(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 105556891 A
(43)申请公布日 2016.05.04

(21)申请号 201480034146.6
(22)申请日 2014.06.12
(30)优先权数据
61/835,538 2013.06.15 US
14/016,237 2013.09.03 US
(85)PCT国际申请进入国家阶段日
2015.12.15
(86)PCT国际申请的申请数据
PCT/US2014/042024 2014.06.12
(87)PCT国际申请的公布数据
WO2014/201192 EN 2014.12.18
(71)申请人 微软技术许可有限责任公司
地址 美国华盛顿州
(72)发明人 S·玛尼 W·D·泰勒
H·阿布埃-富图 T·C·迈伦
M·D·萨塔戈潘
(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 胡利鸣
(51)Int.Cl.
H04L 9/32(2006.01)
H04L 29/06(2006.01)

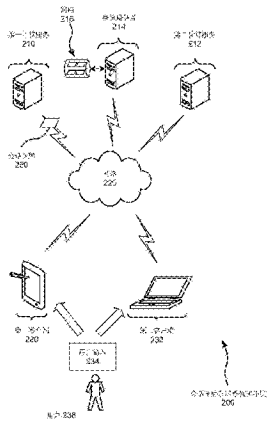
权利要求书2页 说明书13页 附图7页

(54)发明名称

通过被动客户端发送会话令牌

(57)摘要

会话令牌可被请求从第二计算服务发送到第一计算服务，并且第一计算服务可接收来自第二计算服务的所请求的会话令牌。第一计算服务可通过被动客户端向第二计算服务发送包括该会话令牌的消息。第二计算服务可接收包括来自被动客户端的会话令牌的消息，并且第二计算服务可验证该消息是有效的。这个对该消息的有效性的验证可包括验证从被动客户端接收回的会话令牌匹配第二计算服务发送到第一计算服务的会话令牌。



CN 105556891 A

1.一种计算机实现的方法,包括:

请求要从第二计算服务发送到第一计算服务的证明令牌;

所述第一计算服务接收来自所述第二计算服务的证明密钥以及所请求的证明令牌;以及

所述第一计算服务通过被动客户端向所述第二计算服务发送包括所述证明令牌的消息。

2.如权利要求1所述的方法,其特征在于,所述方法进一步包括所述第一计算服务用所述证明密钥来对一组附加数据进行签名并将该组附加数据包括在所述包括所述证明令牌的消息中。

3.如权利要求2所述的方法,其特征在于,该组附加数据包括简档身份令牌,所述简档身份令牌指示与所述被动客户端相关联的所标识的简档被授权使用所述第一计算服务。

4.如权利要求1所述的方法,其特征在于,进一步包括:

授权第一简档来使用所述第一计算服务;以及

所述第一计算服务接收使用所述第二计算服务的请求,所述使用所述第二计算服务的请求是从所述被动客户端接收的,所述被动客户端与所述第一简档相关联,并且所述第一计算服务向所述第二计算服务请求所述证明令牌是响应于所述第一计算服务接收所述使用所述第二计算服务的请求来执行的。

5.如权利要求4所述的方法,其特征在于,所述第一计算服务授权所述第一简档来使用所述第一计算服务包括所述第一计算服务使用提供与所述第一计算服务分开的服务的身份来认证所述第一简档。

6.如权利要求1所述的方法,其特征在于,所述被动客户端在所述第一计算服务和所述第二计算服务的远程。

7.如权利要求1所述的方法,其特征在于,所述被动客户端是浏览器客户端。

8.如权利要求1所述的方法,其特征在于,所述方法至少部分地由硬件逻辑执行。

9.一种计算机系统,包括:

至少一个处理器;以及

包括存储于其上的指令的存储器,所述指令在由所述至少一个处理器执行时致使所述至少一个处理器执行以下动作:

将第一会话令牌从第二计算服务发送到第一计算服务;

所述第二计算服务接收来自被动客户端的包括声称匹配所述第一会话令牌的第二会话令牌的消息,所述消息指示简档被授权来使用所述第一计算服务;

所述第二计算服务验证所述消息是有效的,并且验证所述消息是有效的包括验证所述第二会话令牌匹配所述第一会话令牌;以及

响应于所述第二计算服务验证所述消息是有效的,所述第二计算服务授权对应于所述简档的身份来使用所述第二计算服务。

10.一种或多种其上包含有计算机可执行指令的计算机可读存储介质,所述计算机可执行指令在由至少一个处理器执行时使至少一个处理器执行以下动作,包括:

第一计算服务向第二计算服务请求证明令牌;

所述第一计算服务从所述第二计算服务接收所请求的证明令牌和证明密钥,所述证明

令牌对所述第一计算服务是不透明的；

所述第一计算服务用所述证明密钥来对一组附加数据进行签名，该组附加数据包括指示与被动浏览器客户端相关联的所标识的简档被授权来使用所述第一计算服务的简档身份令牌；

所述第一计算服务将经签名的该组附加数据和所述证明令牌包括在消息中；以及

所述第一计算服务在计算机网络上并通过所述被动浏览器客户端将所述消息发送到所述第二计算服务，通过所述被动浏览器客户端发送所述消息包括所述第一计算服务向所述被动浏览器客户端标识所述第二计算服务并指令所述被动浏览器客户端将所述消息发送到所述第二计算服务。

通过被动客户端发送会话令牌

[0001] 背景

[0002] 在线计算服务经常在计算机网络上与客户端(诸如远程客户端)通信。如本文中使用的,计算服务是在主机上运行的计算组件(诸如计算机应用),该主机包括一个或多个计算机器并针对一个或多个本地和/或远程客户端执行动作。在一些实例中,第一计算服务向客户端发送重定向消息,从而指令客户端重定向到另一计算服务。这样的重定向消息可包括客户端要向第二计算服务发送的信息。

[0003] 有时,这样的重定向消息被用于指令被动客户端与要求认证的第二计算服务通信。在这样的情况下,用户输入被要求来登录到第二计算服务,即使用户输入已经被提供来登录到发送重定向消息的第一计算服务。

[0004] 概述

[0005] 本文中讨论的各工具和技术涉及将会话令牌从第一计算服务发送到第一计算服务从其获得该会话令牌的第二计算服务。会话令牌是包括足够的信息以供会话令牌的发送者(诸如第二计算服务)在该令牌被返回到该发送者时验证该令牌匹配并且没有被篡改的令牌。会话令牌可通过被动客户端来发送,诸如第一计算服务在会话令牌被发送之前与其通信的并且第二计算服务在会话令牌被发送之后与其通信的被动客户端。如本文中使用的,被动客户端是缺乏作出其自己的关于客户端要将会话令牌发送到哪个特定计算实体或哪些特定计算实体的合乎逻辑的判定的能力的普通计算机客户端。相反,被动客户端盲目地转发会话令牌(在被动客户端被明确指令这么做的情况下),诸如在被动客户端被第一计算服务指令来将会话令牌转发到第二计算服务的情况下(例如,在第二计算服务被标识在来自第一计算服务的重定向消息中的情况下)。例如,被动客户端可以是在移动设备(例如,智能手机)、平板设备或台式设备(例如,膝上型计算机或台式计算机)上运行的被动客户端,诸如移动应用、移动浏览器客户端、平板浏览器客户端、平板应用、台式应用和/或台式浏览器客户端。

[0006] 在一个实施例中,各工具和技术可包括请求要从第二计算服务发送到第一计算服务的会话令牌,以及第一计算服务接收来自第二计算服务的所请求的会话令牌。第一计算服务可通过被动客户端向第二计算服务发送包括该会话令牌的消息。

[0007] 在各工具和技术的另一实施例中,第一会话令牌可从第二计算服务发送到第一计算服务。第二计算服务可从被动客户端接收包括声称匹配第一会话令牌的第二会话令牌的消息。第二计算服务可验证该消息是有效的,其可包括验证第二会话令牌匹配第一会话令牌。如本文中使用的,会话令牌匹配指会话令牌相互对应,使得第二令牌没有以不想要的方式被修改。例如,在一些技术中,两个会话令牌在它们相互相同的情况下匹配。

[0008] 提供本概述是为了以简化的形式介绍一些概念。这些概念将在以下详细描述中进一步描述。本发明内容并不旨在标识所要求保护主题的关键特征或必要特征,也不旨在用于限制所要求保护主题的范围。类似地,本发明不限于解决在背景、详细描述、或附图中讨论的专用技术、工具、环境、缺点、或优点的实现。

