(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 106105090 B
(45)授权公告日 2019.10.22

(21)申请号 201480077216.6

(22)申请日 2014.12.27

(65)同一申请的已公布的文献号
申请公布号 CN 106105090 A

(43)申请公布日 2016.11.09

(30)优先权数据
61/979,289 2014.04.14 US

(85)PCT国际申请进入国家阶段日
2016.09.14

(86)PCT国际申请的申请数据
PCT/US2014/072454 2014.12.27

(87)PCT国际申请的公布数据
WO2015/160389 EN 2015.10.22

(73)专利权人 迈克菲股份有限公司
地址 美国加利福尼亚州

(72)发明人 G·怀特赛德 R·布鲁诺
R·赖纳

(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 张欣

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 9/32(2006.01)

(56)对比文件
US 2004143669 A1,2004.07.22,
US 2010024015 A1,2010.01.28,
CN 102736916 A,2012.10.17,
US 2006026286 A1,2006.02.02,
US 2010185875 A1,2010.07.22,
CN 1492656 A,2004.04.28,

审查员 于兰

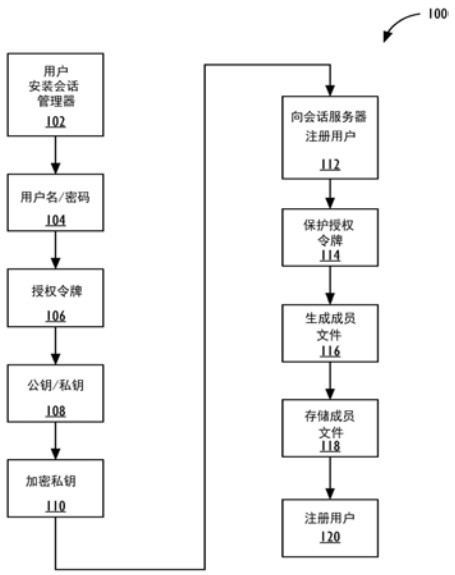
权利要求书2页 说明书18页 附图15页

(54)发明名称

利用会话共享自动登录和登出会话

(57)摘要

一种技术允许在不访问用户凭据的情况下透明地管理、暂停、恢复、共享、限制和迁移在设备上的用户会话。用户可以即时自动登录和登出其在线账户中的每一个或者所有在线账户，并且在这样做时，用户可以在不共享密码的情况下跨客户端设备以及与其他经认证且经授权的用户共享会话。可以采用安全的方式来完成共享，其中，所述发起用户能够限定共享会话权限，并且能够去除对所述共享会话中的每一个共享会话的访问。



CN 106105090 B

1.一种用于恢复和共享会话的方法,所述方法包括:

传输用于在第一设备的网络浏览器上针对与网络域相关联的网页创建第一活动会话的用户信息,其中,所述用户信息包括用户凭据;

访问来自第二设备的共享会话信息,所述共享会话信息使用公钥被加密,以便从所述第一活动会话创建与所述第二设备的锁定的共享会话;

传输登出信息,从而将所述锁定的共享会话转换为终止的会话;

传输对于无需所述用户凭据来取回所述终止的会话的请求;以及

访问会话信息以在所述网络浏览器中注入所述终止的会话,从而创建第二活动会话。

2.如权利要求1所述的方法,进一步包括:

响应于传输所述登出信息而存储与所述锁定的共享会话相关的会话数据;以及

从所述网络浏览器中删除与所述锁定的共享会话相关的会话cookie。

3.如权利要求1所述的方法,其中,所述第一设备包括移动设备。

4.如权利要求1所述的方法,进一步包括将针对所述共享会话的限制传输至第二用户。

5.如权利要求1所述的方法,进一步包括防止在传输对于取回所述终止的会话的所述请求之后传输所述用户凭据,其中,所述用户凭据包括用户的用户名和密码中的至少一者。

6.如权利要求1所述的方法,进一步包括将请求传输至所述网络域以保持所述锁定的共享会话活跃,所述请求为非会话修改请求。

7.如权利要求1所述的方法,进一步包括判定针对与所述网络域相关联的所述网页是否存在之前的会话。

8.如权利要求1所述的方法,进一步包括在第一设备上终止所述锁定的共享会话,并且在所述第二设备上取回所述终止的会话,所述第一设备和所述第二设备与所述用户相关联。

9.一种用于恢复和共享会话的第一设备,所述第一设备包括:

一个或多个处理器;以及

存储器,所述存储器包括指令,所述指令当被执行时使处理器中的一个或多个处理器:

访问用于在所述第一设备的网络浏览器上针对与网络域相关联的网页创建第一活动会话的用户信息,其中,所述用户信息包括用户凭据;

访问来自第二设备的共享会话信息,所述共享会话信息使用公钥被加密,以便从所述第一活动会话创建与所述第二设备的锁定的共享会话;

传输登出信息,从而将所述锁定的共享会话转换为终止的会话;

传输对于无需所述用户凭据来取回所述终止的会话的请求;以及

访问会话信息以在所述网络浏览器中注入所述终止的会话,从而创建第二活动会话。

10.如权利要求9所述的第一设备,其中,所述一个或多个处理器用于:

响应于传输所述登出信息而存储与所述锁定的共享会话相关的会话数据;以及

从所述网络浏览器中删除与所述锁定的共享会话相关的会话cookie。

11.如权利要求9所述的第一设备,其中,所述一个或多个处理器用于传输针对与所述第二设备相关的所述共享会话的限制。

12.如权利要求9所述的第一设备,其中,所述一个或多个处理器用于防止所述用户凭据响应于传输对于取回所述终止的会话的所述请求而被传输,其中,所述用户凭据包括用

户的用户名和密码中的至少一者。

13.如权利要求9所述的第一设备，其中，所述一个或多个处理器用于将请求传输至所述网络域以保持所述锁定的共享会话活跃，所述请求为非会话修改请求。

14.一种机器可读介质，包括指令，所述指令当被执行时使至少一个机器至少执行：

传输用于在第一设备的网络浏览器上针对与网络域相关联的网页创建第一活动会话的用户信息，其中，所述用户信息包括用户凭据；

从第二设备获取共享会话信息，所述共享会话信息使用公钥被加密，以便从所述第一活动会话创建与所述第二设备的锁定的共享会话；

传输登出信息以终止所述锁定的共享会话，从而生成终止的会话，所述终止的会话的指示将在终止之后持续；

传输对于无需所述用户凭据来取回所述终止的会话的请求；以及

获取会话信息以在所述网络浏览器中注入所述终止的会话，从而创建第二活动会话。

15.如权利要求14所述的机器可读介质，其中，所述指令使所述至少一个机器：

响应于传输所述登出信息而存储与所述锁定的共享会话相关的会话数据；以及

从所述网络浏览器中删除与所述锁定的共享会话相关的会话cookie。

16.如权利要求14所述的机器可读介质，其中，所述第一设备包括移动设备。

17.如权利要求14所述的机器可读介质，所述指令使所述至少一个机器将针对所述共享会话的限制传输至所述第二设备。

18.如权利要求14所述的机器可读介质，所述指令使所述至少一个机器防止在传输对于取回所述终止的会话的所述请求之后传输所述用户凭据，其中，所述用户凭据包括用户的用户名和密码中的至少一者。

19.如权利要求14所述的机器可读介质，所述指令使所述至少一个机器将对于以下至少一项的请求传输至所述网络域：(i)保持所述锁定的共享会话活跃；或者(ii)修改所述会话信息以保持所述锁定的共享会话活跃，所述请求为非会话修改请求。

20.如权利要求14所述的机器可读介质，所述指令使所述至少一个机器判定针对与所述网络域相关联的所述网页是否存在之前的会话。

21.如权利要求14所述的机器可读介质，所述指令使所述至少一个机器在所述第一设备上终止所述锁定的共享会话，并且在所述第二设备上取回所述终止的会话，所述第一设备和所述第二设备与用户相关联。

利用会话共享自动登录和登出会话

[0001] 相关申请的交叉引用

[0002] 本申请要求于2014年4月14提交的题为“Transparent management,suspension,restoration,sharing,limiting and migration of user sessions without access to user credentials(在不访问用户凭据的情况下对用户会话进行透明管理、暂停、恢复、共享、限制和迁移)”的美国临时申请序列号61/979,289的优先权,该临时申请以其全部内容通过引用结合在此。

技术领域

[0003] 本发明总体上涉及用于允许用户在不共享密码的情况下跨客户端设备以及与其他经认证且经授权的用户安全地共享会话的方法和过程。

背景技术

[0004] 想要登出应用或网站的用户通常至少需要用户名和密码。并且,用户每个应用可以具有不止一个账户。为了使认证用户访问其应用、网站和数据,他们通常针对其大多数(如果不是全部的话)账户采用基本上类似的手段。并且,如果用户期望与其他设备和/或用户共享会话,那么他们需要通过至少共享相关的用户名和密码来执行这一操作。这导致系统的不安全性以及针对身份欺诈的手段。当今,网站和应用始终坚持在允许用户访问其应用和数据的一部分或另一部分之前使用更强大的用户名和密码以及信息层和交互层。在标准网络连接下,这成为在多个设备上打开一个或多个会话或者在多个用户之间共享会话的阻碍。并且,网站和应用不时地改变其登录方式和过程,以确保只有可信的人类用户才被允许访问。这使得访问和取回(retrieval)安全但却令人失望,不只针对发起用户(所谓的主人),而且对于被允许与主用户以及他的或她的发起设备安全地共享会话的那些设备和第三方用户而言更是如此。

[0005] 一旦正确认证任何设备和/或用户,在保证合法用户可以无缝地访问应用和数据的同时需保护系统免受不希望有的侵入和篡改。已经提出了各种方法和过程来解决这些问题。

[0006] 题为“Systems and methods for cookie proxy jar management across cores in a multi-core system(用于在多核系统中跨多核的cookie代理jar管理的系统和方法)”的美国专利号8,484,287公开了用于由多核设备管理cookie的系统和方法。所述设备在客户端与一个或多个服务器的中间。多核设备的第一核通过用户会话接收来自服务器的针对客户端请求的响应。响应包括cookie。第一核从响应中去除cookie并且针对会话将cookie存储在相应的存储设备中。第一核将不具有cookie的响应转发至客户端。之后,第二核经由会话接收来自客户端的第二请求。第二核从第二请求中将第一核的标识确定为会话的所有者。之后,第二核针对会话将对cookie信息的第三请求传达至第一核。

[0007] 题为“Systems and methods for AAA-traffic management information sharing across cores in a multi-core system(用于在多核系统中跨多核共享AAA流量

管理信息的系统和方法)”的美国专利号8,667,575公开了用于将认证会话信息传播至多核设备的多个核的方法,所述方法包括由在至少一个客户端与服务器中间的设备的第一核上运行的认证虚拟服务器针对用户建立会话,该认证虚拟服务器认证该会话。流量管理虚拟服务器在设备的第二核上运行,并且经由会话接收访问服务器的请求。流量管理虚拟服务器可以响应于判定第二核未存储会话而从会话的标识符中标识第一核建立了会话。第二核可以向第一核发送针对由标识符标识的会话的数据的请求。第二核可以从第一核中接收针对标识会话是否有效的第二请求的响应。

[0008] 题为“Cloud based service logout using cryptographic challenge response(使用加密挑战响应的基于云的服务登出)”的美国专利号8,656,154公开了基于云的服务使用可以通过多个客户端设备同时登录服务。提供了多种基于加密挑战响应的方法、系统和计算机程序产品,以在与用户相关联的一个或多个已登录的客户端设备处高效且安全地同时实现从基于云的服务中登出。当基于云的服务接收有效的登出请求时,与用户相关联的当前密钥无效,并且在某些实例中,被新的密钥代替。在由用户随后尝试使用基于云的服务时,驻留在与用户相关联的任何之前已登录的客户端设备上的一个或多个令牌将不允许对基于云的服务的使用,直至用户有效地登录到基于云的服务中并且在每一个客户端设备处基于新的密钥接收一个或多个新的令牌。

[0009] 题为“Authenticating an auxiliary device from a portable electronic device(由便携式电子设备认证辅助设备)”的美国专利号8,578,461公开了一种用于利用在便携式电子设备上运行的网络服务来认证在辅助设备上运行的浏览器的方法。所述方法包括接收来自浏览器的资源请求,判定请求是否标识所保护的资源,以及基于请求是否标识所保护的资源来选择性地认证请求。

[0010] 题为“Systems and methods for configuration driven rewrite of SSL VPN clientless sessions(用于对SSL VPN无客户端会话进行配置驱动重写的系统和方法)”的美国专利号8,667,146公开了企业为各种各样的客户端提供服务以使客户端能够在将请求和响应转发至预期目的地之前通过修改接收到的URL以及来自于服务器的针对客户端请求的响应的URL来使用由企业提供的资源,的解决方案。中介可以标识针对经由无客户端SSL VPN会话访问服务器的客户端请求的访问设定档。中介可以使用访问设定档的一个或多个正则表达式响应于所述请求在由所述服务器服务的内容上检测一个或多个URL。中介可以根据由访问设定档的一个或多个重写策略指定的URL变换响应于检测而重写或修改所检测的一个或多个URL。可以将具有修改的URL的响应转发至客户端。

[0011] 题为“Methods and apparatus for browsing using alternative linkbases(用于使用替代链接库来进行浏览的方法和装置)”的美国专利号8,661,495公开了用于使用多个协调的输入/输出设备集来导航超媒体的系统和方法。所公开的系统和方法允许用户和/或程序设计者控制在哪个设备集(不管其是否被整合)上呈现什么资源,并且提供协调浏览活动以使得能够跨多个独立系统采用此类用户界面。所公开的系统和方法还支持超媒体浏览以及相关的商业活动的新且丰富的方面和应用。

[0012] 然而,存在对在不访问用户凭据的情况下在设备上透明地管理、暂停、恢复、共享、限制和迁移用户会话的方法和过程的需要。

附图说明

[0013] 图1是流程图，展示了根据至少一个实施例的应用安装和用户注册会话。

[0014] 图2A是流程图，展示了根据至少一个实施例的不具有虚拟专用网络的认证会话。

[0015] 图2B是流程图，展示了根据至少一个实施例的通过虚拟专用网络的认证会话。

[0016] 图3A是流程图，展示了根据至少一个实施例的不具有虚拟专用网络的登出会话。

[0017] 图3B是流程图，展示了根据至少一个实施例的通过虚拟专用网络的登出会话。

[0018] 图4A是根据至少一个实施例的具有活动虚拟专用网络的登录/登出会话的流程图。

[0019] 图4B是流程图，展示了根据至少一个实施例的不具有活动虚拟专用网络的登录/登出会话。

[0020] 图5是流程图，展示了根据至少一个实施例的共享会话的发起。

[0021] 图6是流程图，展示了根据至少一个实施例的虚拟专用网络功能。

[0022] 图7A是流程图，展示了根据至少一个实施例的接收具有活动虚拟专用网络的共享会话。

[0023] 图7B是流程图，展示了根据至少一个实施例的接收不具有活动虚拟专用网络的共享会话。

[0024] 图8是流程图，展示了根据至少一个实施例的具有主用户的活动会话管理的运作。

[0025] 图9是图示，展示了根据一个实施例的与本文中所描述的技术一起使用的计算设备。

[0026] 图10是框图，展示了根据另一个实施例的与本文中所描述的技术一起使用的计算设备。

[0027] 图11是图示，展示了根据一个实施例的可编程设备的网络。

具体实施方式

[0028] 在接下来的描述中，出于解释的目的，许多特定细节被阐述以便提供对本发明的详尽理解。然而，将明显的是，对本领域技术人员而言，可以在没有这些具体细节的情况下实践本发明。在其他情况下，为了避免模糊本发明，结构和设备以框图形式表示。对不带下标或后缀的数字的引用被理解为引用对应于该被引用数字的所有带下标和后缀的实例。此外，本公开中使用的语言主要是为了可读性和指导的目的而被原理性选择的，并且可能未被选择为描绘或限制创造性主题，有必要借助权利要求来确定这样的创造性主题。在说明书中提及“一个实施例”或者“实施例”意味着结合实施例所描述的特定特征、结构或特性被包含在本发明的至少一个实施例中，并且多次提及“一个实施例”或“实施例”不应当被理解为一定都是指相同的实施例。

