层。数据管理器可以识别响应于该请求的数据，并将所识别的数据返回给策略管理器。例如，来自策略管理器的搜索请求可以返回响应于与该请求包括在一起的搜索标准(例如，过滤器、策略标识符、策略类型等) 的策略列表。在一些实施例中，如果没有提供标准，那么可以取得并返回所有的策略。当添加新的策略时，策略管理器1104可以创建标识符，并随后将新的策略与该标识符相关联。在一些实施例中，多个策略可以与相同的标识符相关联。策略管理器1104随后可以将包括标识符和策略的列表传递到数据管理器122。类似地，更新操作可以包括与一个或多个现有策略相关联的标识符和更新的策略信息。策略管理器1104可以将标识符和更新的策略发送到数据管理器122，数据管理器122可以存储更新的策略。删除请求可以包括一组标识符，并且数据管理器122可以删除所标识的

策略并返回针对删除的状态信息。在一些实施例中，可以通过客户端设备从终端用户和/或通过管理控制台从管理员接收策略管理请求。

[0099] 在一些实施例中，策略管理器1104可以管理应用模板。每个应用模板可以是一个对象，其包括对要如何向特定应用提供SSO服务的定义。例如，应用模板可以定义SSO系统要如何与特定应用交互、如何将SSO服务匹配到、注入到以及提供到特定应用。给定的应用模板可以与一个或多个子表单相关联，该一个或多个子表单中的每个可以与各种匹配类型(例如，登入UI、密码改变UI、成功/失败UI、交互方法等)相对应。在一些实施例中，特定的应用模板可以与许多用户相关联，并且用户可以有权访问许多应用模板。附加地，在一些实施例中，应用模板可以与许多凭证相关联。在一些实施例中，应用模板可以与一个或多个其它策略(例如，密码策略、凭证共享策略等)相关联。

[0100] 在一些实施例中，策略管理器1104可以管理密码策略。如上面所描述的，每个密码策略可以与共享该密码策略的一个或多个应用模板相关联。供应管理器1112和/或密码重置管理器1114在为应用建立或更新密码时可以使用密码策略。在一些实施例中，在供应和/或密码重置期间可以使用密码策略来自动生成密码，或者可以使用密码策略来证实从用户接收到的密码。在一些实施例中，策略管理器1104可以对管理策略进行管理，该管理策略覆盖用户或本地部署的设置。

[0101] 如图11B所示，凭证管理器1110可以在存储在不同的库120中的一个或多个不同凭证类型上提供对终端用户凭证管理的集中式访问。凭证管理器1110可以对来自客户端的凭证管理操作进行抽象，从而通过减少所需要的逻辑的量来简化新客户端的开发。附加地，凭证管理器1110是独立于平台的，并且可以与用于通过网络发送并接收消息的任何客户端进行通信。

[0102] 在一些实施例中，凭证管理器1110可以对在多个库120上存储和获取凭证进行管理，并且提供后向兼容以访问现有的用户凭证。凭证管理器1110可以使客户端能够管理各种类型的SSO凭证(包括委托的凭证和享有特权的凭证)。通过网络接口104，凭证管理器可以发布API，该API提供针对凭证的CRUD操作，诸如获得、添加、更新和删除。这提供了针对每个凭证存储装置的抽象层，例如，客户端仅仅需要知道如何与凭证管理器进行通信，而不用知道如何与多个所支持的凭证数据存储装置进行通信。当凭证管理器1110通过网络接口104接收到凭证请求时，凭证管理器可以利用与不同类型的凭证相对应的一个或多个子管理器(诸如享有特权的凭证管理器1114、委托的凭证管理器1118以及SSO凭证管理器1120)来分析该请求，以识别适当的凭证数据存储装置并完成凭证请求。

[0103] 在一些实施例中，凭证管理器1110可以接收给定用户的凭证请求。凭证管理器1110可以向每个子管理器1114、1118、1120发送请求，以识别与用户相关联的凭证，并返回任何匹配的凭证。在一些实施例中，凭证管理器1110可以接收获得凭证(诸如享有特权的账户的凭证)的请求。凭证管理器可以将获得凭证的请求发送到相应的子管理器(例如，为了添加享有特权的账户的凭证，凭证管理器可以将请求发送到享有特权的凭证管理器1114)以获得该凭证。相应的子管理器可以检查该凭证(例如，来自享有特权的服务器1116)，并将该凭证返回给凭证管理器1110。在一些实施例中，可以在将该凭证发送到凭证管理器1110之前，对该凭证中的敏感字段进行加密。

[0104] 在一些实施例中，当凭证管理器1110接收到获得凭证操作时，凭证管理器可以基

于该请求(例如,与在该请求中标识的用户相关联、凭证ID、凭证类型或其它标准)而请求凭证列表。在一些实施例中,如果在请求中没有指定标准,那么凭证管理器1110可以请求与请求的用户相关联的所有凭证。在一些实施例中,凭证管理器1110可以接收针对一个用户或多个用户添加一个凭证或多个凭证的请求。凭证管理器1110可以基于要添加的凭证的类型,针对每个凭证生成凭证标识符,并且调用相应的子管理器。子管理器可以证实接收到的凭证,并向数据管理器122发送将该凭证存储在适当的数据的库120中的请求。数据管理器可以返回每个所添加的凭证的状态。类似地,凭证管理器 1110可以接收更新凭证的请求。凭证管理器1110可以将包括更新的凭证的请求发送到每个相应的子管理器。子管理器可以证实更新的凭证,并向数据管理器122发送存储更新的凭证的请求。可以返回更新状态。在一些实施例中,凭证管理器1110可以接收删除凭证的请求。凭证管理器1110可以识别相应的子管理器,并向该子管理器发送删除凭证的请求。在一些实施例中,如果凭证已经被委托,那么可以在删除之前撤回委托。

[0105] 图12描绘了根据本发明的实施例的通过基于网络的接口来提供 SSO服务的方法1200的方框图。在方框1202,接收对单点登录服务的请求。该请求可以是从客户端设备、管理控制台、应用或任何其它实体接收的。可以经由与单点登录服务相关联的网络接口来接收该请求。在一些实施例中,单个网络接口可以用作指向一个或多个SSO服务的所有请求的中央进入点。当接收到请求时,可以识别与该请求相关联的特定的SSO服务,并且可以将该请求转发到与该SSO服务相关联的端点。

[0106] 在一些实施例中,可以由代理接收处于第一协议的请求,代理将该请求从第一协议转换到第二协议,并将转换后的请求转发给单点登录服务。例如,请求可以是HTTP/S请求,并且代理可以通过访问协议(诸如NAP或OAP)来隧道化传输HTTP/S请求。在一些实施例中,第二代理可以接收隧道化传输的请求,并提取要被传递到进行接收的SSO服务的HTTP/S请求。在一些实施例中,可以对响应进行类似的隧道化传输,以便将响应返回给请求的客户端。例如,第二代理可以接收来自SSO服务的响应(例如,包括所请求的凭证、策略、验证消息等)。该响应可以是HTTP/S响应。代理可以使用NAP、OAP 或类似的访问协议来隧道化传输HTTP/S响应,并经由代理将隧道化传输的响应返回给请求的客户端。

[0107] 在方框1204,基于请求,可以将数据请求发送到数据管理器以管理策略或凭证。在一些实施例中,对SSO服务的请求可以是例如策略管理请求(诸如创建、读取、更新或删除策略的请求)或凭证管理请求(诸如创建、读取、更新或删除凭证的请求)。

[0108] 因为不同类型的策略可以存储在通过特定于数据源的接口可访问的不同数据源中,因此SSO系统通常仅仅在有限数量的策略类型的情况下进行工作。这限制了终端用户的可用选项或迫使终端用户支持多个应用。然而,如上面所描述的,本发明的实施例提供了一种可以通过第一(通用)接口接收请求的策略管理器。请求可以根据接口指定要执行的特定策略管理操作(例如,CRUD操作)。策略管理请求可以是数据源不可知的(例如,请求可以不指定策略存储在哪或如何存储或者不包括任何特定于数据源的操作)。策略管理器随后可以识别与策略管理请求相关联的策略管理插件,并基于所识别的策略管理插件将策略管理请求转换为用于第二(特定于数据源的)接口的格式。策略管理器随后可以基于一个或多个策略管理操作生成数据请求。

[0109] 类似地,凭证可以存储在各种凭证存储装置中,每个存储装置可通过其自己的接

口访问。这通常将SSO应用限制到那些使用相同类型的凭证的应用。本发明的实施例提供了一种凭证管理器，其可以被配置为对存储在不同凭证存储装置中的各种类型的凭证进行管理。当接收到凭证管理请求时，可以将该凭证管理请求发送给凭证管理器。与策略管理器类似，凭证管理器可以通过通用的接口来接收请求。这用作做出凭证管理请求的客户端与可以服务于该请求的特定凭证存储装置之间的抽象层。在一些实施例中，凭证管理器可以识别与凭证管理请求相关联的子管理器，并基于所识别的子管理器将凭证管理请求转换为用于第二接口的格式。第二接口可以与子管理器所管理的特定凭证存储装置相对应。凭证管理器随后可以基于一个或多个策略管理操作生成数据请求。

[0110] 在方框1206，经由相关联的网络接口返回响应。响应可以包括根据请求获取的数据(例如策略或凭证)。在一些实施例中，响应可以指示创建、更新或删除操作是成功地完成了还是失败了。

[0111] 策略和凭证数据源的虚拟化数据存储和管理

[0112] 如上面所描述的，本发明的实施例可以支持利用不同的访问类型 (诸如表单填充、联合的、受保护的和其它类型)的一个或多个不同应用的单点登录。与不同的访问类型相关联的策略和凭证可以存储在不同类型的库中。根据实施例，为了通过统一的接口支持不同的访问类型，提供了虚拟化的数据管理系统，其对于实际的物理存储(OID、AD、ADMA、数据库等)是不可知的。该数据管理系统可以提供用于管理凭证和策略的SPI层。该数据管理系统还可以提供用于执行 GRUD操作的API，并且可以管理许可(诸如ACL许可和数据水平许可)，而无需知道正在使用的数据存储容器。在一些实施例中，该数据管理系统可以使用基于多个哈希映射(harsh map)的高速缓存来进行较快速的数据访问。

[0113] 在一些实施例中，数据管理系统提供集中式的库，通过该库可以维护凭证、策略、管理服务和其它配置以及安全服务。这使得用户能够通过各种客户端106来访问并消费SSO服务。数据管理系统可以向不同的库和服务(诸如Oracle目录服务器(OID、ODSEE、OUD)、Microsoft活动目录、Microsoft ADAM/AD-LDS和其它LDAP兼容的目录、以及SQL数据库和本地或联网的文件系统)呈现统一的接口。附加地，数据管理是可扩展的，使得可以通过实现兼容的插件来将新的数据源和服务与数据管理系统集成。

[0114] 在一些实施例中，数据管理系统可以将客户端本地存储的凭证与存储在数据管理系统所管理的一个或多个特定于凭证的数据存储装置中的凭证进行同步。当触发同步事件时(例如，在启动时或者在添加、删除或更新凭证时)，数据管理系统可以将存储在客户端高速缓存中的凭证数据与存储在数据管理系统所管理的库中的凭证数据进行比较。可以在客户端处(例如，由用户)本地地更新凭证，或者可以在凭证库处(例如，由管理员或者通过第三方凭证服务)直接更新凭证。在同步期间，可以检测在本地存储的凭证与存储在一个或多个凭证数据存储装置中的凭证之间的冲突。冲突策略可以定义要保存哪个凭证。在一些实施例中，可以保存最近更新的凭证，并且可以丢弃任何其它凭证。在一些实施例中，可以保存存储在凭证数据存储装置中的凭证，并且可以丢弃本地存储的任何其它凭证。同步还可以维护与基于桌面的SSO服务的后向兼容。基于桌面的服务使用本地维护的凭证和策略来提供SSO服务，这样使本地存储装置与基于网络的库保持同步，基于桌面的SSO服务可以继续提供最新的SSO服务。

[0115] 图13示出了根据本发明的实施例的数据管理器体系架构1300。如图13所示，数据

管理器122提供用于SSO数据管理的集中式接口，该数据管理器122可以经由可扩展的插件1304支持一个或多个不同的物理存储系统1302。每个插件可以使得从SSO服务接收到的数据请求能够在相应的物理存储系统上被执行。数据管理器是可扩展的，使得它可以通过添加相应的插件来支持新类型的物理数据源。数据管理器与基于桌面的SSO服务后向兼容。

[0116] 数据管理器122提供单个接口以实现在多个库1302上存储并获取策略。数据管理器122可以通过不需要特定的库信息或特定于库的操作的单个API来接收数据请求。作为替代，数据管理器122可以识别用于该请求的适当的库，并通过相应的插件1304向适当的库发送请求。在一些实施例中，数据管理器122提供与每个插件对接的SPI层。数据管理器122公开用于与策略、凭证和供应数据有关的CRUD操作的统一接口。

[0117] 基于GRUD请求的类型，SPI层可以自动初始化每个插件实例。在一些实施例中，数据管理器122可以提供通用接口，该通用接口用于执行GRUD操作而不需要指定底层数据存储装置1202。在一些实施例中，可以为每种类型的操作(例如凭证、策略和供应操作)提供通用接口。当通过通用接口接收到请求时，数据管理器122可以通过由SSO系统102(例如，由数据管理器122)维护的配置信息来识别特定于数据存储装置的操作和连接信息。数据管理器122随后可以将相应插件初始化以便与该数据存储装置进行通信。

[0118] 在一些实施例中，在首次调用插件实例并且初始化发生时，可以为数据存储装置创建上下文对象池(Context Object Pool)。这可以提供高可用性和线程安全。对于每个CRUD操作，可以从池中分配单独的上下文对象，并且一旦操作完成就将该上下文对象返回给池。数据管理器122可以使用连接池(connection pooling)(例如，JNDI 服务提供商所提供的)和上下文池(context pooling)，通过在应用启动时组建连接池来节约资源，并且从而减少创建连接或断开连接所需要的时间。附加地，通过发起连接池，可以简化对到数据存储装置的连接的管理，这是因为可以将连接的创建、针对应用的连接的最大数量、连接的最大空闲时间以及其它的配置细节委托给连接池管理器。

[0119] 在一些实施例中，当查找存储在各个数据库1302上的策略和凭证时，数据管理器122可以使用一个或多个哈希映射来改进性能。在一些实施例中，一个哈希映射可以将策略类型映射到标识符和策略对象。另一个哈希映射可以将策略名称映射到策略引用。另一个哈希映射可以将密钥映射到策略对象。另一个哈希映射可以将值映射到策略对象列表。

[0120] 在一些实施例中，可以针对凭证、策略和供应服务来支持创建、读取、更新和删除(CRUD)操作。每个CRUD操作可以由数据管理器122通过网络接口公开。例如，凭证操作可以包括创建针对指定对象(例如，应用或服务)的新凭证、读取(例如，获取)与用户和至少一个应用相关联的凭证、更新指定的凭证(例如，修改凭证或提供新的凭证)以及删除针对指定对象的凭证。可以为策略和供应服务提供类似的操作。