[0009] 附图简述

[0010] 图1是其中可实现所描述的各实施例中的一个或多个实施例的合适的计算环境的框图。

[0011] 图2是用于通过被动客户端跨各服务发送会话令牌的环境的示意图。

[0012] 图3是描绘用于通过被动客户端在各服务之间委派用户身份的示例证明令牌方式的调用流的调用流图。

[0013] 图4是可与图3的方法一起使用的浏览器显示示例的说明。

[0014] 图5是描绘用于通过被动客户端在各服务之间在会话令牌中安全地发送信息的方式的调用流图。

[0015] 图6是示出用于通过被动客户端发送会话令牌的技术的流程图。

[0016] 图7是示出用于通过被动客户端发送会话令牌的另一技术的流程图。

[0017] 图8是示出用于通过被动客户端发送会话令牌的又一技术的流程图。

[0018] 详细描述

[0019] 本文描述的各实施例涉及用于计算服务之间通信的技术和工具。这样的改进可源于分开或组合地使用各种技术和工具。

[0020] 这样的技术和工具可包括将会话令牌返回给第二服务的第一服务，该令牌由第一服务从第二服务接收。会话令牌可以是第二服务对第一服务和被动客户端保留的秘密，其中该令牌通过该被动客户端返回给第二服务。例如，会话令牌可被加密，使得会话令牌对于第一服务和对于被动客户端而言是不透明的，但可由第二服务解密和处理。会话令牌可通过被动客户端返回。这样的工具和技术可被用于允许第一计算服务安全地将信息发送到第二计算服务，即使被动客户端不被信任。例如，要被发送的信息可被包括在会话令牌中。作为一个示例，会话令牌可以是证明令牌，其可与证明密钥一起被发送到第一计算服务。如本文中使用的，证明令牌是与证明密钥一起提供的令牌，其可被用于对附加信息进行签名。证明令牌、证明密钥以及用证明密钥来签名的信息提供了一个指示，即经签名的信息来自于第二计算服务将证明令牌和证明密钥提供给的第一计算服务。因此，第一计算服务可用该证明密钥来对附加信息进行签名。第一计算服务可通过被动客户端将用该证明密钥来签名的附加信息发送到第二计算服务。这可允许第二计算服务以被动客户端发起与第二计算服务的通信的方式来接收来自被动客户端的附加信息。浏览器和第二计算服务此后可在客户端－服务器配置(诸如计算机网络(诸如全球计算机网络)上的Web浏览器和Web服务配置)中继续通信。

[0021] 在本文中讨论的各工具和技术的一实现的一个示例中，两个受信任的服务可在计算机网络(诸如因特网)上通过被动客户端(例如，没有插件或被具体指引来处理身份委派场景的其他代码的Web浏览器)安全地委派身份(诸如用户和/或应用身份)。

[0022] 由此，从此处描述的工具和技术中可以实现一个或多个实质的益处。例如，本文中的各工具和技术可允许两个服务通过被动客户端安全地通信，即使该客户端和这样的通信通过其来传递的网络是不安全或不受信任的的。作为一个示例，这样的通信可包括将身份从一个服务委派到另一个的信息。这可提供效率，避免了诸如在认证用户输入已经被匹配身份(诸如与匹配第二计算服务的第二简档的第一计算服务的第一简档相关联)在第一计算服务上提供时用于在第二计算服务处认证的用户输入的必要。附加地，通过以上讨论的证明令牌示例，只要证明令牌和证明密钥可被从第二服务发送到第一服务一次，则证明令

牌和密钥就可被使用多次来通过一个或多个被动客户端将多个安全消息从第一计算服务发送到第二计算服务。通过避免针对每个要通过被动客户端从第一计算服务发送到第二计算服务的新消息来将新的令牌从第二计算服务发送到第一计算服务，这可提供附加的效率。

[0023] 所附权利要求中定义的主题不必限于此处描述的益处。本发明的专用实现可提供本文描述的益处的全部、一些、或未提供本文描述的益处。尽管本文出于呈现的目的以专用的顺序次序描述了用于各种技术的操作，但应理解除非要求专用的排序，否则这种描述方式涵盖了操作顺序上的重新安排。例如，在某些情况下，可以重新安排或并发执行顺序地描述的操作。此外，为了简单起见，流程图可能未示出可结合其他技术来使用专用技术的各种方式。

[0024] 在此描述的技术可被用于在此描述的一个或多个系统和/或用于一个或多个其他系统。例如，在此描述的各种过程可用硬件或软件、或两者的组合来实现。例如，以下参考图1讨论的处理器、存储器、存储、输出设备、输入设备和/或通信连接中的每一个可以是一个或多个硬件组件的至少一部分。专用硬件逻辑组件可被构建以实现在此描述的一个或多个技术的至少一部分。例如，但非限制，这样的硬件逻辑组件包括现场可编程门阵列(FPGA)、程序专用的集成电路(ASIC)、程序专用的标准产品(ASSP)、片上系统(SOC)、复杂可编程逻辑器件(CPLD)等。可包括各实施例的装置和系统的应用可广泛地包括各种电子和计算机系统。可使用具有相关的控制和数据信号的两个或更多个内联硬件模块或装置或作为应用专用的集成电路的一部分来实现各技术，其中控制和数据信号可在模块之间并通过模块进行通信。此外，在此描述的各技术可由计算机系统可执行的软件程序来实现。作为一个示例，实现可包括分布的处理、组件/对象分布的处理、以及平行处理。此外，虚拟计算机系统进程可被构建以实现在此描述的一个或多个技术或功能。例如，本文中讨论的计算服务、身份提供者以及客户端可被实现为硬件逻辑和/或实现为在硬件组件上运行的软件，诸如以下讨论的类型的组件。

[0025] I.示例性计算环境

[0026] 图1示出其中可实现所描述的各实施例中的一个或多个的合适的计算环境(100)的通用示例。例如，一个或多个这样的计算环境可被用作第一计算服务和/或第二计算服务、身份提供者和/或用作主控被动客户端的计算机器。一般而言，可使用各种不同的通用或专用计算系统配置。适用于此处所描述的工具和技术的公知计算系统配置的示例包括，但不限于，服务器场和服务器群集、个人计算机、服务器计算机、智能电话、膝上型设备、平板设备、游戏控制台、多处理器系统、基于微处理器的系统、可编程消费电子产品、网络PC、小型机、大型计算机、包括上述系统或设备中的任一个的分布式计算环境等。

[0027] 计算环境(100)不旨在对本发明的使用范围或功能提出任何限制，因为本发明可以在完全不同的通用或专用计算环境中实现。

[0028] 参考图1，将讨论各种示出的基于硬件的计算机组件。如将讨论的，这些硬件组件可存储和/或执行软件。计算环境(100)包括至少一个处理单元或处理器(110)和存储器(120)。在图1中，这一最基本的配置(130)被包括在虚线内。处理单元(110)执行计算机可执行指令，并且可以是真实或虚拟处理器。在多处理系统中，多个处理单元执行计算机可执行指令以提高处理能力。存储器(120)可以是易失性存储器(例如，寄存器、高速缓存、RAM)、非

易失性存储器(例如,ROM、EEPROM、闪存)或两者的某一组合。存储器(120)存储实现通过被动客户端发送会话令牌的软件(180)。作为软件(180)的替代或补充,通过被动客户端发送会话令牌的实现可涉及嵌入在硬件逻辑中的处理器(110)和存储器(120)的动作的全部或部分。

[0029] 尽管为了清楚起见用线条示出了图1的各框,但是,实际上,描绘各组件并不是那样清楚,并且用比喻方法,图1以及下文讨论的其他附图的线条更精确地将是灰色的和模糊的。例如,可以将诸如显示设备等呈现组件认为是I/O组件(例如,如果显示设备包括触摸屏)。而且,处理器也具有存储器。发明人关于此点认识到,这是本领域的特性,并且重申,图1的图示只是例示可结合本发明的一个或多个实施例来使用的示例性计算设备。诸如"工作站"、"服务器"、"膝上型计算机"、"手持式设备"等分类之间没有区别,它们全部都被认为是在图1的范围之内的并且被称为"计算机"、"计算环境"、或"计算设备"。

[0030] 计算环境(100)可具有附加特征。在图1中,计算环境(100)包括存储(140)、一个或多个输入设备(150)、一个或多个输出设备(160)以及一个或多个通信连接(170)。诸如总线、控制器或网络等互连机制(未示出)将计算环境(100)的各组件互连。通常,操作系统软件(未示出)为在计算环境(100)中执行的其他软件提供了操作环境,并协调计算环境(100)的组件的活动。