[0029] 在至少一个实施例中，本发明可以提供用于在不访问用户的登录凭据的情况下在设备上透明地管理、暂停、恢复、共享、限制和迁移用户会话的多种方法和过程。用户可以共享会话并且向经授权的用户提供只读访问。其他实施例可以包括延长活跃会话的寿命。

[0030] 如在此所使用的，术语“计算机系统”可指用于执行被描述为在计算机系统上或由计算机系统执行的功能的单台计算机或一起工作的多台计算机。

[0031] 如在此所使用的，术语“可编程设备”可以指用于执行被描述为在可编程设备上或

由可编程设备执行的功能的单台可编程设备或一起工作的多台可编程设备。类似地，“机器可读介质”可以指可以一起存储被描述为存储在机器可读介质上的材料的单个物理介质或多个介质。

[0032] 如在此所使用的，术语“会话”可以指可以在用户的浏览器与运行在远程服务器上的特定网络服务之间共享的数据，在某些实施例中，应每一个请求而传递所述数据。除了将易于被技术人员所理解的其他安排之外，可以在浏览器或者任何其他可用本地存储设备上将会话存储为cookie。

[0033] 如在此所使用的，术语“凭据”可以指可专供某一用户用于在网络上使用特定服务进行认证的数据。这些凭据可以包括但不限于用户名和密码。

[0034] 如在此所使用的，术语“会话管理器”可以指在用户的设备上运行的服务，所述服务可以允许用户使会话数据与会话服务器同步，并且与用户的浏览器进行通信以暂停和恢复会话。

[0035] 如在此所使用的，术语“虚拟专用网络”(VPN)可以指跨公共网络(如互联网)延伸专用网络。除了将易于被技术人员所理解的其他专用网络特征之外，在从专用网络的功能、安全和管理策略中获益的同时，虚拟专用网络可以使计算机能够跨共享或公用的网络发送和接收数据，就如同被直接连接至专用网络一样。除了将易于被技术人员所理解的其他安排之外，可以通过使用例如专用连接、虚拟隧道协议或者流量加密来建立虚拟点对点连接，从而创建VPN。

[0036] 如在此所使用的，术语“VPN客户端”可以指在用户设备上运行的服务，所述用户设备可以允许用户访问VPN。

[0037] 如在此所使用的，术语“主密码(MP)”可以指用户提供的密码，该用户提供的密码可用于使用例如会话管理器、VPN客户端和VPN进行认证。将主密码与用户名和推衍机制组合以产生认证信息。

[0038] 如在此所使用的，术语“授权令牌”可以指主密码的衍生版本，该主密码的衍生版本可用于验证用户的真实性并且用于解密用户数据。可以将授权令牌从用户设备传输至会话服务器，并且可以针对那个特定用户将其与存储在会话服务器上的真实性令牌的版本进行比较。

[0039] 如在此所使用的，术语“加密密钥”可以指密码算法，所述密码算法可以需要两个单独的密钥，其中一个密钥可以是秘密的(或者私有的)而另一个密钥可以是公共的(公钥/私钥对)。尽管这个密钥对的两个部分是不同的，但是它们被算术地联接。

[0040] 如在此所使用的，术语“公钥”可以指可用于加密明文或者用于验证数字签名的密钥。

[0041] 如在此所使用的，术语“私钥”可以指可用于解密密文或者用于创建数字签名的密钥。

[0042] 如在此所使用的，术语“会话服务器”可以指用于跨设备和用户同步会话数据的集中式存储设备。在至少一个实施例中，会话服务器可以提供对用户的经加密的会话数据的访问。

[0043] 如在此所使用的，术语“会话服务器应用编程接口(API)”可以指会话管理器和用于远程认证用户并同步经加密的会话数据的VPN客户端的编程接口。会话服务器应用编程

接口还为会话管理器和VPN客户端提供一种用于取回(retrieve)用户的公钥以共享会话数据的方式。

[0044] 如在此所使用的,术语“成员文件”可以指可以与特定用户相关联的并且存储在会话服务器上的数据。此成员文件可以包括(但不限于)用户名、认证令牌、经加密的私钥和公钥。

[0045] 如在此所使用的,术语“认证信息”在至少一个实施例中可以指用于使用会话管理器、VPN客户端和VPN来认证用户的用户名与主密码的衍生版本的组合。

[0046] 如在此所使用的,术语“会话数据”可以指与用户的会话相关的数据的集合。当位于用户的设备上并且位于VPN上时,这些会话数据可以采用明文非加密的形式。当与会话服务器同步时,这些会话数据可以采用加密的形式。

[0047] 如在此所使用的,术语“经加密的用户数据”可以指可以使用授权令牌来进行经加密的用户的会话数据

[0048] 如在此所使用的,术语“经加密的私钥”可以指可用于解密与用户共享的会话的用户的经加密的私钥。经加密的私钥可以以经加密的状态存储在会话服务器上,并且可以使用授权令牌在用户设备上被解密。

[0049] 如在此所使用的,术语“cookie”可以指在用户浏览网站时可以从该网站发送并且存储在用户的网络浏览器中的小数据片。cookie也被称为超文本传输协议(“HTTP”)cookie、网络cookie或者浏览器cookie。在某些实施例中,当用户加载网站时,浏览器将cookie发回至服务器以将用户之前的活动告知网站。

[0050] 如在此所使用的,术语“浏览器存储设备”可以指作为用于将数据存储在网络浏览器中的网络应用软件方法和协议的网络存储设备和/或DOM(文档对象模型)存储设备。网络存储设备支持永久性数据存储,类似于cookie,但具有大大增强的容量并且没有信息存储在HTTP请求报头中。存在两种主要的网络存储设备类型:本地存储设备和会话存储设备,分别表现得与永久性cookie和会话cookie类似。

[0051] 如在此所使用的,术语“会话共享”可以指以下事实:设想用户可以通过使用接收的用户的公钥来加密一个或多个会话从而与其他用户共享该一个或多个会话。可以通过会话服务器同步共享会话。

[0052] 如在此所使用的,术语“共享限制”可以指以下事实:设想用户可以对第一用户与第二用户共享的会话施加限制。可以逐会话地施加这些限制,并且限制了接收器修改共享会话的状态的能力。

[0053] 如在此所使用的,术语“共享会话数据”可以指可以从另一个用户接收的会话数据。共享会话数据可以处于两种状态:锁定状态或解锁状态(见下文)。

[0054] 如在此所使用的,术语“锁定的共享会话数据”在至少一个实施例中可以指不能由接收器查看或者修改的共享会话数据。在至少一个实施例中,接收器可以使用VPN来使用此数据。

[0055] 如在此所使用的,术语“解锁的共享会话数据”在至少一个实施例中可以指可以由激发的接收器查看或者修改的共享会话数据。在至少一个实施例中,接收器可以使用会话管理器或者VPN来使用此数据。

[0056] 如在此所使用的,术语“输入过滤器”可以指可由VPN应用于传入请求以限制关于

共享会话的某些类型的HTTP请求的过滤器。例如，可以限制共享会话，以便不允许接收器登出会话。在此情况下，发布(POST)至/登出可以被过滤并且不被允许。

[0057] 如在此所使用的，术语“输出过滤器”可以指可由VPN和会话管理器应用于共享会话上的HTTP响应以限制将某一超文本标记语言(“HTML”)内容显示给用户的过滤器。例如，输出过滤器可以从返回的HTML内容中去除“登出”按钮，或者隐藏将允许共享会话的接收器修改会话状态的链接。

[0058] 如在此所使用的，术语“没有限制”可以指当没有限制地共享会话时，没有输入或输出过滤器被应用于传入请求和传出响应。

[0059] 如在此所使用的，术语“安全套接层(SSL)”可以指可以从被称为SSL握手(SSL Handshake)的消息交换开始的安全套接层(“SSL”)会话。握手允许服务器通过使用公钥技术来向客户端认证其自身，并且然后允许客户端和服务器协作创建用于在之后的会话过程中进行快速加密、解密和篡改检测的对称密钥。可选地，握手还允许客户端向服务器认证其自身。

[0060] 如在此所使用的，术语“文档对象模型(DOM)”可以指用于代表在HTML、可扩展超文本标记语言(“XHTML”)和可扩展标记语言(“XML”)文档中的对象并与其进行交互的跨平台且与语言无关的约定。可以通过使用关于DOM树中的对象的方法来对所述对象进行寻址和操纵。

[0061] 如将易于被技术人员所理解的，可以通过任何已知的手段来完成在此讨论的所有加密和解密。

[0062] 技术允许在不访问用户凭据的情况下在设备上透明地管理、暂停、恢复、共享、限制和迁移用户会话。用户可以即时自动登录和登出其在线账户中的每一个或者所有在线账户，并且在这样做时，用户可以在不共享密码的情况下跨客户端设备以及与其他经认证且经授权的用户共享会话。通过所述发起用户能够限定共享会话权限以及能够去除对所述共享会话中的每一个共享会话的访问，可以采用安全的方式完成共享。技术效果包括在不访问用户凭据的情况下可以使用户登录保存、恢复或保持活跃于网站中持续一段延长的时间的系统。

[0063] 现在转到图1，在过程100中展示了本发明的一个实施例，其中，可以将应用存储在如例如图11的移动设备1114的用户设备上，并且用户可以被注册。在102中，根据一个实施例，用户可以将会话管理器安装在用户客户端设备1114(图11)上作为独立式应用或者与至少一个其他第三方应用捆绑(除了将易于被技术人员所理解的其他安排之外)。可替代地，在其他实施例中，用户可以将虚拟专用网络(“VPN”)客户端(或者会话管理器VPN客户端)安装在客户端设备1114(图11)上。

[0064] 在104中，除了将易于被技术人员所理解的其他登录信息之外，然后可以提示客户端设备1114(图11)的用户提供例如用户名和主密码(“MP”)。

[0065] 在106中，然后可以基于从用户接收此登录信息生成授权令牌。

[0066] 在108中，在一个实施例中，可以生成公共加密密钥和私有加密密钥。

[0067] 在110中，可以对生成的私钥进行加密。

[0068] 在112中，客户端设备1114(图11)的用户可以通过会话服务器的应用编程接口(API)经由如例如网络1102(图11)的网络将授权令牌和公钥发送至远程会话服务器(例如，

服务器1104(图11))来注册到会话服务器中。在会话服务器收到登录信息时,用户可以被注册。

[0069] 在114中,在一个实施例中,会话服务器可以使用基于密码的密钥衍生功能(如,例如,scrypt)来在算法上保护授权令牌。进一步地,在一个实施例中,会话服务器可以删除从客户端设备1114(图11)接收到的未受保护的授权令牌的任何副本。

[0070] 在116中,除了将易于被技术人员所理解的其他用户信息之外,可以生成由以下各项组成的成员文件:如但不限于,用户名、算法上受保护的授权令牌、公钥以及经加密的私钥。

[0071] 在118中,除了易于被技术人员所理解的其他类似的位置之外,然后可以采用安全或不安全的方式将成员文件存储在会话服务器上。在120中,与客户端设备1114(图11)相关联的用户现在可以响应于成员文件的创建进行注册。虽然图1是参照图11的设备1114进行描述的,但是任何其他设备也被设想与过程100一起使用,包括设备1106、1110或1112(如图11所示)。

[0072] 现在转到图2A,展示了本发明的一个实施例,其中,在没有VPN的情况下发生对用户的认证。在204中,除了将易于被技术人员所理解的其他类型的认证信息之外,用户可以经由安装在客户端设备1114(图11)上的会话管理器202提交用户的认证信息,如但不限于用户名和主密码(MP)。在206中,此输入的认证信息可以连同对于技术人员而言将非常明显的任何其他适当的多条信息一起用于生成授权令牌。在208中,授权令牌可用于使用会话服务器210来认证会话。在一个实施例中,用户名可以连同授权令牌一起用于通过会话服务器API对在会话服务器210上的用户进行认证。

[0073] 在212中,会话服务器210接收来自会话管理器202的授权令牌以进行比较。在214中,会话服务器210判定从会话管理器202接收的授权令牌是否与存储在成员文件(在图1的步骤118中所讨论的)中的在算法上受保护的授权令牌相匹配。如下讨论的,如果接收的授权令牌与会话服务器210中的在算法上受保护的授权令牌相匹配(即,步骤214=“是”),那么,在220中,用户被认证并且可以接收经加密的私钥以进行解密。替代地,如果接收的授权令牌与存储在成员文件中的在算法上受保护的授权令牌不匹配(即,步骤214=“否”),那么,在218中,可以经由会话管理器202或者在客户端设备1114(图11)上的其他用户接口将指示用户未被授权和/或凭据错误的消息返回至用户。以类似的方式,针对此认证判定步骤,可以将在认证会话中的任何接收到的信息与存储在成员文件中的信息进行比较。

[0074] 在220中,如果用户被认证,那么可以从相应的成员文件中取回用户信息,如,但不限于,公钥和经加密的私钥。可以对客户端设备1114(图11)上的经加密的私钥和客户端设备1114(图11)上的经加密的私钥进行解密。

[0075] 在222中,可以从会话服务器210中取回会话数据。在示例中,可以由会话管理器202通过会话服务器API向会话服务器210做出与用户名相关联的请求来做出来自于会话服务器210的针对会话数据的请求。如随后将关于以下描绘的图5所讨论的,会话服务器210可以响应于这个请求而返回例如经加密的用户数据和任何经加密的解锁的共享会话。

[0076] 在226中,可以接收经加密的用户数据并且使用授权令牌对其进行解密。以类似的方式,在228中,可以使用用户的私钥对经加密的共享会话进行解密。在230中,用户自己的会话数据以及与用户共享的会话数据可供会话管理器202使用。

[0077] 现在转到图2B,展示了本发明的一个实施例,其中,通过VPN发生认证。在236中,除了将易于被技术人员所理解的其他类型的认证信息之外,用户可以通过VPN客户端232提交认证信息(如但不限于用户名和主密码(MP))。在238中,此输入的认证信息可以连同对于技术人员而言将非常明显的任何其他适当的多条信息(如,但不限于,个人信息)一起用于生成授权令牌。在240中,生成的授权令牌可用于使用会话服务器210认证会话。在实施例中,用户名和授权令牌可用于通过会话服务器API对在会话服务器210上的用户进行认证。

[0078] 在246中,可以接收授权令牌并且将其存储在会话服务器210中。在248中,会话服务器210可以在实施例中判定接收的授权令牌是否与存储在成员文件(如在图1的步骤118中所示和描述的)中的在算法上受保护的授权令牌匹配。如果令牌匹配(即,步骤248=“是”),那么,在252中,可以根据从会话服务器210中取回的信息对在客户端设备上的私钥进行解密。在实施例中,可以从相应的成员文件中安全地取回来自于会话服务器210的信息(如,但不限于,公钥和经加密的私钥)。并且,可以使用授权令牌对取回的经加密的私钥进行解密。

[0079] 但是,如果接收的授权令牌与存储在成员文件中的在算法上受保护的授权令牌不匹配(即,步骤248=“否”),那么,在250中,可以将指示由于用户凭据错误所以用户未被授权的消息返回至用户。在实施例中,针对此认证判定步骤248,可以将在认证会话中的任何接收到的信息与存储在成员文件中的信息进行比较。

[0080] 接下来,在254中,如以下在图5处进一步详细讨论的,可以经由VPN客户端232从会话服务器210中取回未锁定和锁定的共享会话两者。在实施例中,在通过会话服务器API向会话服务器210提交共享会话数据请求时发生取回。可以取回请求的数据并将其发送至VPN客户端232,所述请求的数据在某些非限制性示例中可以包括经加密的锁定的共享会话数据和经加密的解锁的共享会话数据。在258中,可以使用经解密的私钥对此加密的共享会话数据进行解密,以产生经经解密的锁定的会话数据和经解密的解锁的会话数据。应当理解的是,如将在图5处进一步详细讨论的,仍然可以使用会话管理器202(图2A)的公钥对经解密的锁定的会话数据进行加密。

