(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 102449976 A
(43)申请公布日 2012.05.09

(21)申请号 201080023487.5

(22)申请日 2010.05.07

(30)优先权数据
09305500.2 2009.05.29 EP

(85)PCT申请进入国家阶段日
2011.11.29

(86)PCT申请的申请数据
PCT/EP2010/056288 2010.05.07

(87)PCT申请的公布数据
WO2010/136323 EN 2010.12.02

(71)申请人 阿尔卡特朗讯公司
地址 法国巴黎

(72)发明人 B·弗兰肯 P·博施
M·斯特鲁加鲁

(74)专利代理机构 北京市中咨律师事务所 11247
代理人 杨晓光 于静

(51)Int.Cl.
H04L 29/06(2006.01)
G06F 21/00(2006.01)

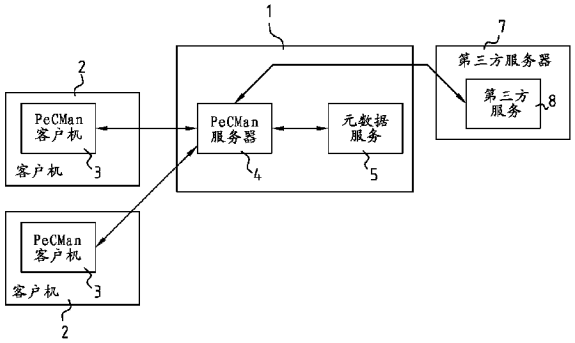
权利要求书 3 页 说明书 10 页 附图 9 页

(54)发明名称

用于访问私人数字内容的系统和方法

(57)摘要

一种用于提供访问由所有者拥有并安装在内容服务器上的私人数字内容的方法，其中内容管理服务器具有潜在地对私人内容感兴趣的多个客户机，该方法包括在内容管理服务器处执行的下列步骤：被告知所有者已经在内容服务器上安装私人内容；从内容服务器获得委托令牌；从内容管理服务器的多个客户机中的客户机接收用于私人数字内容的查询；利用使客户机能够访问私人内容的委托令牌给所述客户机提供令牌。



CN 102449976 A

1. 一种用于提供对由所有者拥有并安装在内容服务器上的私人数字内容进行访问的方法，其中内容管理服务器具有潜在地对私人内容感兴趣的多个客户机，该方法包括在内容管理服务器处执行的下列步骤：

被告知所有者已经在内容服务器上安装了私人内容 (202 ;602 ;802)；

从内容服务器获得委托令牌 (203-210)；(603-610)；(803-810)，在私人数字内容的所有者的帮助下产生委托令牌，并且将委托令牌用于代表内容所有者讲话；

从内容管理服务器的多个客户机中的一个客户机接收用于私人数字内容的查询 (300 ; 400 ;700)；

利用使客户机能够访问私人内容的委托令牌给所述客户机提供令牌 (301-303)；(407-410)；(708-710)；(901-903)。

2. 根据权利要求 1 所述的方法，其中通过内容管理服务器获得委托令牌包括：

从内容服务器获得第一令牌 (203-204)；(603-604)；(803-804)；

请求所有者对第一令牌进行授权 (205)；(605)；(805)；

接收经过授权的第一令牌 (208)；(608)；(808)；

请求通过内容服务器将经过授权的第一令牌替换为第二令牌 (209-210)；(609-610)；(809-810)，其中所述第二令牌形成委托令牌。

3. 根据权利要求 1 或 2 所述的方法，其中使用委托令牌给所述客户机提供令牌包括由内容管理服务器执行的下列步骤：

将用于把委托令牌替换为用于客户机的访问令牌的请求发送给内容服务器 (301)；(901)；

接收访问令牌 (302)；(902)；以及

将访问令牌转发给客户机 (303)；(903)。

4. 根据权利要求 1 或 2 所述的方法，其中使用委托令牌给所述客户机提供令牌包括由内容管理服务器执行的下列步骤：

从客户机接收请求令牌 (407)；(707)；

使用委托令牌对所述令牌进行授权 (408-409)；(708-709)；

将所述经过授权的请求令牌发送给客户机 (410)；(710)，以使客户机能够通过内容服务器将该经过授权的请求令牌换为访问令牌 (411-412)；(711-712)。

5. 一种用于通过内容管理服务器的客户机来获得私人数字内容的方法，其中私人内容由所有者拥有并且被安装在内容服务器上，包括由客户机执行的下列步骤：

将用于获得私人数字内容的请求发送给具有与数字私人内容相关联的委托令牌的内容管理服务器 (300)；(400)；(700)，

在私人数字内容的所有者的帮助下产生委托令牌，并且将委托令牌用于代表内容所有者讲话；

从内容管理服务器获得使用委托令牌产生的并允许客户机访问私人数字内容的令牌 (303)；(410)；(710)；

访问私人数字内容 (304-305)；(413-414)；(713-714)。

6. 根据权利要求 5 所述的方法，其中从内容管理服务器获得令牌在于获取由内容管理服务器先前基于它的委托令牌通过内容服务器获取的访问令牌 (301)；(302)。

7. 根据权利要求 5 所述的方法，其中从内容管理服务器获得令牌包括由客户机执行的下列步骤：

将用于令牌的请求发送给内容服务器 (405)；

从内容服务器接收请求令牌 (406)；

将接收的请求令牌发送给内容管理服务器以进行授权 (407)；

由内容管理服务器使用其委托令牌接收请求令牌 (408-410)；

将该经过授权的请求令牌发送给内容服务器 (411)；以及

从内容服务器接收使客户机能够访问私人内容的访问令牌 (412)。

8. 一种用于通过内容管理服务器的客户机提供对私人数字内容的访问的方法，其中私人内容由所有者拥有并且被安装在内容服务器上，包括由内容服务器处执行的下列步骤：

为内容管理服务器产生由用户授权的委托令牌 (207)，在私人数字内容的所有者的帮助下产生委托令牌，并且将委托令牌用于代表内容所有者讲话；

将所述委托令牌发送给内容管理服务器 (208)。

9. 根据前述权利要求中任意一项所述的方法，其中标准 OAuth 呼叫用于执行方法步骤。

10. 一种用于访问私人数字内容的系统，包括：

内容管理服务器 (1)；

拥有存储在内容服务器上的数字私人内容的第一客户机 (7)；

多个第二客户机 (2)；其中内容管理服务器 (1) 适于从内容服务器获得与数字私人内容相关联的委托令牌，并利用使第二客户机能够访问数字私人内容的委托令牌将令牌传递给第二客户机 (2)，在私人数字内容的所有者的帮助下产生委托令牌，并且将委托令牌用于代表内容所有者讲话；以及

第二客户机 (2) 适于将传递的令牌提供给用于获得对数字私人内容的访问的内容服务器 (7)。

11. 根据权利要求 10 所述的系统，其中第一客户机适于对通过内容服务器从内容管理服务器接收的请求令牌进行授权；并且所述内容管理服务器适于接收经过授权的请求令牌，并使用所述经过授权的请求令牌来获得委托令牌。

12. 一种用于组织多个客户机的私人数字内容的内容管理服务器 (1)，第一客户机拥有存储在内容服务器上的数字私人内容，

所述内容管理服务器适于从内容服务器获得与所有者客户机的数字私人内容相关联的委托令牌，并使用委托令牌将令牌传递给第二客户机 (12) 以使第二客户机能够访问所有者客户机的私人内容，

在私人数字内容的所有者的帮助下产生所述委托令牌，并且将所述委托令牌用于代表内容所有者讲话。

13. 根据权利要求 12 所述的内容管理服务器，其中内容管理服务器是诸如 PeCMan 服务器的内容集合器。

14. 根据权利要求 12 或 13 所述的内容管理服务器，其中内容管理服务器进一步适于将与私人内容相关的令牌提供给客户机，其中相比于委托令牌，令牌具有相同或更少的访问权利。

15. 一种包括计算机可执行指令的计算机程序产品，当程序在计算机上运行用于执行根据权利要求 1 至 9 中任一项所述的方法。

用于访问私人数字内容的系统和方法

技术领域

[0001] 本发明涉及用于访问私人 (private) 数字内容的系统和方法、内容管理服务器、安全内容服务器、和用于安全通信的方法。

背景技术

[0002] 存在开放认证 (OAuth) 协议 (见 OAuth 规范 1.0, 可从 http://oauth.net/license/core/1.0 处获得) 以处理网络上多方之间的用户凭证。此外,存在多个基于令牌的共享方案,其中共享方案能够在与上述 OAuth 系统相似的网络实体之间进行内容共享。例如,脸谱 (Facebook)、Flickr、谷歌 (Google)、Smugmug 和 Photobucket 都使用令牌进行认证。

发明内容

[0003] 根据本发明的实施方式,提供了用于共享私人内容的改进的方法和系统,其可为私人内容的所有者提供便利,并提供充分安全性。

[0004] 根据本发明的一个实施方式,提供一种用于提供对由所有者拥有且安装在内容服务器上的私人数字内容的访问的方法,其中内容管理服务器具有多个潜在地对私人内容感兴趣的客户机,该方法包括在内容管理服务器处执行的下列步骤 :

[0005] 被告知所有者已经在内容服务器上安装私人内容 ;

[0006] 从内容服务器获得委托令牌 (delegate token) ;

[0007] 从内容管理服务器的多个客户机中的一个客户机接收用于私人数字内容的查询 ;

[0008] 使用能够使客户机访问私人内容的委托令牌给所述客户机提供令牌。

[0009] 在本发明的上下文中,应当广义地将内容管理服务器理解为涉及能够管理例如多个用户的公共和 / 或私人共享的和 / 或私人不共享的诸如图像、视频等的数字内容的任何服务器。内容自身可存储在本地或存储在远程位置。这种内容管理服务器的实例是,例如由像 Flickr、TourTube 等的内容提供商、诸如 PeCMan、SecondBrain、iGoogle 的任意类型的内容集合器 (aggregator)、任意类型的所有者代理 (具有选择代理功能的代理) 等使用的简单的内容管理服务器。这样的内容管理服务器的优选实施方式可适于允许对内容作标记。