[0031] 存储(140)可以是可移动或不可移动的,并可包括诸如闪存驱动器、磁盘、磁带或磁带盒、CD-ROM、CD-RW、DVD之类的计算机可读存储介质,或者可用于储存信息并可在计算环境(100)内访问的任何其它介质。存储(140)存储用于软件(180)的指令。

[0032] 输入设备(150)可以是各种不同输入设备的一个或多个。例如,输入设备(150)可包括诸如鼠标、键盘、轨迹球等的用户设备。输入设备(150)可实现一个或多个自然用户界面技术,诸如语音识别、触摸和指示笔识别、与输入设备(150)接触和邻近该输入设备(150)的姿势的识别、头和眼睛跟踪、语音和话音识别、感测用户脑部活动(例如,使用EEG和相关方法)以及机器智能(例如,使用及其智能来理解用户意图和目的)。作为其它示例,输入设备(150)可包括扫描设备;网络适配器;CD/DVD读取器;或向计算环境(100)提供输入另一设备。输出设备(160)可以是显示器、打印机、扬声器、CD/DVD刻录机、网络适配器、或从计算环境(100)提供输出的另一设备。输入设备(150)和输出设备(160)可被结合在单个系统或设备中,诸如触摸屏或虚拟现实系统。

[0033] (诸)通信连接(170)允许通过通信介质与另一计算实体通信。此外,计算环境(100)的各组件的功能可被实现在单个计算机器中或能够通过通信连接通信的多个计算机器中。因此,计算环境(100)可使用通往诸如手持计算设备、个人计算机、服务器、路由器、网络PC、对等设备或另一常见网络节点等一个或多个远程计算设备的逻辑连接而工作在联网环境中。通信介质传达诸如数据或计算机可执行指令之类的信息、或者已调数据信号形式的请求。

[0034] 已调制数据信号是使其一个或多个特征以在信号中编码信息的方式设置或改变的信号。作为示例而非局限,通信介质包括以电、光、RF、红外、声学或其他载波实现的有线或无线技术。

[0035] 可在可以是存储介质或通信介质的计算机可读介质的一般上下文中描述这些工具和技术。计算机可读存储介质可以是可在计算环境内访问的任何可用存储介质,但是术

语计算机可读存储介质不指传播的信号本身。作为示例而非限制，结合计算环境(100)，计算机可读介质包括存储器(120)、存储(140)、和以上的组合。

[0036] 这些工具和技术可在诸如程序模块中所包括的、在目标真实或虚拟处理器上的计算环境中执行的计算机可执行指令的一般上下文中描述。一般而言，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、库、对象、类、组件、数据结构等。如各实施例中所描述的，这些程序模块的功能可以被组合，或者在这些程序模块之间拆分。用于程序模块的计算机可执行指令可以在本地或分布式计算环境中执行。在分布式计算环境中，程序模块可位于本地和远程计算机存储介质两者中。

[0037] 出于说明的目的，具体实施方式使用了如“确定”、“发送”、“接收”和“操作”等术语来描述计算环境中的计算机操作。这些以及其他类似术语是对计算机执行的操作的高层抽象，并且不应混淆于人类执行的动作，除非明确指出人类(诸如“用户”)的动作执行。对应于这些术语的实际的计算机操作取决于实现而不同。

[0038] II.会话令牌发送系统和环境

[0039] 图2是结合使用其可实现所描述的各实施例中的一个或多个实施例的环境(200)的示意图。环境(200)可包括第一计算服务(210)以及不同于该第一计算服务(210)的第二计算服务(212)。计算服务(210和212)可在计算机连接上诸如向本地客户端(例如，其中一个或两个服务(210和212)在同一机器上作为服务)或向远程客户端提供服务。例如，计算服务(210和212)可以是在全球计算机网络(诸如因特网)上与被动客户端通信的基于Web的服务。这种基于Web的服务可包括电子邮件服务、日历服务、社交联网服务、金融支付和/或帐户管理服务、文字处理服务、电子表格服务、数据存储和/或分享服务等。由此，本文中所讨论的在不同的计算服务之间和/或在一个或多个计算服务和被动客户端之间发送的消息中的每一个可在全球计算机网络(诸如因特网)上被发送。第一和第二计算服务(210和212)可具有分开的认证机制。服务(210和212)的标识可由单个身份提供者(214)管理(如图2中示出的)，或由多个身份提供者管理，诸如针对每个服务(210和212)的单个身份提供者。身份提供者(214)可管理简档(216)，其是表示诸如能够访问一个或多个计算服务的一个或多个用户或一个或多个应用之类的实体的数据单元，该实体的身份(即，可被用于授权使用对应的服务的对应的简档(216)的身份)由身份提供者(214)管理。计算服务(210和212)以及身份提供者(214)可被托管在相互远离的一个或多个机器上，或它们可相互地位于本地。例如，第一计算服务(210)和第二计算服务(212)可被托管在同一数据中心中的不同的机器上、被托管在不同数据中心中的机器上、或甚至被托管在同一机器上。每个计算服务(210和212)可被托管在一个机器或多个机器上。

[0040] 第一计算服务(210)、第二计算服务(212)和身份提供者(214)可被连接来通过一个或多个连接(诸如计算机网络(220))相互通信和/或与其他计算实体通信。计算服务(210和212)和身份提供者(214)也可被连接来与一个或多个客户端(诸如第一客户端(230)和第二客户端(232))通信。简档(216)可表示与客户端(230和/或232)中的一个或多个相关联的身份，其中身份可以是一个或多个用户、应用、主机或设备的身份。第一客户端(230)和第二客户端(232)可运行在不同的客户端设备上或运行在同一客户端设备上。客户端设备可接收来自一个或多个用户(236)的用户输入(234)并可将用户输入(234)传递到对应的客户端(230或232)。例如，这样的用户输入(234)可由用户(236)以触摸输入、鼠标点击、键盘输入、

非接触手势(手部运动等)或某个其他类型的用户输入的形式来发起。

[0041] 在图2中示出的示例中,第一客户端(230)、第二客户端(232)、第一计算服务(210)、第二计算服务(212)、以及身份提供者(214)可全部被连接来通过单个网络(220)(诸如因特网)通信。除了或替代于通用网络(220),客户端(230和232)、计算服务(210和212)以及身份提供者(214)可被连接到一个或多个其他网络。例如,第一计算服务(210)、第二计算服务(212)和身份提供者(214)可全部被连接来通过专用网络(例如,安全专用网络)相互通信,该专用网络不利用通过其计算服务(210和212)和身份提供者(214)与客户端(230和232)通信的公共网络(220)。网络(220)可包括网络硬件,诸如附加的计算机器、路由器、交换机、有线通信线、无线通信设备等。

[0042] 因此,数据(诸如会话令牌(250))可在不同的计算组件(210、214、212、230和232)之间被传递并可被那些计算组件(210、214、212、230和232)以各种方式来处理,诸如以下讨论的示例。

[0043] III.通过被动客户端发送会话令牌的示例方法和使用

[0044] 现在将讨论用于通过被动客户端发送会话令牌的方法以及对其使用的一些示例。也可在本文所讨论的工具和技术的范围内实现其他替换的方法和使用。

[0045] A.用于通过被动客户端在各服务之间委派用户身份的证明令牌方法

[0046] 本章节中讨论的示例方法可被用于两个服务来以安全的方式在浏览器客户端上通知用户身份。该方法将参考图3中示出的示例调用流来讨论,该示例调用流示出客户端(302)、第一计算服务(304)、第二计算服务(306)和身份提供者(308)之间的通信。作为一个示例,joe@contoso.com可以是订阅第一计算服务(304)并可被授权来使用第一计算服务的简档的名称,并还可以是订阅第二计算服务(306)并可被授权来使用第二计算服务(306)的简档的名称。例如,第一计算服务(304)可以是电子邮件和日历安排Web服务,并且第二计算服务(306)可以是文件存储和共享Web服务。身份提供者(308)可以是管理具有被授权来使用计算服务(304和306)的许可的简档的身份的身份提供者。替代地,每个分开的计算服务(304和306)可担当其自己的身份提供者和/或使用不同的身份提供者。客户端(302)可以是可以与计算服务(304和306)以及身份提供者(308)通信的被动客户端。例如,客户端(302)可以是在客户端计算设备(诸如个人计算机、膝上型计算机、平板计算机或智能手机)上运行的标准Web浏览器。

[0047] 在图3的示例中,各计算组件(302、304、306和308)之间的通信可以是在计算机网络上发送的通信。例如,通信可以被格式化为通过一个或多个计算机网络(诸如因特网)在TCP/IP上发送的HTTP消息。在其他示例中,通信可被不同地格式化,诸如在计算机器内(例如,在不同的计算服务(302和304)驻留在同一计算机器上的情况下)的应用编程接口调用、或根据某个其他通信协议来格式化的消息。