[0081] 在260中,可以使用VPN 234进行VPN客户端232认证,所述认证可以包括向VPN API发送除了将易于被技术人员所理解的其他认证数据之外的认证信息(如,但不限于,与授权令牌相关的信息、用户名和经解密的解锁的会话数据)。在264中,可以使用授权令牌对用户数据进行解密。进一步地,在266中,可以使用会话管理器公钥对经解密的锁定的共享会话数据进行解密。在268中,会话数据现在可供VPN 234使用并且VPN 234现在准备好接收请求。

[0082] 现在转到图3A,展示了本发明的实施例,其中,可以在没有VPN的情况下登出会话。如果用户未使用VPN,会话管理器202可以发起登出304。在实施例中,会话管理器202可以请求从用户浏览器302中读取会话数据306并且可以对此取回的会话数据进行加密以形成经加密的会话数据310。在实施例中,可以使用授权令牌对此会话数据306进行加密以创建经加密的用户数据310(或者经加密的会话数据310)。在一个实施例中,可以将此经加密的用户数据310传达至会话服务器210用于存储。除了将易于被理解的其他安排之外,存储设备可以被配置成将易于被技术人员所理解的任何适当的数据存储安排,包括远程存储设备、本地存储设备、安全存储设备、不安全存储设备和易失性存储设备。

[0083] 接下来，可以清除314浏览器302的会话数据，该清除在一个实施例中可以涉及删除来自浏览器302的存储设备的的cookie。然后可以通过将登出命令发送至会话服务器210来开始从会话服务器316中登出。在框318中，用户现在可以成功地登出在浏览器302上的会话。

[0084] 现在转到图3B，展示了本发明的一个实施例，其中，可以在具有VPN的情况下执行登出会话。如果VPN客户端232的用户正在使用VPN 234，那么用户可以发起从VPN 234中登出340。可以通过发起从VPN客户端232到VPN API 344的登出请求343来进行从VPN 342登出。从这里，可以从存储器346中清除所有会话数据，除了将易于被认识到的其他安排之外，所述存储器在实施例中可以是安全或者不安全的易失性存储器或永久性存储器。用户的状态可以被设置为登出。一旦用户的状态改变并且会话数据被清除，用户登出348就成功了。

[0085] 现在转到图4A，展示了本发明的一个实施例，其中，通过活动VPN 234执行登录/登出会话。如在以上关于图2B所讨论的，在通过会话浏览器302的会话之前，用户登出410并且可以通过VPN 402进行认证。用户使用VPN客户端232来登录412。在浏览器302上，会话可以是不存在的404。并且，在VPN 234的存储器中可以存在414之前的会话。可以发起会话(当用户使用浏览器302访问网页406时)。可以将请求407发送至作为VPN 408的代理的VPN 234并且VPN客户端232可以检查在网页服务器417上的会话416以判定与相同的域名相关联的之前的会话是否存在(如在图6处进一步详细讨论的)。如果合适的会话存在，则可以通过VPN 234将作为代理响应418的响应415发送回至作为VPN 408响应的代理的浏览器302。

[0086] 在一个实施例中，在框408中，可以由VPN的代理通过VPN 234发送请求407，并且VPN 234可以检查以查看与相同的网页相关联的之前的会话是否存在414。如果合适的会话存在，则可以将此会话添加至请求407从而有效地启动请求407上的会话。在实施例中，如以下将在图6中进一步讨论的，然后可以由VPN客户端232将请求407正常地代理至网页服务器417，并且通过VPN代理响应418接收响应415并将其直接发送回至用户。

[0087] 现在，与特定网页相关联的会话是活动的420，并且可以通过合适的会话422来渲染网页。如果用户从VPN 234登出424(如图3A所示)，那么可以从存储器428中清除会话数据，并且如果在某些实施例中用户随后访问网页406，那么可以发送VPN代理请求431。可以经由VPN客户端232正常地将作为VPN 432的代理的请求431代理至网页服务器417。可以从网页服务器417中取回响应435并且在框434中由VPN客户端232通过VPN代理响应418直接将其发送回至浏览器302。在无需相关联的网页会话是活动的440情况下，可以在浏览器302中对特定网页进行渲染。

[0088] 现在转到图4B，展示了本发明的一个实施例，其中，可以在没有有活动VPN的情况下执行登录/登出会话。在实施例中，如之前在图2A中详述的，过程以在浏览器302中不存在450会话而开始，并且用户登录到会话管理器202中并且可以取回所有之前的会话452并将它们453注入用户的浏览器302中。然后可以在浏览器302中激活454会话。

[0089] 接下来，在一个实施例中，如图3A中所示出和描述的，用户可以在框456中登出会话管理器202并且暂停所有正在进行的会话。之后，可以在浏览器302上通过响应457将这些会话暂停458。

[0090] 现在转到图5，展示了本发明的用于在用户(如，例如，会话创建者(例如，用户A))与接收器用户(例如，用户B)之间共享会话的一个实施例，其中，可以发起共享会话。在一个

实施例中，用户A可以直接通过会话管理器202或者通过VPN客户端232进行认证502(如图2A或图2B中所描绘的)。之后，用户A可以发起与用户B共享当前会话504。在实施例中，用户A也可以选择要应用于可能正在进行的所述共享会话的限制或者访问506。通过一个非限制性示例，除了将易于被技术人员所理解的其他安排之外，用户A可以限制用户B访问注入特定会话中的任何cookie，或者可替代地，用户A可以限制用户B修改与共享会话相关联的代码。

[0091] 在本发明的一个实施例中，用户A可以指定是否要防止用户B能够读取共享会话或者对其或对共享限制做出修改508。如果用户A决定限制共享会话并防止会话修改(即，步骤508＝“是”)，那么，共享会话被描述为“锁定的”。在实施例中，会话管理器202或者用户A的VPN客户端232可以通过在会话服务器210上的会话服务器API请求会话管理器的公钥510。在实施例中，会话管理器202或者VPN客户端232可以取回会话管理器202的公钥510作为响应513并且可以使用它来加密共享会话(步骤514)。对共享会话进行加密创建了锁定的会话515。然而，如果用户A决定不限制共享会话(即，步骤508＝“否”)，那么共享会话被描述为“解锁的”516，并且假设有能力的接收器可以查看/修改会话和/或相关联的限制。

[0092] 接下来，会话管理器202或者VPN客户端232可以请求用户B的公钥518。在实施例中，可以将用户B的公钥518存储在相互可访问的位置(如，但不限于，会话服务器210)中。之后，可以从会话服务器210取回519用户B的公钥。用户B的公钥可以用于加密用户A与用户B之间的共享会话520。在一个实施例中，除了将易于被技术人员设想的任何其他安排之外，可以将用户B的公钥存储在任何适当的位置中以供稍后使用，包括但不限于远程地、本地地、安全地或不安全地存储。

[0093] 可以将用户A与B之间的经加密的会话发送524至会话服务器210并存储在会话服务器210上。可以将经加密的会话与在共享会话中涉及的用户A和B中的任一者或两者进行关联。

[0094] 图6展示了根据一个实施例的描绘用于VPN功能的技术的过程600。在实施例中，VPN(例如，VPN 234)可以在602中接收来自第二用户(即，会话接收器)的针对会话的请求。在604中，可以判定第二用户是否登录到会话管理器(例如，会话管理器202)中。如果第二用户登录到会话管理器中(步骤604＝“是”)，那么，在606中，可以判定是否通过安全协议形成了连接。如果通过安全协议形成了连接(步骤606＝“是”)，那么，在608中，SSL握手可以与第二用户进行协商。在610中，可以判定针对来自于步骤602的用户会话请求是否存在之前的会话。

[0095] 然而，如果没有通过安全协议形成连接(即，步骤606＝“否”)，那么，过程600行进到步骤610，在该步骤中，可以判定针对该请求是否存在之前的会话。如果针对特定会话请求不存在之前的会话(即，步骤610＝“否”)，那么，在612中，可以生成代理请求。类似地，在步骤604中，如果第二用户没有登录到会话管理器中，那么可以在612中生成代理请求。

[0096] 如果对应于特定请求的之前会话存在(即，步骤610＝“是”)，那么，在616中，判定是否共享之前的会话。如果该会话未被共享(即，步骤616＝“否”)，那么，在618中，可以将之前可能存在的会话cookie注入到生成的代理请求中。然而，如果该之前的会话被共享(即，步骤616＝“是”)，那么，在620中，判定HTTP或HTTPS请求是否由共享会话的参数授权。如果HTTP或HTTPS请求被授权(即，步骤620＝“是”)，那么，在618中，可以将会话cookie注入到代理请求中。然而，如果HTTP或HTTPS请求未被共享会话许可授权(即，步骤620＝“否”)，那么，

在622中，可以向第二用户返回指示第二用户未被授权参加与第一用户(即，会话创建者)的共享的会话的消息“请求未授权”。在实施例中，可以将多个输入过滤器与特定共享会话进行关联，并且在一个实施例中，可以由主动地共享会话的第一用户进行设置。

[0097] 从步骤612继续，一旦生成代理请求，就可以在614中将代理请求发送至网络服务器(例如，HTTP或HTTPS服务器)并且在624中可以从HTTP或HTTPS服务器取回针对会话管理器的响应。在626中，可以判定第二用户是否登录到会话管理器中。如果第二用户登录到会话管理器中(即，步骤626＝“是”)，那么，在630中，可以判定会话是否与第二用户共享。如果会话未与第二用户共享(即，步骤630＝“否”)，那么，在步骤628中，可以向第二用户返回指示第二用户没有与第二用户共享会话的响应。类似地，如果第二用户没有登录到会话管理器中(即，步骤626＝“否”)，那么，在628中，可以将该响应发送至第二用户。

[0098] 另一方面，如果与第二用户共享了会话(即，步骤630＝“是”)，那么，在632中，可以将与特定共享会话相关联的参数和输出过滤器应用于响应。在628中，可以从服务器中取回该响应并且可以将修改或过滤的响应发送至第二用户。可以设想的是，在一个实施例中，可以对与该响应相关联的HTML做出直接修改，如，但不限于，可以禁止第二用户在页面上执行某些动作(如，登出)，或者可以从该响应中去除会话cookie以便不可用于共享的第二用户。在一个实施例中，可以设想的是，由共享会话的第一用户对输出过滤器进行设置。虽然图6是关于第二用户进行讨论的，应当认识到的是，在图6的讨论中也设想任何附加数量的共享用户。

[0099] 现在转到图7A，展示了本发明的一个实施例，其中，可以通过活动VPN 234接收共享会话。在实施例中，第一用户A可以与共享的第二用户B共享与特定的网页或域名710相关的会话(如之前在图5中所描绘的)。而且，用户B可能之前已经注册708并且创建了用于共享的公钥和私钥(如之前在图1中所描绘的)。为了接收共享会话，用户B可以在框712中使用VPN客户端704登录VPN 234并且取回和解密与特定网站相关联的共享会话(如之前在图2B中所描绘的)。

[0100] 如果共享会话在浏览器706上之前并不存在(即，会话不存在714)，那么用户B可以通过用户B的浏览器706将请求716发送至与共享会话相关联的网页或域名。可以由代理通过VPN 234发送这个请求并且可以由VPN 234将任何必要的输入过滤器应用于请求716(如之前在图6中所讨论的)。可以将代理请求发送至网页或域名服务器720并且基于所述请求取回722响应并在框724中由代理通过VPN 234将响应发送至浏览器706。在实施例中，VPN 234可以相应地将任何输出过滤器应用于发送至浏览器706的请求(如之前在图6中所讨论的)。VPN 234可以基于合适的输出过滤器渲染响应726并且可以使用所应用的合适的限制和过滤器来在浏览器706中激活共享会话。之后，可以在浏览器706中激活728所述会话。

[0101] 现在转到图7B，展示了本发明的一个实施例，其中，可以在没有活动VPN的情况下取回共享会话。在实施例中，第一用户A可以与共享的或者第二用户B共享与特定的网页或域名711相关的会话(如之前在图5中所描绘的)。而且，用户B可能之前已经注册709并且创建了用于共享的公钥和私钥(如之前在图1中所描绘的)。为了接收共享会话，用户B可以登录会话管理器730并且取回和解密与特定网站相关联的共享会话732(如之前在图2A中所描绘的)。在实施例中，如果共享会话在浏览器706上之前并不存在(会话不存在732)，那么用户B可以将经解密的共享会话732注入733到浏览器706中，可以在没有限制734的情况下在

浏览器706中激活所述经解密的共享会话。

[0102] 在实施例中，用户B可以使用浏览器706来发送针对与HTTP服务器720相关联的网页的请求736。相关联的响应可以从服务器中被取回并且由浏览器706接收738。当接收了738响应，可以由浏览器706经由通知739告知会话管理器702。会话管理器702可以同时监听来自于浏览器706的响应740。浏览器706可以渲染来自于网络服务器720的响应742，并且会话管理器702可以将任何要求的限制744应用于响应742。在实施例中，会话管理器702可以通过在所渲染的网页中修改文档对象模型(“DOM”)元素745来应用限制，然而，也设想了对于技术人员而言将为非常明显的其他安排。可以在浏览器706中渲染网页，其中，共享会话在框746中被应用于所渲染的网页。

[0103] 图8展示了根据一个实施例的活动会话管理。在实施例中，第一用户(例如，用户A)可以使用会话管理器202进行认证802(如之前在图2A和图2B中所描绘的)。之后，用户可以随后在浏览器302上在与特定域名804相关联的网页上创建新会话。如果在浏览器302上的会话到期了，那么会话管理器202可以检测到此到期808并增加会话的寿命。在实施例中，除了将易于被技术人员所理解的其他安排之外，增加寿命可以被修改，从而使得例如与浏览器302上的特定域名相关联的所有随后的会话可以具有延长的寿命，或者可代替地，可以在逐案例基础上增加会话的寿命。

[0104] 如果用户登出会话管理器202，那么然后可以由会话管理器202暂停810所有活动会话(如图3A中所示出和描述的)。

[0105] 在未来的某个后续时间处，在之前没有登录会话管理器202或使用所述会话管理器进行认证的情况下，用户可以在网页812上创建与浏览器302上的相同的特定域名相关联的新会话。如果尝试了登陆会话管理器202的后续尝试，(如图2A中所示出和描述的)，那么会话管理器202可以检测在新会话与同那个域名相关联的之前暂停的会话之间的冲突814。在实施例中，用户之后可以判定是否使用暂停的会话覆盖新创建的会话或者代替地维持新创建的会话816。可代替地，如图2A和图2B所描绘的，用户可以取回之前创建的会话。

[0106] 在示例中，针对在线银行应用，用户可以经由浏览器302在银行网站上创建新会话818，并且会话管理器202可以通过发送非会话修改请求820来周期性地“触发”银行服务器，以保持银行网站上的会话活跃。因此，在会话通常在短时间的不活跃之后超时的情况下，可以维持活动会话。

[0107] 在一个实施例中，除了其他非常明显的安排之外，用户可以在多账户网站822(如，但不限于，Google®)上创建第一会话A(GOOGLE是谷歌公司的注册商标)。之后，用户可以随后在那个相同的多账户网站824上创建第二会话B。在实施例中，会话管理器202可以提供用户界面，该用户界面允许用户通过访问共享会话并且在不要求用户登录或登出多个不同的会话的情况下在单独的多账户会话826之间以无缝的方式进行切换。

[0108] 现在参照图9，框图展示了根据一个实施例的可以与图1至图8中所描述的过程一起使用的可编程设备900。图9中所示的可编程设备900是包括第一处理元件970和第二处理元件980的多处理器可编程设备。虽然示出了两个处理元件970和980，可编程设备900的实施例也可以只包括一个这样的处理元件。