[0010] 在本发明的上下文中,内容服务器典型地涉及安全内容服务器,并且例如可以是安全网络服务器。其它实例为具有共享文件能力的本地磁盘,在其上安装服务器程序使得将计算机用作内容服务器的任意计算机等。

[0011] 在本发明的上下文中,令牌是在对令牌请求者的多个凭证 (credential) 进行验证的基础上产生的值。该值典型地是由内容服务器随机产生的多个字符的字符串。

[0012] 根据本发明的优选实施方式,在私人数字内容所有者的帮助下产生委托令牌并且委托令牌用于代表内容所有者讲话 (speak for)。通过内容管理服务器来获得委托令牌,包

括例如：

[0013] 从内容服务器获得第一令牌 T1；

[0014] 请求所有者对第一令牌进行授权 (authorize)；

[0015] 接收经过授权的第一令牌；

[0016] 请求通过内容服务器将经过授权的第一令牌替换为第二令牌 T2，其中所述第二令牌 T2 形成委托令牌。第一令牌典型地会是所谓的请求令牌，其中请求令牌是由客户机（这里是内容管理服务器）用于从所有者获得授权的值，并且可替换为典型地称为访问令牌的第二令牌，其中访问令牌是由客户机（内容管理服务器）使用以代表所有者增加对保护内容的访问，而不使用所有者的内容服务器凭证。

[0017] 根据可能的实施方式，使用委托令牌给所述客户机提供令牌包括由内容管理服务器执行的下列步骤：

[0018] 将用于把委托令牌替换为客户机访问令牌 T3 的请求发送给内容服务器；

[0019] 接收访问令牌 T3；和

[0020] 将访问令牌 T3 转发给客户机。

[0021] 相比于委托令牌允许的权利，最新创建的访问令牌 T3 典型地具有相同或较少的权利。该方法的优势是客户机不必向内容服务器注册。

[0022] 根据可替换的实施方式，使用委托令牌给所述客户机提供令牌包括由内容管理服务器执行的下列步骤：

[0023] 从客户机接收请求令牌 T4；

[0024] 使用委托令牌对所述令牌进行授权；

[0025] 将所述经过授权的请求令牌 T4 发送给客户机，能够使客户机通过内容服务器将该经过认证的请求令牌换为访问令牌。

[0026] 根据本发明的另一方面，提供一种用于通过内容管理服务器的客户机获得私人数字内容的方法，其中私人内容由所有者拥有并且私人内容被安装在内容服务器上，包括由客户机执行的下列步骤：

[0027] 将用于获得私人数字内容的请求发送给具有与数字私人内容相关联的委托令牌的内容管理服务器；

[0028] 从内容管理服务器获得使用委托令牌产生的并允许客户机访问私人数字内容的令牌；

[0029] 访问私人数字内容。

[0030] 根据第一实施例，从内容管理服务器获得令牌在于获得由内容管理服务器之前根据其委托令牌通过内容服务器已经获得的访问令牌 T3。

[0031] 根据第二实施例，从内容管理服务器获得令牌可以包括由客户机执行的下列步骤：

[0032] 将用于令牌的请求发送给内容服务器；

[0033] 从内容服务器接收请求令牌 T4；

[0034] 将接收的请求令牌发送给内容管理服务器以进行授权；

[0035] 通过内容管理服务器使用其委托令牌来接收请求令牌；

[0036] 将该经过授权的请求令牌发送给内容服务器；以及

[0037] 从内容服务器接收能够使客户机访问私人内容的访问令牌 T5。

[0038] 根据本发明的另一方面，提供一种用于提供对私人数字内容的访问的方法，其中私人数字内容由所有者拥有并且被安装在内容服务器上，所述方法包括在内容服务器执行的下列步骤：

[0039] 为内容管理服务器产生由用户授权的委托令牌；

[0040] 将所述委托令牌发送给内容管理服务器。

[0041] 根据优选实施方式，一个或多个标准的开放认证呼叫用于执行方法步骤。

[0042] 根据本发明系统的实施方式，系统包括：内容管理服务器，其具有拥有存储在内容服务器上的数字私人内容的第一客户机(primary client)；和多个第二客户机(secondary client)；其中内容管理服务器适于从内容服务器获得与数字私人内容相关联的委托令牌，并适于使用能够使第二客户机访问数字私人内容的委托令牌将令牌传递给第二客户机；以及

[0043] 第二客户机适于将传递的令牌提供给内容服务器以用于获得对数字私人内容的访问。

[0044] 根据优选实施方式，第一客户机进一步适于对通过内容服务器从内容管理服务器接收的请求令牌进行认证；所述内容管理服务器于是可以进一步适于接收经过授权的请求令牌，并使用所述经过授权的请求令牌来获得委托令牌。

[0045] 根据本发明的另一方面，提供一种用于组织多个客户机的私人数字内容的内容管理服务器，第一客户机拥有存储在内容服务器上的数字私人内容，所述内容管理服务器适于从内容服务器获得与所有者客户机的数字私人内容相关联的委托令牌，并使用委托令牌将令牌传递给第二客户机以使第二客户机能够访问所有者客户机的私人内容。根据示例性实施方式，内容管理服务器是诸如 PeCMan 服务器的内容集合器。

[0046] 根据另一开发的实施方式，内容管理服务器进一步适于将与私人内容相关的令牌提供给客户机，其中相比于委托令牌，与私人内容相关的令牌具有相同或较少的访问权利。

[0047] 根据本发明的另一方面，提供一种存储所有者的私人数字内容的诸如安全网络服务器的内容服务器，适于

[0048] 从内容管理服务器接收由所有者授权的请求令牌，

[0049] 将该经授权的请求令牌换为委托令牌，以及

[0050] 将委托令牌发送给内容管理服务器。

[0051] 最后，本发明涉及计算机程序产品，包括当程序在计算机上运行时用于执行本发明任一方法的计算机可执行指令。

[0052] 根据本发明的实施方式，提供一种开放认证协议方法，其扩展为支持将委托令牌传递给管理服务器，例如 PeCMan 服务器、用户代理或任何其它适合的实体。在私人数字内容的所有者的帮助下产生这些委托令牌，并将这些委托令牌用于代表内容所有者讲话。在这种方式下，每次第二客户机请求访问私人数字内容时，所有者不必将所有者凭证提供给私人内容网络服务器，可以由管理服务器提供委托令牌，而不必需要所有者干预。当管理服务器获得委托令牌时，所有者将仅干预一次。优势是第二客户机可以访问私人内容而不用持有所有者的用户凭证。当该方法应用于 PeCMan 中时，PeCMan 服务器不要求现有技术方法中的用于共享私人内容的代理功能。

[0053] 根据本发明的实施方式，已经利用认证委托 (delegate) 操作来扩展 OAuth 协议方法以使诸如 PeCMan 或用户代理的内容管理器能够代表内容所有者讲话。因此：当客户机在存储提供商处存储私人内容时，其安排创建进行存储的具有 URL 的长期委托令牌。如果通过内容管理器共享私人数据，该委托令牌可用于 OAuth 协议以对请求令牌进行认证。

[0054] 根据本发明的另一实施方式，提供一种持有用于私人内容的委托令牌的内容管理服务器，例如 PeCMan 服务器或用户代理。根据可能的实施方式，内容管理服务器适于对来自第二客户机的请求令牌进行授权，利用该请求令牌，所述第二客户机可访问诸如安全网站的私人内容位置上的数据，而不用再进一步牵扯所有者。

[0055] 根据本发明的一个实施方式，提供一种使用扩展的 OAuth 协议以支持将认证授权从内容所有者委托给诸如 PeCMan 服务器或用户代理的内容管理服务器的系统。更具体地，内容所有者能够将用于网络服务器认证的责任委托给内容管理服务器，从而当与朋友、伙伴、或其它有关方共享内容时，内容所有者不必对自己进行认证，并且甚至不用出现。

[0056] 根据本发明的一个实施方式，提供一种使用通过委托认证授权的过程来扩展的 OAuth 协议的方法，包括在内容所有者、私人内容服务器和内容管理服务器之间共享的委托令牌的概念。当第二客户机需要访问私人内容时，内容管理服务器可以提供其委托令牌以作为内容所有者已授权内容管理服务器代表其讲话的证据。典型地，内容管理服务器可作为原始内容所有者的代理。

[0057] 根据另一实施方式，新的 OAuth 委托机制意味着内容管理服务器可以增强其自身在内容上的访问控制策略，其中内容通过内容管理服务器进行共享。委托令牌能够以特定访问权利来访问私人共享的内容。根据可能的实施方式，内容管理服务器适于限制这些访问权利。

附图说明

[0058] 附图用于解释本发明目前优选的非限制性的示例性实施方式。通过下面的详细描述，并结合附图进行阅读，本发明的上述和其它有益特点和目标会变得更加明显并且可以更好地理解本发明，其中：

[0059] 图 1 是 PeCMan 架构的示意图；

[0060] 图 2 描述了根据本发明方法的第一实施方式的用于对 PeCMan 服务器进行委托的呼叫流程；

[0061] 图 3 描述了根据本发明方法的第一实施方式的用于通过第二 PeCMan 客户机获取私人内容的呼叫流程；

[0062] 图 4 描述了根据本发明方法的第二实施方式的用于通过第二 PeCMan 客户机获取私人内容的呼叫流程；

[0063] 图 5 描述了根据本发明方法的第三实施方式的用于获取私人内容的呼叫流程；

[0064] 图 6 描述了根据本发明方法的第二实施方式的用于对 PeCMan 服务器进行委托的呼叫流程；

[0065] 图 7 描述了根据本发明方法的第四实施方式的用于通过第二 PeCMan 客户机获取私人内容的呼叫流程；

[0066] 图 8 描述了根据本发明方法的第三实施方式的用于对 PeCMan 服务器进行委托的

呼叫流程；

[0067] 图 9 描述了根据本发明方法的第五实施方式的用于获取私人内容的呼叫流程。

[0068] 下面将个人内容管理 (PeCMan) 服务器作为内容管理服务器来解释本发明，但是本领域技术人员可以理解的是，本发明可以应用于如上定义的任意类型的内容管理服务器（包括所有者的代理）。PeCMan 是组织诸如文档、照片、视频等的用户数字内容的网络工具。图 1 示出了 PeCMan 架构的示意图。用户通过使用客户机元件 3（例如，网络客户机、桌上型客户机或 PDA 上的客户机等）与系统 1 进行交互，其中用户以可通过客户机元件 3 来增加、移动文档或给文档增加标签。服务器元件 4 接收来自客户机 2 的输入请求以由系统 1 进行处理。系统进一步包括元数据部分 5，其中元数据部分 5 用于存储从文档中提取的元数据，或存储用户以标签形式产生的元数据。服务器元件 4 可以进一步与多个第三方服务器 7 的第三方服务 8 进行通信。