[0048] 依然参考图3,客户端(302)可接收选择第一计算服务(304)的用户输入(未显示)。客户端(302)可通过向第一计算服务(304)发送对该第一计算服务(304)的选择(310)来对这样的用户输入进行响应。第一计算服务(304)可用重定向消息(315)来进行响应,该重定向消息可指令客户端(302)向身份提供者(308)发送标识请求(320)。

[0049] 响应于接收来自客户端(302)的标识请求(320),身份提供者(308)可用认证信息请求(325)来进行响应。例如,认证信息请求(325)可包括客户端(302)可显示来接收具有认

证信息(例如,用户名和口令)的用户输入的登录页。如被认证信息请求(325)指令的并且响应于这样的用户输入,客户端(302)可向身份提供者(308)发送认证信息(330)。身份提供者(308)可验证认证信息与订阅来使用第一服务(304)的简档的存储的认证信息相匹配。如果是,则身份提供者(308)可用认证令牌(335)以及指令客户端(302)将认证令牌转发到第一服务(304)的重定向消息来对客户端(302)进行响应。

[0050] 客户端(302)可通过将认证令牌(335)发送到第一服务(304)来进行响应。第一服务(304)可通过以下方式来进行响应:验证认证令牌(335)是有效的,并且如果是,则提供响应(380),其可揭示相关联的简档被授权来使用第一服务(304)。例如,在该响应(380)中,第一服务(304)可提供列出由第一服务(304)所提供的特征的网页。简档可被登录到由相关联的承租人向第一服务(304)的订阅所定义的领域上。例如,如果简档的名称是joe@contoso.com,则领域可以是与"contoso.com"相关联的领域,并且可以存在与contoso.com领域相关联的一个或多个订阅。这可允许简档使用由第一服务(304)提供的与该领域相关联的特征(例如,访问由contoso.com领域的其他用户简档提供的文件)。当简档被登录到第一服务(304)时,第一服务(304)和/或身份提供者(308)可维护与简档相关联的标识符,诸如"个人唯一标识符"(PUID)。

[0051] 在用户简档使用第一服务(304)时,可在客户端(302)处提供选择第二服务(306)的用户输入。例如,用户输入可通过选择由第一服务(304)提供的网页内的链接来提供。参考图3-4,浏览器显示(400)的示例被示出在图4中,诸如其中被动客户端(302)是Web浏览器。浏览器显示(400)特征化接收自第一服务(304)的页(例如,HTML页或具有某个其他格式的页)的网页显示(410)的示例,诸如在图3的响应(380)中。示例网页显示(410)包括由第一服务(304)提供的特征列表,其被选择来调用这些特征。对于示出的示例,这些特征包括电子邮件特征、日历特征、任务特征、联系人特征以及帐户管理特征。附加地,网页显示(410)包括用于选择第二服务(306)的链接(420),该第二服务是示出的示例中的文件共享服务。用户输入可被提供来选择第二服务链接(420),诸如通过触摸触摸屏上的链接。

[0052] 参考图3,响应于被用户输入选择的第二服务(306),根据被包括在来自第一服务(304)的响应中的指令(例如,在网页中),客户端(302)可向第一服务(304)发送第二服务选择(350)。响应于第二服务选择(350),第一服务(304)可作出对第二服务(306)的服务到服务调用。这个服务到服务调用可包括服务到服务令牌(352)并可请求证明令牌。服务到服务令牌(352)可能已经由第一服务(304)从另一源获得,诸如从身份提供者(308)。响应于接收来自第一服务(304)的服务到服务令牌(352),第二服务(306)可验证该服务到服务令牌(352)以验证该消息来自第一服务(304)。服务到服务令牌(352)可在包括第一服务(304)和第二服务(306)在内的服务池的生命周期期间仅被从第一服务(304)发送到第二服务(306)一次,即使第一服务(304)作出对第二服务(306)的多次服务到服务调用。作为一个示例,可向第二服务(306)的API(例如,名为"GetProofToken()(取得证明令牌())"的API)作出用于请求证明令牌的服务到服务调用。

[0053] 第二服务(306)可通过生成证明令牌(360)和证明密钥(365)并将该证明令牌(360)和该证明密钥(365)发送到第一服务(304)来对该服务到服务调用进行响应。例如,响应可包括可包含证明令牌(360)和证明密钥(365)的Java脚本对象记法(JSON)对象,诸如具有以下格式:(1)proof_token(证明_令牌):证明令牌(360),其对第一服务(304)而言可以

是不透明的，诸如加密值；(2)exp：证明令牌的期满；以及(3)证明密钥(365)，其可以是明文、base64编码密钥。证明密钥(365)可以是在被发送之前由第二服务(306)使用将允许第一服务(304)解密证明密钥(365)的各种不同加密方案中的任一种来加密的对称密钥。替代地，非对称密钥对可被使用，其中证明密钥(365)是公共密钥，其可在不加密的情况下被发送。包括证明令牌(360)和证明密钥(365)的对象可由第二服务(306)签名。例如，第二服务(306)可使用256位RSA密钥或某个其他签名方案来对该对象签名。

[0054] 在接收证明令牌(360)和证明密钥(365)之际，第一服务(304)可确保包括证明令牌(360)和证明密钥(365)的对象的签名是有效的，并且可解密证明密钥(365)。第一服务可包括具有证明令牌(360)的附加信息，并可用证明密钥(365)来对该附加信息签名以产生经签名的信息(370)。例如，第一服务可生成要作为附加的经签名的信息(370)被包括的用户身份令牌。

[0055] 在一个示例中，用户身份令牌可包括以下特征：(1)令牌格式：JWT(JSONWeb令牌)；(2)签名：SHA-256，其可以是以下类型的签名：与证明密钥一起使用来对身份令牌签名；以及(3)声明。以下表格列出一些可被包括在用户身份令牌的示例中的声明：

[0056]

声明	使用	样本值
aud	令牌的受众	0003/contoso-appweb1.firstservice.com@123-456-677
upn	用户的用户主名称	joe@contoso.com
nameid	用户的 PUID	1234567890
nii	NameId 颁发者	urn:servicegroup:federation
nbf	起始时间：何时令牌开始有效	
exp	令牌的期满	
smtp	用户的 SMTP 主电子邮件	joe@contoso.com
sip	用户的 SIP 地址	
iss	令牌的颁发者	
isuser	标识主题简档是否是用户简档，如与应用简档相比等。	

[0057] nameid、upn、smtp或sip声明中的一个或多个可被用于标识作为令牌的主题的简档。如果简档作为匿名用户被登录到第一服务(304)，则nameid声明可以是指示这个事实的一般值，诸如特定符号(例如，“@”符号)。

[0058] 第一服务(304)可向客户端(302)发送包括经签名的附加信息(370)(例如，用户身

份令牌)和证明令牌(360)的消息以及将该消息转发到第二服务(306)(例如,作为重定向消息)的指令。这个消息的主体可包括针对用户身份令牌的字段以及针对证明令牌的字段。

[0059] 以下是证明令牌和身份令牌的内容的一个示例,但是可以使用针对这种内容的各种不同格式中的任一种,其中各字段如在以上被讨论,并且"alg"字段是签名算法标识字段,"x5t"字段包括证明密钥,并且"prf"字段包括证明令牌:

[0060]

Proof Token contents(证明令牌内容)

{

"typ":JWT

"alg":RS256

"x5t":CC-CF-D8-41-0F-A0-17-DD-91-EC-AA-AB-CB-95-4F-DE-94-E1-4C-ED

}

{

"aud":0002/*.firstservice.com@*

"iss":0003@1234-2232

"nbf": 1366053429

"exp":2013-04-16 19:17:09Z (4/16/2013 12:17:09 PM) - 1366139829

"prf":wd4eXqy5qtxH9TzwG4dDnt5EvTTsn+v25EzeZcN7sV3dTc/rldNYInv9CFgi+IQg3LnXTlxc5xz1c/cKswzt4+dKU3wGSK8jnUTKAF/rStNs75wo+VreX/pLpUtZ9KYYKpkdfOo01Deofz23LGoe4eMTe7DeQ88dcZWWi+fpYz6yAbtRXJCMfCqck5ypj9TcJG7AZEGADr4tc5ZF8Nu+b/xqKMG9aZb7LyGlpPZqKfSPfCuRfcmHlV2SbmESPMflYRtrUgK27fBVZS4szJEXBKnFz4ccNnqct8L5ITy14ir03vMh3NdEfB8vuwZpN6QIwrkDj21hkafXsAR1KObSvw==