[0121] 在一些实施例中，数据管理器122可以支持在策略数据上执行的 CRUD操作，该策略数据包括应用模板、密码策略、凭证共享组、以及管理性数据。在一些实施例中，数据管理器122还可以支持对凭证数据、供应数据(例如，指令/密钥)、用户设置、数据管理设置、用户秘密(UAM)、加密密钥(UAM)和登入凭证(UAM)进行的CRUD 操作。

[0122] 图14描绘了根据本发明的实施例的对存储在多个数据存储装置上的凭证进行管理的方法1400的方框图。在方框1402，可扩展的数据管理器可以向一个或多个单点登录服务提供一个或多个存储系统的统一视图。在一些实施例中，每个单点登录服务与网络接口

相关联。

[0123] 在方框1404,可以在可扩展数据管理器处从单点登录服务接收对凭证的数据请求。可扩展数据管理器可以用作一个或多个存储系统的抽象层,使得请求可以是存储系统不可知的。例如,数据请求可以包括可以用于识别所请求的一个凭证或多个凭证的标准。该标准可以足够宽泛以便与不同类型的凭证相对应。在先前的系统之下,用户将必须单独地搜索不同的凭证存储装置以获得匹配的凭证。然而,根据本发明的实施例,数据管理器可以接收一个请求,并在多个凭证存储装置上进行搜索。

[0124] 在方框1406,可以识别与该请求相关联的至少一个存储系统。例如,基于与请求包括在一起的标准(诸如,凭证ID、凭证类型或其它标准),数据管理器可以识别一个或多个相应的存储系统。在一些实施例中,数据管理器可以通过使用该标准,使用哈希映射来识别相关的存储系统。

[0125] 在方框1408,可以识别与至少一个存储系统中的每一个相对应的存储系统插件。数据管理器可以包括SPI层,通过提供插件,多个存储系统可以通过SPI层对接。每个插件可以将在数据管理器处通过第一(例如通用)接口接收到的数据请求转换为与插件的相应存储系统相兼容。在一些实施例中,可以通过向数据管理器添加插件来提供对新的存储系统的支持。数据管理器可以从管理员接收与新的存储系统相关联的存储系统插件。在一些实施例中,插件可以实现由数据管理器提供的SPI。数据管理器可以验证插件(例如,确保提供了任何需要的方法或配置文件),并随后向SPI层添加存储系统插件。

[0126] 在方框1410,可以使用存储系统插件从存储系统获取与数据请求相关联的数据。在一些实施例中,随后可以通过第二接口(特定于存储系统)将转换后的数据请求发送到存储系统,以创建、读取、更新或删除与数据请求相关联的数据。所获取的数据可以包括所请求的凭证或策略或者对创建、更新或删除操作的成功完成或失败的验证。

[0127] 在方框1412,可以将所请求的数据返回给SSO服务。在一些实施例中,所请求的数据可以包括与搜索请求相匹配的一个或多个凭证。在一些实施例中,所请求的数据可以包括对创建、更新或删除操作成功或失败的验证。在一些实施例中,数据管理器可以通过第二(特定于存储系统的)接口从存储系统接收包括凭证的响应。数据管理器可以在通过第一接口返回该响应之前,对该凭证的至少一部分进行加密,并基于第一接口重新格式化该响应。

[0128] 在一些实施例中,数据管理器还可以接收与和应用相关联的策略有关的数据请求。数据管理器可以识别与该请求相关联的至少一个存储系统以及与该至少一个存储系统相对应的至少一个存储系统插件。数据管理器随后可以通过该至少一个存储系统插件来创建、读取、更新或删除与该应用相关联的、来自该至少一个存储系统的一个或多个策略。在一些实施例中,数据管理器可以将来自第一(例如通用)接口的请求转换成第二(例如,特定于策略存储装置的)接口,并通过第二接口将转换后的数据请求发送到存储系统,以便响应于第二数据请求获取至少一个策略。在将响应返回给请求的应用之前,可以类似地将响应从第二接口重新格式化成第一接口。

[0129] 图15描绘了用于实现一个实施例的分布式系统1500的简化图。在所示的实施例中,分布式系统1500包括一个或多个客户端计算设备 1502、1504、1506和1508,该一个或多个客户端计算设备被配置为通过一个或多个网络1510执行并操作客户端应用,诸如网络浏览器、专用客户端(例如,Oracle Forms)等。服务器1512可以经由网络1510 与远程客户端

计算设备1502、1504、1506和1508通信耦合。

[0130] 在各个实施例中，服务器1512可以被适配以运行由系统的一个或多个组件提供的一个或多个服务或软件应用。在一些实施例中，这些服务可以作为基于网络或云的服务被提供或在软件即服务(SaaS) 模型下被提供给客户端计算设备1502、1504、1506和/或1508的用户。操作客户端计算设备1502、1504、1506和/或1508的用户进而可以利用一个或多个客户端应用与服务器1512交互，以利用这些组件所提供的服务。

[0131] 在该图中所描绘的配置中，系统1500的软件组件1518、1520和 1522被示出在服务器1512上实现。在其它实施例中，系统1500的一个或多个组件和/或这些组件所提供的服务也可以由客户端计算设备1502、1504、1506和/或1508中的一个或多个来实现。操作客户端计算设备的用户随后可以利用一个或多个客户端应用来使用这些组件所提供的服务。可以用硬件、固件、软件或其组合来实现这些组件。应当理解的是，可以与分布式系统1500不同的各种不同系统配置是可能的。在该图中示出的实施例因此是用于实现实施例系统的分布式系统的一个例子，而不旨在是限制性的。

[0132] 客户端计算设备1502、1504、1506和/或1508可以是便携式手持设备(例如，**iPhone®**、蜂窝电话、**iPad®**、计算平板、个人数字助理(PDA))或可穿戴设备(例如，Google **Glass®**安装于头部的显示器)，在其上运行诸如Microsoft Windows **Mobile®**之类的软件、和/ 或各种移动操作系统(诸如iOS、Windows Phone、Android、BlackBerry 10、Palm OS等)，并且是因特网、电子邮件、短消息服务(SMS)、**Blackberry®**或其它通信协议使能的。客户端计算设备可以是运行各种版本的Microsoft **Windows®**、Apple **Macintosh®**和/ 或Linux操作系统的通用个人计算机，以示例的方式包括个人计算机和/或膝上型计算机。客户端计算设备可以是运行各种商用的**UNIX®**或类UNIX操作系统(包括但不限于各种GNU/Linux操作系统，例如 Google Chrome OS)中的任何一种的工作站计算机。可替换地或附加地，客户端计算设备1502、1504、1506和1508可以是能够通过网络1510进行通信的任何其它电子设备，诸如瘦客户端计算机、因特网使能的游戏系统(例如，具有或不具有**Kinect®**姿势输入设备的Microsoft Xbox游戏控制台)和/或个人消息传送设备。

[0133] 虽然示例性的分布式系统1500被示为具有四个客户端计算设备，但是可以支持任何数量的客户端计算设备。其它设备(诸如具有传感器等的设备)可以与服务器1512进行交互。

[0134] 分布式系统1500中的网络1510可以是本领域技术人员所熟悉的任何类型的网络，该网络可以支持使用各种商用的协议(包括但不限于TCP/IP(传输控制协议/因特网协议)、SNA(系统网络体系架构)、 IPX(因特网分组交换)、AppleTalk等)中的任何一种的数据通信。仅仅以示例的方式，网络1510可以是局域网(LAN)，诸如基于以太网、令牌环等的局域网。网络1510可以是广域网和因特网。网络 1510可以包括虚拟网络，包括但不限于虚拟专用网络(VPN)、内联网、外联网、公共交换电话网络(PSTN)、红外网络、无线网络(例如，在电气和电子协会(IEEE)802.11协议组、**蓝牙®**和/或任何其它无线协议中的任何一个下操作的网络)；和/或这些和/或其它网络的任何组合。

[0135] 服务器1512可以由一个或多个通用计算机、专用服务器计算机（以示例的方式包括PC(个人计算机)服务器、UNIX ®服务器、中型服务器、大型机计算机、机架式服务器等)、服务器集、服务器群或任何其它适当的布置和/或组合组成。在各个实施例中，服务器1512 可以被适配为运行在上面的公开中所描述的一个或多个服务或软件应用。例如，服务器1512可以与用于执行根据本公开的实施例上面所描述的处理的服务器相对应。

[0136] 服务器1512可以运行包括上面讨论的那些操作系统中的任何一个以及任何商用的服务器操作系统在内的操作系统。服务器1512还可以运行各种附加的服务器应用和/或中间层应用中的任何一个，包括 HTTP(超文本传输协议)服务器、FTP(文件传输协议)服务器、 CGI(公用网关接口)服务器、JAVA ®服务器、数据库服务器等。示例性的数据库服务器包括但不限于那些商业上可从Oracle、 Microsoft、IBM(国际商业机器)等获得的数据库服务器。

[0137] 在一些实现中，服务器1512可以包括用于对从客户端计算设备 1502、1504、1506和1508的用户接收到的数据馈送和/或事件更新进行分析和联合的一个或多个应用。作为例子，数据馈送和/或事件更新可以包括但不限于Twitter®馈送、Facebook®更新或从一个或多个第三方信息源接收到的实时更新和连续数据流，可以包括与传感器数据应用、财务自动收报机、网络性能测量工具(例如，网络监视和业务管理应用)、点击流分析工具、自动流量监视等有关的实时事件。服务器1512还可以包括用于经由客户端计算设备1502、1504、1506和 1508的一个或多个显示设备显示数据馈送和/或实时事件的一个或多个应用。

[0138] 分布式系统1500还可以包括一个或多个数据库1514和1516。数据库1514和1516可以位于各种位置。以示例的方式，数据库1514 和1516中的一个或多个可以位于服务器1512本地的(和/或处于服务器1512之中的)非暂时性存储介质上。可替代地，数据库1514和1516可以远离服务器1512，并经由基于网络的连接或专有连接与服务器 1512进行通信。在一组实施例中，数据库1514和1516可以位于存储区域网络(SAN)中。类似地，视情况而定，用于执行归因于服务器 1512的功能的任何必要文件可以本地地存储在服务器1512上和/或远程地存储。在一组实施例中，数据库1514和1516可以包括被适配为响应于SQL格式的命令来存储、更新以及获取数据的关系数据库，诸如Oracle提供的数据库。

[0139] 图16是根据本公开的实施例的系统环境1600的一个或多个组件的简化方框图，通过该系统环境，由实施例系统的一个或多个组件提供的服务可以被提供为云服务。在所示实施例中，系统环境1600包括一个或多个客户端计算设备1604、1606和1608，该一个或多个客户端计算设备可以被用户用来与提供云服务的云基础设施系统1602进行交互。客户端计算设备可以被配置为操作客户端应用，诸如网络浏览器、专用客户端应用(例如Oracle Form)或某种其它应用，客户端计算设备的用户可以使用所述客户端应用与云基础设施系统1602 进行交互，以便使用云基础设施系统1602所提供的服务。

[0140] 应当理解的是，除了所描绘的那些组件之外，该图中描绘的云基础设施系统1602还可以具有其它组件。此外，在该图中所示的实施例仅仅是可以包含本发明的实施例的云基础设施系统的一个例子。在一些其它实施例中，云基础设施系统1602可以具有与附图所示的组件相比更多或更少的组件，可以将两个或更多个组件组合，或者可以具有不同的组件配置或组件布置。

[0141] 客户端计算设备1604、1606和1608可以是与上面针对1502、1504、1506和1508描述的那些类似的设备。

[0142] 虽然示例性的系统环境1600被示为具有三个客户端计算设备，但是可以支持任何数量的客户端计算设备。其它设备(诸如具有传感器等的设备)可以与云基础设施系统1602进行交互。

[0143] 网络1610可以有助于客户端1604、1606和1608与云基础设施系统1602之间的数据通信和交换。每个网络可以是本领域技术人员所熟悉的任何类型的网络，该网络可以支持使用各种商用的协议(包括上面针对网络1510所描述的那些协议)中的任何一个的数据通信。

[0144] 云基础设施系统1602可以包括一个或多个计算机和/或服务器 (其可以包括上面针对服务器1512所描述的那些)。

[0145] 在某些实施例中，云基础设施系统所提供的服务可以包括可供云基础设施系统的用户按需使用的许多服务，诸如在线数据存储和备份方案、基于网络的电子邮件服务、托管的办公套件和文档协作服务、数据库处理、受管理的技术支持服务等。云基础设施系统所提供的服务可以动态地调整以满足其用户的需要。云基础设施系统所提供的服务的具体实例化在本文中被称为“服务实例”。一般地，来自云服务提供商的系统的、经由诸如因特网之类的通信网络可供用户使用的任何服务被称为“云服务”。通常，在公共云环境中，组成云服务提供商的系统的服务器和系统与客户自己的内部服务器和系统不同。例如，云服务提供商的系统可以托管应用，并且用户可以根据需要经由诸如因特网之类的通信网络订购和使用该应用。

[0146] 在一些例子中，计算机网络云基础设施中的服务可以包括对云供应商提供给用户的存储、托管的数据库、托管的网络服务器、软件应用、或其它服务、或者本领域中已知的其它进行受保护的计算机网络访问。例如，服务可以包括通过因特网对云上的远程存储进行的密码受保护的访问。作为另一个例子，服务可以包括供联网开发者专有使用的基于网络服务的托管的关系数据库以及脚本语言中间件引擎。作为另一个例子，服务可以包括对托管在云供应商的网站上的电子邮件软件应用的访问。

[0147] 在某些实施例中，云基础设施系统1602可以包括一套应用、中间件和数据库服务供应，这些通过自助服务、基于订阅、弹性可扩展、可靠、高可用性以及安全的方式被传递给客户。这样的云基础实施系统的例子是由本受让人所提供的Oracle公共云。

[0148] 在各个实施例中，云基础设施系统1602可以被适配为自动地供应、管理和跟踪客户对云基础设施系统1602所提供的服务的订阅。云基础设施系统1602可以经由不同的部署模型来提供云服务。例如，可以在公共云模型下提供服务，在公共云模型中，云基础实施系统1602 由销售云服务的组织所有(例如，由Oracle所有)，并且服务可供公众或不同行业的企业使用。作为另一个例子，可以在私有云模型下提供服务，在私有云模型中，云基础设施系统1602仅仅针对单个组织来运行，并且可以为该组织内的一个或多个实体提供服务。也可以在共同体云模型下提供云服务，在共同体云模型中，云基础设施系统1602 以及云基础设施系统1602所提供的服务由相关共同体中的若干组织共享。也可以在混合云模型下提供云服务，混合云模型是两个或更多个不同模型的组合。

[0149] 在一些实施例中，云基础设施系统1602所提供的服务可以包括在软件即服务

(SaaS)类别、平台即服务(Paas)类别、基础设施即服务(IaaS)类别或包括混合服务的其它服务类别下提供的一个或多个服务。客户经由订阅订单可以订购云基础设施系统1602所提供的一个或多个服务。云基础实施系统602随后执行处理以提供客户的订阅订单中的服务。