[0069] 例如，用户可以在 PeCMan 中上载 URL，在语义上利用自由格式的标签给信息增加标签，并且稍后通过利用相同的标签查询 PeCMan 以找回该信息。由于可以利用相同的标签给多个 URL 增加标签，从而 PeCMan 可使用户通过一个类似于“虚拟驱动器”的逻辑位置来组织被保持在多个存储器提供商（例如，网络服务器、家庭存储或邮件服务器）上的所有对象。

[0070] PeCMan 识别三种基准：公共内容、私人非共享内容和私人共享内容。公共内容是指向公众可获得的网络资源的 URL。访问这样的内容不需要用户的凭证，其中凭证暗示人们可以容易地将这样的内容与对该内容感兴趣的任何人共享。当在用户之间共享公共信息时，PeCMan 简单地将所请求的 URL 直接发送给发送请求的客户机或第二 PeCMan 客户机，并且第二 PeCMan 客户机通过例如 WebDAV 或 HTTP 来获取内容。

[0071] 私人内容通常是仅能通过安全的位置、典型地是通过安全网站（也就是存储器提供商）来访问的内容。为了访问安全存储器提供商 7，网络客户机 3 首先例如通过 SSL/TLS 来建立安全连接，并且随后提供用户凭证（典型地是用户 ID 和口令）以对用户进行认证。在用户通过认证后，网络客户机 3 可以访问私人存储的内容。典型地，在进行寻址的网络服务器 7 中分配与通信信道相关联的状态。该状态指示网络服务器 7，发送请求的网络客户机 3 已经进行了自我认证。

[0072] 根据现有技术，为了支持私人非共享和共享内容，PeCMan 典型地存储具有被指向的 URL 的用户凭证。如果对私人内容进行寻址，第二 PeCMan 客户机 3 建立与 PeCMan 1 的通信信道，PeCMan 1 从而代表第二 PeCMan 客户机建立与存储器提供商 7 的连接，也就是，PeCMan 服务器 4 用作第二 PeCMan 客户机 3 的代理。该代理保持与网络服务器 7 的安全连接，且该代理也是将用户凭证提供给存储器提供商 7 的代理。PeCMan 为共享的和非共享的私人内容基准 (reference) 进行这些操作。

[0073] 在用于私人内容的 PeCMan 中共享数据的所述方法的下一步是将与指向对象相关联的全部数据通过 PeCMan 代理进行传送。这意味着 PeCMan 会成为访问私人内容的瓶颈，并且如果费用和通过 PeCMan 传输的数据相关联，则 PeCMan 运营商可能遭受用于提供私人内容的巨额费用。此外，由于将意味着用户的用户凭证需要与第二 PeCMan 客户机共享，因此在网络客户机领域内执行代理不是典型的选择。

[0074] 开放认证 (OAuth) 协议是处理网络上多方之间的用户凭证的开放协议（见 OAuth

规范 1.0,可从 http://oauth.net/license/core/1.0 处获得)。

[0075] 根据本发明的一个实施方式,将 OAuth 用于在私人内容提供商和第三方之间共享私人数据,从而第三方在不需要通过基于令牌的认证机制知道用户凭证的情况下可以访问用户的私人数据,其中基于令牌的认证机制在图 2 和图 3 中进行解释。

[0076] 在本发明方法实施方式的第一阶段,通过诸如 PeCMan 服务器的内容管理服务器获得委托 (delegate) 令牌,如图 2 的呼叫流程所示,其中图 2 示出了用于对 PeCMan 服务器进行授权以代表内容所有者 O 进行讲话的示例性委托过程。PeCMan 服务器可起到私人内容服务器的客户机的作用,这里是安全网络服务器 WS。

[0077] 在初始阶段 I,PeCMan 服务器与网络服务器 WS 建立安全连接,其中在它们之间建立用户密钥 (consumer key)Ck 和秘密密钥 Cs,见箭头 200。同样,所有者 O 直接在网络服务器 WS 上安装私人内容 xyz,见箭头 200。典型地,所有者将使用用户名和口令登录安全网络服务器,从而他可以安装私人内容 xyz。接下来,所有者 O 通知 PeCMan 服务器其已经在受保护的网络服务器上安装了私人内容 xyz,见箭头 202。

[0078] 在呼叫流程的阶段 A,在接到关于安装了私人内容的通知时,PeCMan 服务器将请求令牌并通过所有者对该令牌进行认证。首先,PeCMan 服务器从网络服务器 WS 请求令牌,见箭头 206。这可以是标准的 OAuth 请求呼叫,其包括下列参数 :用户密钥 Ck(oauth_consumer_key),签名方法 Sm(oauth_signature_method),签名 S1(oauth_signature),时间戳 Ot(oauth_timestamp) 和临时信息 (nonce)N(oauth_nonce)。例如,可以使用 Cs 来创建签名 S1。典型地,客户机会首先产生时间戳,并且然后为每个请求产生唯一的临时信息值。网络服务器 WS 随后产生令牌 T1(oauth_token) 和令牌秘密 Ts1(oauth_token_secret),并将这些信息发送给 PeCMan 服务器,见步骤 204。PeCMan 服务器随后将重新定向消息发送给所有者 (步骤 205),以通过将所有者定向到网络服务器 WS,从所有者获得批准 (approval)。这可以是对于网络服务器的用户认证 URL“WS ://auth ?”的标准 OAuth 请求,包括令牌 T1 和回叫 (call back)URL C,其中 C 是网络服务器用于将所有者重新定向回 PeCMan 服务器的 URL。随后将授权请求传递给网络服务器 (步骤 206),并且网络服务器将对令牌 T1 进行认证,典型地验证 PeCMan 服务器的身份,并请求所有者准许 (步骤 207)。例如,建立与私人内容提供商 (网络服务器 WS) 的安全连接,通过提供 PeCMan 凭证进行登录并将令牌与安全连接相关联。随后由所有者 O 利用诸如标准 OAuth 呼叫的回叫 URL 通知 PeCMan 服务器 :令牌 T1 已经通过授权 (步骤 208)。

[0079] PeCMan 服务器现在将使用他的第一令牌 T1 来请求第二令牌 (步骤 210)。例如,这可以通过使用利用下列参数将请求令牌换成访问令牌的标准 OAuth 请求来完成,参数包括 :用户密钥 Ck(oauth_consumer_key)、先前获得的令牌 T1(oauth_token)、签名方法 Sm(oauth_signature_method)、签名 S2(oauth_signature)、时间戳 Ot(oauth_tiemstamp) 和临时信息 N(oauth_nonce)。签名 S2 例如可以基于 Cs 和 Ts1 进行计算。作为响应,由网络服务器 WS 授予第二令牌 T2 和令牌秘密 Ts2(步骤 210)。该第二令牌 T2 可以用作使第二客户机 (访问者) 访问所有者的私人内容的委托令牌,这将在图 3 和图 4 中进行说明。

[0080] 私人内容 xyz 还可由 PeCMan 服务器通过将令牌 T2 提供给网络服务器 WS 来获得,见图 2 的呼叫流程中的阶段 C。这可以通过使用例如包括下列参数的标准访问请求来完成 :用户密钥 Ck(oauth_consumer_key)、令牌 T2(oauth_token)、签名方法 Sm(oauth_

signature_method)、签名 S3(oauth_signature)、时间戳 Ot(oauth_tiemstamp) 和临时信息 N(oauth_nonce)。例如,可以使用 Cs 和 Ts2 来计算签名 S3。需要注意的是,由于 T2 还可以仅用作使第二客户机访问所有者私人内容而不会干扰所有者的委托令牌,因此阶段 C 的步骤不是必须由 PeCMan 服务器来执行。

[0081] 在图 3 中描述了用于通过访问者获取访问令牌的方法的第一实施方式。在第一步骤 301,PeCMan 客户机将查询发送给 PeCMan 服务器以获得对特定私人内容的访问。响应于该查询,例如通过使用具有下列参数的请求,PeCMan 服务器将令牌请求消息发送给网络服务器,参数包括 :用户密钥 Ck(oauth_consumer_key)、令牌 T2(oauth_token)、签名方法 Sm(oauth_signature_method)、签名 S3(oauth_signature)、时间戳 Ot(oauth_tiemstamp) 和临时信息 N(oauth_nonce)、访问 URL Au(Access_url)、访问权利 Ar(Access_rights)、访问时间段 At(Access_timePeriod) 和访问 IP Ai(Access_IP)。签名 S3 例如可以利用 Cs 和 Ts2 来计算。访问 URL 典型地涉及私人数据的收集,例如包含获取 xyz 的数据的特定目录。访问权利是涉及内容(读取、修改等)的权利。时间段是令牌有效的时间。访问 IP 通常是可选的,且涉及访问者的地址。在下面的步骤 302 中,网络服务器将第三令牌 T3 和相应的令牌秘密 Ts3 授予 PeCMan 服务器,其中 PeCMan 服务器通知访问者所请求的私人内容 xyz 与令牌 T3 和令牌秘密 Ts3 相关联(步骤 303)。访问者现在可以获得私人数据 xyz,如步骤 304 和步骤 305 所示。这可以通过使用包括例如下列参数的访问请求来完成 :访问 IP Ai、令牌 T3(oauth_token)、签名方法 Sm(oauth_signature_method)、签名 S4(oauth_signature)、时间戳 Ot(oauth_timestamp) 和临时信息 N(oauth_nonce)。签名 S4 例如通过使用 Ts3 来计算。

[0082] 当相比于原始的令牌 2 时,最近创建的令牌 T3 可以具有相同或更少的权利。利用这些得到的访问令牌 T3,第二 PeCMan 客户机可以直接从网络服务器获得内容而不必与所有者交互。