}

Identity Token contents(身份令牌内容)

[0061]

```
{
    "typ":JWT
    "alg":HS256
}
{
    "aud":0002/secondservice.com@1234-2232
    "iss":0003@1234-2232
    "nbf":2013-04-15 19:17:09Z (4/15/2013 12:17:09 PM) -
1366053429
    "exp":2013-04-16 19:17:09Z (4/16/2013 12:17:09 PM) -
1366139829
    "upn":"foo@contoso.com"
    "nameid":1234567890
    "nii":urn:servicegroup:federation
    "smtp":"fooSMTP@contoso.com"
    "sip":"cfooSip@contoso.com"
    "isuser":true
}
```

[0062] 如指令的，客户端(302)可将具有证明令牌(360)和经签名的附加信息(370)的消息发送到第二服务(306)。作为响应，第二服务(306)可解析并证实在该消息中接收到的信息。例如，第二服务(306)可执行以下：(1)证实证明令牌的签名；(2)解密证明令牌；(3)证实证明令牌的期满；(4)从证明令牌中提取对称密钥；(5)使用该对称密钥来证实用户身份令牌上的签名；(6)验证用户身份令牌的期满；以及(7)证实受众(“aud”)声明，诸如其中格式是<app-id>/<hostname>@<realm(领域)>并且预期值是：<app-id>＝＝第二服务的主id；<hostname>＝＝该令牌被发送到的URL的主机名；并且<realm>＝＝当前第一服务承租人的ID(如果存在的话，其可被证实)。

[0063] 第二服务(306)可使用身份令牌中的信息来执行到第二服务的对应简档的映射，使得第二服务的简档可被授权来使用第二服务(306)。例如，第二服务(306)可执行以下：

[0064] 如果nameid存在则检查nii值，如果nii值匹配urn:servicegroup:federation值(指示联合服务组的值)，则nameid中的值是用户的PUID。针对用户简档的第二服务的数据库来尝试映射nameid。

[0065] 如果没有找到这样的映射，则从令牌中取得smtp声明(如果存在的话)。针对用户简档的第二服务的数据库来尝试映射smtp声明。

[0066] 如果smtp声明没被找到并且如果upn存在，则作出对身份提供者(308)的调用来取

得简档的电子邮件别名。如果它们中没有一者映射到用户简档的第二服务的数据库，则通过客户端(302)来提示用户。

[0067] 只要在第二服务(306)中找到对现有简档的映射，则将简档的PUID添加到第二服务(306)的映射表，并向客户端(302)发送显示该主题简档被授权使用第二服务(306)的响应。例如，响应(380)可包括发送包括和/或列出由第二服务(306)提供的特征的网页。这样的网页可被客户端(302)显示。

[0068] B.用于通过被动客户端在各服务之间在会话令牌中安全地发送信息的方法

[0069] 本章节中讨论的示例方法可被用于通过被动客户端在两个服务之间在会话令牌中安全地发送信息。参考图5的调用流程图，这个方法涉及客户端(502)、第一服务(504)和第二服务(506)之间的通信。除非在本章节中另外说明，各通信的格式可与如在先前章节中讨论的方法中的格式相同、或某个其他格式。在该示例中，第二服务选择(550)可由客户端(502)发送到第一服务(504)。例如，客户端(502)可响应于由客户端(502)的用户提供的用户输入来发送第二服务选择(550)。替代地，这个方法可在第一服务(504)没有从客户端(502)接收到这一第二服务选择(550)的情况下被执行。第一服务(504)可向第二服务发送会话令牌请求(555)。例如，会话令牌请求(555)可标识要通过客户端(502)从第一服务(504)发送到第二服务(506)的信息。例如，会话令牌请求可标识被授权来使用第一服务(504)并且其身份要被委派到第二服务(506)的用户简档，使得针对第二服务的对应的用户简档(或同一用户简档)也可被授权来使用第二服务(506)。

[0070] 作为响应，第二服务可将所请求的信息包括在会话令牌(560)中，并可加密该会话令牌(560)。具有该信息的会话令牌(560)可从第二服务(506)发送到第一服务(504)。第一服务(504)可将会话令牌(560)以及将会话令牌(560)转发到第二服务(506)的指令转发到客户端(502)(例如，通过包括具有重定向消息的会话令牌)。客户端(502)可通过将会话令牌(560)如指令的那样转发到第二服务(506)来对这些指令进行响应。第二服务(506)可处理会话令牌(560)，并可向客户端(502)提供响应(580)。

[0071] 本文中讨论的方法的多个不同的变型可被使用。例如，会话令牌可被用于通过被动客户端在各服务之间传递除了身份委派信息之外的信息。并且，各种不同的加密方案、签名方案等可被用于确保所发送的信息在各服务之间没有在途中被篡改和/或这样的篡改可被检测。

[0072] IV.用于通过被动客户端发送会话令牌的技术

[0073] 现在将讨论用于通过被动客户端发送会话令牌的若干技术。可以在计算环境中执行这些技术中的每一个。例如，可在包括至少一个处理器和存储器的计算机系统中执行每种技术，该存储器包括存储于其上的、在由该至少一个处理器执行时使该至少一个处理器执行该技术的指令(存储器存储指令(例如，对象代码)，并且当处理器执行这些指令时，处理器执行该技术)。类似地，一个或多个计算机可读存储介质可具有收录于其上的计算机可执行指令，该些指令在由至少一个处理器执行时使该至少一个处理器执行该技术。以下讨论的技术可至少部分通过硬件逻辑来执行。

[0074] 参考图6，将讨论用于通过被动客户端来发送会话令牌的技术。该技术可包括第一计算服务向第二计算服务请求(610)会话令牌。第一计算服务可从第二计算服务接收(620)所请求的会话令牌。第一计算服务可通过被动客户端向第二计算服务发送(630)包括该会

话令牌的消息。

[0075] 该会话令牌可以是证明令牌，并且第一计算服务也可接收具有证明令牌的证明密钥。该技术还可包括第一计算服务用证明密钥来对一组附加数据进行签名并将该组附加数据包括在包括证明令牌的消息中。该组附加数据可被称为第一组附加数据并且包括证明令牌的消息可被称为第一消息。该技术还可包括第一计算服务用证明令牌来对第二组附加数据进行签名。该技术还可包括将该第二组附加数据包括在第二消息中。第二消息可包括证明令牌。第二消息可通过被动客户端(通过其第一消息被发送的同一被动客户端或与通过其第一消息被发送的被动客户端不同的被动客户端)被发送到第二计算服务。第一和/或第二组附加数据可包括指示与被动客户端相关联的所标识的简档被授权使用第一计算服务的简档身份令牌。

[0076] 图6的技术还可包括授权第一简档来使用第一计算服务，以及第一计算服务接收使用第二计算服务的请求。可接收到来自被动客户端的使用第二计算服务的请求，并且被动客户端可与第一简档相关联。第一计算服务向第二计算服务请求会话令牌可响应于第一计算服务接收使用第二计算服务的请求来完成。第一计算服务授权第一简档来使用第一计算服务可包括第一计算服务使用与第一计算服务分开的身份提供服务来认证第一简档。例如，该授权可包括第一计算服务将被动客户端重定向到身份提供服务。作为另一示例，该授权可包括第一计算服务编程地调用身份提供服务。

[0077] 被动客户端可以在第一计算服务的远程。在一个示例中，被动客户端可以是浏览器客户端，诸如在网络(诸如全球计算机网络)上与第一计算服务和第二计算服务交互的Web浏览器客户端。

[0078] 参考图7，将讨论用于通过被动客户端来发送会话令牌的另一技术。该技术包括将第一会话令牌从第二计算服务发送(710)到第一计算服务。第二计算服务可从被动客户端接收(720)包括声称匹配第一会话令牌的第二会话令牌的消息。第二计算服务可验证(730)该消息是有效的，其可包括验证第二会话令牌匹配第一会话令牌，诸如验证第二会话令牌与第一会话令牌相同。

[0079] 该消息可指示简档(诸如用户简档或应用简档)被授权来使用第一计算服务。图7的技术还可包括，响应于第二计算服务验证该消息是有效的，第二计算服务授权对应于该简档的身份来使用第二计算服务(例如，通过授权相同的简档来使用第二计算服务和/或授权不同的对应简档来使用第二计算服务)。经认证的消息可包括第二计算服务可用于第二计算服务的内部授权技术的身份信息。因此，第二计算服务可在授予对所标识的简档的访问之前执行分开的内部授权。例如，这可包括通过确保这样的订阅当前是活动且有效的等来将简档中的信息映射到为对第二计算服务的订阅维护的简档信息。