[0109] 可编程设备900被展示为点对点互连系统，在该系统中，第一处理元件970和第二处理元件980经由点对点互连950相耦合。图9中所展示的任何或所有互连中可以被实现为

多分支总线而不是点对点互连。

[0110] 如图9中所展示的，处理元件970和980中的每一个处理元件可以是多核处理器，包括第一处理器核和第二处理器核(即，处理器核974a和974b以及处理器核984a和984b)。此类核974a、974b、984a和984b可以被配置成用于以与以上关于图1至图8讨论的方式类似的方式执行指令代码。然而，如所期望的，其他实施例可以使用作为单核处理器的处理元件。如所期望的，在具有多个处理元件970，980的实施例中，可以使用不同数量的核来实现每一个处理元件。

[0111] 每个处理元件970，980可以包括至少一个共享高速缓存器946。共享高速缓存器946a，946b可以存储分别由处理元件的一个或多个部件(如，核974a，974b以及984a，984b)使用的数据(如，指令)。例如，共享高速缓存器可以本地缓存存储在存储器932，934中的数据，以供处理元件970，980的部件更快速地访问。在一个或多个实施例中，共享高速缓存器946a，946b可以包括一个或多个中级缓存器，如二级(L2)、三级(L3)、四级(L4)或其他级别的缓存器、终级缓存器(LLC)、或其组合。

[0112] 虽然为了附图的清晰性，图9展示了具有两个处理元件970，980的可编程设备，但是本发明的范围不受这样的限制，并且可以存在任意数量的处理元件。可代替地，处理元件970，980中的一个或多个处理元件可以是除处理器以外的元件，如，图形处理单元(GPU)、数字信号处理(DSP)单元、现场可编程门阵列、或者任何其他可编程处理元件。处理元件980可以是异构的或者与处理元件970不对称。就包括架构特性、微架构特性、热特性、功耗特性等等在内的优点的度量谱而言，处理元件970，980之间可能有各种各样的差异。这些差异可以有效地表明它们是处理元件970，980之间的不对称性和异构性。在某些实施例中，各种处理元件970，980可以驻留在同一裸片封装体中。

[0113] 第一处理元件970还可以进一步包括存储器控制器逻辑(MC)972以及点对点(P-P)互连976和978。类似地，第二处理元件980可以包括MC 982以及P-P互连986和988。如图9所示的，MC 972和MC 982将处理元件970，980耦合至对应的存储器(即，存储器932和存储器934)，这些存储器可以是主存储器的本地附接至对应处理器的部分。虽然MC逻辑972和982被展示为集成在处理元件970、980中，但是在某些实施例中，存储器控制器逻辑可以是处理元件970、980之外而不是集成在其中的离散逻辑。

[0114] 处理元件970和处理元件980可以通过链路952和954经由对应的P-P互连976和986耦合至I/O子系统990。如图9中所示的，I/O子系统990包括P-P互连994和998。此外，I/O子系统990包括用于将I/O子系统990与高性能图形引擎938耦合的接口992。在一个实施例中，总线(未示出)可以用于将图形引擎938耦合至I/O子系统990。可替代地，点对点互连939可以对这些部件进行耦合。

[0115] 反过来，I/O子系统990可以经由接口996耦合至第一链路916。在一个实施例中，第一链路916可以是外围组件互连(PCI)总线，或如PCI Express总线或另一个I/O互连总线的总线，尽管本发明的范围不受此限制。

[0116] 如图9中所示的，各个I/O设备914，924可连同桥918一起耦合至第一链路916，该桥可以将第一链路916耦合至第二链路920。在一个实施例中，第二链路920可以是低引脚数(LPC)总线。在一个实施例中，各个设备可以耦合至第二链路920，所述设备包括例如键盘/鼠标912、(多个)通信设备926(所述通信设备进而可以与计算机网络903进行通信)、以及可

以包括代码930的数据存储单元928(如磁盘驱动器或者其他大容量存储设备)。代码930可以包括用于执行以上描述的技术中的一项或多项技术的实施例的指令。进一步地,音频I/O 924可以耦合至第二总线920上。

[0117] 注意,设想了其他实施例。例如,系统可以实现多分支总线或另一个这种通信拓扑,而不是图9的点对点架构。虽然链路916和920在图9中被展示为总线,但是可以使用任何期望类型的链路。而且,可以可替代地使用比图9中所示的更多或更少的集成芯片来对图9的元件进行分区。

[0118] 现在参照图10,框图展示了根据另一个实施例的可编程设备1000。已经从图10中省略了图9的某些方面,以便避免模糊图10的其他方面。

[0119] 图10展示了处理元件1070、1080可以分别包括集成存储器和I/O控制逻辑("CL")1072和1082。在某些实施例中,1072、1082可以包括如以上结合图9所描述的存储器控制逻辑(MC))。此外,CL 1072、1082还可以包括I/O控制逻辑。图10展示了不但存储器1032、1034可以耦合至1072、1082,而且那个I/O设备1044也可以耦合至控制逻辑1072、1082。遗留I/O设备1015可以通过接口1096耦合至I/O子系统1090。每个处理元件1070,1080可以包括多个处理器核,所述多个处理器核在图10中被展示为处理器核1074A,1074B,1084A以及1084B。如图10所示,I/O子系统1090包括使用链路1052和1054连接至处理元件1070和1080的P-P互连1076和1086的P-P互连1094和1098。也可以分别通过链路1050以及互连1078和1088将处理元件1070与1080进行互连。

[0120] 在图9和图10中描绘的可编程设备是可编程设备的实施例的示意图解,其可以用来实现在此讨论的各个实施例。在图9和图10中描绘的可编程设备的各种部件可以组合在片上系统(SoC)架构中。

[0121] 现在参照图11,示意性地展示了在其中可以实现以上描述的技术的示例基础设施1100。基础设施1100包含计算机网络1102。计算机网络1102可以包括当今可用的许多不同类型的计算机网络,如,互联网、企业网络或者局域网(LAN)。这些网络中的每一个网络可以包含有线或无线可编程设备并且可以使用任何数量的网络协议(例如,TCP/IP)来运行。网络1102可以连接至网关和路由器(由1108表示)、终端用户计算机1106、以及计算机服务器1104。基础设施1100还可以包括用于与移动通讯设备一起使用的蜂窝网络1103。移动蜂窝网络支持移动电话以及许多其他类型的移动设备。在基础设施1100中的移动设备被展示为移动电话1110、膝上计算机1112、以及平板计算机1114。在移动设备移动时,移动设备(如移动电话1110)可以与一个或多个移动提供方网络进行交互,通常与多个移动网络塔1120,1130和1140进行交互以用于连接至蜂窝网络1103。虽然在图11中被称为蜂窝网络,但是移动设备可以与多于一个提供方网络的塔以及与多个非蜂窝设备(如无线接入点和路由器1108)进行交互。此外,针对期望的服务,移动设备1110,1112和1114可以与非移动设备(如计算机1104和1106)进行交互,所述交互可以包括在不提供以上描述的用户凭据的情况下跨多个客户端设备以及与其他经授权的用户共享会话。客户端设备的功能可以在图11中所示的任何设备或设备组合中实现;然而,最常见的是在网关或路由器中在防火墙或入侵防御系统中实现。

[0122] 以下示例涉及进一步的实施例。

[0123] 示例1是一种在其上存储有指令的机器可读介质,所述指令包括当被执行时使机

器执行以下各项的指令:传输与在网络浏览器上针对与网络域(web domain)相关联的网页创建会话相关的用户信息,其中,所述用户信息包括用户凭据;传输与终止所述会话相关的登出信息,从而创建终止的会话;传输对取回(retrieve)所述终止的会话的请求;以及接收与在所述网络浏览器中注入所述终止的会话相关的会话信息,从而创建活动会话。

[0124] 在示例2中,示例1的主题可以可选地包括:其中,用于传输登出信息的所述指令进一步包括当被执行时使所述机器执行以下各项的指令:响应于传输所述登出信息而存储与所述会话相关的会话数据;以及从所述网络浏览器中删除与所述会话相关的会话cookie。

[0125] 在示例3中,示例1或示例2的主题可以可选地包括:其中,所述指令进一步包括当被执行时使所述机器在与移动设备相关联的所述网络浏览器上创建所述会话的指令。

[0126] 在示例4中,示例1至示例3的主题可以可选地包括:其中,所述指令进一步包括当被执行时使所述机器传输同与第二用户共享所述会话相关的信息从而创建共享会话的指令。

[0127] 在示例5中,示例4的主题可以可选地包括:其中,用于共享所述会话的所述指令进一步包括当被执行时使所述机器传输针对与所述第二用户相关的所述共享会话的限制的指令。

[0128] 在示例6中,示例1至示例5的主题可以可选地包括:其中,所述指令进一步包括当被执行时使所述机器防止用户名和密码中的一者或多者响应于传输对取回所述终止的会话的所述请求而被传输的指令。

[0129] 在示例7中,示例1至示例6的主题可以可选地包括:其中,所述指令进一步包括当被执行时使所述机器将请求传输至所述网络域或者修改所述会话信息以保持所述会话活跃的指令,所述请求为非会话修改请求。

[0130] 在示例8中,示例1至示例7的主题可以可选地包括:其中,用于接收与取回所述终止的会话相关的会话信息的所述指令进一步包括当被执行时使所述机器判定针对与所述网络域相关联的所述网页是否存在之前的会话的指令。

[0131] 在示例9中,示例1至示例6的主题可以可选地包括:其中,所述指令进一步包括当被执行时使所述机器在第一设备上终止所述会话并且在第二设备上取回所述终止的会话的指令,所述第一和第二设备与用户相关联。

[0132] 示例10是一种用于恢复和共享会话的方法,所述方法包括:传输与在网络浏览器上针对与网络域相关联的网页创建会话相关的用户信息,其中,所述用户信息包括用户凭据;传输来自会话管理器的与终止所述会话相关的登出信息,从而创建终止的会话;传输对使用所述会话管理器来取回所述终止的会话的请求;以及使用所述会话管理器接收与在所述网络浏览器中注入所述终止的会话相关的会话信息,从而创建活动会话。

[0133] 在示例11中,示例10的主题可以可选地包括:响应于传输所述登出信息而存储与所述会话相关的网络浏览器数据;以及从所述网络浏览器中删除与所述会话相关的会话cookie。

[0134] 在示例12中,示例10至示例11的主题可以可选地包括:在与移动设备相关联的所述网络浏览器上创建所述会话。

[0135] 在示例13中,示例10至示例12的主题可以可选地包括:传输同与第二用户共享所述会话相关的信息,从而创建共享会话。

[0136] 在示例14中，示例10至示例13的主题可以可选地包括：防止所述用户凭据响应于传输对取回所述终止的会话的所述请求而被传输，其中，所述用户凭据包括用户的用户名和密码中的至少一者。

[0137] 在示例15中，示例10至示例14的主题可以可选地包括：将请求传输至所述网络域以保持所述会话活跃

[0138] 示例16是一种用于恢复和共享会话的方法，所述方法包括：传输与在网络浏览器上针对与网络域相关联的网页创建会话相关的用户信息，其中，所述用户信息包括用户凭据；传输来自会话管理器的与终止所述会话相关的登出信息，从而创建终止的会话；传输对使用所述会话管理器来取回所述终止的会话的请求；以及使用所述会话管理器接收与在所述网络浏览器中注入所述终止的会话相关的会话信息，从而创建活动会话。

[0139] 在示例17中，示例16的主题可以可选地包括：响应于传输所述登出信息而存储与所述会话相关的网络浏览器数据；以及从所述网络浏览器中删除与所述会话相关的会话cookie。

[0140] 在示例18中，示例16至示例17的主题可以可选地包括：在与移动设备相关联的所述网络浏览器上创建所述会话。

[0141] 在示例19中，示例16至示例17的主题可以可选地包括：传输同与第二用户共享所述会话相关的信息，从而创建共享会话。

[0142] 在示例20中，示例19的主题可以可选地包括：传输针对与所述第二用户相关的所述共享会话的限制。

[0143] 在示例21中，示例16至示例17的主题可以可选地包括：防止所述用户凭据响应于传输对取回所述终止的会话的所述请求而被传输，其中，所述用户凭据包括用户的用户名和密码中的至少一者。

[0144] 在示例22中，示例16至示例17的主题可以可选地包括：将请求传输至所述网络域以保持所述会话活跃，所述请求为非会话修改请求。

[0145] 在示例23中，示例16至示例17的主题可以可选地包括：判定针对与所述网络域相关联的所述网页是否存在之前的会话。

[0146] 在示例24中，示例16至示例17的主题可以可选地包括：在第一设备上终止所述会话并且在第二设备上取回所述终止的会话，所述第一和第二设备与所述用户相关联。

[0147] 示例25是一种用于恢复和共享会话的计算机系统，所述计算机系统包括：一个或多个处理器；以及耦合至所述一个或多个处理器的存储器，在所述存储器上存储有指令，所述指令包括当被执行时使所述处理器中的一个或多个处理器执行以下各项的指令：传输与在网络浏览器上针对与网络域相关联的网页创建会话相关的用户信息，其中，所述用户信息包括用户凭据；传输来自会话管理器的与终止所述会话相关的登出信息，从而创建终止的会话；传输对使用所述会话管理器来取回所述终止的会话的请求；以及使用所述会话管理器接收与在所述网络浏览器中注入所述终止的会话相关的会话信息，从而创建活动。

[0148] 在示例26中，示例25的主题可以可选地包括：其中，用于传输登出信息的所述指令进一步包括当被执行时使所述一个或多个处理器执行以下各项的指令：响应于传输所述登出信息而存储与所述会话相关的会话数据；以及从所述网络浏览器中删除与所述会话相关的会话cookie。

[0149] 在示例27中，示例25和示例26的主题可以可选地包括：其中，所述指令进一步包括当被执行时使所述一个或多个处理器在与移动设备相关联的网络浏览器上创建所述会话的指令。

[0150] 在示例28中，示例25和示例26的主题可以可选地包括：其中，所述指令进一步包括当被执行时使所述一个或多个处理器传输同与第二用户共享所述会话相关的信息从而创建共享会话的指令。

[0151] 在示例29中，示例28的主题可以可选地包括：其中，用于共享所述会话的所述指令进一步包括当被执行时使所述一个或多个处理器传输针对与所述第二用户相关的所述共享会话的限制的指令。

[0152] 在示例30中，示例25和示例26的主题可以可选地包括：其中，所述指令进一步包括当被执行时使所述一个或多个处理器防止所述用户凭据响应于传输对取回所述终止的会话的所述请求而被传输的指令。

[0153] 在示例31中，示例25和示例26的主题可以可选地包括：其中，所述指令进一步包括当被执行时使所述一个或多个处理器将请求传输至所述网络域以保持所述会话活跃的指令，所述请求为非会话修改请求。

[0154] 示例32是一种用于共享会话的方法，所述方法包括：传输与在服务器上认证用户相关的认证信息；传输对创建与第二用户共享的会话的请求；接收用于加密所述共享会话的加密密钥，其中，所述加密秘钥与所述第二用户相关联；加密所述共享会话以响应于接收所述加密秘钥而创建经加密的会话；以及响应于创建所述经加密的会话，将所述经加密的会话传输至所述服务器。

[0155] 在示例33中，示例32的主题可以可选地包括：传输针对与所述第二用户相关的所述共享会话的限制。

[0156] 在示例34中，示例33的主题可以可选地包括：响应于传输针对所述共享会话的限制而接收所述服务器公钥。

[0157] 在示例35中，示例32和示例33的主题可以可选地包括：进一步包括响应于传输针对所述共享会话的所述限制而限制所述第二用户访问cookie或者修改在所述共享会话中的代码。