[0083] 上述实施方式的一个优势是共享其内容的第二客户机不需要向网络服务器注册。通过使 PeCMan 服务器能够进一步将令牌 T3 委托给第二客户机(访问者),可将内容与没有向网络服务器 WS 注册的用户进行共享,而不用将内容完全公开。PeCMan 服务器的另一优势是其可以在网络服务器的策略上面加强其自己的策略。利用该实施方式,基于由所有者定义的粒度,PeCMan 服务器可以通过特定的网络服务将内容分发或委托给第二用户。当另一客户机请求访问来自所有者的内容时,在发布得到的访问令牌 T3 之前,PeCMan 服务器例如通过检查客户机数据库,验证所有者是否已经将信息与所述第二客户机进行共享。

[0084] 图 4 示出了由通过委托令牌访问私人内容的第二 PeCMan 客户机执行的过程的另一实施方式。第二 PeCMan 客户机(访问者)通过 PeCMan 服务器来请求内容(步骤 400),并且 PeCMan 服务器指示可以通过受保护的网络服务器 WS 来获得内容 xyz(步骤 401)。典型地,客户机会通过首先尝试访问安全内容来开始,参见建立用户密钥和秘密密钥的步骤 402,和请求内容的步骤 403。然而,由于内容是仅通过令牌可以访问的私人内容,网络服务器 WS 对认证失败作出响应(步骤 404)。因此,通过使用例如具有下列参数的标准 OAuth 请求,然后客户机请求并从网络服务器获得令牌 T4,参见步骤 406 和 407,其中参数包括 :用户密钥 Ck2(oauth_consumer_key)、签名方法 Sm(oauth_signature_method)、签名 S5(oauth_signature)、时间戳 Ot(oauth_timestamp) 和临时信息 N(oauth_nonce)。例如,利用 Cs2 来

计算签名。假设存在用于所述内容的委托令牌，将请求令牌 T4 提供给用于认证的 PeCMan 服务器（步骤 407）。当 PeCMan 服务器接收到具有客户机的请求令牌的认证请求时，PeCMan 服务器确定谁请求访问内容。如果 PeCMan 服务器可以授予对客户机的访问，其授权使用其委托令牌 T2、委托密秘密 Ts2 进行访问，参见步骤 408。当网络服务器接收基于委托令牌的认证请求时，网络服务器对客户机的请求令牌 T4 进行认证，参见步骤 409。然后，将该请求令牌 T4 通过 PeCMan 返回给发送请求的第二客户机，参见步骤 410。发送请求 (requesting) 的客户机在接收到经认证的请求令牌 T4 时使用标准 OAuth 过程呼叫来完成该过程（步骤 411 至步骤 414）：客户机将经认证的请求令牌 T4 换为访问令牌 T5（步骤 411 和步骤 412），其中消息例如可利用基于 Cs2 和 Ts4 计算的签名 S6 进行签名。然后，可以通过将访问令牌 T5 提供给网络服务器 WS 来获得实际的数据 xyz，参见步骤 413，从而将数据 xyz 发送给客户机 C，参见步骤 414。GET 消息 413 例如可以利用基于 Cs2 和 Ts5 计算的签名进行签名。

[0085] 图 5 描述了本发明方法的更为普通的实施方式，其中均通过认证并对一些内容具有一些权利的客户机和第一服务器 S1、第二服务器 S2，能够询问各自的访问令牌持有者（从 C 来看 S2 是持有者，从 S2 来看 S1 是持有者，从 S1 来看 WS 是持有者）以获得另一访问令牌，其相比于各自的第一服务器和第二服务器的委托令牌具有相同或更少的权利。服务器 S1 和 S2 典型地都是内容管理服务器，例如都可以是 PeCMan 服务器。S1 还可以是本地网站上的内容管理服务器。实施例描述了访问者作为服务器 S2 的客户机可以对服务器 S2 进行查询。服务器 S2 具有用于所请求的内容的委托令牌，并可从内容服务器 WS 获得用于该内容的访问令牌（参见步骤 503 和步骤 504）。然后，服务器 S1 将具有相同或较少权利的访问令牌发送给服务器 S2（步骤 505），其中服务器 S2 接着将具有相同或较少权利 (right) 的访问令牌发送给访问者（步骤 506）。本领域技术人员可以理解的是，通过使用图 4 中所示的获取方式也可以实现相似的可传递共享的实施方式。

[0086] 图 6 描述了图 2 的呼叫流程的变型，其中图 2 中的令牌 T1 对应于图 6 中的令牌 Tr，图 2 中的令牌 T2 对应于图 6 中的令牌 Td。步骤 601 至 603 对应于步骤 301 至 303，其中获取 (GET) 或发布 (POST) 呼叫用于通知 PecMan 服务器他应间接获取安装在网络服务器上的私人内容。在步骤 603 和步骤 604 中，PecMan 服务器通过隧道（例如 TLS 或 https）获得令牌 Tr。这些呼叫都通过安全通信信道进行传送，例如由具有题目为“传输层安全 (TLS) 协议”的 RFC4346 定义的 SSL/TLS。PeCMan 服务器于是请求内容的所有者通过安全网络服务器 WS 来认证请求令牌，与标准 OAuth 方法相似，参见步骤 605-606。所有者 O 将凭证提供给网络服务器 WS，并且网络服务器 WS 分配记录请求令牌现在有效的并经过认证的状态，参见步骤 606 和 607。最后，网络服务器回叫 PeCMan 服务器以通知它请求令牌现在已经通过认证，参见步骤 608。PeCMan 服务器于是请求通过网络服务器 WS 利用委托令牌来替换经过认证的请求令牌，参见步骤 609。网络服务器 WS 通过隧道将委托令牌 (Td)、相关联的秘密委托令牌 (Td_s) 和临时信息 (Nd) 返回给 PeCMan 服务器，参见步骤 610。最后，在步骤 611 中，PeCMan 服务器对用于标识委托过程成功或失败的原始 HTTP POST 请求（步骤 602）作出响应。网络服务器存储委托令牌 Td、其生命期、和内容的原始所有者。该委托令牌 Td 替换用户凭证，也就是，委托令牌 Td 的持有者可以认证请求令牌，就好像他是内容的所有者。利用委托令牌 Td 进行签名的“请求访问”消息表示请求访问的网络服务器 WS 基于被委托的授权。

[0087] 根据另一实施方式，原始的经认证的请求令牌可以用作委托令牌。然而，通常更希望具有单独的令牌以在功能差别上进行区分。在现在的 OAuth 中，经认证的请求令牌 Tr 仅可以用于替换访问令牌 Ta，并且访问策略由网络服务器 WS 来设置。利用其委托令牌 Td 的授权委托过程可以进一步用于限制对内容的访问。

[0088] 图 7 示出了图 4 用于通过委托的令牌 Td 访问私人内容的过程的实施方式的变型。步骤 700 至 704 与步骤 400 至 404 相似。然后，客户机请求并通过 TLS 隧道从网络服务器 WS 获得具有下列参数的请求令牌 Tr（参见步骤 705 和 706），所述参数包括：公共密钥 Ck、秘密密钥 Ks、和临时信息 Nr。假设存在用于该内容的委托令牌 Td，将请求令牌 Tr 提供给 PeCMan 服务器以进行认证（步骤 707）。当 PeCMan 服务器接收具有客户机的请求令牌的认证请求时，PeCMan 服务器确定谁请求访问所述内容。如果 PeCMan 服务器可以授予对客户机的访问，其使用由下列参数产生的签名（强制访问控制，MAC）对访问进行授权：它的委托令牌 Td、委托秘密 Td_s 和临时信息 Nd，参见步骤 708。当网络服务器 WS 接收基于委托令牌的认证请求 708 时，网络服务器对客户机的请求令牌 Tr 进行认证，参见步骤 709。然后，通过 PeCMan 将该请求 Tr 返回给发送请求的第二客户机，参见步骤 710。在接收到经过认证的请求令牌 Tr 时，发送请求的客户机使用标准的 OAuth 过程呼叫来完成该过程（步骤 711 至 714）：客户机通过 TLS 隧道将经过认证的请求令牌 Tr_s 替换为访问令牌 Ta（步骤 711 和 712）。然后，可以通过将访问令牌 Ta 提供给网络服务器来获得实际数据 xyz（使用秘密密钥 Ks、Ta、令牌秘密 Ta_s 和临时信息 Na 的签名形式），参见步骤 713，从而将数据 xyz 发送给客户机，参见步骤 714。

[0089] 图 8 描述了用于使访问令牌持有者能够进一步委托令牌的图 2 的方法的变型，其中图 2 中的令牌 T1 和 T1s 对应于 Tr 和 Tr_s，并且令牌 T2 和 T2s 对应于 Ta 和 Ta_s。在该实施方式中，可以将 PeCMan 服务器视为执行标准过程呼叫（步骤 803 至 810）的 OAuth 用户，其中标准过程呼叫用于请求和获得用于特定内容的访问令牌，其中所述特定内容先前由所有者安装在网络服务器上并且向 PeCMan 服务器注册（步骤 801 至 803）。利用 PeCMan 服务器持有的访问令牌 Ta，其可以进一步创建访问令牌，并将访问令牌委托给新的第二客户机。在该实施方式中，由 https 隧道组成使用，其中 https 隧道用于使用如公共密钥 Ck、秘密密钥 Ks 和临时信息 Nr 的参数来请求和交换令牌。

[0090] 在图 9 中描述了由第二客户机获取访问令牌方法的另一实施方式。该实施方式与图 3 的实施方式相似，并且步骤 900 至 905 与步骤 300 至 305 相似，其中令牌 T3 对应于访问令牌 At。在图 9 的实施方式中，https 隧道用于使用如公共密钥 Ck、秘密密钥 Ks 和临时信息 Nr 的参数来请求和交换令牌。不同于在图 2 中利用令牌秘密 Ts3 进行工作，在图 9 的实施方式中使用基于下列参数集 (At、Ck、Ks 和临时信息 Na) 的签名 (MAC) 以提供必要的安全性。相比于通过 PeCMan 获得的原始访问令牌 Ta（见图 8），最新创建的访问令牌 At 可以具有相同或较少的权利。利用这些得到的访问令牌 At，第二 PeCMan 客户机可以从网络服务器 WS 直接获得内容，而不必与所有者 O 交互。