[0150] 在一些实施例中,云基础设施系统1602所提供的服务可以包括但不限于应用服务、平台服务和基础实施服务。在一些实施例中,应用服务可以由云基础实施系统经由SaaS平台来提供。SaaS平台可以被配置为提供落入SaaS类别的云服务。例如,SaaS平台可以在集成的开发和部署平台上提供建立并交付一套按需应用的能力。SaaS平台可以管理和控制用于提供SaaS服务的底层软件和基础实施。通过利用SaaS平台所提供的服务,客户可以利用在云基础实施系统上执行的应用。客户可以在不需要客户购买单独的许可和支持的情况下获取应用服务。可以提供各种不同的SaaS服务。例子包括但不限于为大型组织提供用于销售业绩管理、企业集成以及商业灵活性的方案的服务。

[0151] 在一些实施例中,平台服务可以由云基础设施系统经由PaaS平台来提供。PaaS平台可以被配置为提供落入PaaS类别的云服务。平台服务的例子可以包括但不限于:使得组织(诸如Oracle)能够在共享的共同的体系架构上联合现有应用的服务,以及建立利用平台所提供的共享服务的新应用的能力。PaaS平台可以管理和控制用于提供 PaaS服务的底层软件和基础实施。客户可以获取云基础实施系统所提供的PaaS服务,而不需要客户购买单独的许可和支持。平台服务的例子包括但不限于Oracle Java云服务(JCS)、Oracle数据库云服务 (DBCS)等。

[0152] 通过利用PaaS平台所提供的服务,客户可以利用云基础实施系统所支持的编程语言和工具,并且还可以控制所部署的服务。在一些实施例中,云基础设施系统所提供的平台服务可以包括数据库云服务、中间件云服务(例如,Oracle融合中间件服务)和Java云服务。在一个实施例中,数据库云服务可以支持共享服务部署模型,该共享服务部署模型使得组织能够把数据库资源集中在一起并且以数据库云的形式向客户提供数据库即服务。在云基础实施系统中,中间件云服务可以给客户提供用于开发和部署各种商业应用的平台,并且Java云服务可以给客户提供用于部署Java应用的平台。

[0153] 在云基础设施系统中,各种不同的基础设施服务可以由IaaS平台来提供。基础设施服务有助于对底层计算资源(诸如存储、网络和其它基本计算资源)进行管理和控制,以供客户使用SaaS平台和PaaS 平台所提供的服务。

[0154] 在某些实施例中,云基础设施系统1602还可以包括基础设施资源1630,其提供用于向云基础实施系统的客户提供各种服务的资源。在一个实施例中,基础设施资源1630可以包括用于执行PaaS平台和 SaaS平台所提供的服务的硬件(诸如服务器、存储装置和网络资源) 的预先集成和优化的组合。

[0155] 在一些实施例中,云基础设施系统1602中的资源可以被多个用户共享,并且可以按需被动态地重新分配。附加地,可以将资源分配给处于不同时区的用户。例如,云基础设施系统1630可以使得处于第一时区的第一组用户能够在指定数量的小时中利用云基础实施系统的资源,并随后使得相同的资源能够被重新分配给位于不同时区的另一组用户,从而最大化资源的利用。

[0156] 在某些实施例中,可以提供多个内部共享服务1632,该多个内部共享服务被云基础设施系统1602的不同组件或模块共享,并且被云基础设施系统1602所提供的服务共享。

这些内部共享服务可以包括但不限于:安全和身份服务、集成服务、企业库服务、企业管理器服务、病毒扫描和白名单服务、高可用性、备份和恢复服务、用于实现云支持的服务、电子邮件服务、通知服务、文件传输服务等。

[0157] 在某些实施例中,云基础设施系统1602可以提供对云基础设施系统中的云服务(例,如SaaS、PaaS和IaaS服务)的综合管理。在一个实施例中,云管理功能可以包括用于供应、管理和跟踪云基础设施系统1602所接收到的用户的订阅的能力等等。

[0158] 在一个实施例中,如在图中所描绘的那样,云管理功能可以由一个或多个模块(诸如订单管理模块1620、订单调配模块1622、订单供应模块1624、订单管理和监视模块1626、以及身份管理模块1628) 来提供。这些模块可以包括一个或多个计算机和/或服务器或者可以通过使用一个或多个计算机和/或服务器来提供,该一个或多个计算机和 /或服务器可以是通用计算机、专用服务器计算机、服务器集、服务器群或者任何其它适当的布置和/或组合。

[0159] 在示例性操作1634中,使用客户端设备(诸如客户端设备1604、1606或1608)的客户可以通过请求云基础实施系统1602所提供的一个或多个服务并发出对云基础设施系统1602所提供的一个或多个服务进行订阅的订单,来与云基础设施系统1602进行交互。在某些实施例中,客户可以访问云用户接口(UI)、云UI 1612、云UI 1614和/ 或云UI 1616,并经由这些UI来发出订阅订单。响应于客户发出订单,云基础设施系统1602接收到的订单信息可以包括标识客户的信息以及客户意图订阅的由云基础设施系统1602提供的一个或多个服务。

[0160] 在客户已经发出订单之后,订单信息经由云UI 1612、1614和/ 或1616而被接收。

[0161] 在操作1636中,订单被存储在订单数据库1618中。订单数据库 1618可以是云基础设施系统1618所操作的并且结合其它系统元件操作的若干数据库中的一个。

[0162] 在操作1638,订单信息被转发给订单管理模块1620。在一些实例中,订单管理模块1620可以被配置为执行与订单相关联的计费和会计功能,诸如验证订单,并且在验证之后接受订单。

[0163] 在操作1640,关于订单的信息被传送到订单调配模块1622。订单调配模块1622可以利用订单信息来调配针对客户发出的订单的服务和资源的供应。在一些实例中,订单调配模块1622可以调配资源的供应,以便使用订单供应模块1624的服务来支持订阅的服务。

[0164] 在某些实施例中,订单调配模块1622实现对与每个订单相关联的商业过程的管理,并应用商业逻辑来确定订单是否应当继续供应。在操作1642,在接收到新订阅的订单时,订单调配模块1622向订单供应模块1624发送分配资源以及对完成订阅订单所需要的那些资源进行配置的请求。订单供应模块1624实现对用于客户所订购的服务的资源的分配。订单供应模块1624提供云基础设施系统1600所提供的云服务与物理实现层之间的抽象级别,物理实现层用于供应用于提供所请求的服务的资源。订单调配模块1622因此可以与实现细节隔离,实现细节诸如服务和资源被即时实际供应还是被预先供应并且仅仅在请求时被分配/指派。

[0165] 在操作1644,一旦供应了服务和资源,云基础设施系统1602的订单供应模块1624就可以将所提供的服务的通知发送给客户端设备 1604、1606和/或1608上的客户。

[0166] 在操作1646,客户的订阅订单可以由订单管理和监视模块1626 来管理和跟踪。在

一些实例中，订单管理和监视模块1626可以被配置为收集订阅订单中的服务的使用统计数据，诸如所使用的存储的量、传输的数据的量、用户的数量以及系统开机的时间量和系统停机的时间量。

[0167] 在某些实施例中，云基础设施系统1600可以包括身份管理模块 1628。身份管理模块1628可以被配置为提供身份服务，诸如云基础设施系统1600中的访问管理和授权服务。在一些实施例中，身份管理模块1628可以控制与期望利用云基础设施系统1602所提供的服务的客户有关的信息。这样的信息可以包括认证这样的客户的身份的信息以及描述相对于各种系统资源(例如，文件、目录、应用、通信端口、存储器段等)那些客户被授权执行哪些动作的信息。身份管理模块 1628还可以包括对描述性信息的管理，该描述性信息与每个客户有关，并且与该描述性信息可以被如何访问和修改以及可以被谁访问和修改有关。

[0168] 图17示出了示例性计算机系统1700，在该示例性计算机系统中，可以实现本发明的各个实施例。系统1700可以用于实现上面描述的计算机系统中的任何一个。如该图所示，计算机系统1700包括处理单元 1704，处理单元1704经由总线子系统1702与多个外围子系统进行通信。这些外围子系统可以包括处理加速单元1706、I/O子系统1708、存储子系统1718和通信子系统1724。存储子系统1718包括有形的计算机可读存储介质1722和系统存储器1710。

[0169] 总线子系统1702提供让计算机系统1700的各个组件和子系统按照期望彼此进行通信的机构。虽然总线子系统1702被示意性地示为单个总线，但是总线子系统的可替代实施例可以利用多个总线。总线子系统1702可以是使用各种总线体系架构中的任何一种的若干种类型的总线结构(包括存储器总线或存储器控制器、外围总线以及本地总线)中的任何一种。例如，这样的体系架构可以包括工业标准体系架构(ISA)总线、微通道体系架构(MCA)总线、增强ISA(EISA) 总线、视频电子标准协会(VESA)本地总线以及外围组件互连(PCI)总线，它们可以被实现为根据IEEE P1386.1标准制成的夹层总线 (Mezzanine bus)。

[0170] 可以被实现成一个或多个集成电路(例如，常规的微处理器或微控制器)的处理单元1704控制计算机系统1700的操作。在处理单元 1704中可以包括一个或多个处理器。这些处理器可以包括单核处理器或多核处理器。在某些实施例中，处理单元1704可以被实现为一个或多个独立的处理单元1732和/或1734，在每个处理单元中包括有单核或多核处理器。在其它实施例中，处理单元1704还可以被实现为四核处理单元，该四核处理单元是通过将两个双核处理器集成到单个芯片而形成的。

[0171] 在各个实施例中，处理单元1704可以响应于程序代码而执行各种程序，并且可以维持多个并行执行的程序或进程。在任何给定时间，要被执行的程序代码中的一些或全部可以位于处理器1704中和/或位于存储子系统1718中。通过适当的编程，处理器1704可以提供上面描述的各种功能。计算机系统1700可以附加地包括处理加速单元 1706，该处理加速单元1706可以包括数字信号处理器(DSP)、专用处理器等。

[0172] I/O子系统1708可以包括用户接口输入设备和用户接口输出设备。用户接口输入设备可以包括键盘、指向设备(诸如鼠标或轨迹球)、被包含到显示器中的触摸板或触摸屏、滚轮、点击轮、转盘、按钮、开关、小型键盘、具有语音命令识别系统的音频输入设备、麦克风以及其它类型的输入设备。用户接口输入设备可以包括例如运动感测和/ 或姿势识别设备(诸如Microsoft**Kinect®**运动传感器)，其使得用户能够使用姿势和口说命令通过自然的

用户接口控制输入设备(诸如 Microsoft**Xbox®**360游戏控制器)并与输入设备进行交互。用户接口输入设备还可以包括眼睛姿态识别设备(诸如Google**Glass®**眨眼检测器),其检测来自用户的眼睛活动(例如在拍照和/或进行菜单选择时的"眨眼"),并将眼睛姿态作为输入转换到输入设备(例如Google **Glass®**)。附加地,用户接口输入设备可以包括语音识别感测设备,其使得用户能够通过语音命令与语音识别系统(例如**Siri®**导航器)进行交互。

[0173] 用户接口输入设备还可以包括但不限于:三维(3D)鼠标、操纵杆或指向杆、游戏板和图形平板、以及音频/视觉设备(诸如扬声器、数字照相机、数字摄像机、便携式媒体播放器、网络照相机、图像扫描仪、指纹扫描仪、条形码读取器、3D扫描仪、3D打印机、激光测距仪、以及眼睛注视跟踪设备)。附加地,用户接口输入设备可以包括例如医疗成像输入设备,诸如计算机断层扫描、磁共振成像、正电子发射断层扫描、医疗超声设备。用户接口输入设备还可以包括例如音频输入设备,诸如MIDI键盘、数字乐器等。

[0174] 用户接口输出设备可以包括显示子系统、指示灯或非视觉显示器 (诸如音频输出设备等)。显示子系统可以是阴极射线管(CRT)、平板设备(诸如使用液晶显示器(LCD)或等离子显示器的设备)、投影设备、触摸屏等。一般地,术语"输出设备"的使用旨在包括用于从计算机系统1700向用户或其它计算机输出信息的所有可能类型的设备和机构。例如,用户接口输出设备可以包括但不限于视觉地传送文本、图形和音频/视频信息的各种显示设备,诸如监视器、打印机、扬声器、耳机、汽车导航系统、绘图机、语音输出设备以及调制解调器。

[0175] 计算机系统1700可以包括存储子系统1718,其包括软件元件,该软件元件被示为当前位于系统存储器1710内。系统存储器11710 可以存储在处理单元1704上可加载和可执行的程序指令以及在这些程序执行期间生成的数据。

[0176] 依赖于计算机系统1700的配置和类型,系统存储器1710可以是易失性的(诸如随机存取存储器(RAM))和/或非易失性的(诸如只读存储器(ROM)、闪速存储器等)。RAM通常包含处理单元1704 可立即访问的和/或处理单元1704当前正在操作和执行的数据和/或程序模块。在一些实现中,系统存储器1710可以包括多个不同类型的存储器,诸如静态随机存取存储器(SRAM)或动态随机存取存储器 (DRAM)。在一些实现中,通常可以在ROM中存储基本输入/输出系统(BIOS),基本输入/输出系统包含有助于诸如在启动期间在计算机系统1700内的元件之间传输信息的基本例程。以示例而不是限制的方式,系统存储器1710还示出了应用程序1712、程序数据1714和操作系统1716,其中应用程序1712可以包括客户端应用、网络浏览器、中间层应用、关系数据库管理系统(RDBMS)等。以示例的方式,操作系统1716可以包括各种版本的Microsoft**Windows®**、Apple **Macintosh®**和/或Linux操作系统、各种商用的**UNIX®**或类UNIX操作系统(包括但不限于各种GNU/Linux操作系统、Google **Chrome®**OS 等)和/或移动操作系统(诸如iOS、**Windows®**Phone、**Android®**OS、**BlackBerry®**10OS以及**Palm®**OS操作系统)。

[0177] 存储子系统1718还可以提供有形计算机可读存储介质,以用于存储提供一些实施例的功能的基本编程和数据结构。可以在存储子系统1718中存储在被处理器执行时提供上面描述的功能的软件(程序、代码模块、指令)。这些软件模块或指令可以由处理单元1704执

行。存储子系统1718还可以提供用于存储根据本发明使用的数据的库。

[0178] 存储子系统1700还可以包括计算机可读存储介质读取器1720，其可以进一步连接到计算机可读存储介质1722。计算机可读存储介质 1722与系统存储器1710组合在一起并且可选地可以综合地表示远程的、本地的、固定的和/或可移除的存储设备和用于临时地和/或更永久地包含、存储、发送和获取计算机可读信息的存储介质。