[0158] 示例36是一种用于恢复和共享会话的计算机系统，所述计算机系统包括：一个或多个处理器；以及耦合至所述一个或多个处理器的存储器，在所述存储器上存储有指令，所述指令包括当被执行时使所述处理器中的一个或多个处理器执行以下各项的指令：传输与在服务器上认证用户相关的认证信息；传输对创建与第二用户的共享的会话的请求；接收用于加密所述共享会话的加密密钥，其中，所述加密秘钥与所述第二用户相关联；响应于接收所述加密秘钥而加密所述共享会话以创建经加密的会话；以及响应于创建所述经加密的会话而将所述经加密的会话传输至所述服务器。

[0159] 在示例37中，示例36的主题可以可选地包括：其中，所述指令进一步包括当被执行时使所述一个或多处理器传输针对与所述第二用户相关的所述共享会话的限制的指令。

[0160] 在示例38中，示例37的主题可以可选地包括：其中，所述指令进一步包括当被执行时使所述一个或多个处理器响应于传输针对所述共享会话的限制而接收所述服务器公钥的指令。

[0161] 在示例39中，示例36和示例37的主题可以可选地包括：其中，所述指令进一步包括当被执行时使所述一个或多处理器响应于传输针对所述共享会话的所述限制而限制所述第二用户访问cookie或者修改在所述共享会话中的代码的指令。

[0162] 在示例40中，示例36和示例37的主题可以可选地包括：其中，所述指令进一步包括当被执行时使所述一个或多个处理器传输来自于与所述用户相关联的移动设备的请求的指令。

[0163] 应该理解的是，以上描述旨在使说明性的，而不是限制性的。例如，上述实施例可以彼此组合地使用。对本领域技术人员而言，在阅读了上面的描述后，许多其他的实施例都将是明显的。因此，本发明的范围应当参照所附的权利要求以及与这些权利要求所请求的权利相等同的全部范围而被确定。

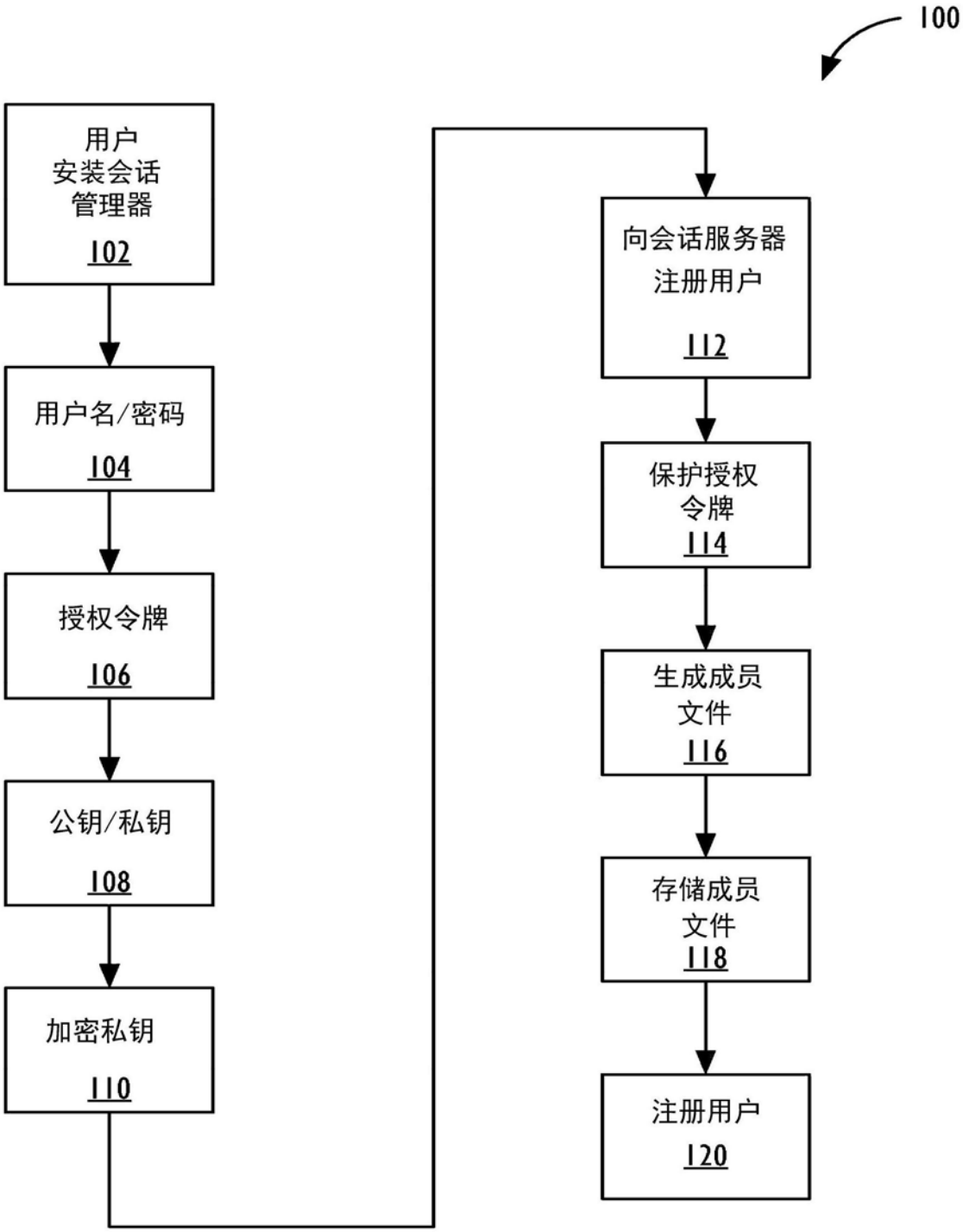

100
用户
安装会话
管理器
102
用户名/密码
104
授权令牌
106
公钥/私钥
108
加密私钥
110
向会话服务器
注册用户
112
保护授权
令牌
114
生成成员
文件
116
存储成员
文件
118
注册用户
120

图1

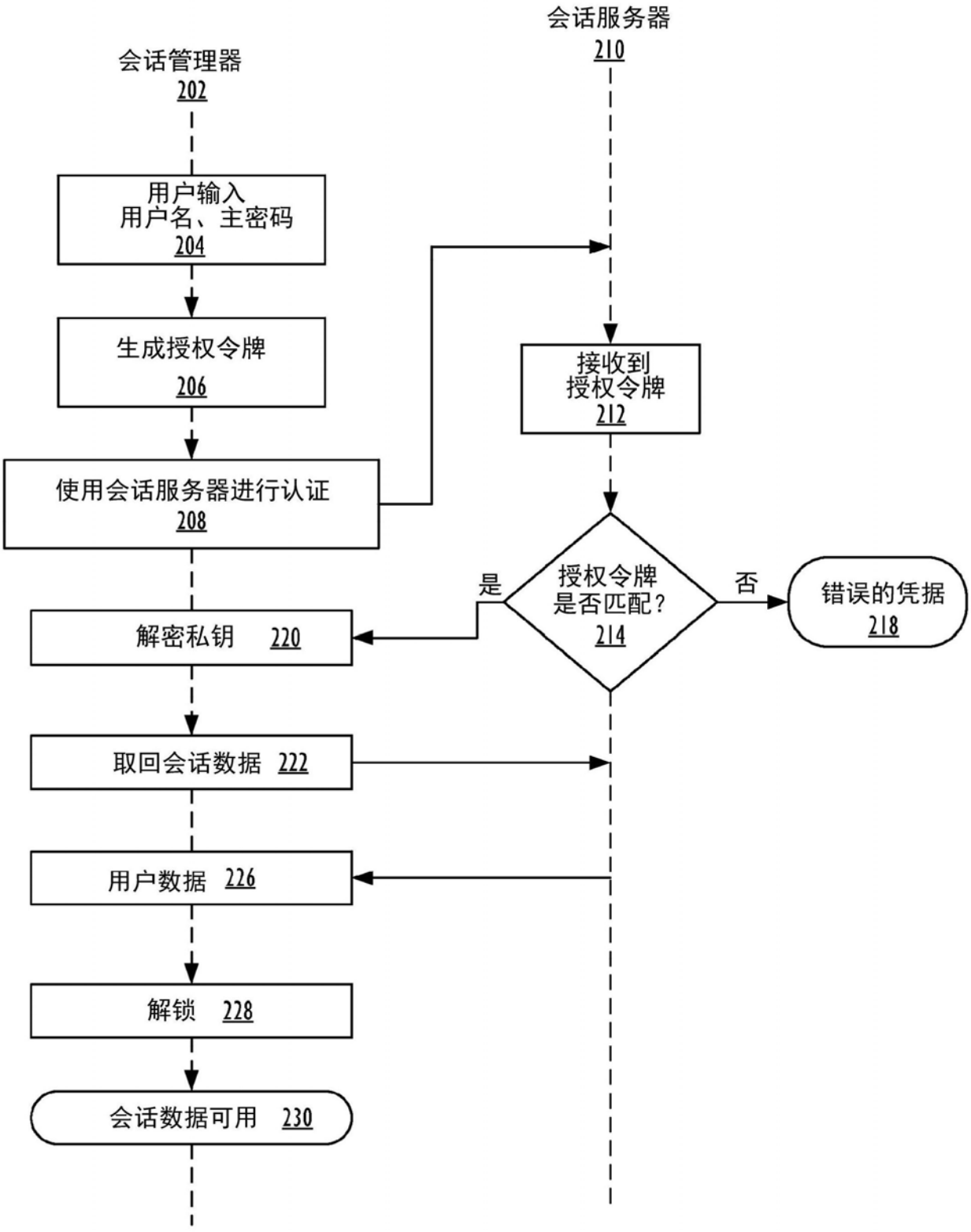

会话管理器
202
会话服务器
210
用户输入
用户名、主密码
204
生成授权令牌
206
使用会话服务器进行认证
208
接收到
授权令牌
212
授权令牌
是否匹配？
214
是
否
错误的凭据
218
解密私钥 220
取回会话数据 222
用户数据 226
解锁 228
会话数据可用 230

图2A

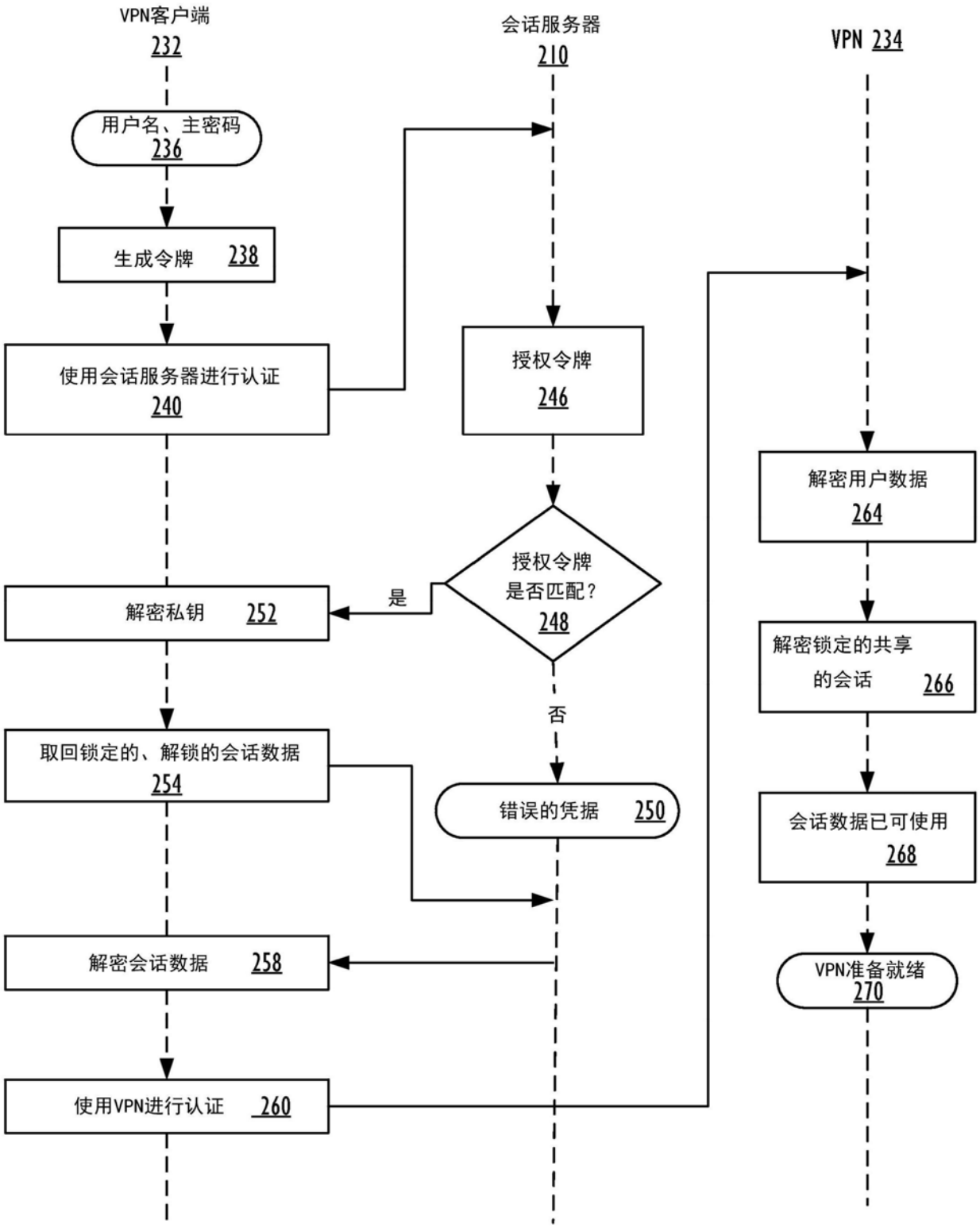

VPN客户端
232
会话服务器
210
VPN 234
用户名、主密码
236
生成令牌 238
使用会话服务器进行认证
240
授权令牌
246
授权令牌
是否匹配?
248
是
否
解密私钥 252
取回锁定的、解锁的会话数据
254
错误的凭据 250
解密会话数据 258
使用VPN进行认证 260
解密用户数据
264
解密锁定的共享
的会话 266
会话数据已可使用
268
VPN准备就绪
270

图2B

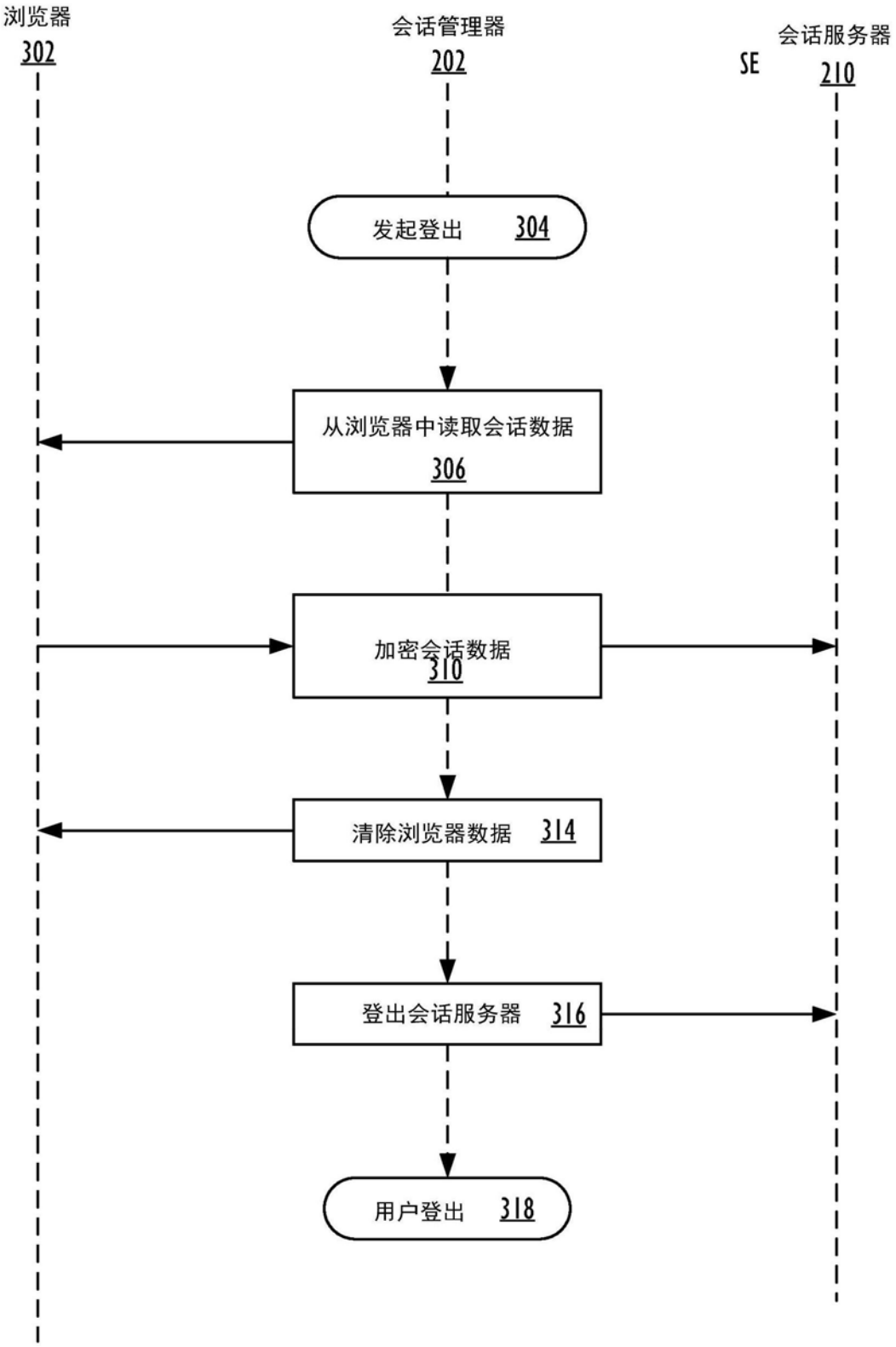

浏览器
302
会话管理器
202
SE
会话服务器
210
发起登出 304
从浏览器中读取会话数据
306
加密会话数据
310
清除浏览器数据 314
登出会话服务器 316
用户登出 318