[0091] 本领域技术人员会容易地认识到，上述各种方法的步骤可由程序控制计算机来执行。这里，一些实施方式也意在涵盖诸如数字数据存储媒介的程序存储设备，其中程序存储设备是机器或计算机可读的，并对指令的机器可执行程序或计算机可执行程序进行编码，其中所述指令执行所述上面介绍的方法的一些或全部步骤。程序存储设备例如可以是数字

存储器、诸如磁盘和磁带的磁存储媒介、硬盘驱动器、或光可读数字数据存储媒介。实施方式还意在涵盖经过编程以执行上面介绍的方法的所述步骤的计算机。

[0092] 尽管已经结合特定实施方式陈述了本发明的原则，可以明确理解的是，该描述仅仅是作为示例，并且并不对保护范围作出限制，保护范围由所附权利要求来确定。

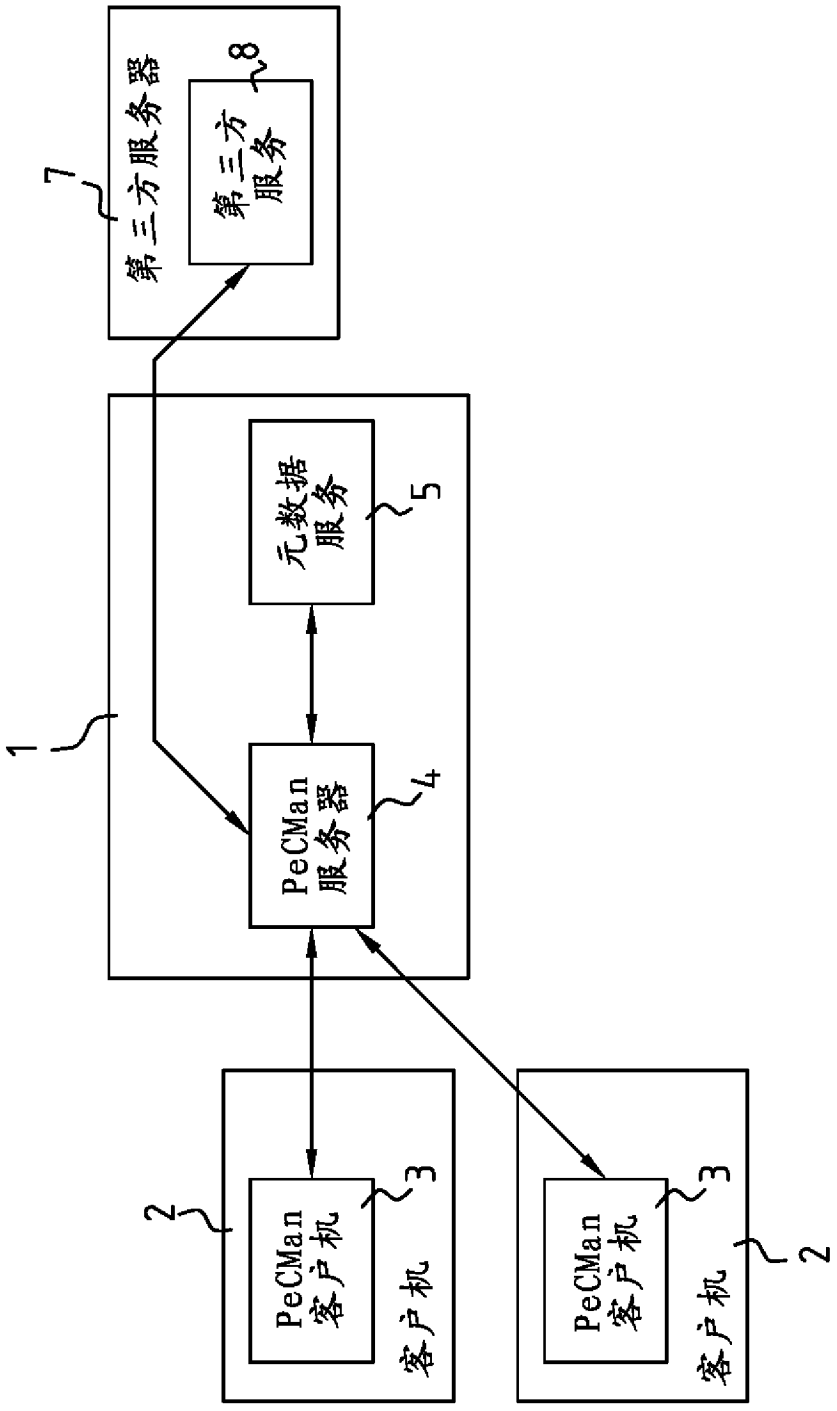

第三方服务器
7
第三方服务
8
元数据服务
5
1
PeCMan服务器
4
2
PeCMan客户机
3
客户机
PeCMan客户机
3
客户机
2

图 1

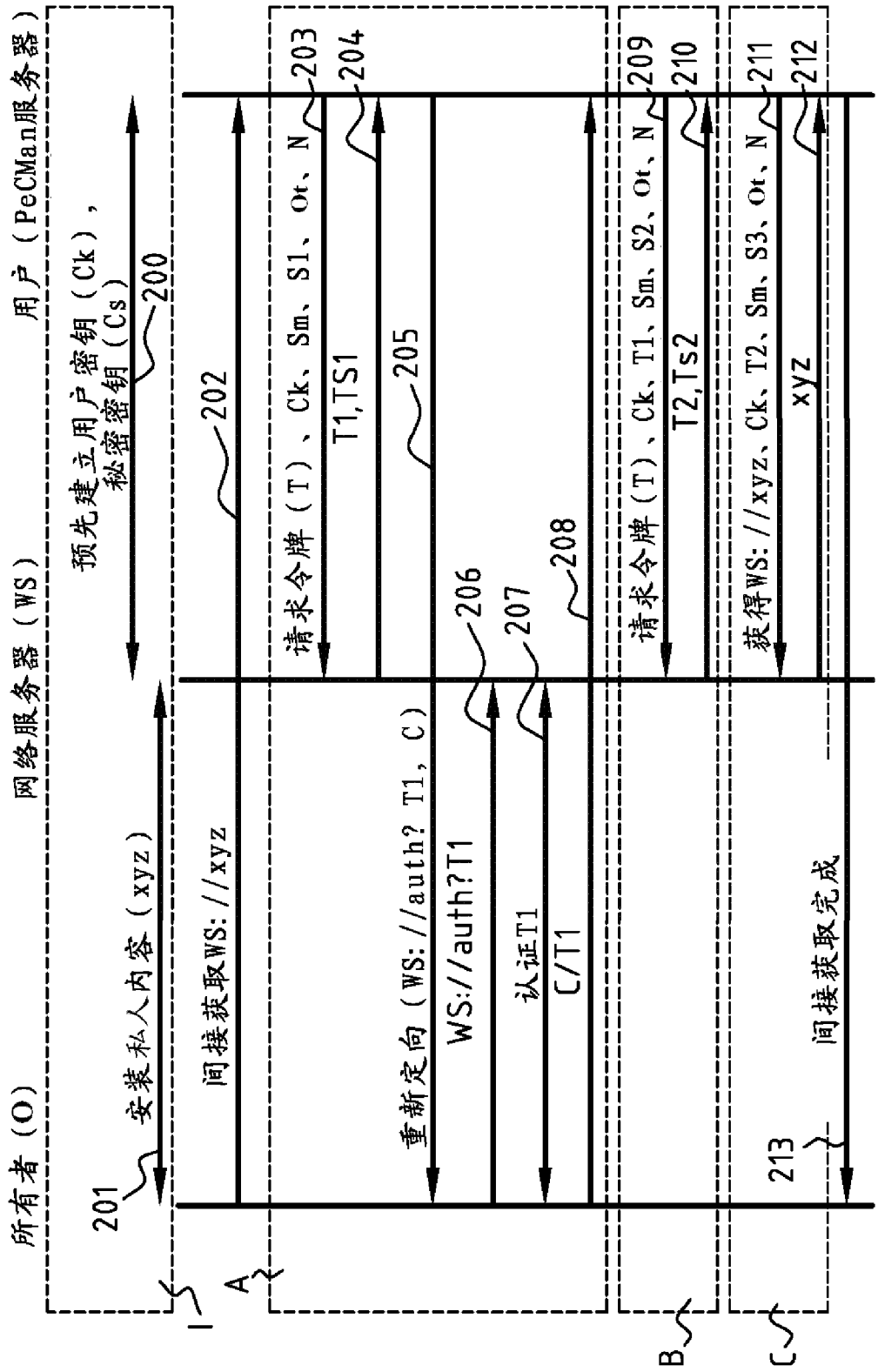

所有者（O）
网络服务器（WS）
用户（PeCMan服务器）
预先建立用户密钥（Ck），
秘密密钥（Cs）
200
201
安装私人内容（xyz）
202
间接获取WS: //xyz
203
请求令牌（T）、Ck、Sm、S1、Ot、N
204
T1,TS1
205
重新定向（WS: //auth? T1, C）
206
WS://auth?T1
207
认证T1
208
C/T1
209
请求令牌（T）、Ck、T1、Sm、S2、Ot、N
210
T2,Ts2
211
获得WS: //xyz、Ck、T2、Sm、S3、Ot、N
212
xyz
213
间接获取完成
A
B
C
1