[0179] 包含代码或代码的一部分的计算机可读存储介质1722还可以包括本领域中已知的或使用的任何适当介质，包括存储介质和通信介质，诸如但不限于：以用于信息的存储和/或传输的任何方法或技术实现的易失性和非易失性的、可移除的或不可移除的介质。这可以包括有形计算机可读存储介质，诸如RAM、ROM、电可擦可编程ROM (EEPROM)、闪速存储器或其它存储器技术、CD-ROM、数字通用盘(DVD)、或其它光学存储装置、磁盒、磁带、磁盘存储装置或其它磁存储设备、或者其它有形计算机可读介质。这还可以包括非有形的计算机可读介质，诸如数据信号、数据传输、或任何其它可以用于传输期望的信息并可以被计算系统1700访问的介质。

[0180] 以示例的方式，计算机可读存储介质1722可以包括：硬盘驱动器，其从不可移除的、非易失性的磁介质读取或向不可移除的、非易失性的磁介质写入；磁盘驱动器，其从可移除的、非易失性的磁盘读取或向可移除的、非易失性的磁盘写入；以及光盘驱动器，其从可移除的、非易失性光盘(诸如CD ROM、DVD和**Blu-Ray®**盘或其它光介质)读取或向可移除的、非易失性光盘写入。计算机可读存储介质 1722可以包括但不限于**Zip®**驱动器、闪存卡、通用串行总线(USB) 闪存驱动器、安全数字(SD)卡、DVD盘、数字视频带等。计算机可读存储介质1722还可以包括基于非易失性存储器的固态驱动器 (SSD)(诸如基于闪存的SSD、企业闪速驱动器、固态ROM等)、基于易失性存储器(诸如固态RAM、动态RAM、静态RAM)的SSD、基于DRAM的SSD、磁阻RAM(MRAM)SSD、以及使用基于DRAM 和基于闪存的SSD的组合的混合SSD。磁盘驱动器以及它们相关联的计算机可读介质可以为计算机系统1700提供计算机可读指令、数据结构、程序模块和其它数据的非易失性存储。

[0181] 通信子系统1724提供与其它计算机系统和网络的接口。通信子系统1724用作用于从计算机系统1700的其它系统接收数据以及向所述其它系统发送数据的接口。例如，通信子系统1724可以使得计算机系统1700能够经由因特网连接到一个或多个设备。在一些实施例中，通信子系统1724可以包括射频(RF)收发器组件、全球定位系统(GPS) 接收器组件和/或其它组件，RF收发器组件用于访问无线语音和/或数据网络(例如，使用蜂窝电话技术，高级数据网络技术，诸如3G、4G 或EDGE(全球演进的增强数据速率)，WiFi(IEEE 802.11标准族或其它移动通信技术或它们的任何组合))。在一些实施例中，除了无线接口以外或者替代无线接口，通信子系统1724可以提供有线网络连接性(例如以太网)。

[0182] 在一些实施例中，通信子系统1724还可以代表可以使用计算机系统1700的一个或多个用户，接收结构化的和/或非结构化的数据馈送1726、事件流1728、事件更新1730等形式的输入通信。

[0183] 以示例的方式，通信子系统1724可以被配置为从社交网络和/或其它通信服务的用户接收实时的数据馈送1726，诸如**Twitter®**馈送、**Facebook®**更新、网络馈送(诸如丰富站点摘要(RSS)馈送)和/或来自一个或多个第三方信息源的实时更新。

[0184] 附加地，通信子系统1724还可以被配置为接收连续数据流形式的数据，连续数据流可以包括实时事件的事件流1728和/或事件更新 1730，其本质上可以是连续的或无界的而不具有明确的结束。生成连续数据的应用的例子可以包括例如传感器数据应用、财务自动收报机、网络性能测量工具(例如，网络监视和流量管理应用)、点击流分析工具、汽车交通监视等。

[0185] 通信子系统1724还可以被配置为向一个或多个数据库输出结构化的和/或非结构化的数据馈送1726、事件流1728、事件更新1730等，该一个或多个数据库可以与耦合到计算机系统1700的一个或多个流数据源计算机进行通信。

[0186] 计算机系统1700可以是各种类型中的一个，包括手持便携式设备(例如iphone®蜂窝电话、iPad®计算平板、PDA)、可穿戴设备 (例如，GoogleGlass®安装在头部的显示器)、PC、工作站、大型机、一体机、服务器机架、或任何其它数据处理系统。

[0187] 由于计算机和网络的不断变化的特点，对附图中描绘的计算机系统1700的描述仅仅旨在作为特定的例子。与附图所描绘的系统相比具有更多或更少组件的许多其它配置是可能的。例如，也可以使用定制的硬件，和/或可以用硬件、固件、软件(包括小应用程序)或组合来实现特定的元件。此外，可以采用与其它计算设备(诸如网络输入/ 输出设备)的连接。基于本文中提供的公开和教导，本领域普通技术人员将理解用于实现各种实施例的其它方式和/或方法。

[0188] 在以上的说明书中，参考本发明的特定实施例描述了本发明的方面，但是本领域技术人员将认识到本发明并不限于此。可以独立地或联合地使用上面描述的发明的各个特征和方面。此外，在不脱离说明书的宽广的精神和范围的情况下，除了本文中描述的内容以外，可以在任何数量的环境和应用中利用实施例。相应地，说明书和附图将被认为是解释性的而非限制性的。

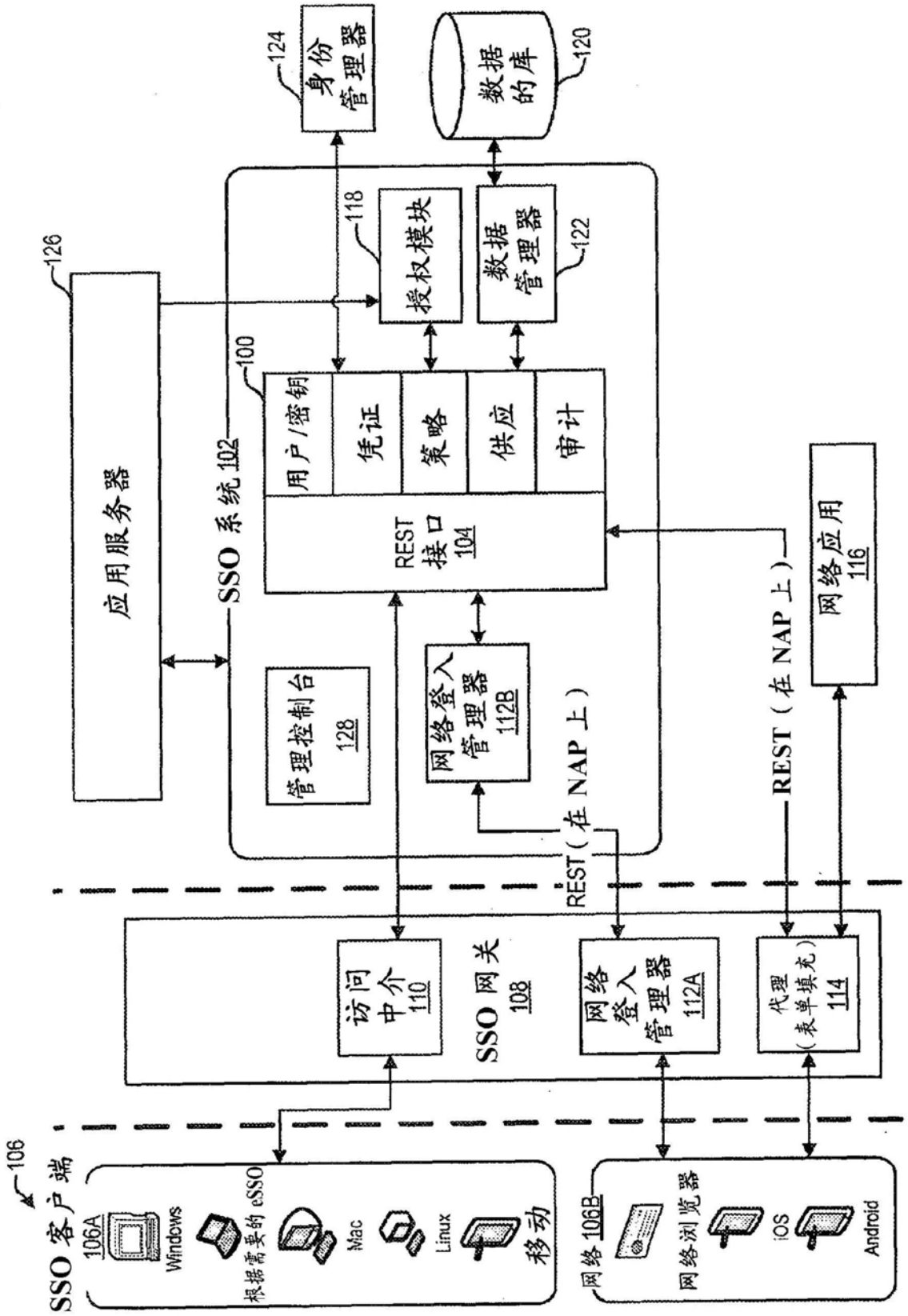

SSO 客户端
106
106A
Windows
根据需要的 eSSO
Mac
Linux
移动
网络 106B
网络浏览器
iOS
Android
SSO 网关
108
访问中介
110
网络登入管理器
112A
代理（表单填充）
114
REST（在 NAP 上）
网络登入管理器
112B
管理控制台
128
SSO 系统 102
100
用户/密钥
凭证
策略
供应
审计
REST 接口
104
授权模块
118
数据管理器
122
应用服务器
126
身份管理器
124
数据的库
120
网络应用
116
REST（在 NAP 上）

图1

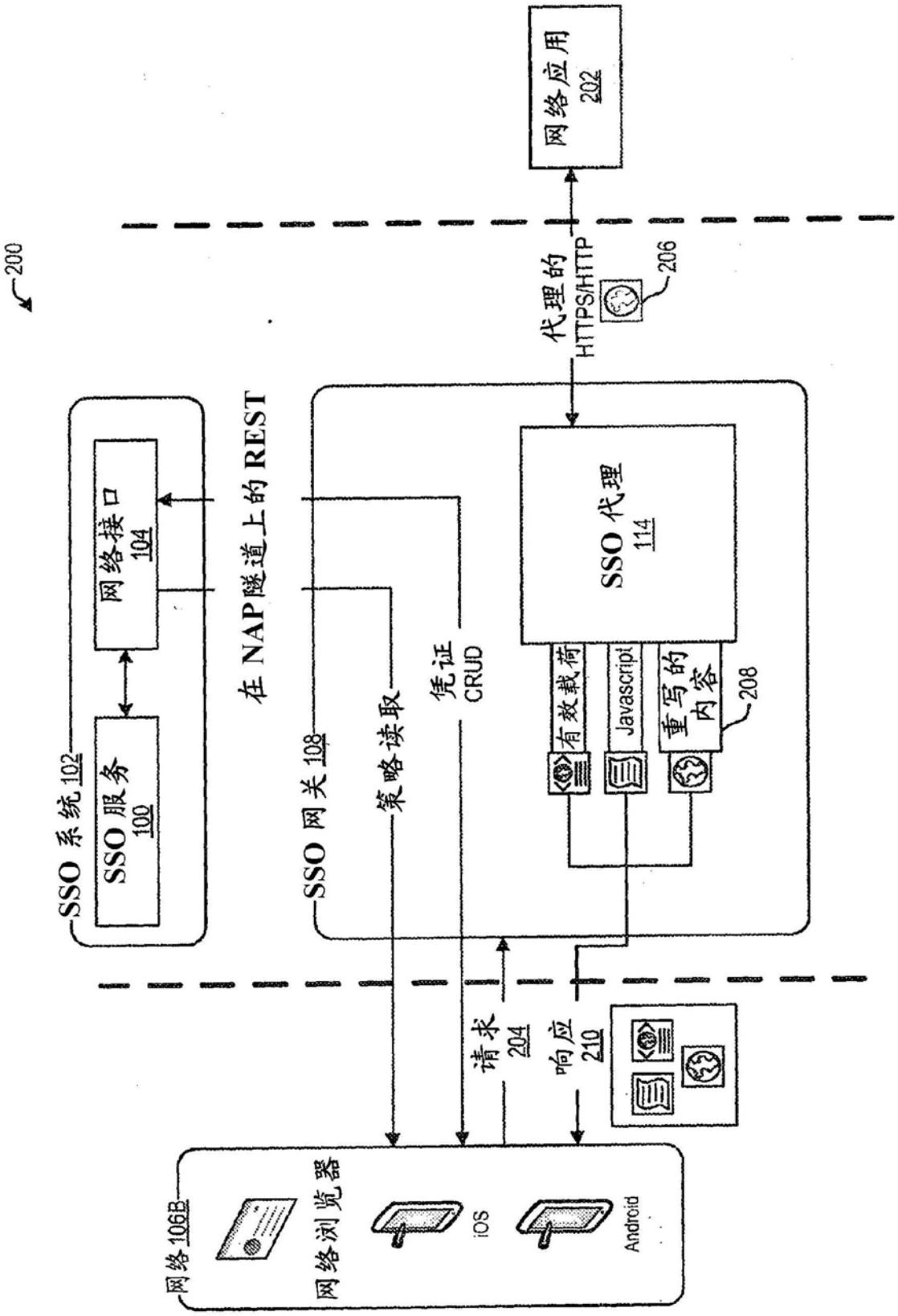

200
网络应用 202
代理的 HTTPS/HTTP
206
在 NAP 隧道上的 REST
SSO 系统 102
网络接口 104
SSO 服务 100
SSO 网关 108
策略读取
凭证 CRUD
SSO 代理 114
有效载荷
Javascript
重写的内容
208
请求 204
响应 210
网络 106B
网络浏览器
iOS
Android