[0080] 在图7的技术中，被动客户端可以在第一计算服务和第二计算服务的远程。被动客户端可以是浏览器客户端，诸如Web浏览器客户端。

[0081] 图7的第一会话令牌可以是第一证明令牌，第二会话令牌可以是第二证明令牌，并且第二计算服务可发送具有第一证明令牌的证明密钥。图7的包括第二证明令牌的消息还可包括被包括在从第二计算服务到第一计算服务的第一证明令牌的发送中的一组附加数据。验证该消息是有效的可包括验证该组附加数据是用证明密钥来签名的。

[0082] 该组附加数据可被称为第一组附加数据并且包括第二证明令牌的消息可被称为

第一消息。该技术还可包括第二计算服务接收包括第二组数据和第三证明令牌的第二消息。第二计算服务可验证第二消息是有效的，其可包括验证第三证明令牌匹配第一证明令牌以及第二组附加数据是用证明密钥来签名的。

[0083] 第一会话令牌从第二计算服务到第一计算服务的发送可包括将第一会话令牌从第二计算服务发送到第一计算服务，而无需将会话令牌引导通过被动客户端。

[0084] 现在参考图8，将讨论用于通过被动客户端来发送会话令牌的又一技术。该技术可包括第一计算服务向第二计算服务请求(810)证明令牌。第一计算服务可从第二计算服务接收(820)所请求的证明令牌和证明密钥。证明令牌对于第一计算服务可以是不透明的。第一计算服务可用证明密钥来对一组附加数据进行签名(830)，其中该组附加数据包括指示与被动客户端相关联的所标识的简档被授权来使用第一计算服务的简档身份令牌。第一计算服务可将经签名的该组附加数据包括(840)在消息中。第一计算服务可在计算机网络上并通过被动客户端向第二计算服务发送(850)包括该消息。该消息通过被动浏览器的发送(850)可包括第一计算服务向被动浏览器标识第二计算服务并指令被动浏览器将该消息发送到第二计算服务，诸如通过向被动浏览器发送标识第二计算服务的重定向消息。

[0085] 以上讨论的各技术可提供各种益处，诸如允许信息(诸如身份委派消息)在客户端－服务器配置内的各计算服务之间被安全且高效地传递，该客户端－服务器配置涉及发起通信的被动客户端以及对被动客户端进行响应的服务(例如，在典型的Web浏览器配置中)。尽管用结构特征和/或方法动作专用的语言描述了本主题，但可以理解，所附权利要求书中定义的主题不必限于上述具体特征或动作。更确切而言，上述具体特征和动作是作为实现权利要求的示例形式公开的。

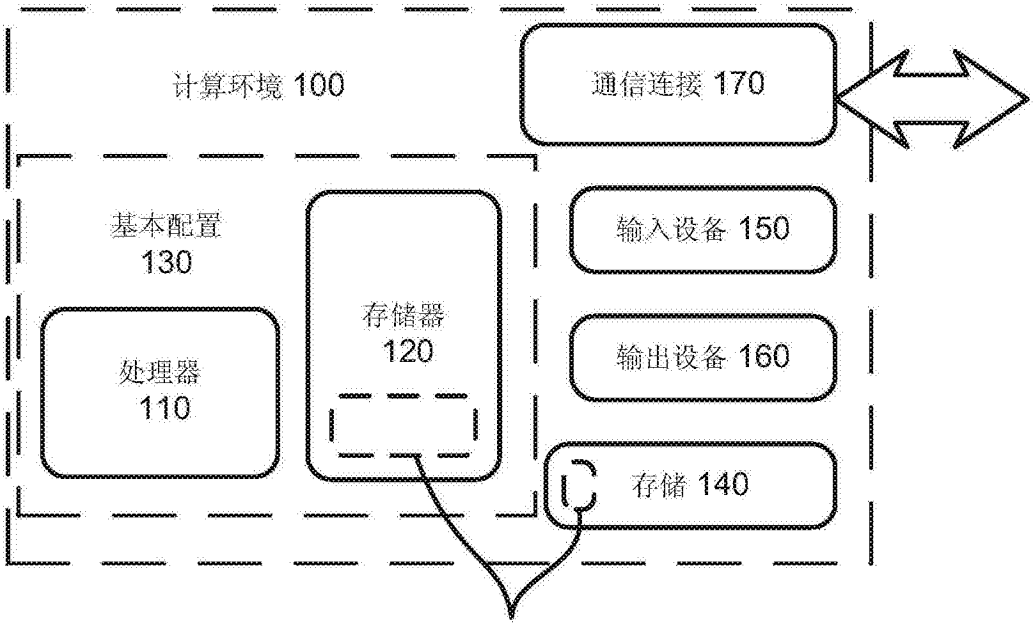

计算环境 100
通信连接 170
基本配置
130
处理器
110
存储器
120
输入设备 150
输出设备 160
存储 140
实现通过被动客户端发送会话令牌的软件180

图1

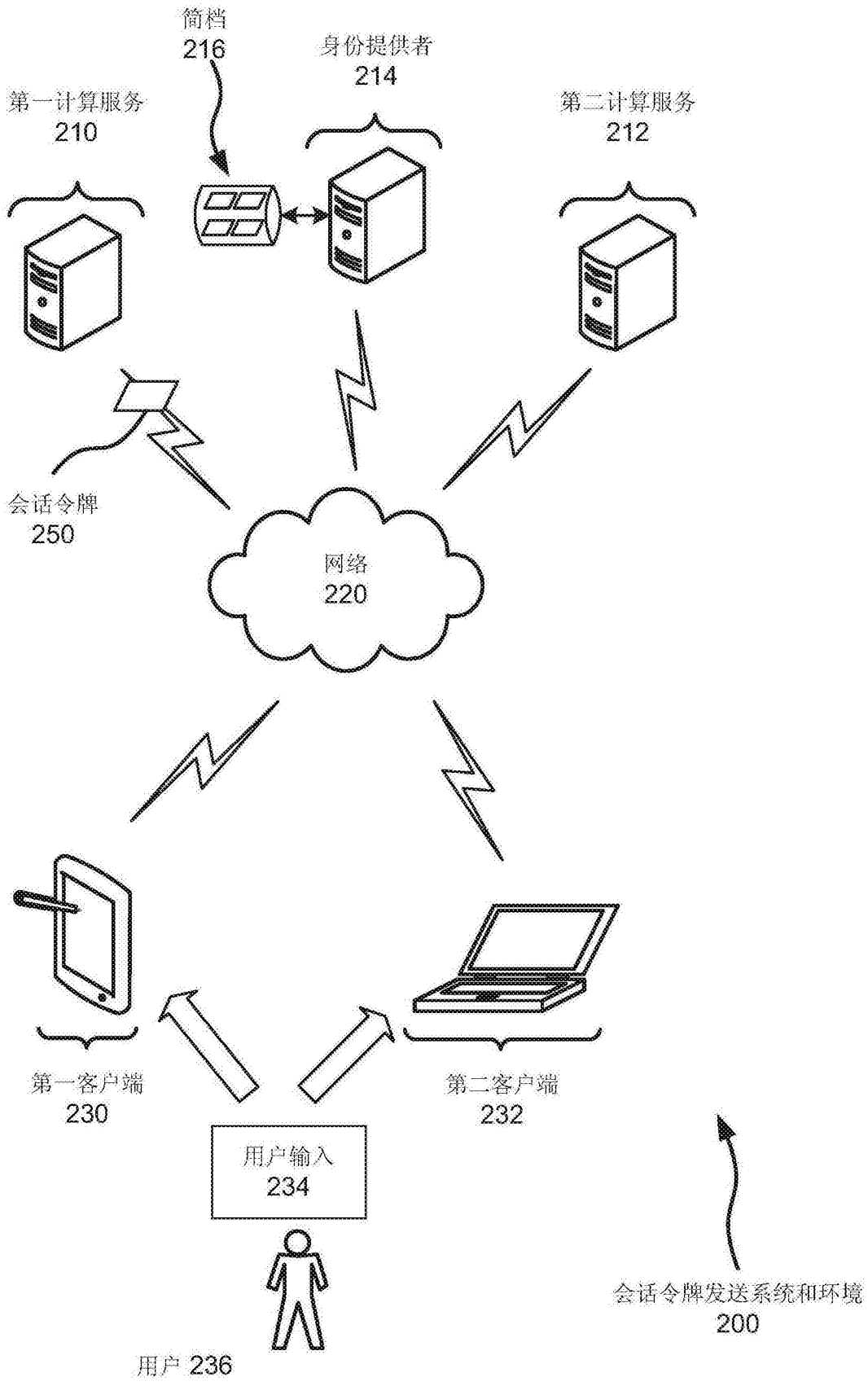

简档
216
身份提供者
214
第一计算服务
210
第二计算服务
212
会话令牌
250
网络
220
第一客户端
230
第二客户端
232
用户输入
234
用户 236
会话令牌发送系统和环境
200