图 2

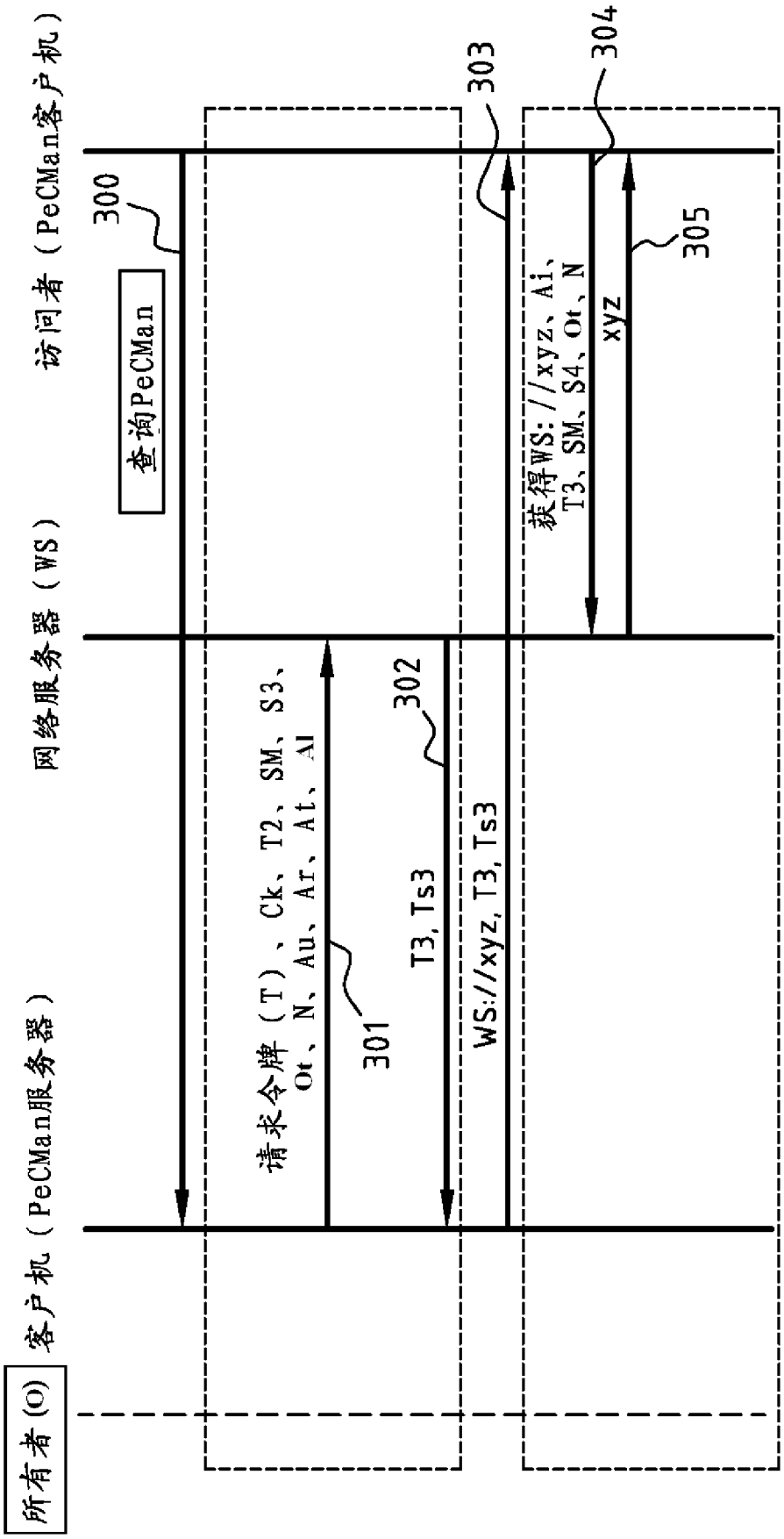

所有者(O)
客户机（PeCMan服务器）
网络服务器（WS）
访问者（PeCMan客户机）
300
查询PeCMan
301
请求令牌（T）、Ck、T2、SM、S3、Ot、N、Au、Ar、At、Al
302
T3, Ts3
WS://xyz, T3, Ts3
303
304
获得WS://xyz、Ai、T3、SM、S4、Ot、N
305
xyz

图 3

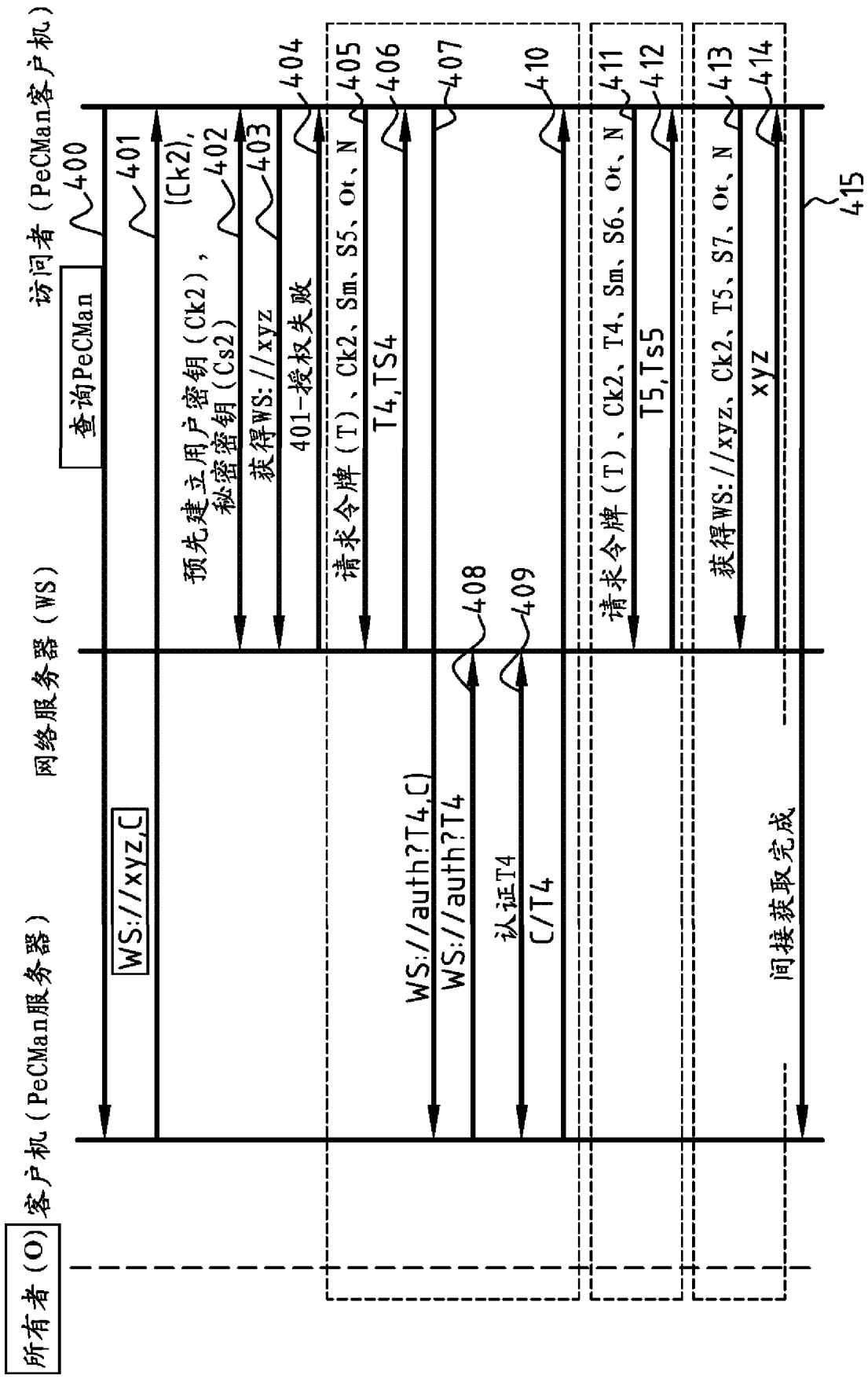

所有者（O）
客户机（PeCMan服务器）
网络服务器（WS）
访问者（PeCMan客户机）
400
查询PeCMan
401
WS://xyz,C
(Ck2),
预先建立用户密钥（Ck2），
秘密密钥（Cs2）
402
获得WS://xyz
403
401-授权失败
404
请求令牌（T）、Ck2、Sm、S5、Ot、N
405
T4,TS4
406
WS://auth?T4,C)
407
WS://auth?T4
408
认证T4
409
C/T4
410
请求令牌（T）、Ck2、T4、Sm、S6、Ot、N
411
T5,Ts5
412
获得WS://xyz、Ck2、T5、S7、Ot、N
413
xyz
414
间接获取完成
415