图2

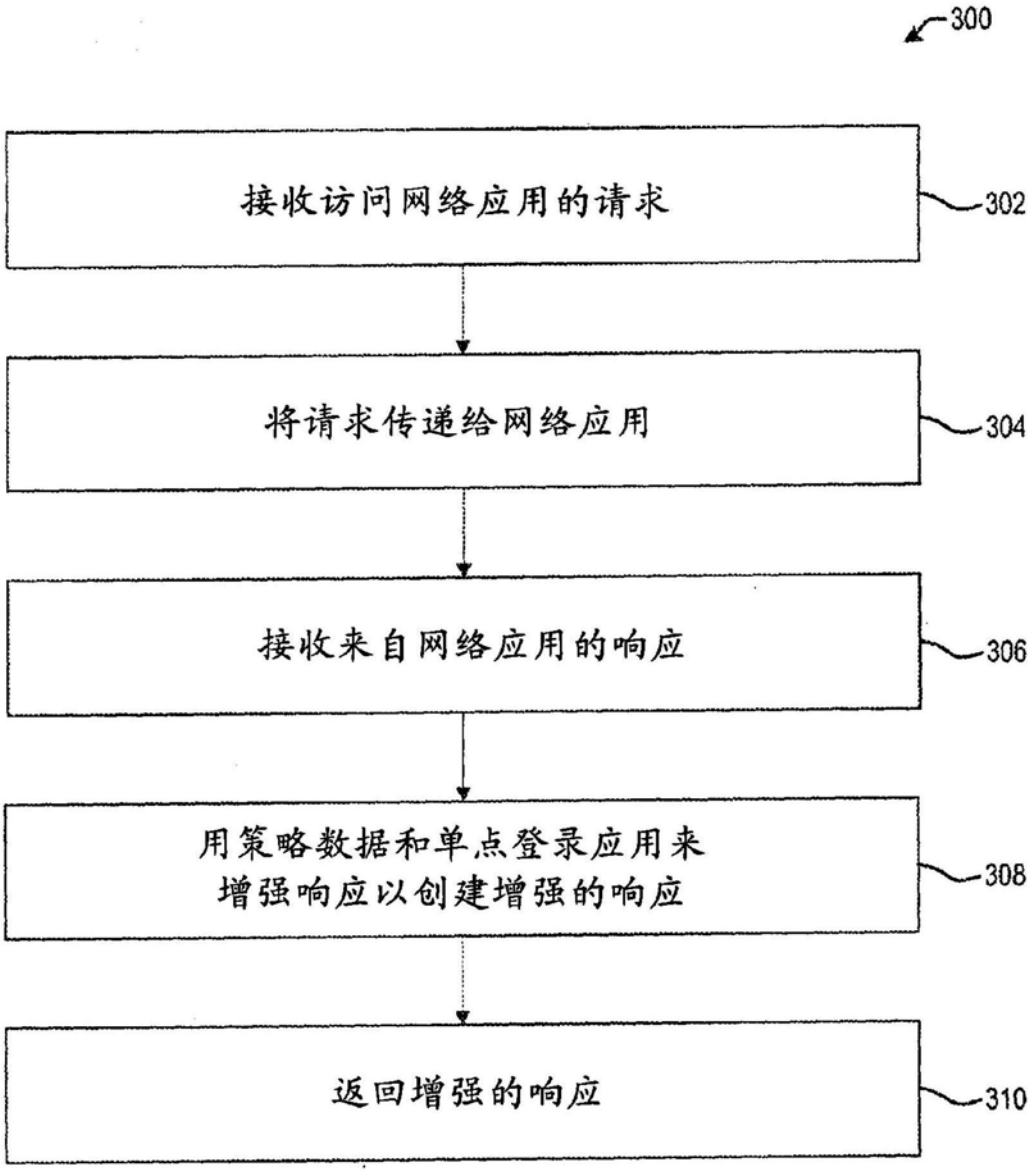

300
接收访问网络应用的请求
302
将请求传递给网络应用
304
接收来自网络应用的响应
306
用策略数据和单点登录应用来
增强响应以创建增强的响应
308
返回增强的响应
310

图3

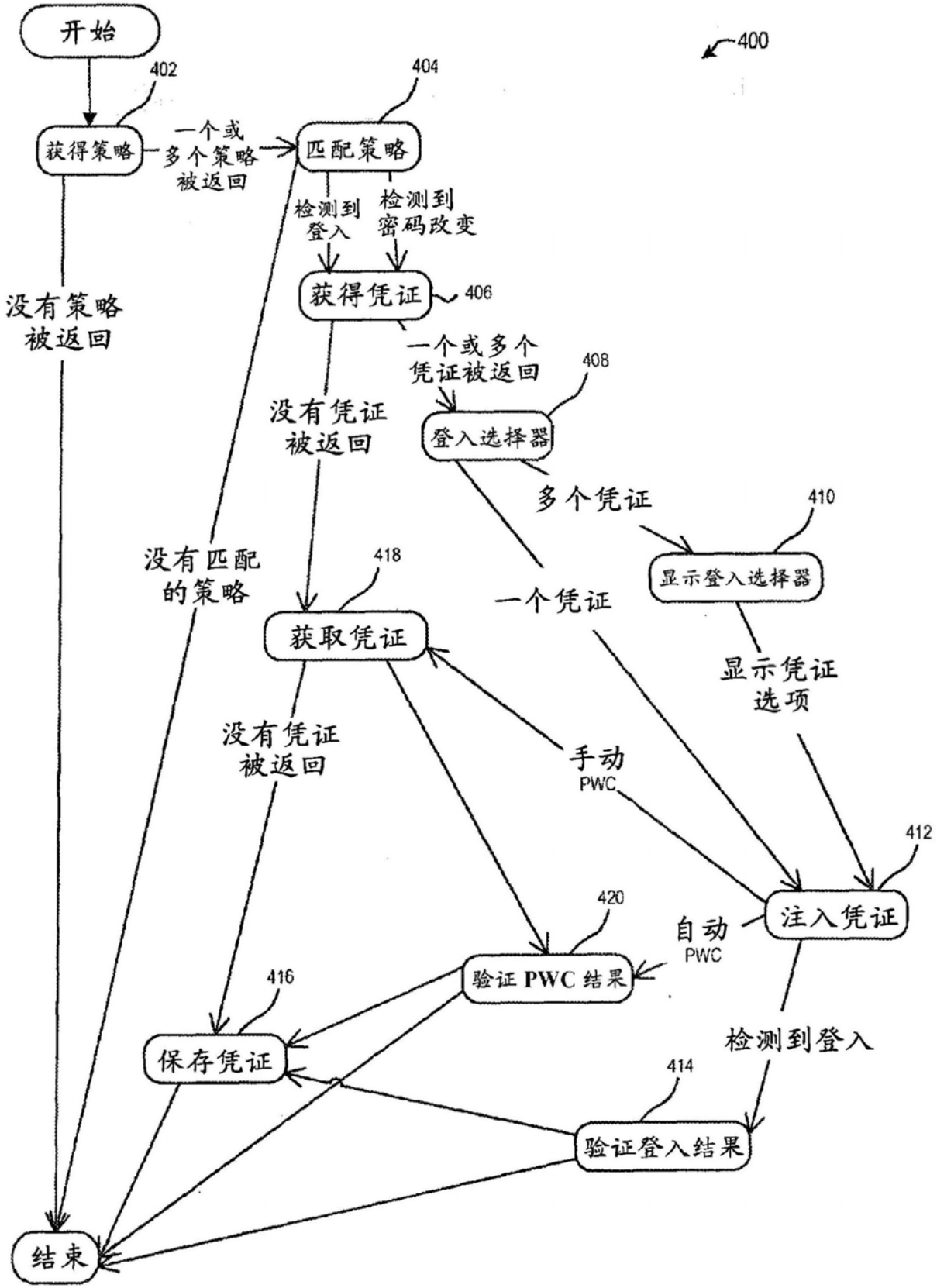

开始
400
402
404
获得策略
一个或
多个策略
被返回
匹配策略
检测到
登入
检测到
密码改变
获得凭证
406
没有策略
被返回
一个或多个
凭证被返回
408
没有凭证
被返回
登入选择器
多个凭证
410
显示登入选择器
没有匹配
的策略
418
一个凭证
获取凭证
显示凭证
选项
没有凭证
被返回
手动
PWC
412
420
自动
PWC
注入凭证
验证 PWC 结果
416
检测到登入
保存凭证
414
验证登入结果
结束

图4

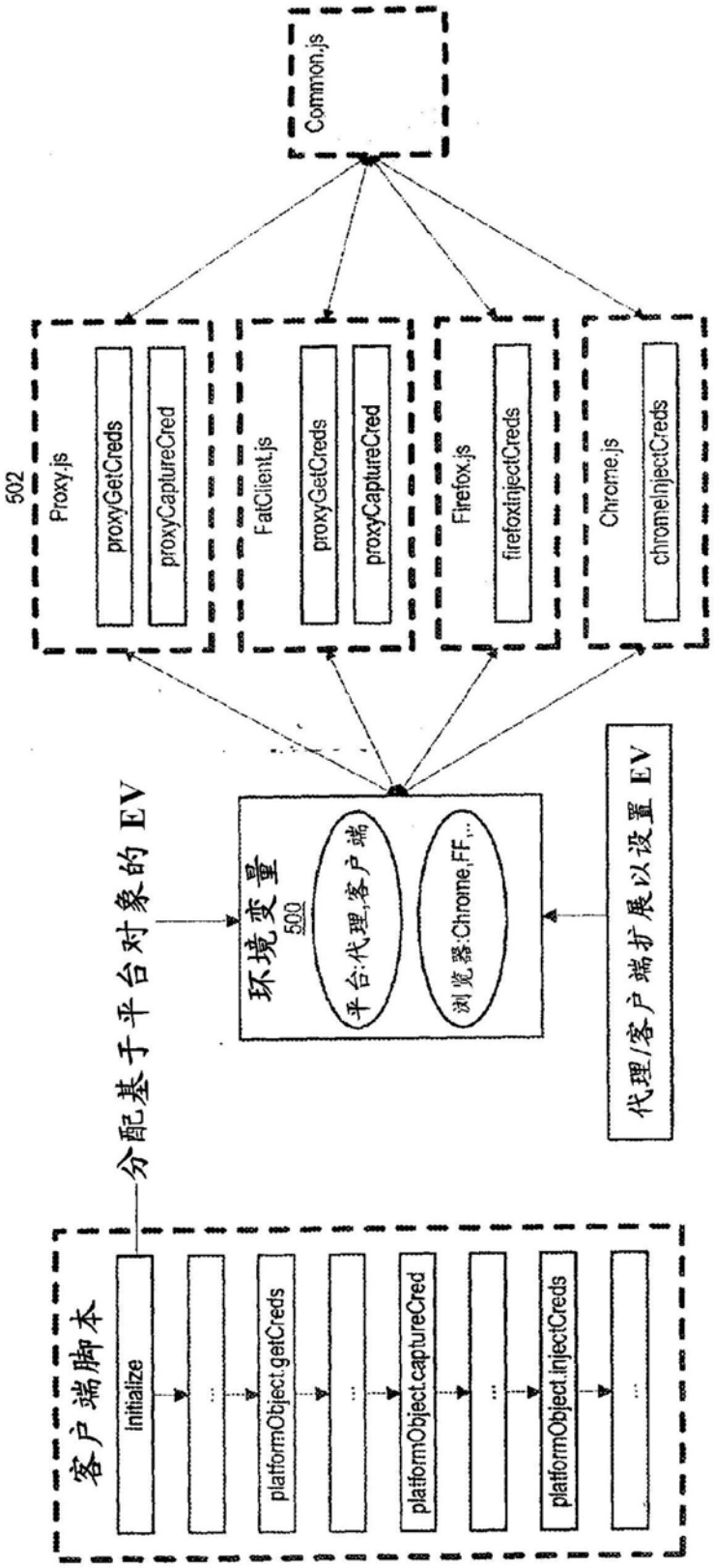

Common.js
502
Proxy.js
proxyGetCreds
proxyCaptureCred
FatClient.js
proxyGetCreds
proxyCaptureCred
Firefox.js
firefoxInjectCreds
Chrome.js
chromeInjectCreds
环境变量
500
平台:代理,客户端
浏览器:Chrome,FF,...
代理/客户端扩展以设置 EV
分配基于平台对象的 EV
客户端脚本
Initialize
...
platformObject.getCreds
...
platformObject.captureCred
...
platformObject.injectCreds
...

图5

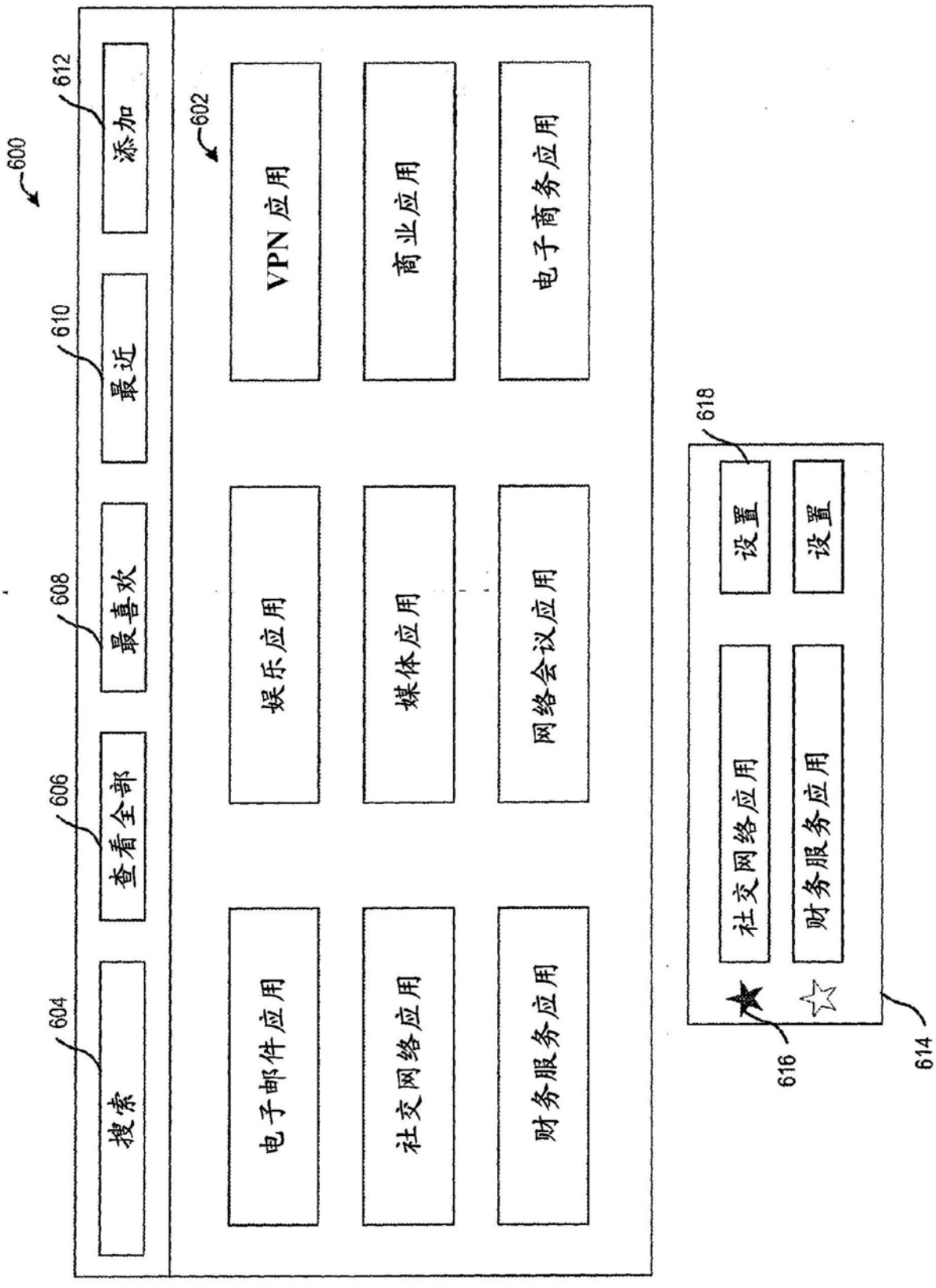

600
602
604
搜索
606
查看全部
608
最喜欢
610
最近
612
添加
VPN 应用
娱乐应用
商业应用
媒体应用
电子商务应用
网络会议应用
电子邮件应用
社交网络应用
财务服务应用
618
设置
设置
社交网络应用
财务服务应用
616
614