图2

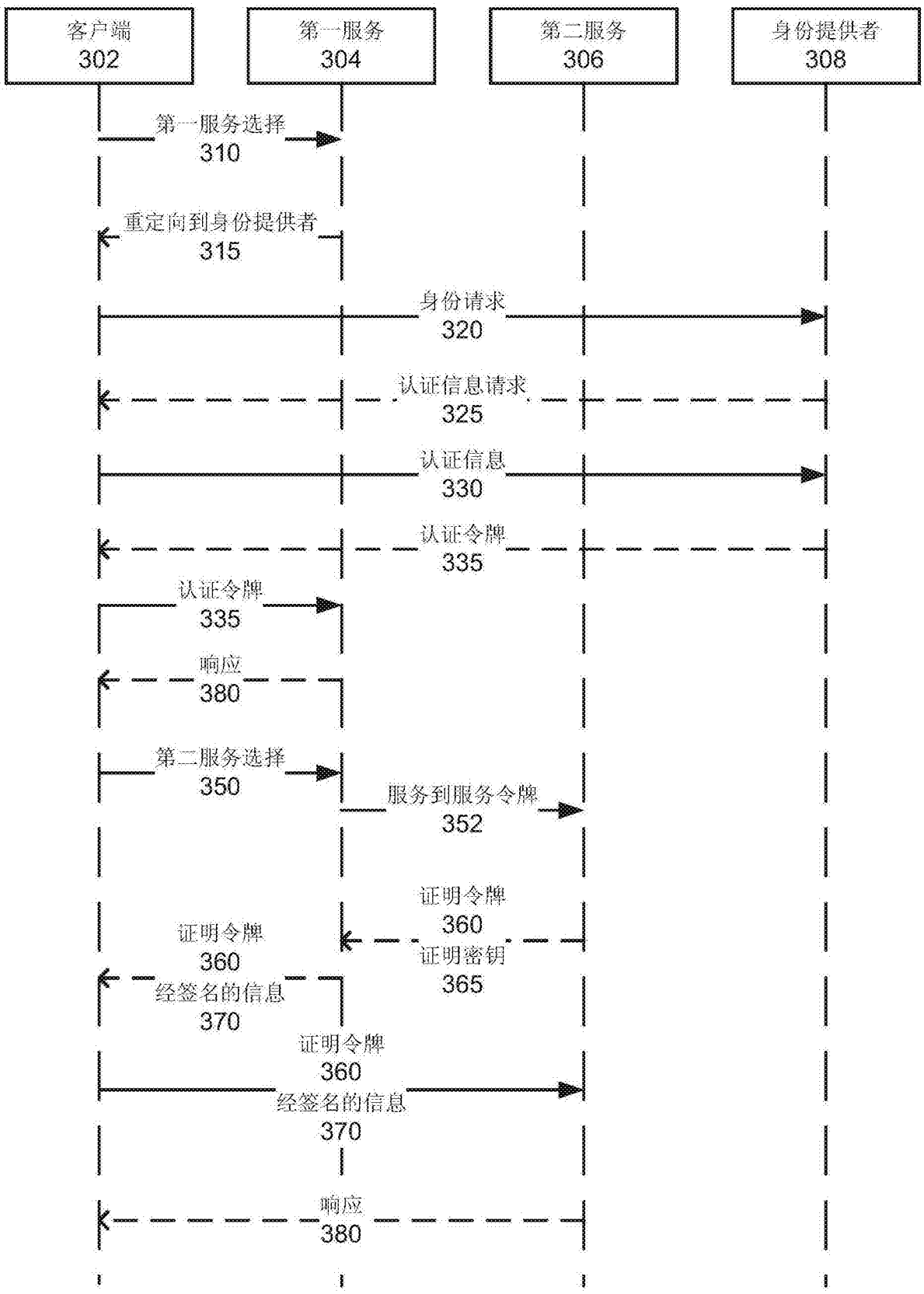

客户端
302
第一服务
304
第二服务
306
身份提供者
308
第一服务选择
310
重定向到身份提供者
315
身份请求
320
认证信息请求
325
认证信息
330
认证令牌
335
认证令牌
335
响应
380
第二服务选择
350
服务到服务令牌
352
证明令牌
360
证明密钥
365
证明令牌
360
经签名的信息
370
证明令牌
360
经签名的信息
370
响应
380

图3

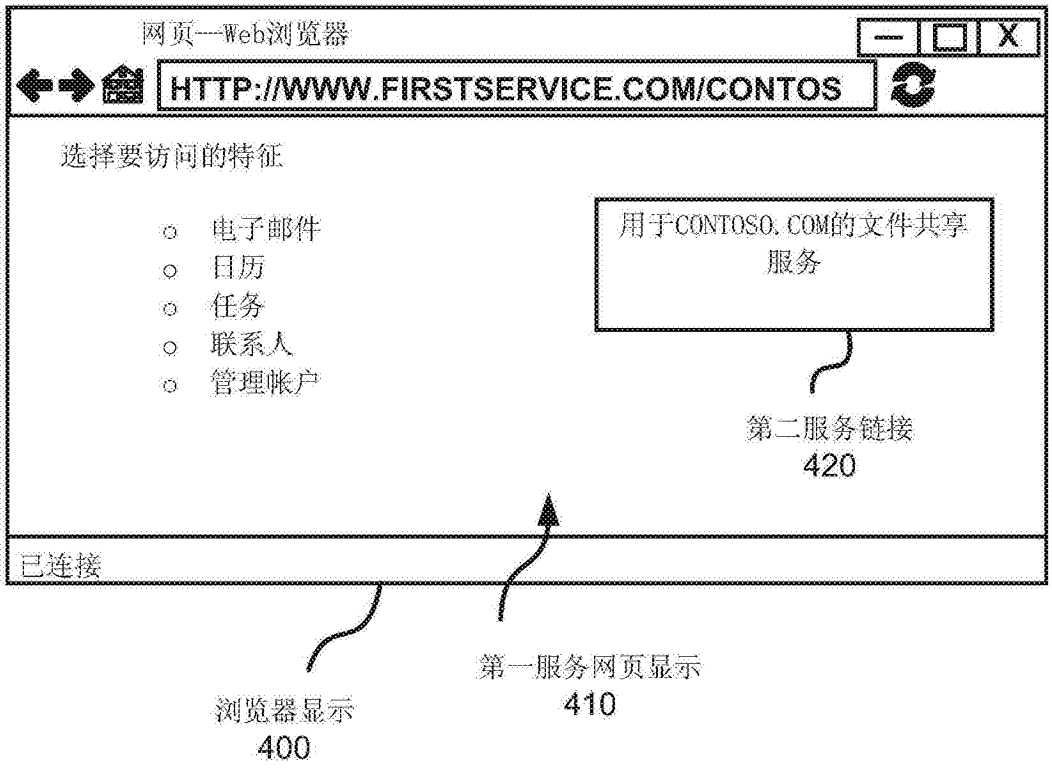

网页—Web浏览器
HTTP://WWW.FIRSTSERVICE.COM/CONTOS
选择要访问的特征
电子邮件
日历
任务
联系人
管理帐户
用于CONTOSO.COM的文件共享服务
第二服务链接
420
已连接
浏览器显示
400
第一服务网页显示
410