图 4

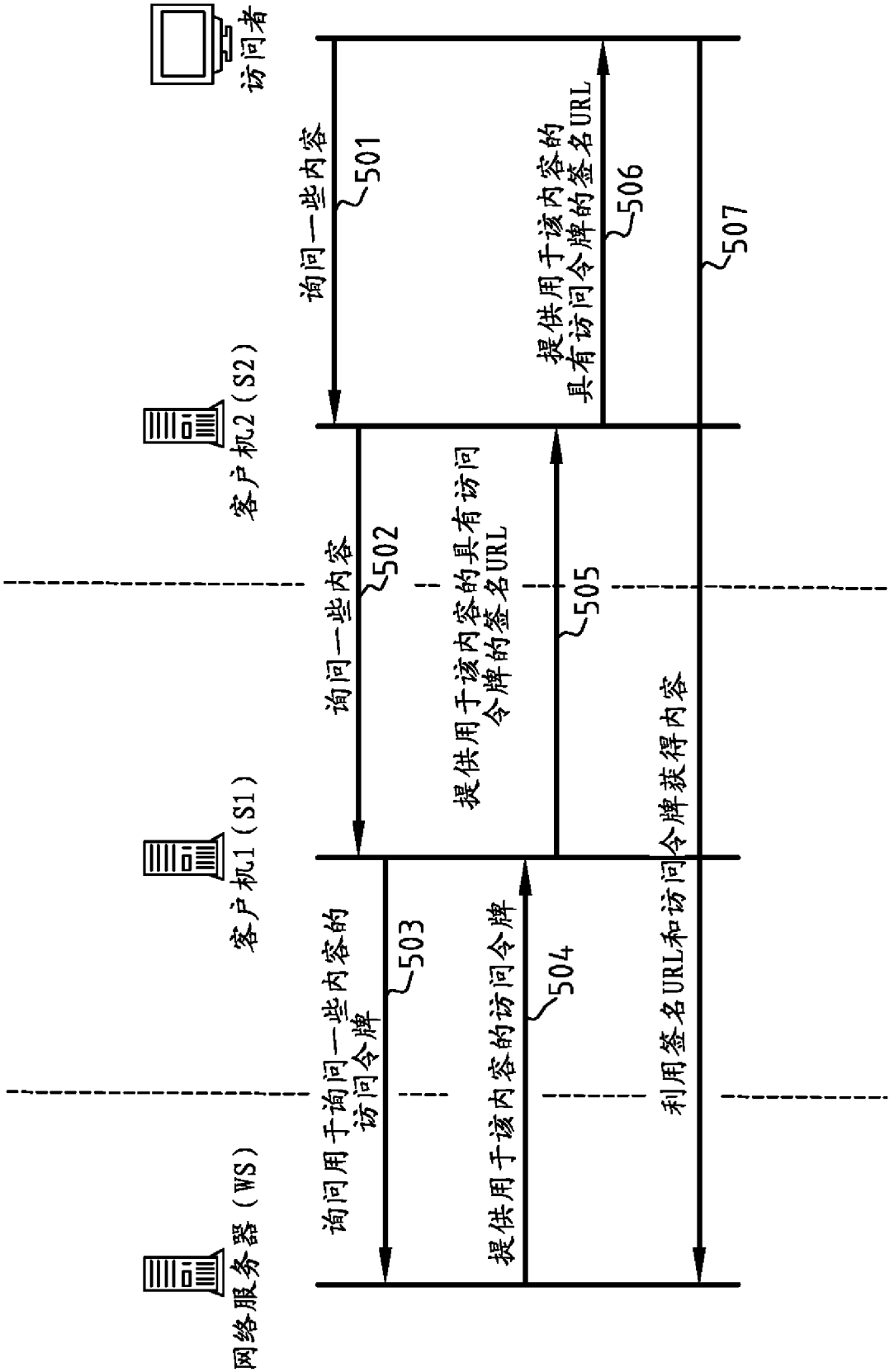

访问者
客户机2（S2）
客户机1（S1）
网络服务器（WS）
询问一些内容
501
提供用于该内容的
具有访问令牌的签名URL
506
507
询问一些内容
502
提供用于该内容的具有访问
令牌的签名URL
505
询问用于询问一些内容的
访问令牌
503
提供用于该内容的访问令牌
504
利用签名URL和访问令牌获得内容

图 5

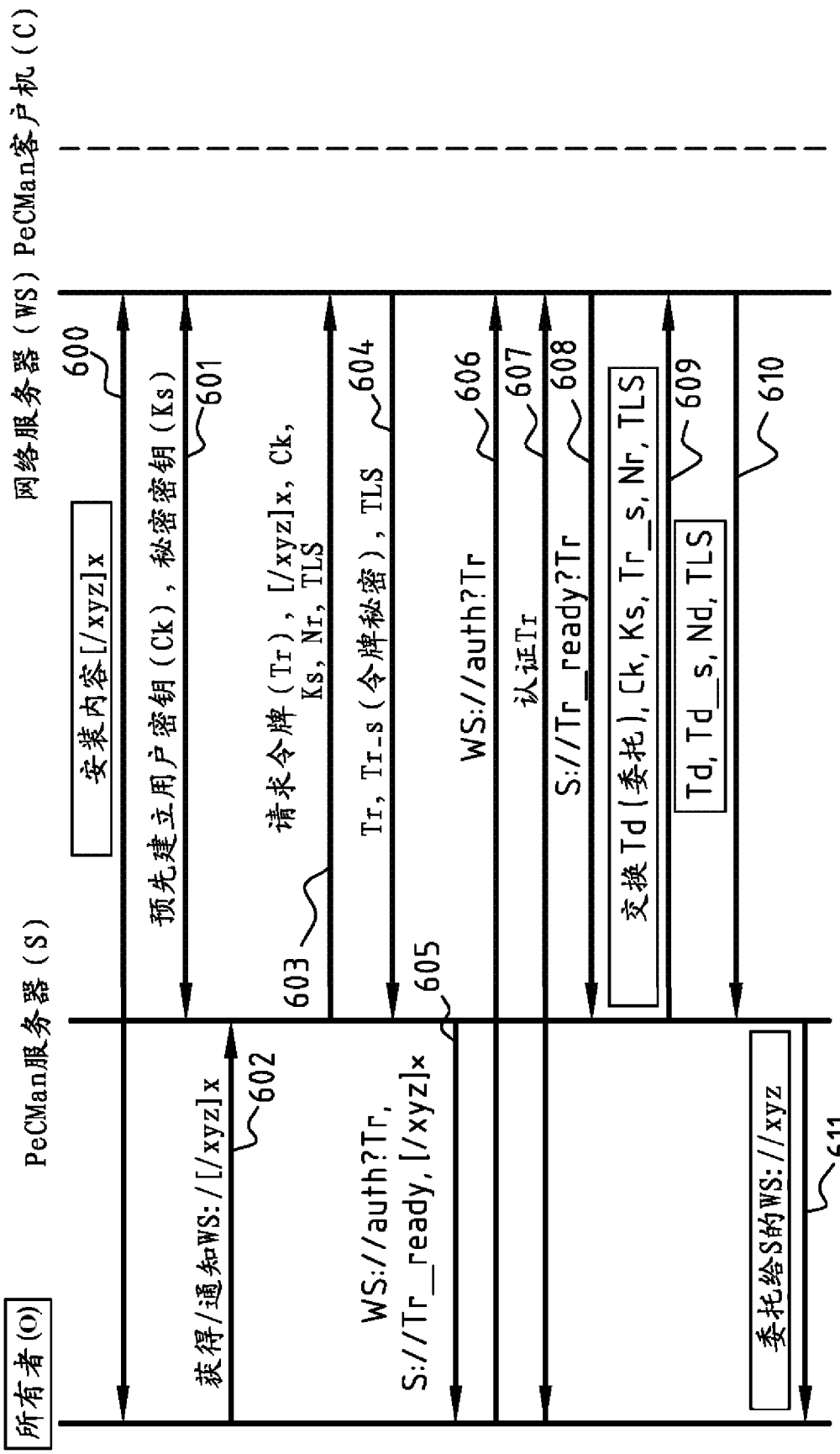

所有者(O)
PeCMan服务器(S)
网络服务器(WS)
PeCMan客户机(C)
600
安装内容[/xyz]x
601
预先建立用户密钥(Ck)，秘密密钥(Ks)
602
获得/通知WS://[/xyz]x
603
请求令牌(Tr)，[/xyz]x，Ck，Ks，Nr，TLS
604
Tr，Tr-s(令牌秘密)，TLS
605
WS://auth?Tr，S://Tr_ready，[/xyz]x
606
WS://auth?Tr
607
认证Tr
608
S://Tr_ready?Tr
609
交换Td(委托)，Ck，Ks，Tr_s，Nr，TLS
610
Td，Td_s，Nd，TLS
611
委托给S的WS://xyz

图 6

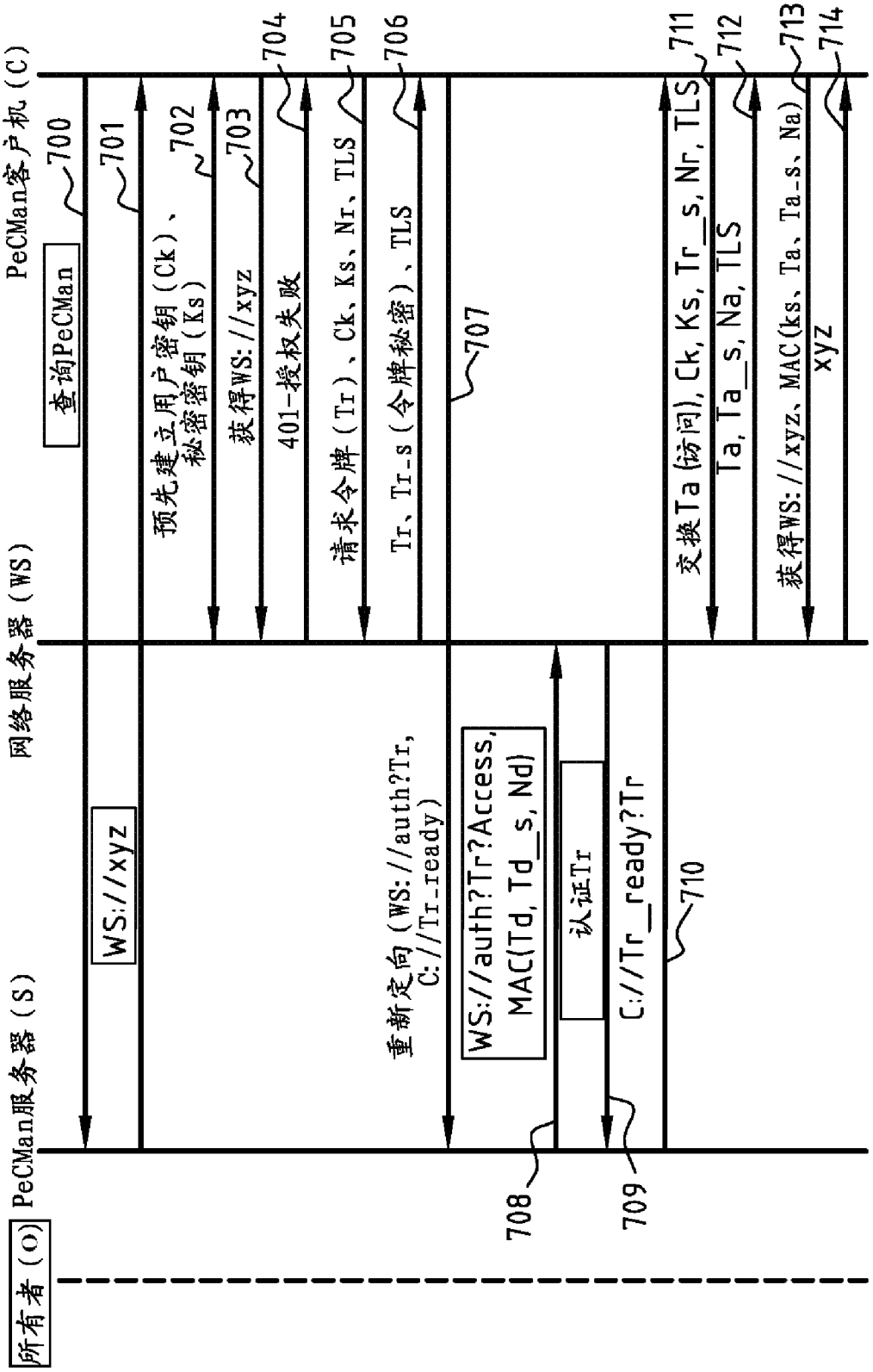

所有者（O）
PeCMan服务器（S）
网络服务器（WS）
PeCMan客户机（C）
查询PeCMan
700
701
预先建立用户密钥（Ck）、
秘密密钥（Ks）
702
获得WS://xyz
703
401-授权失败
704
请求令牌（Tr）、Ck、Ks、Nr、TLS
705
Tr、Tr_s（令牌秘密）、TLS
706
707
交换Ta（访问）, Ck, Ks, Tr_s, Nr, TLS
711
Ta, Ta_s, Na, TLS
712
获得WS://xyz、MAC(ks、Ta、Ta_s、Na)
713
xyz
714
WS://xyz
重新定向（WS://auth?Tr,
C://Tr_ready）
WS://auth?Tr?Access,
MAC(Td, Td_s, Nd)
认证Tr
C://Tr_ready?Tr
710
708
709