图6

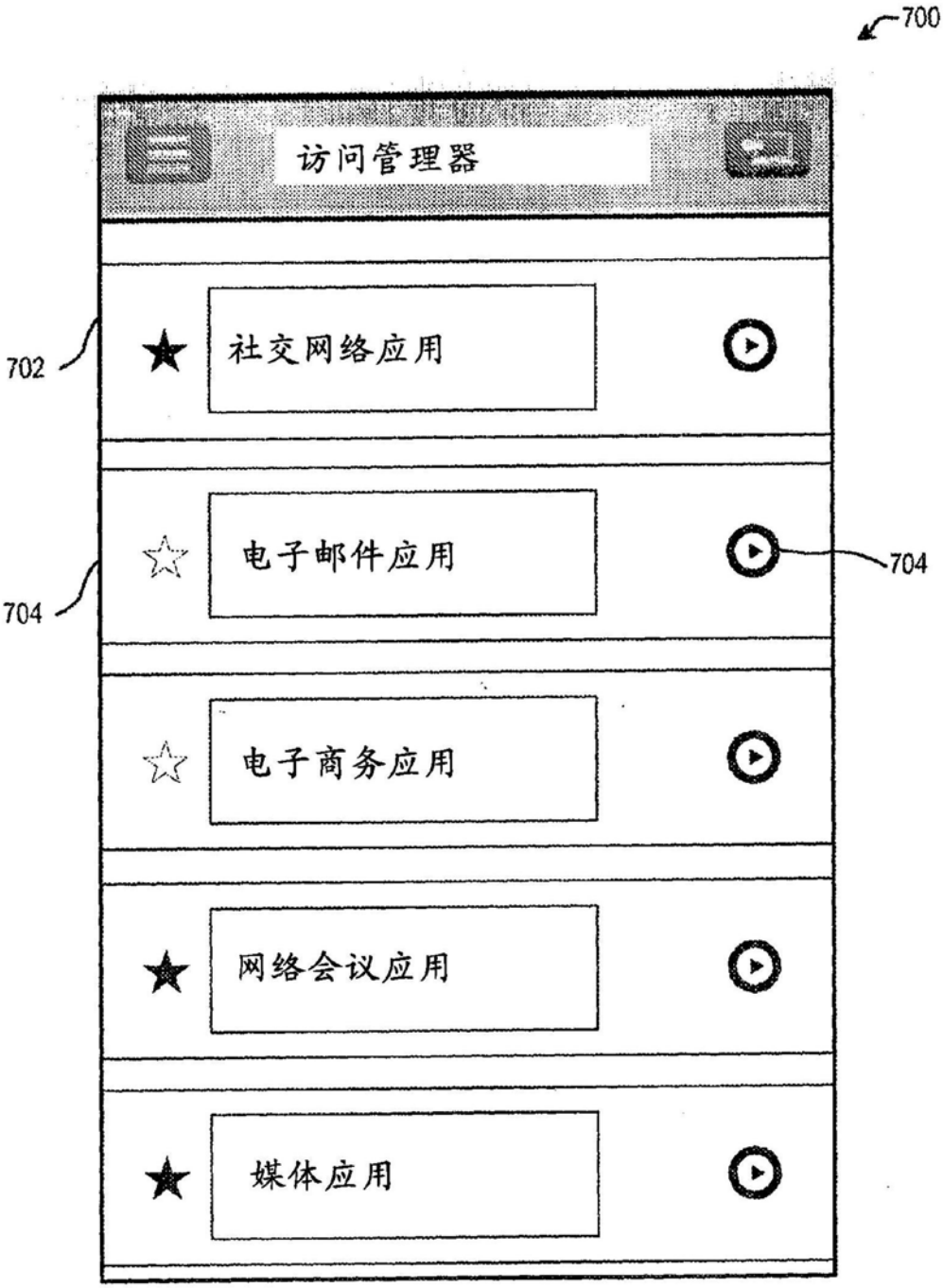


图7

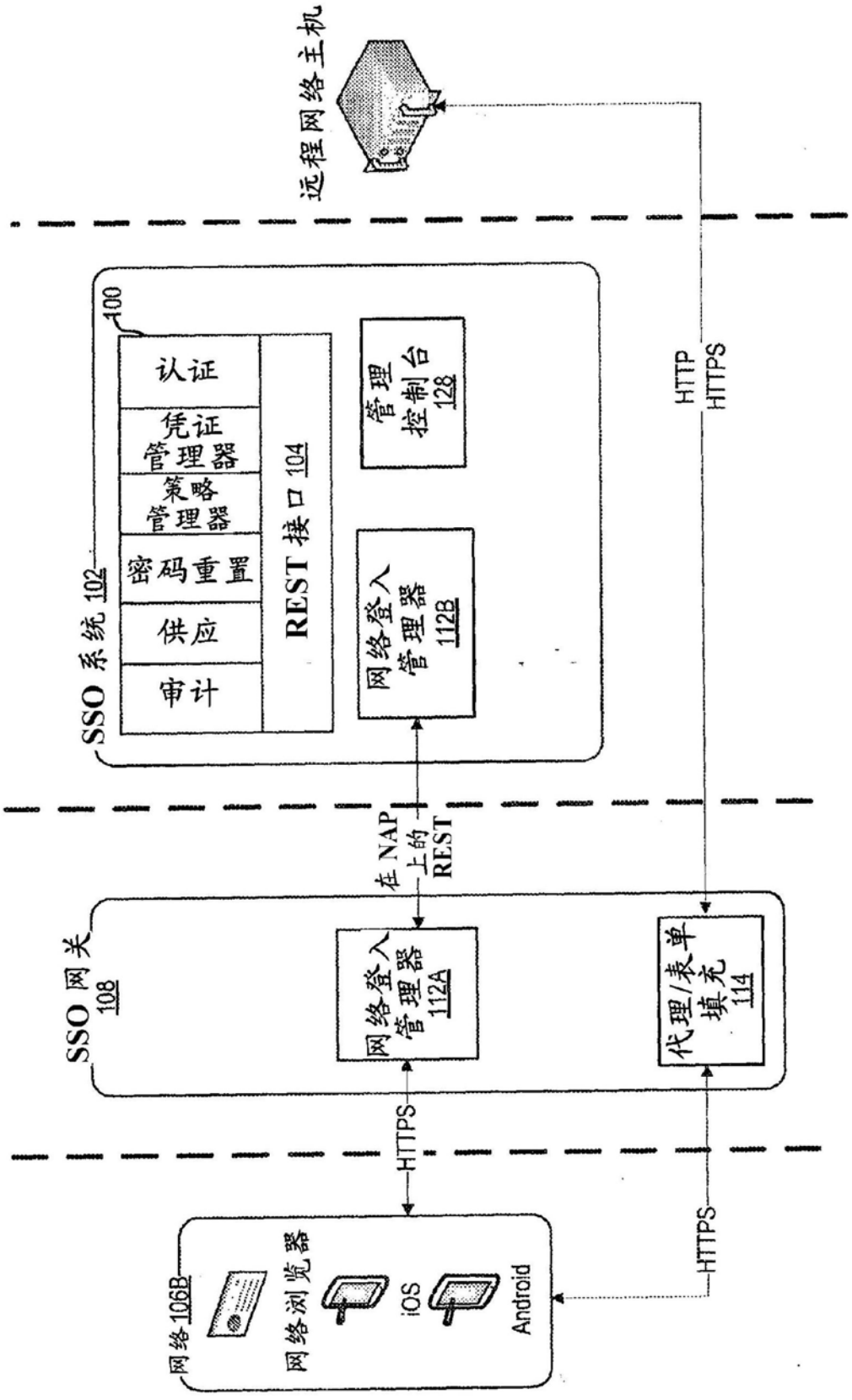

远程网络主机
SSO 系统 102
100
认证
凭证管理器
策略管理器
密码重置
供应
审计
REST 接口 104
管理控制台 128
网络登入管理器 112B
HTTP
HTTPS
在 NAP 上的 REST
SSO 网关 108
网络登入管理器 112A
代理/表单填充 114
HTTPS
HTTPS
网络 106B
网络浏览器
iOS
Android

图8

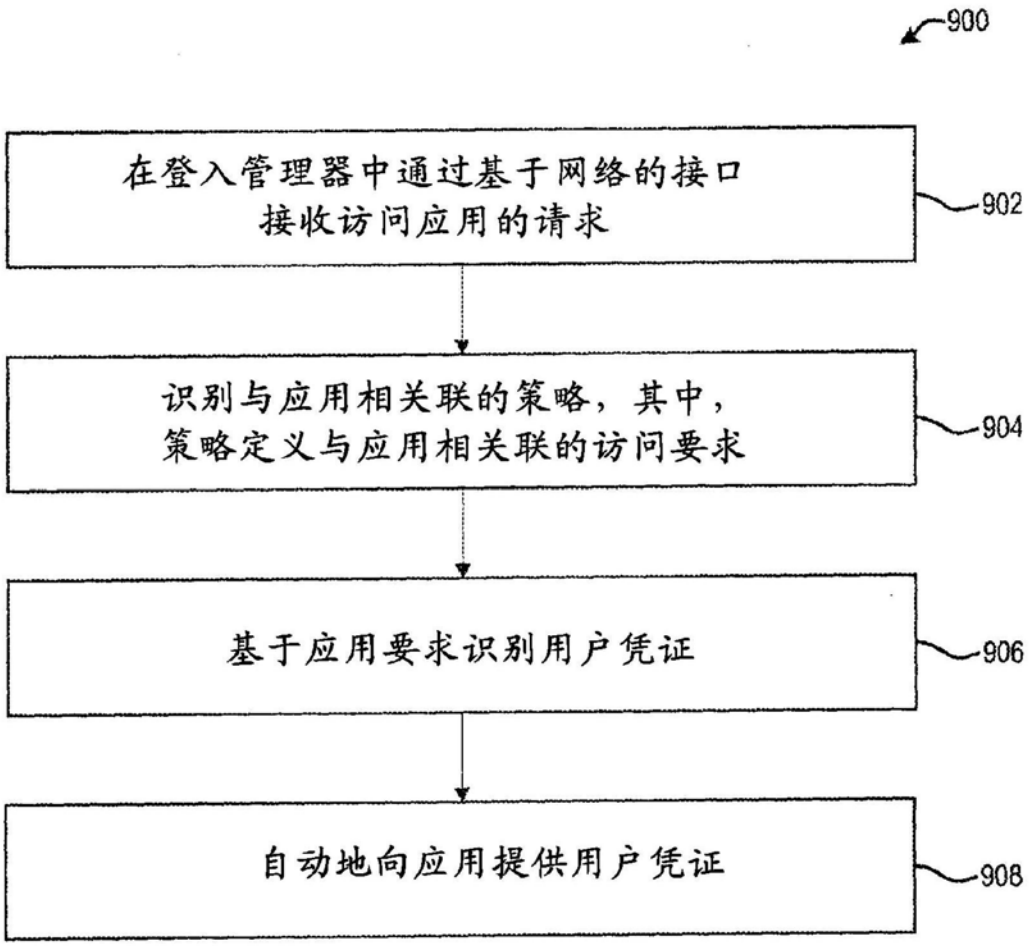

900
在登入管理器中通过基于网络的接口
接收访问应用的请求
902
识别与应用相关联的策略，其中，
策略定义与应用相关联的访问要求
904
基于应用要求识别用户凭证
906
自动地向应用提供用户凭证
908

图9

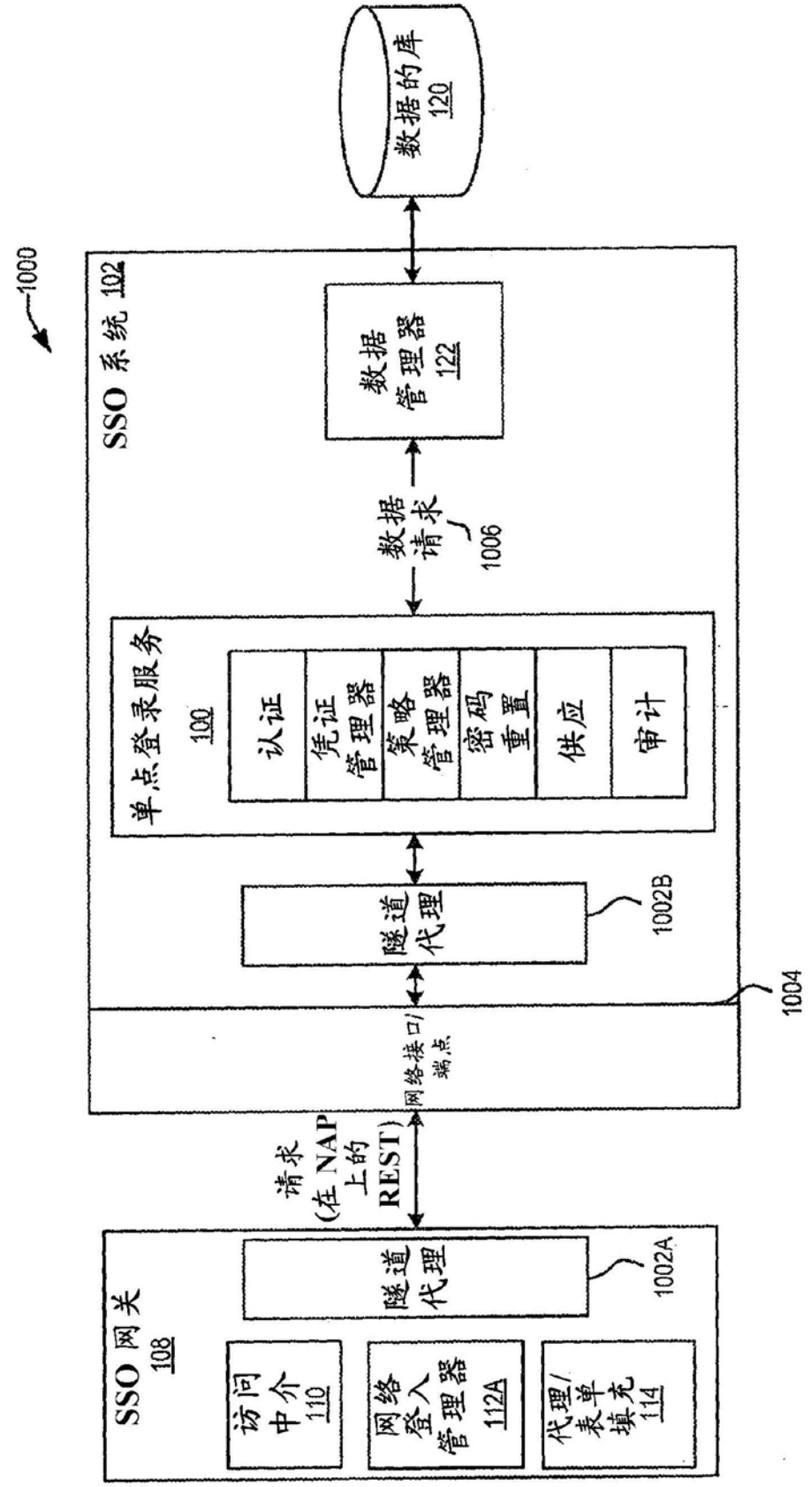

1000
SSO 系统 102
数据的库 120
数据管理器 122
数据请求 1006
单点登录服务 100
认证
凭证管理器
策略管理器
密码重置
供应
审计
隧道代理
1002B
1004
网络接口/端点
请求(在 NAP 上的 REST)
SSO 网关 108
隧道代理
1002A
访问中介 110
网络登入管理器 112A
代理/表单填充 114