图3A

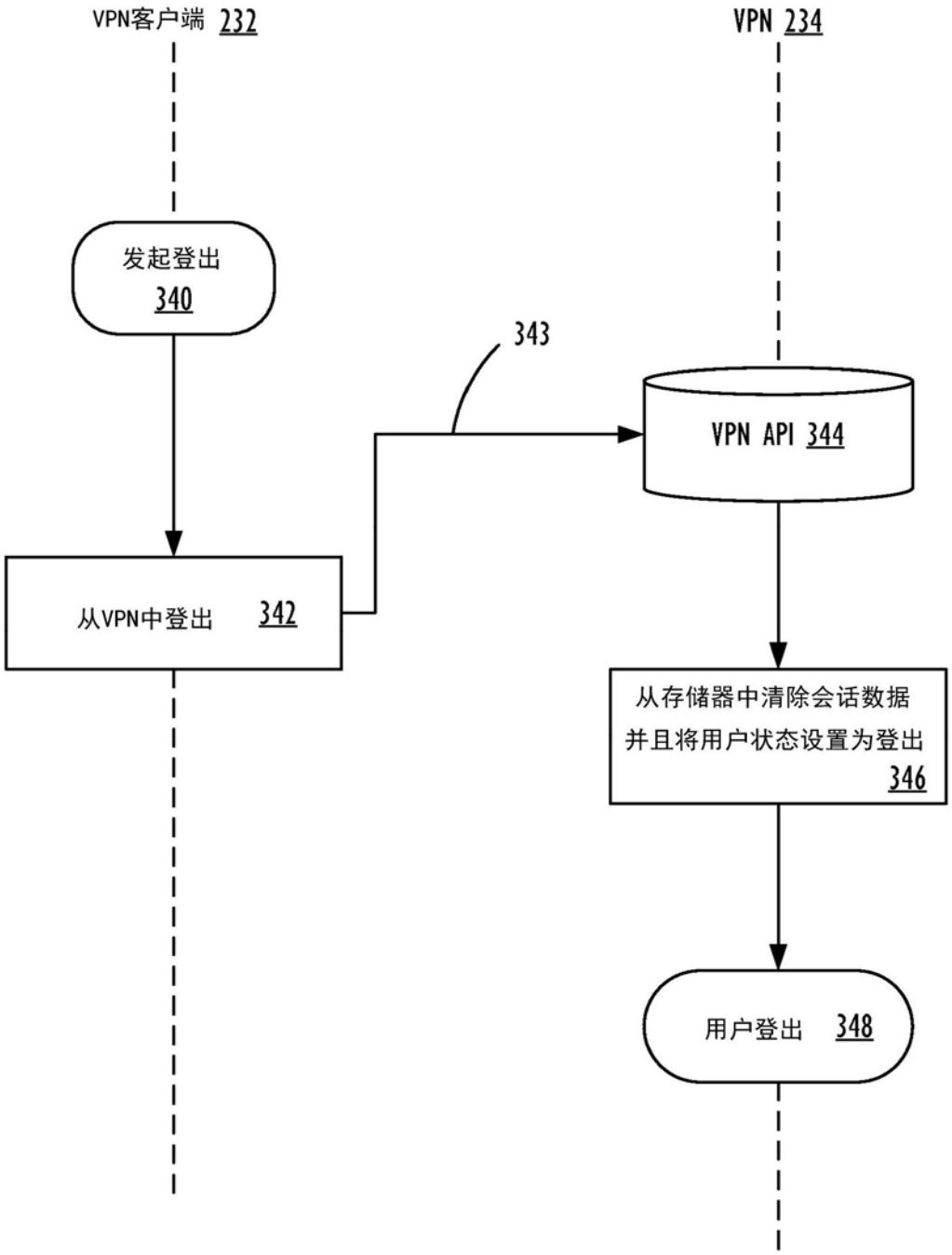

VPN客户端 232
VPN 234
发起登出
340
343
VPN API 344
从VPN中登出 342
从存储器中清除会话数据
并且将用户状态设置为登出
346
用户登出 348

图3B

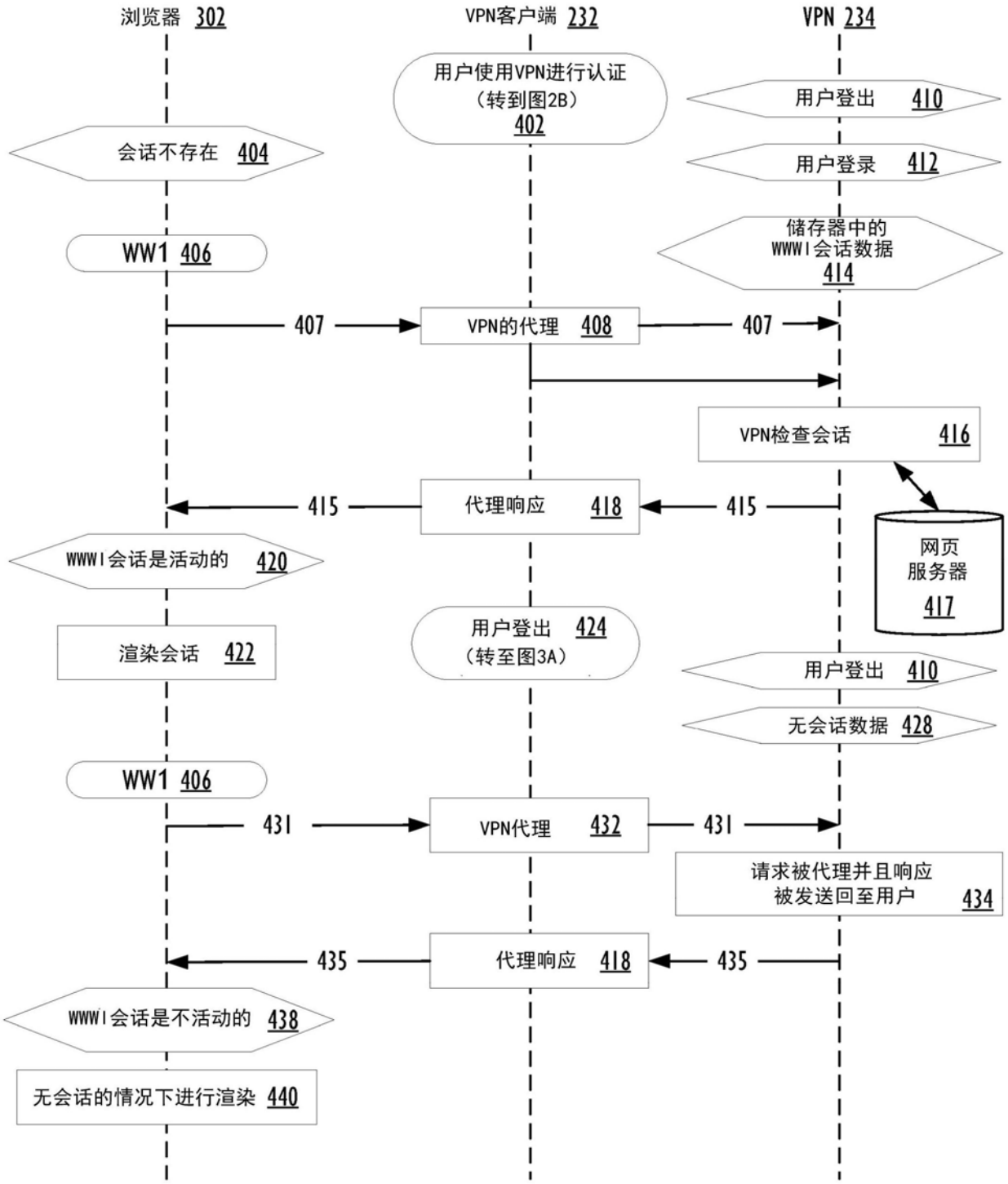

浏览器 302
VPN客户端 232
VPN 234
用户使用VPN进行认证
（转到图2B）
402
用户登出 410
会话不存在 404
用户登录 412
WW1 406
储存器中的
WWW1会话数据
414
407
VPN的代理 408
407
VPN检查会话 416
415
代理响应 418
415
网页
服务器
417
WWW1会话是活动的 420
用户登出 424
（转至图3A）
渲染会话 422
用户登出 410
无会话数据 428
WW1 406
431
VPN代理 432
431
请求被代理并且响应
被发送回至用户 434
435
代理响应 418
435
WWW1会话是不活动的 438
无会话的情况下进行渲染 440

图4A

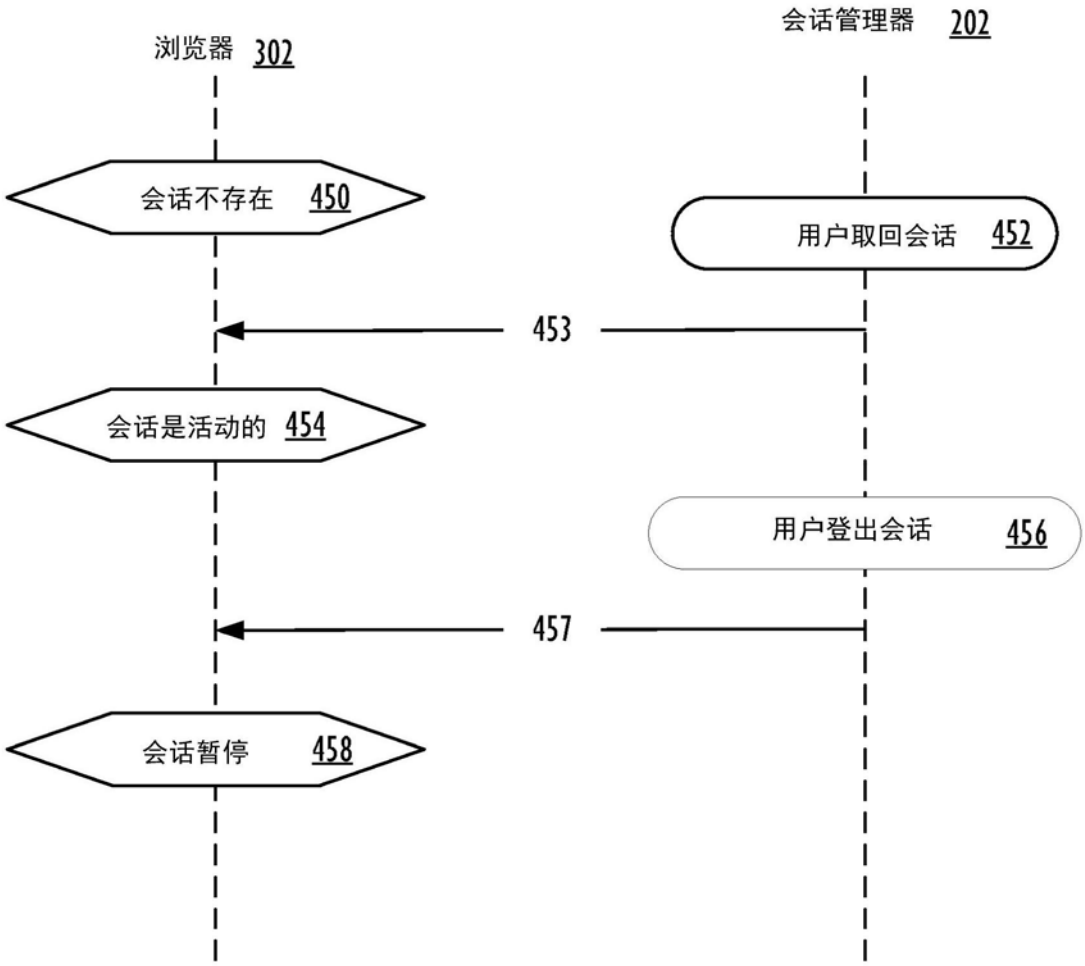

浏览器 302
会话管理器 202
会话不存在 450
用户取回会话 452
453
会话是活动的 454
用户登出会话 456
457
会话暂停 458

图4B

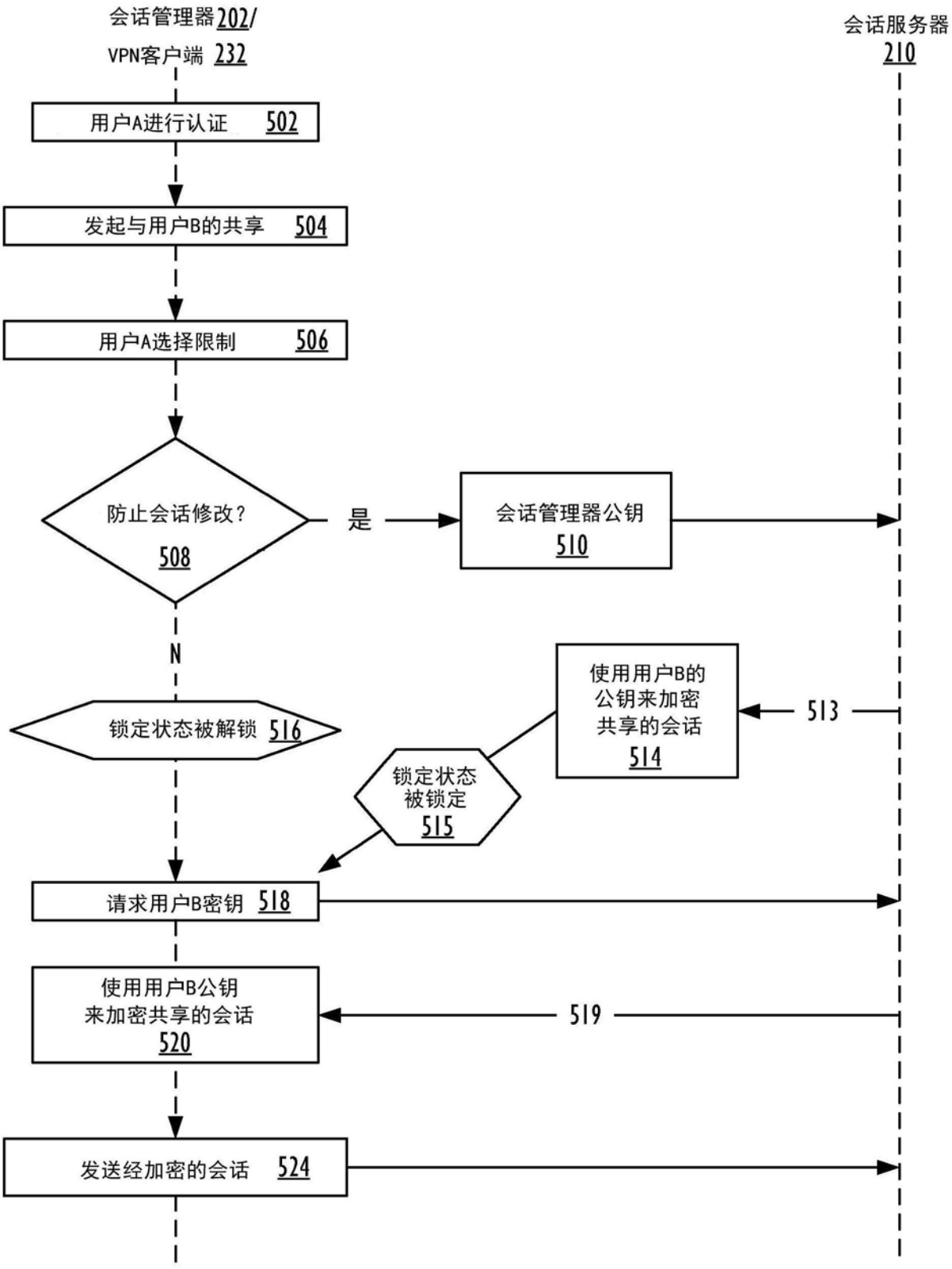

会话管理器202/
VPN客户端 232
会话服务器
210
用户A进行认证 502
发起与用户B的共享 504
用户A选择限制 506
防止会话修改?
508
是
会话管理器公钥
510
N
锁定状态被解锁 516
使用用户B的
公钥来加密
共享的会话
514
513
锁定状态
被锁定
515
请求用户B密钥 518
使用用户B公钥
来加密共享的会话
520
519
发送经加密的会话 524