图 7

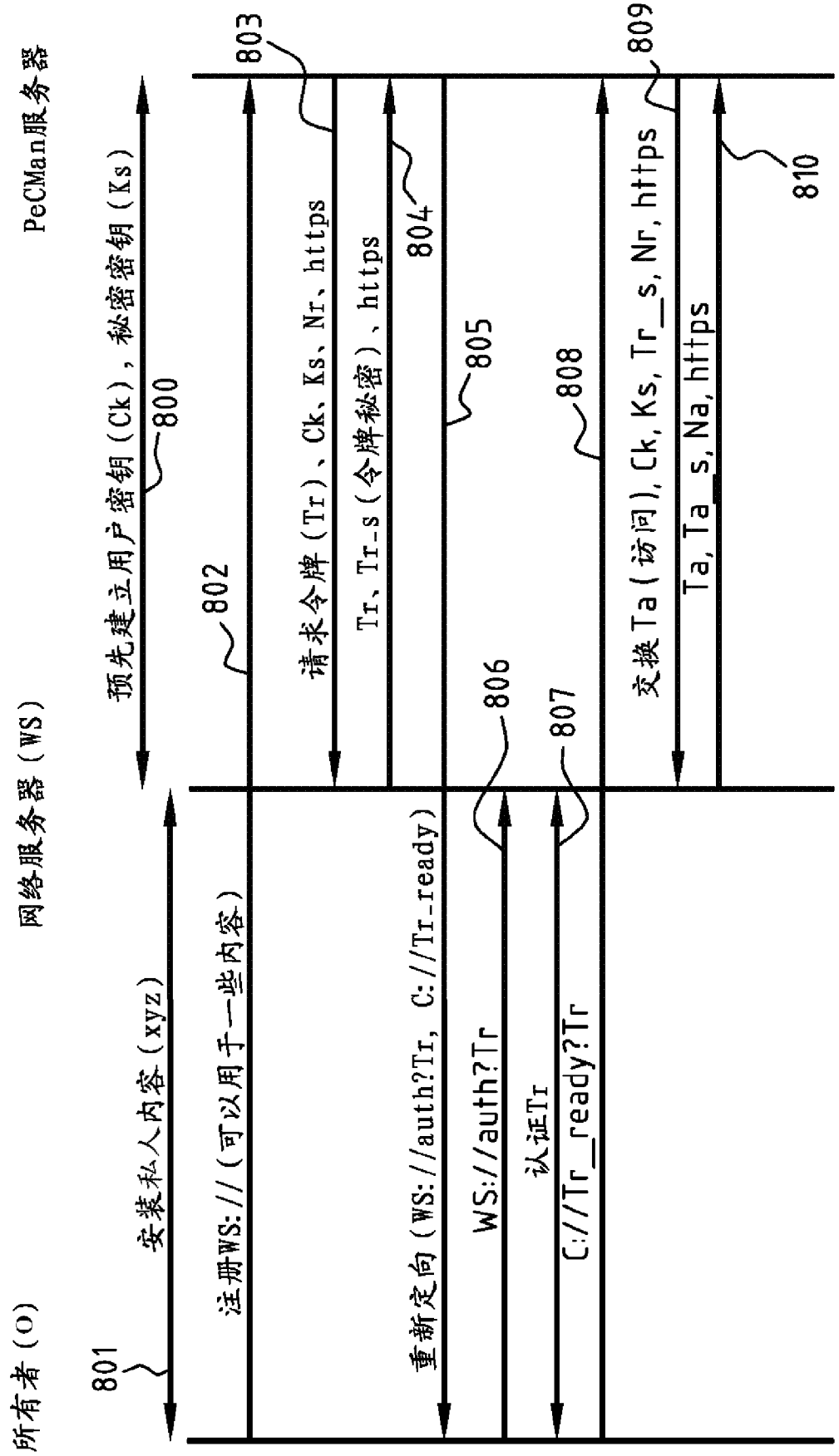

所有者（O）
网络服务器（WS）
PeCMan服务器
801
安装私人内容（xyz）
预先建立用户密钥（Ck），秘密密钥（Ks）
800
802
注册WS://（可以用于一些内容）
803
请求令牌（Tr）、Ck、Ks、Nr、https
804
Tr、Tr_s（令牌秘密）、https
805
重新定向（WS://auth?Tr，C://Tr_ready）
806
WS://auth?Tr
807
认证Tr
808
C://Tr_ready?Tr
809
交换Ta（访问），Ck，Ks，Tr_s，Nr，https
810
Ta，Ta_s，Na，https

图 8

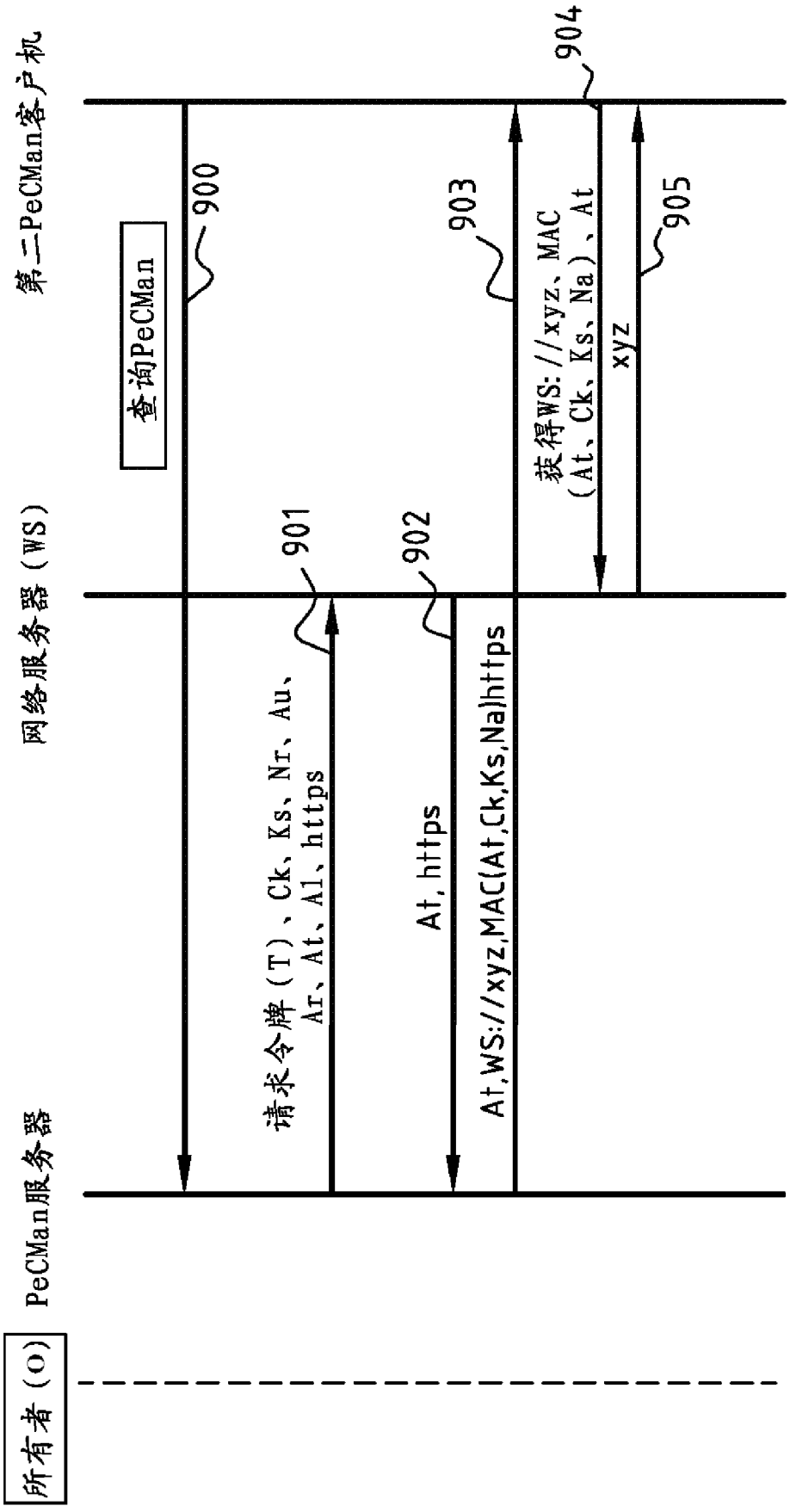

所有者（O）
PeCMan服务器
网络服务器（WS）
第二PeCMan客户机
查询PeCMan
900
901
902
903
904
905
请求令牌（T）、Ck、Ks、Nr、Au、
Ar、At、Al、https
At,https
At,WS://xyz,MAC(At,Ck,Ks,Na)https
获得WS://xyz、MAC
（At、Ck、Ks、Na）、At
xyz

图 9