图4

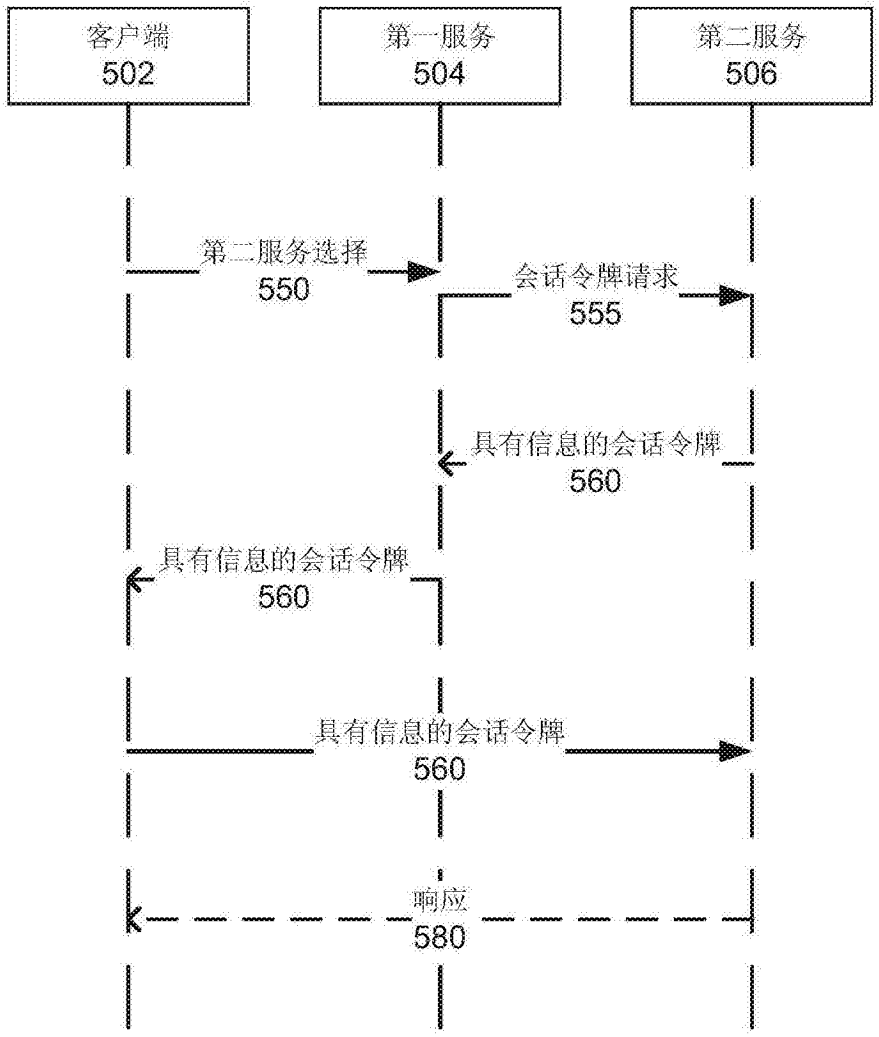

客户端
502
第一服务
504
第二服务
506
第二服务选择
550
会话令牌请求
555
具有信息的会话令牌
560
具有信息的会话令牌
560
具有信息的会话令牌
560
响应
580

图5

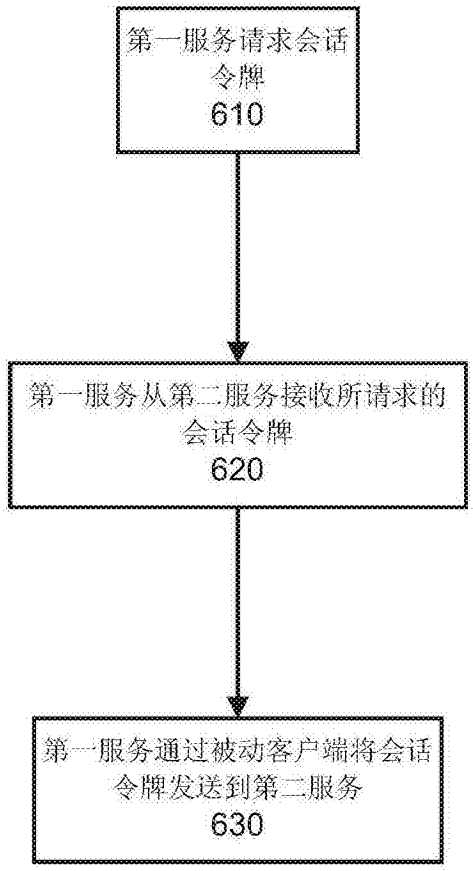

第一服务请求会话令牌
610
第一服务从第二服务接收所请求的会话令牌
620
第一服务通过被动客户端将会话令牌发送到第二服务
630

图6

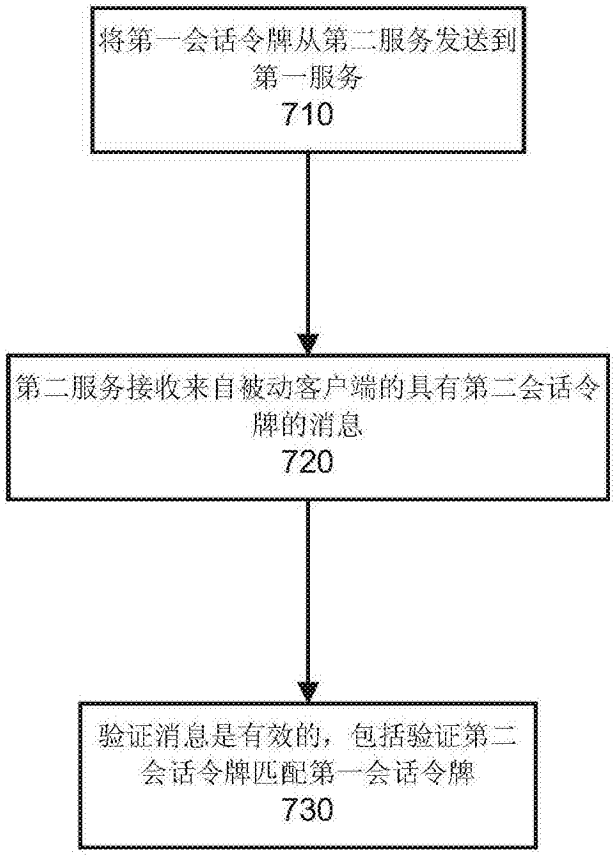

将第一会话令牌从第二服务发送到第一服务
710
第二服务接收来自被动客户端的具有第二会话令牌的消息
720
验证消息是有效的，包括验证第二会话令牌匹配第一会话令牌
730

图7

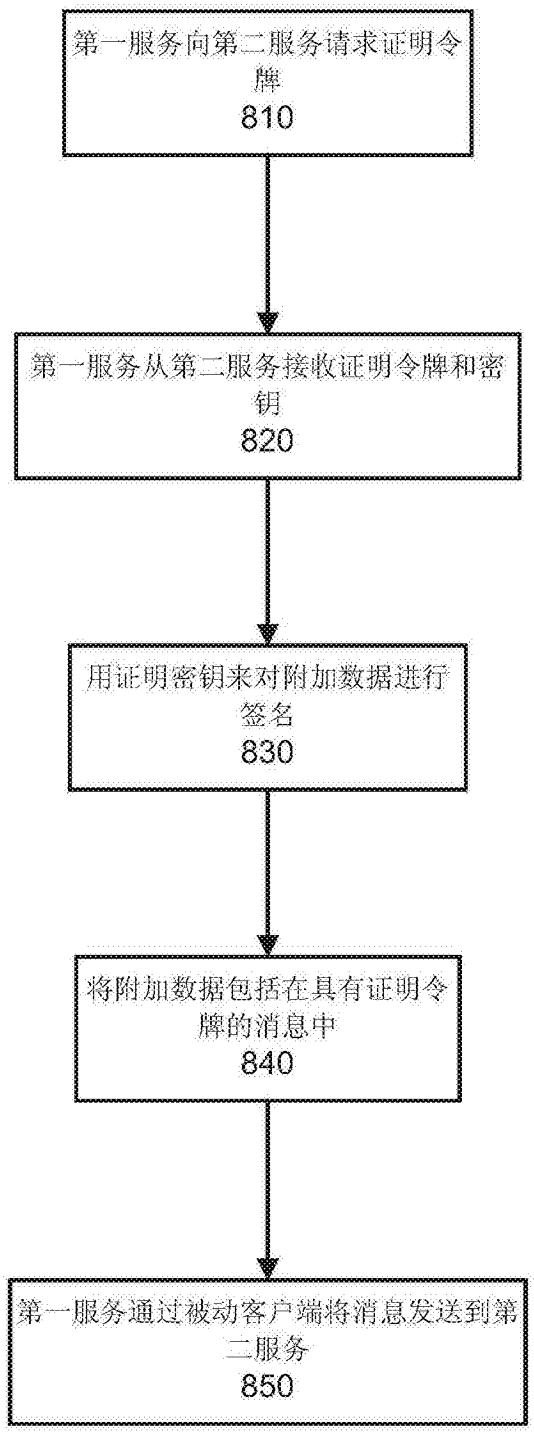

第一服务向第二服务请求证明令牌
810
第一服务从第二服务接收证明令牌和密钥
820
用证明密钥来对附加数据进行签名
830
将附加数据包括在具有证明令牌的消息中
840
第一服务通过被动客户端将消息发送到第二服务
850

图8