图5

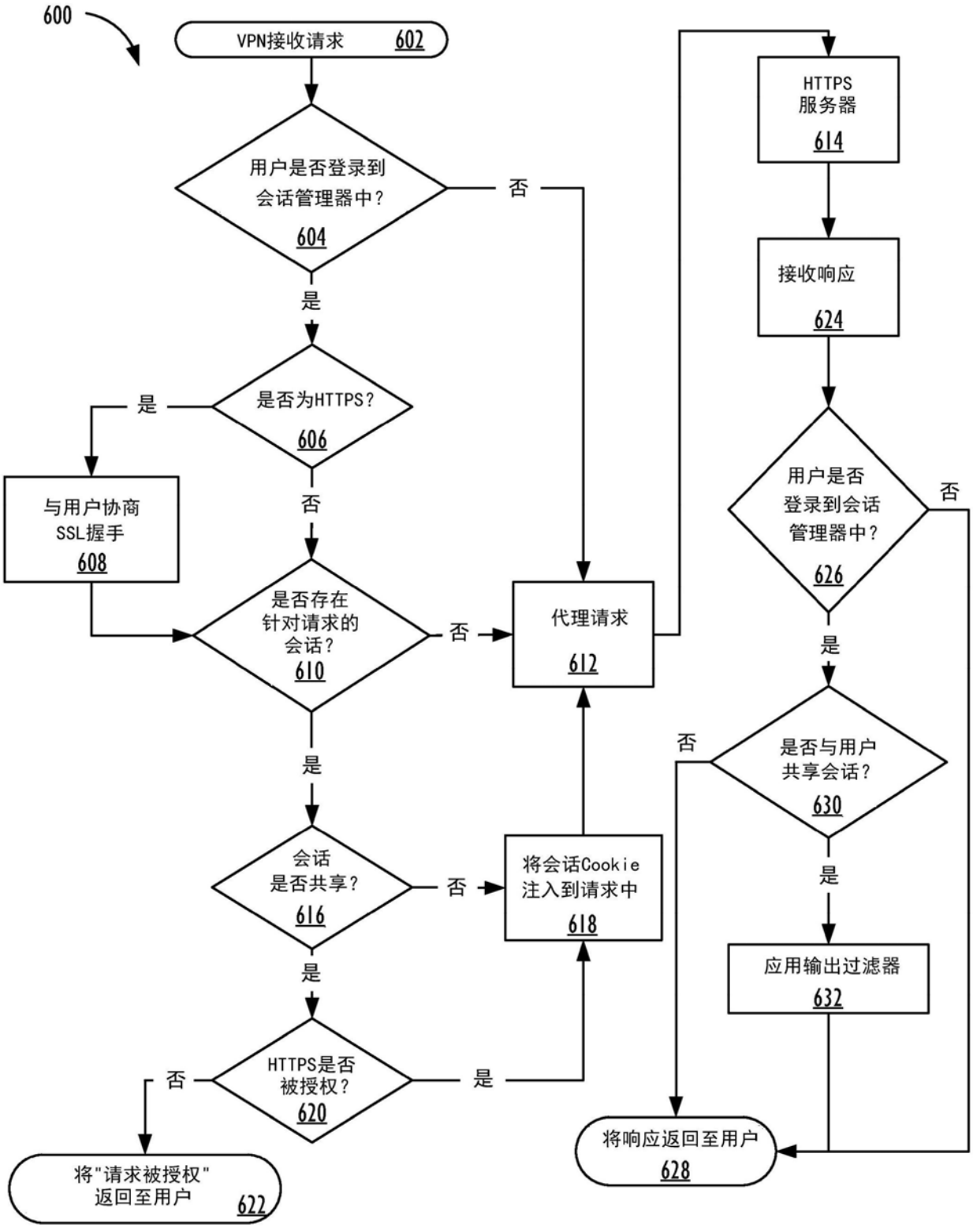

600
VPN接收请求 602
用户是否登录到会话管理器中？ 604
否
是
是否为HTTPS？ 606
是
否
与用户协商SSL握手 608
是否存在针对请求的会话？ 610
否
是
代理请求 612
HTTPS服务器 614
会话是否共享？ 616
否
是
将会话Cookie注入到请求中 618
HTTPS是否被授权？ 620
否
是
将"请求被授权"返回至用户 622
接收响应 624
用户是否登录到会话管理器中？ 626
否
是
是否与用户共享会话？ 630
否
是
应用输出过滤器 632
将响应返回至用户 628

图6

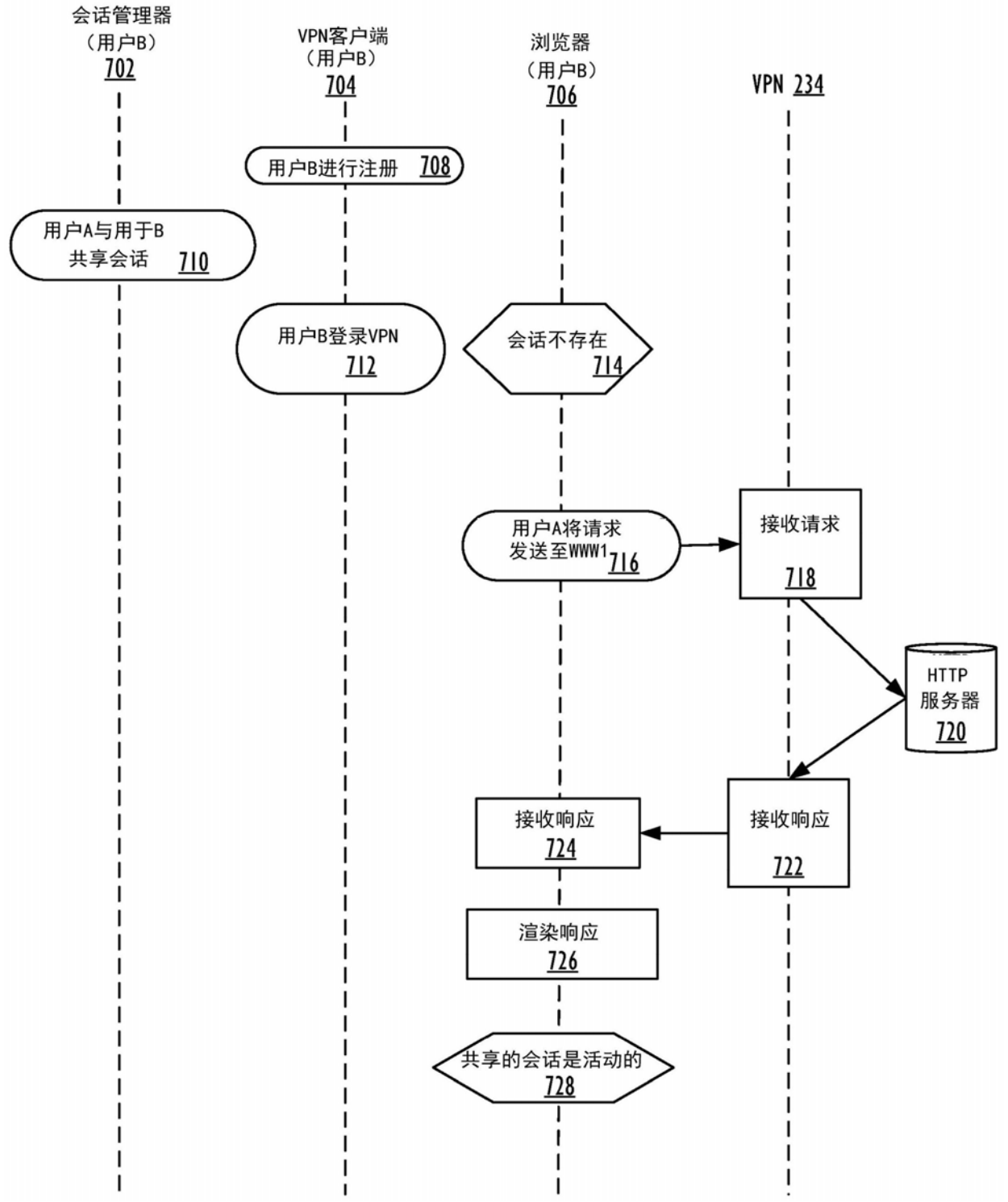

会话管理器
（用户B）
702
VPN客户端
（用户B）
704
浏览器
（用户B）
706
VPN 234
用户B进行注册 708
用户A与用于B
共享会话 710
用户B登录VPN
712
会话不存在
714
用户A将请求
发送至WWW1
716
接收请求
718
HTTP
服务器
720
接收响应
724
接收响应
722
渲染响应
726
共享的会话是活动的
728

图7A

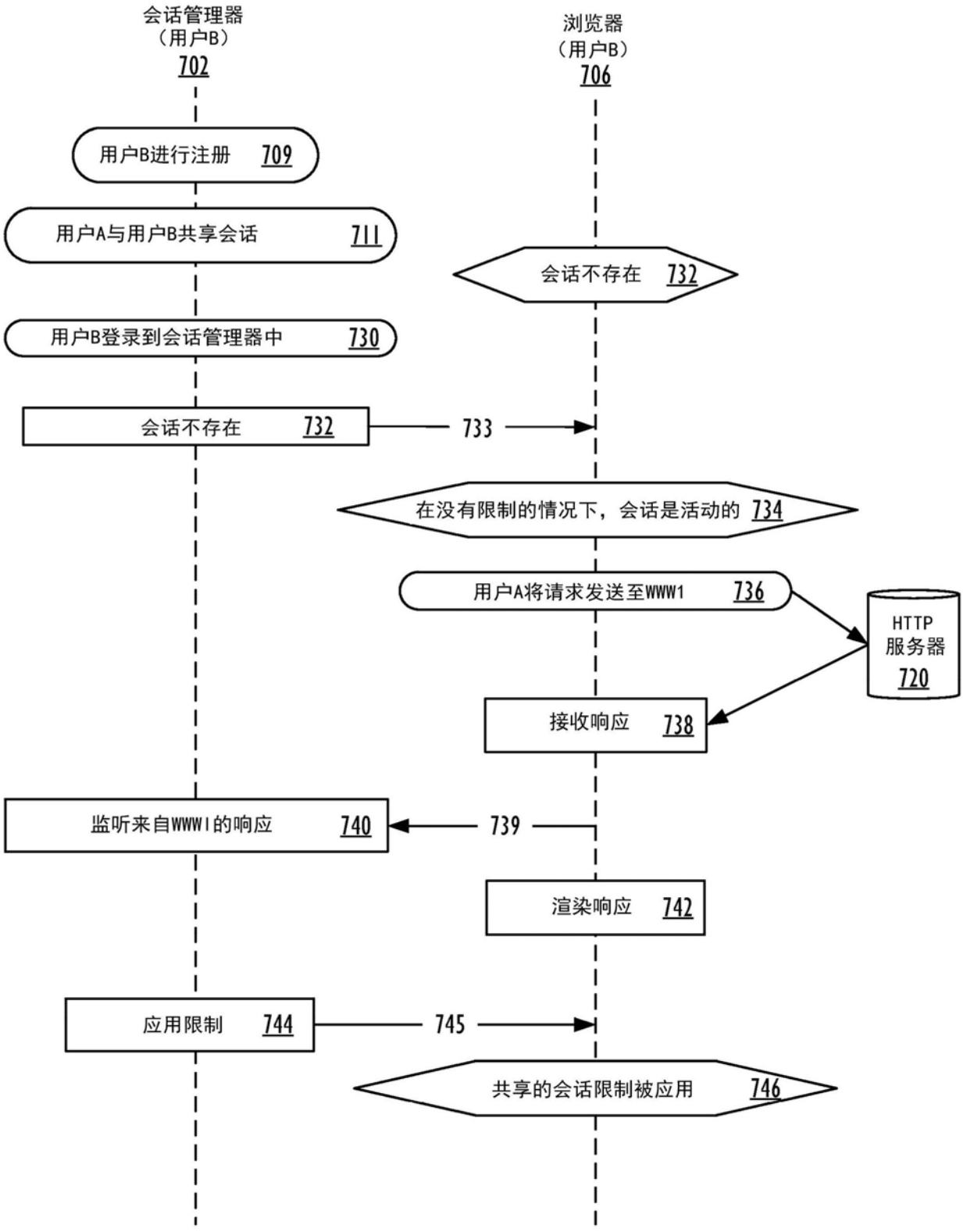

会话管理器
（用户B）
702
浏览器
（用户B）
706
用户B进行注册 709
用户A与用户B共享会话 711
会话不存在 732
用户B登录到会话管理器中 730
会话不存在 732
733
在没有限制的情况下，会话是活动的 734
用户A将请求发送至WWW1 736
HTTP
服务器
720
接收响应 738
监听来自WWW1的响应 740
739
渲染响应 742
应用限制 744
745
共享的会话限制被应用 746