图10

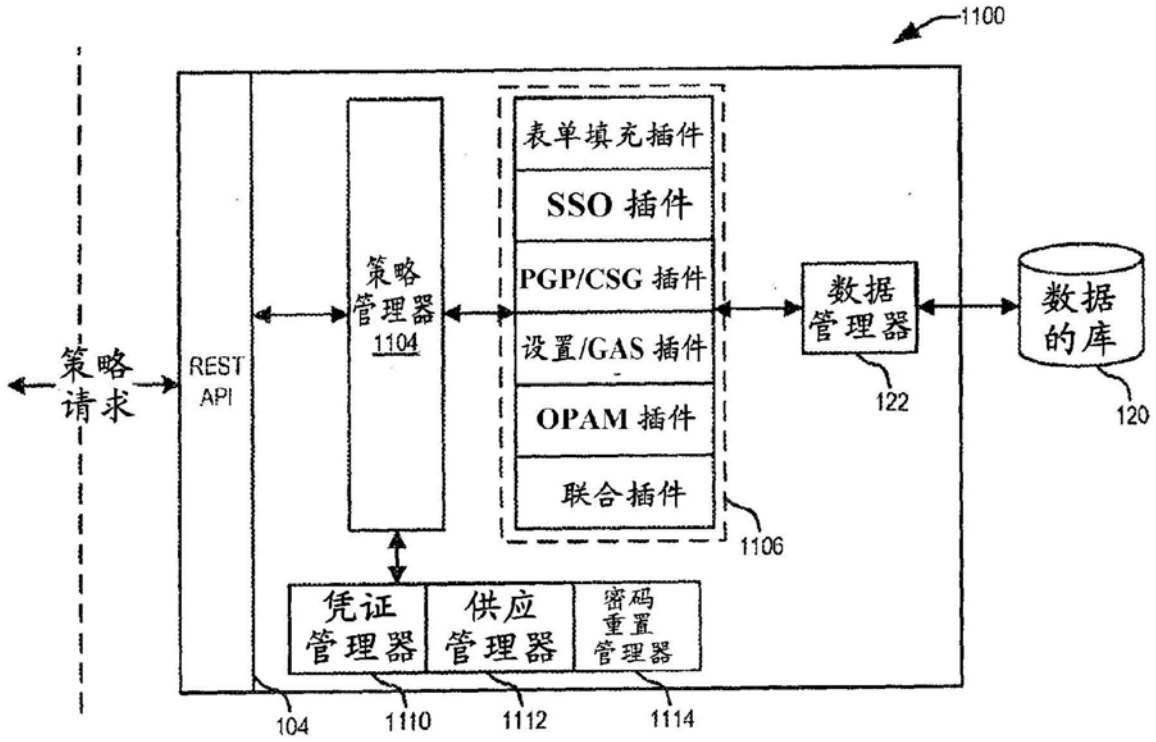

1100
策略请求
REST API
策略管理器 1104
表单填充插件
SSO 插件
PGP/CSG 插件
设置/GAS 插件
OPAM 插件
联合插件
1106
数据管理器
122
数据的库
120
凭证管理器
供应管理器
密码重置管理器
104
1110
1112
1114

图11A

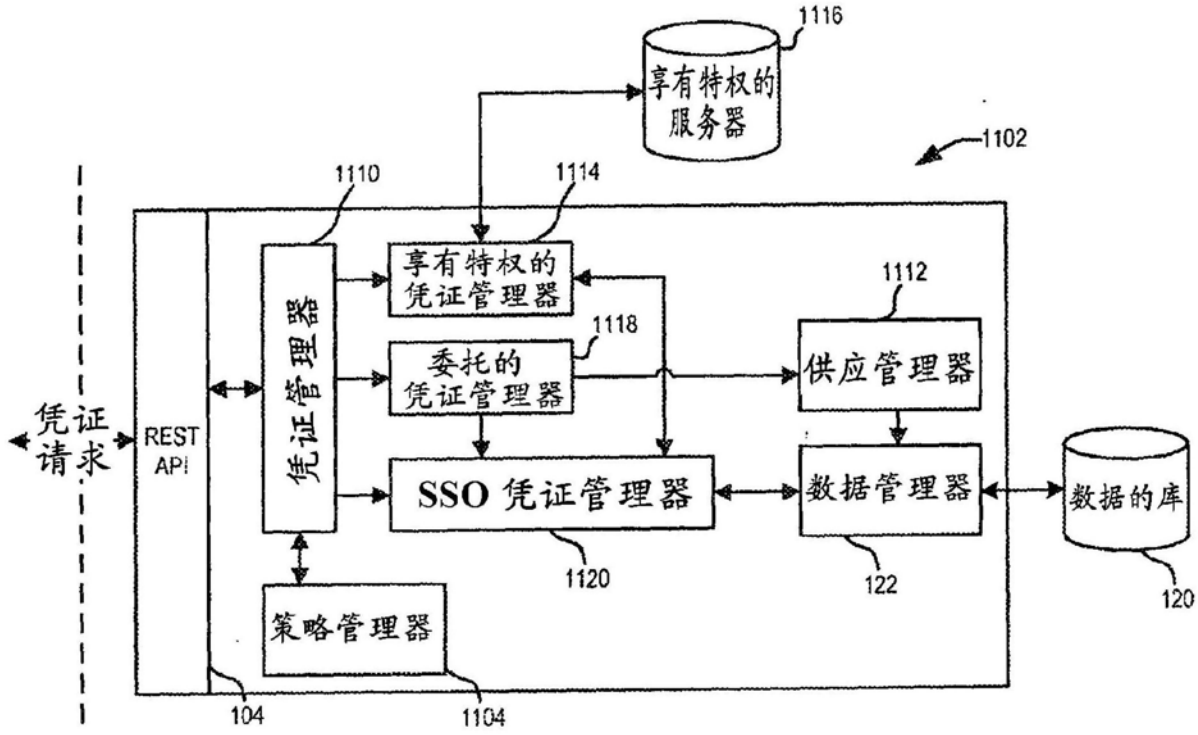

1116
享有特权的服务器
1102
1110
1114
凭证请求
REST API
凭证管理器
享有特权的凭证管理器
委托的凭证管理器
1118
1112
供应管理器
SSO 凭证管理器
1120
数据管理器
122
数据的库
120
策略管理器
104
1104

图11B

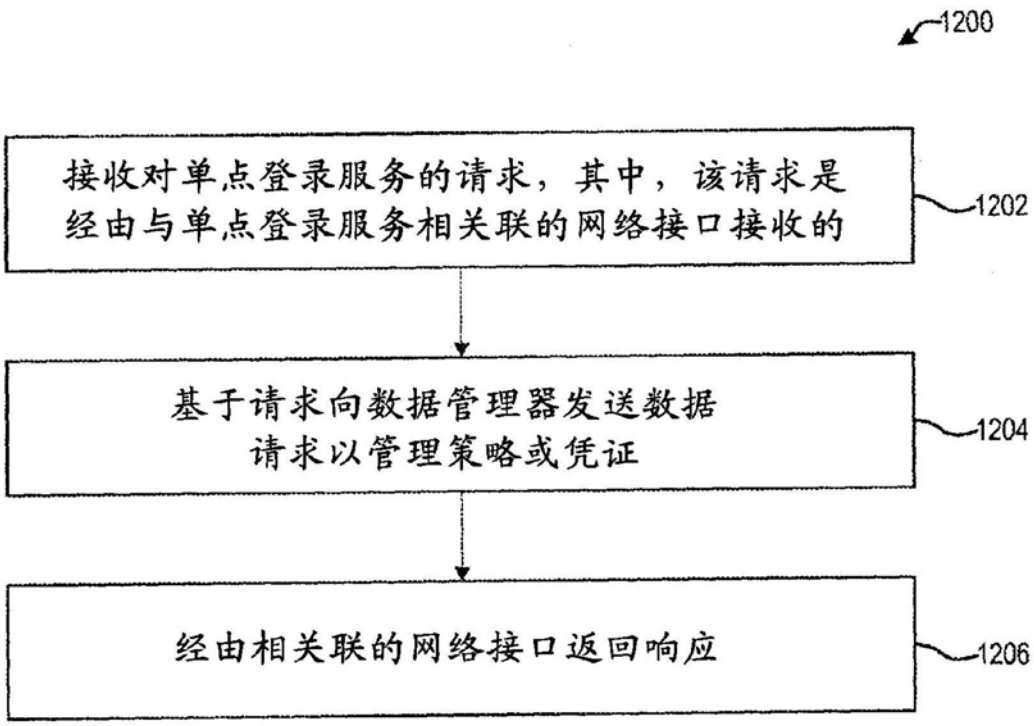

1200
接收对单点登录服务的请求，其中，该请求是经由与单点登录服务相关联的网络接口接收的
1202
基于请求向数据管理器发送数据请求以管理策略或凭证
1204
经由相关联的网络接口返回响应
1206

图12

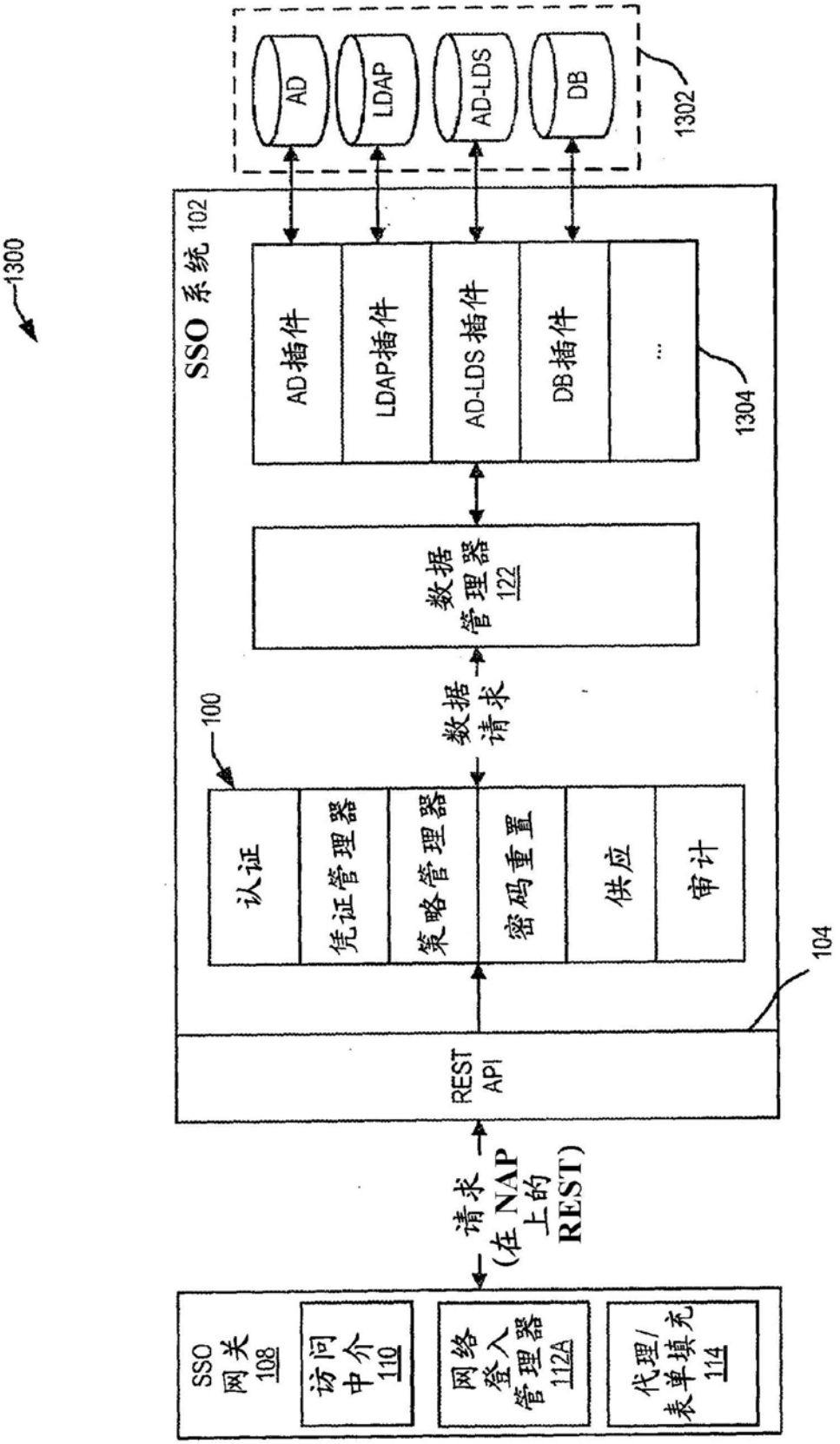

1300
SSO 系统 102
AD
LDAP
AD-LDS
DB
1302
AD插件
LDAP插件
AD-LDS 插件
DB插件
...
1304
数据管理器 122
数据请求
100
认证
凭证管理器
策略管理器
密码重置
供应
审计
104
REST API
请求 (在 NAP 上的 REST)
SSO 网关 108
访问中介 110
网络登入管理器 112A
代理/表单填充 114

图13

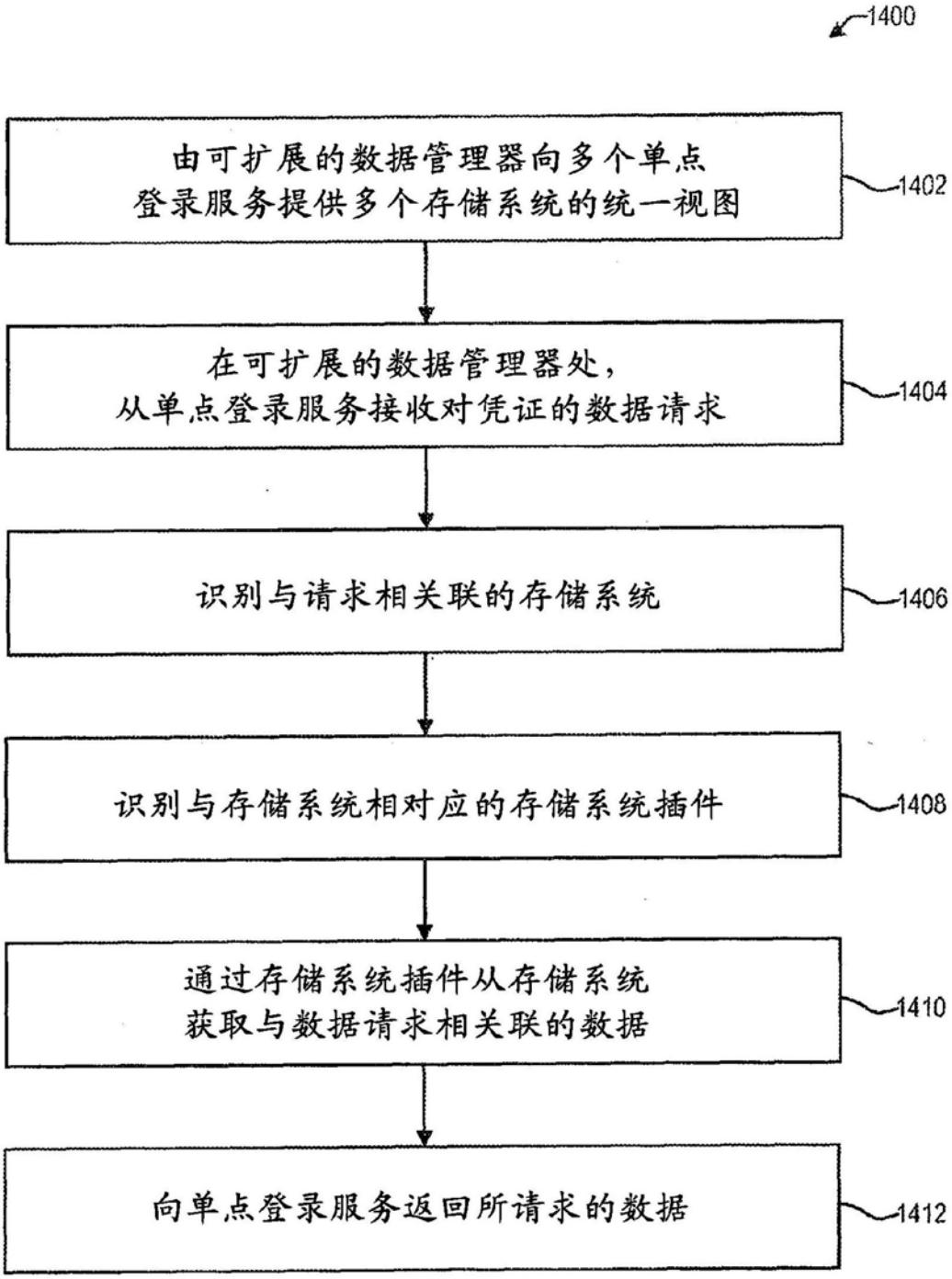

1400
由可扩展的数据管理器向多个单点登录服务提供多个存储系统的统一视图
1402
在可扩展的数据管理器处，从单点登录服务接收对凭证的数据请求
1404
识别与请求相关联的存储系统
1406
识别与存储系统相对应的存储系统插件
1408
通过存储系统插件从存储系统获取与数据请求相关联的数据
1410
向单点登录服务返回所请求的数据
1412

图14

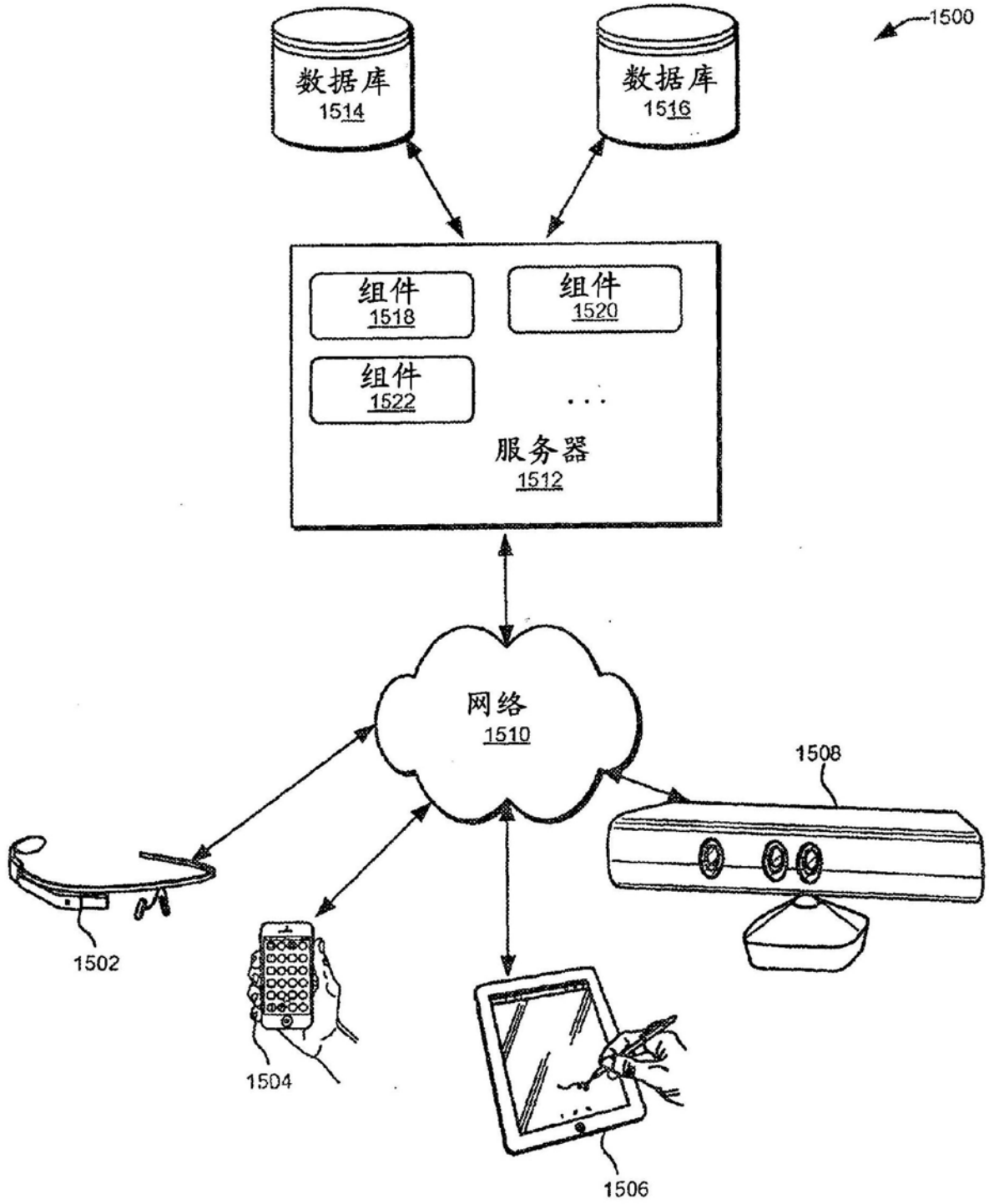

1500
数据库
1514
数据库
1516
组件
1518
组件
1520
组件
1522
...
服务器
1512
网络
1510
1508
1502
1504
1506

图15

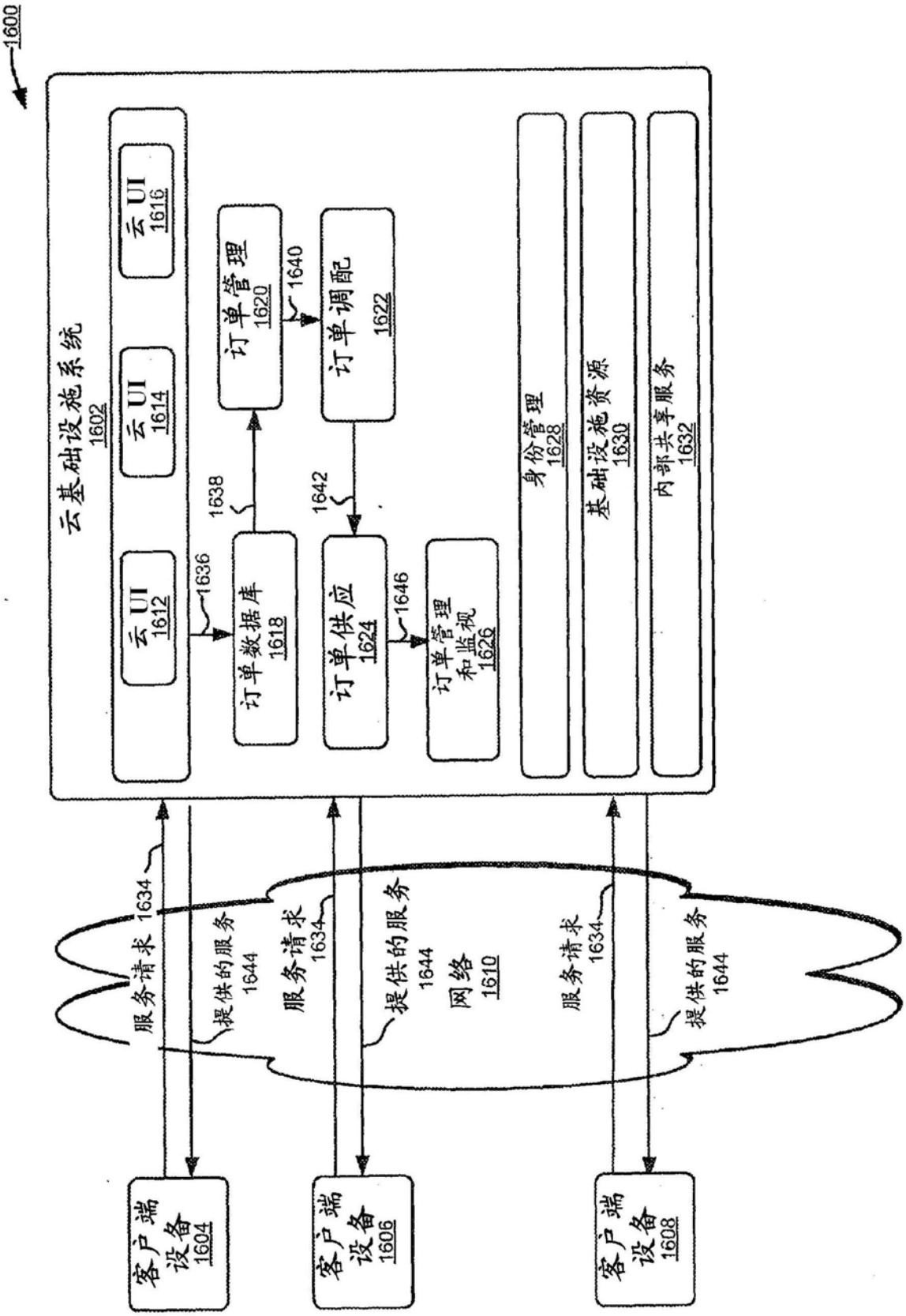

1600
云基础设施系统
1602
云 UI
1612
云 UI
1614
云 UI
1616
订单数据库
1618
订单管理
1620
订单调配
1622
订单供应
1624
订单管理和监视
1626
身份管理
1628
基础设施资源
1630
内部共享服务
1632
1636
1638
1640
1642
1646
服务请求
1634
提供的服务
1644
网络
1610
客户端设备
1604
客户端设备
1606
客户端设备
1608

图16

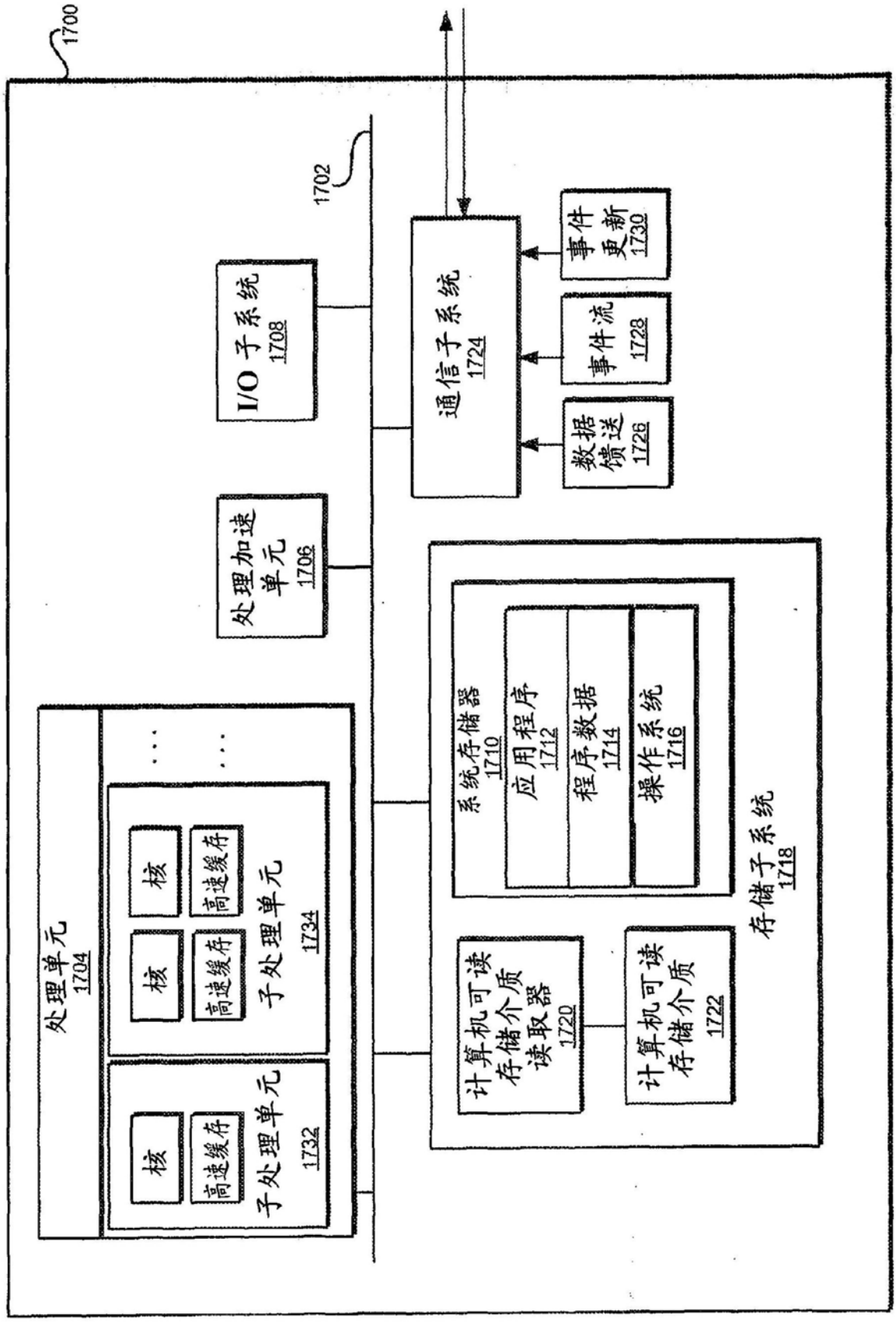

1700
1702
处理单元
1704
核
高速缓存
核
高速缓存
子处理单元
1732
核
高速缓存
核
高速缓存
子处理单元
1734
I/O 子系统
1708
处理加速单元
1706
通信子系统
1724
事件更新
1730
事件流
1728
数据馈送
1726
存储子系统
1718
系统存储器
1710
应用程序
1712
程序数据
1714
操作系统
1716
计算机可读存储介质读取器
1720
计算机可读存储介质
1722

图17