图7B

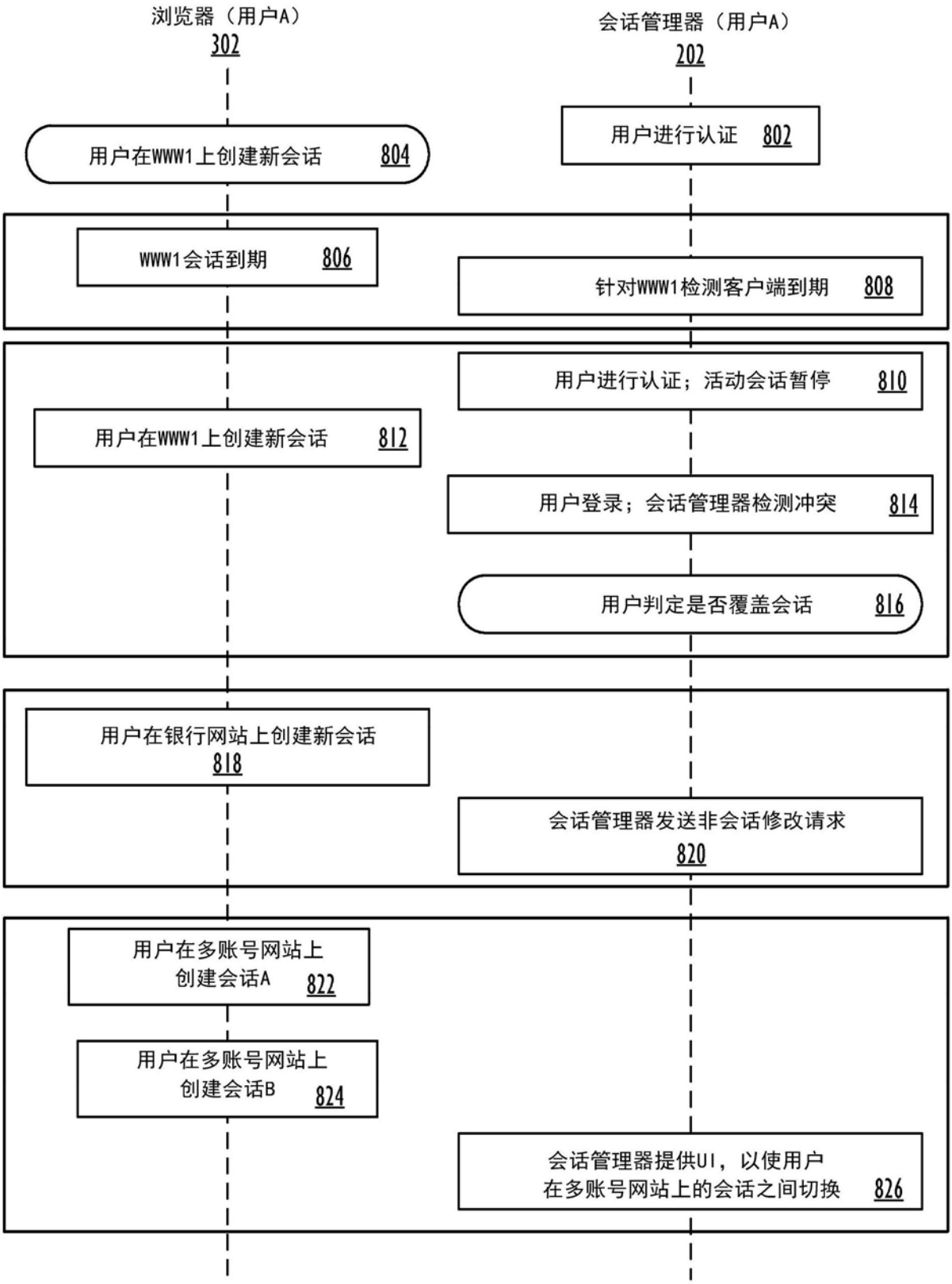

浏览器（用户A）
302
会话管理器（用户A）
202
用户进行认证 802
用户在WWW1上创建新会话 804
WWW1会话到期 806
针对WWW1检测客户端到期 808
用户进行认证；活动会话暂停 810
用户在WWW1上创建新会话 812
用户登录；会话管理器检测冲突 814
用户判定是否覆盖会话 816
用户在银行网站上创建新会话
818
会话管理器发送非会话修改请求
820
用户在多账号网站上
创建会话A 822
用户在多账号网站上
创建会话B 824
会话管理器提供UI，以使用户
在多账号网站上的会话之间切换 826

图8

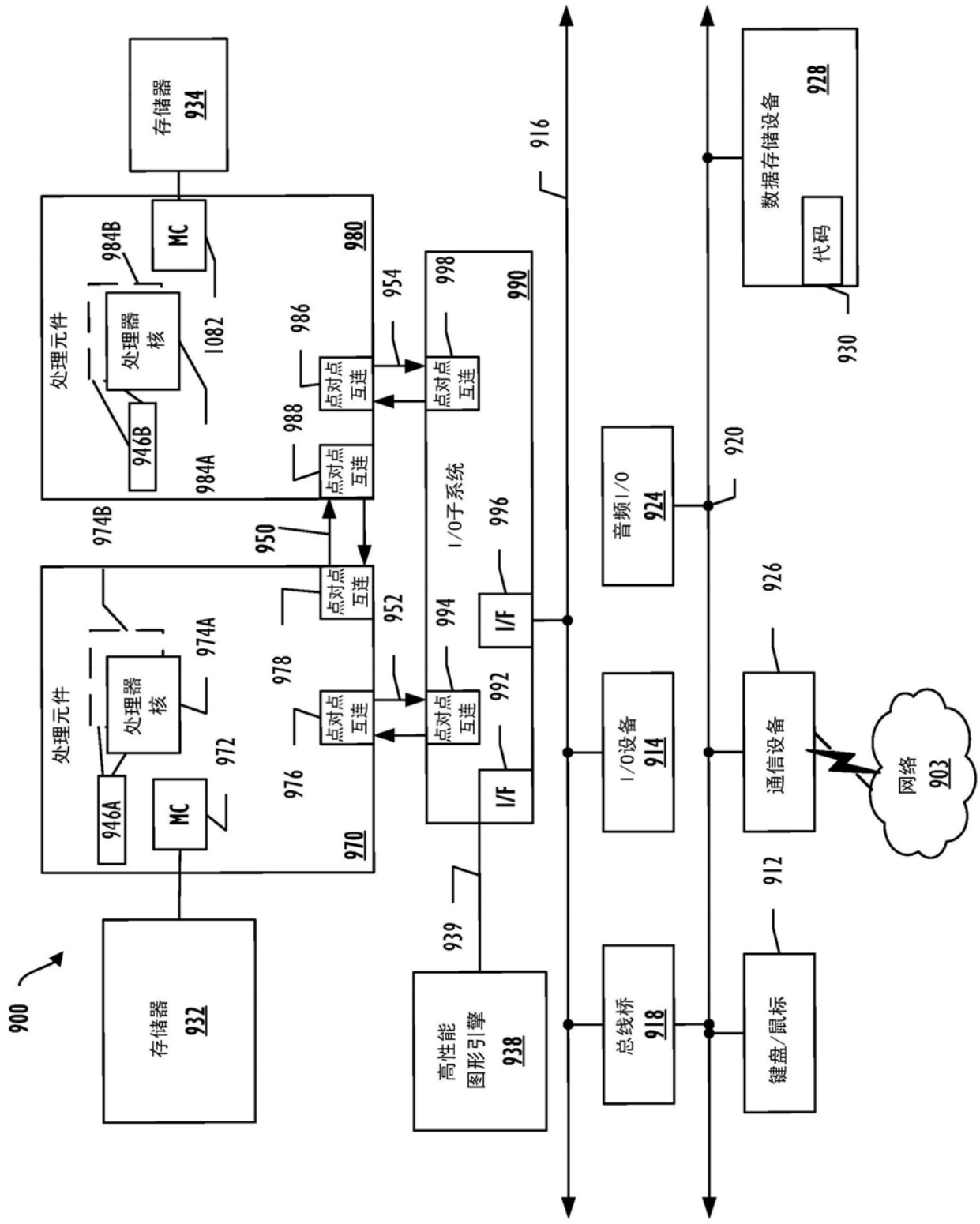

900
存储器 932
处理元件 970
处理器核 972
MC 974A
946A
处理元件 980
处理器核 1082
MC 984B
946B 984A
点对点互连 950
点对点互连 952
点对点互连 954
点对点互连 976
点对点互连 978
点对点互连 986
点对点互连 988
I/O子系统 990
I/F 992
I/F 994
点对点互连 996
点对点互连 998
存储器 934
高性能图形引擎 938
939
916
总线桥 918
I/O设备 914
音频I/O 924
920
数据存储设备 928
代码 930
通信设备 926
网络 903
键盘/鼠标 912

图9

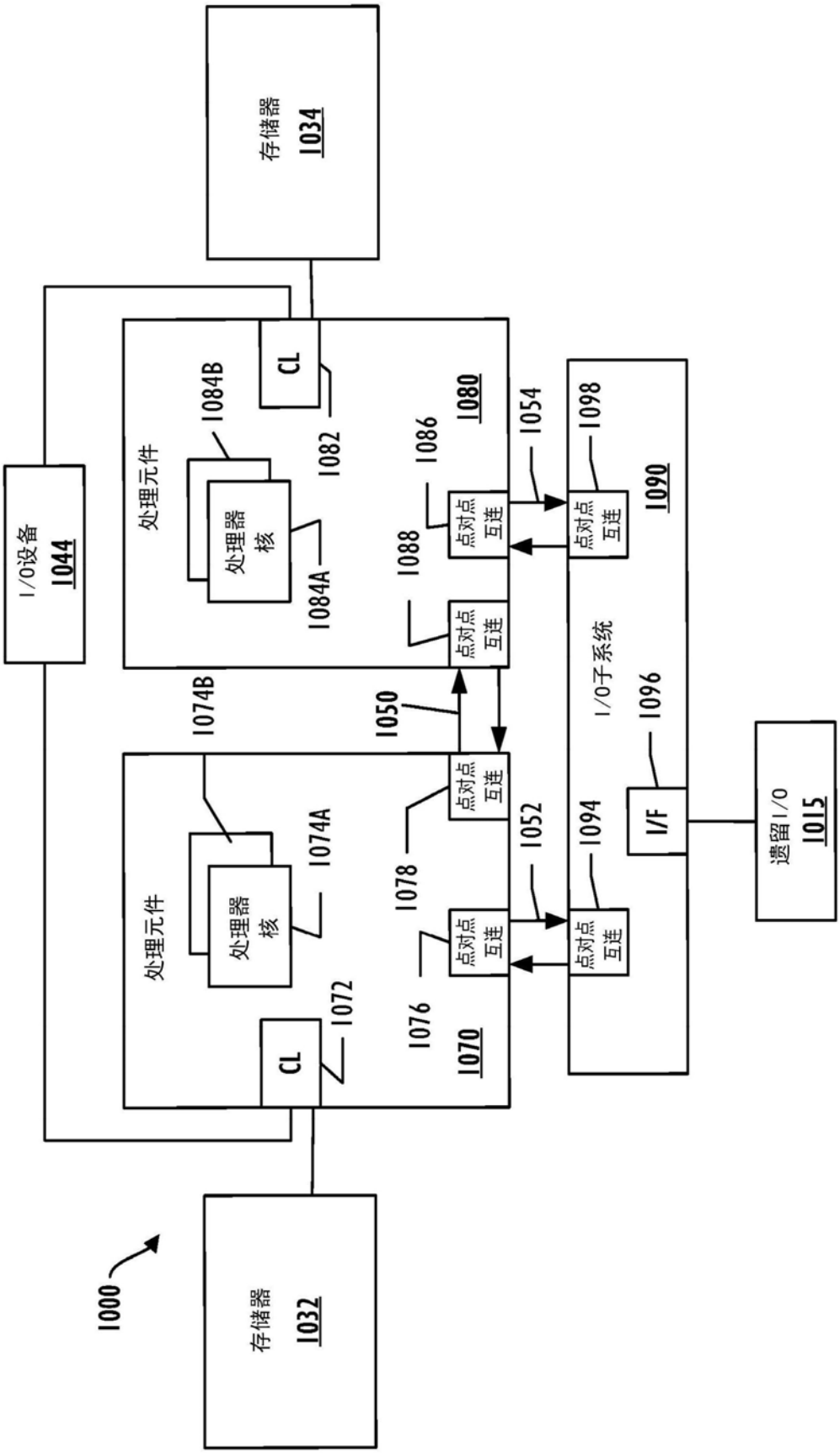

存储器
1034
CL
1082
处理元件
1084B
处理器核
1084A
1080
1086
点对点互连
1088
点对点互连
1054
1098
点对点互连
1090
I/O子系统
1096
I/F
遗留I/O
1015
1094
点对点互连
1052
1078
点对点互连
1074B
1050
点对点互连
处理元件
1074A
处理器核
1072
CL
1076
1070
I/O设备
1044
1000
存储器
1032

图10

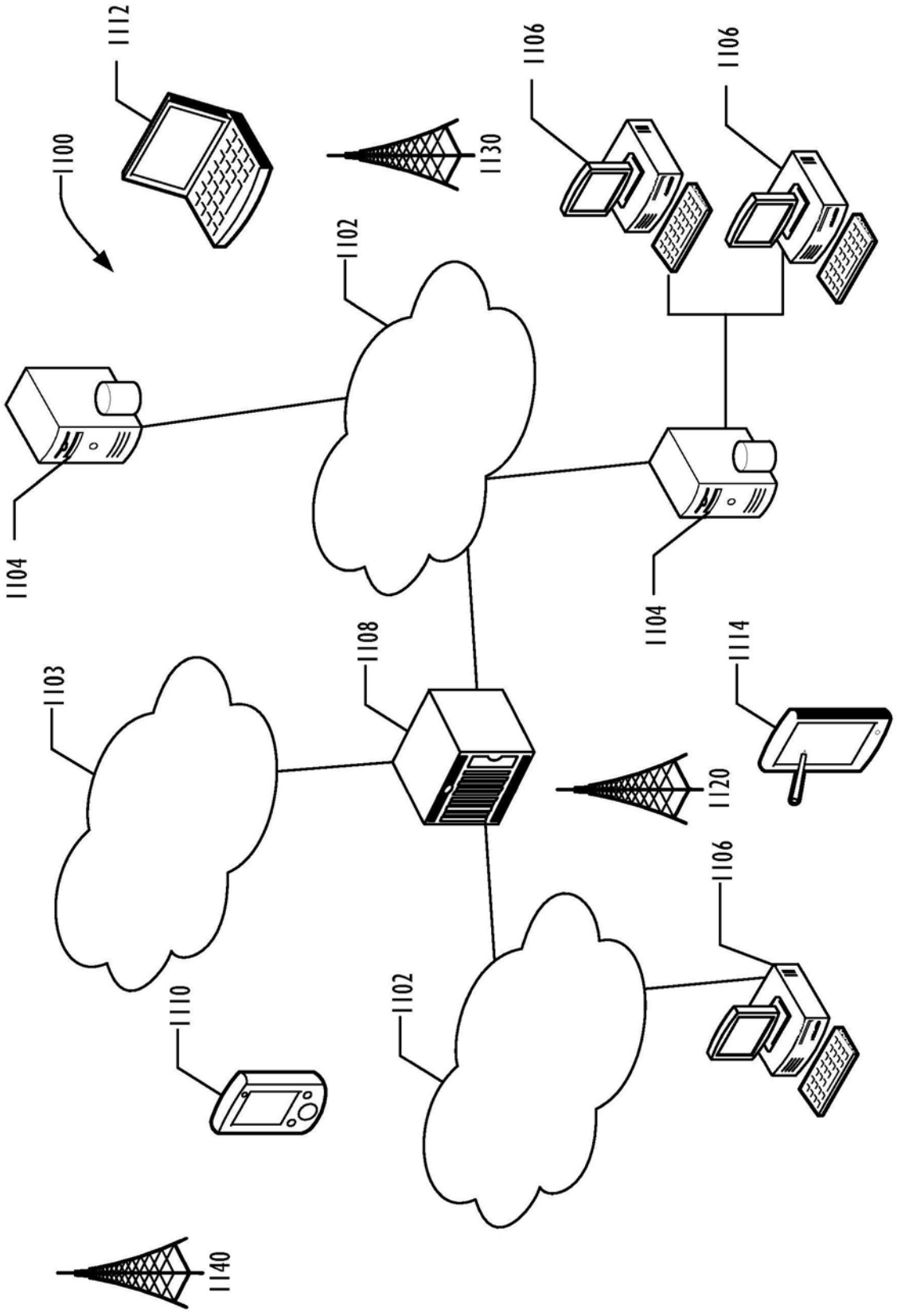

1112
1106
1106
1100
1130
1102
1104
1104
1108
1103
1114
1120
1106
1102
1110
1140

图11