

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 1/00 (2006.01)



[12] 发明专利说明书

专利号 ZL 03809453.3

[45] 授权公告日 2007 年 9 月 26 日

[11] 授权公告号 CN 100339781C

[22] 申请日 2003.3.26 [21] 申请号 03809453.3

[30] 优先权

[32] 2002. 4. 26 [33] EP [31] 02009568.3

[86] 国际申请 PCT/IB2003/001172 2003.3.26

[87] 国际公布 WO2003/091861 英 2003.11.6

[85] 进入国家阶段日期 2004.10.26

[73] 专利权人 国际商业机器公司

地址 美国纽约州

[72] 发明人 伯吉特·M·菲茨曼

迈克尔·韦德纳

[56] 参考文献

CN1156861A 1997.8.13

US5708780A 1998.1.13

" Binding and Profiles for the OASIS Security
AssertionMarkup Language (SAML)" WWW.
OASIS. OPEN. ORG 2002

审查员 盖 浩

[74] 专利代理机构 北京市柳沈律师事务所

代理人 郭定辉 黄小临

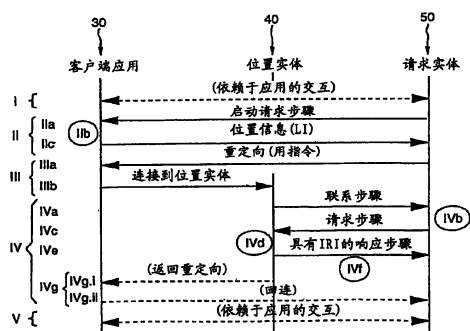
权利要求书 3 页 说明书 17 页 附图 5 页

[54] 发明名称

向请求实体传送身份相关信息的方法和系统

[57] 摘要

本发明允许一种可靠高效的身份管理，其可以利用完全互操作性满足参与者的各种需求。为此，提供了一种向请求实体提供关于用户的身份相关信息的方法与系统。所述方法包含：位置请求步骤，由请求实体发起，用来从客户端应用请求相应于具有身份相关信息的位置实体的位置信息；重定向步骤，用来将客户端应用连接到位置实体，以指令位置实体将身份相关信息传送给请求实体；以及获取步骤，用来获得身份相关信息。获取步骤包含：联系步骤，其中位置实体联系请求实体；请求步骤，其中请求实体请求身份相关信息；以及响应步骤，其中请求实体从位置实体接收身份相关信息。



1. 一种向请求实体提供身份相关信息的方法，所述方法包含：

位置请求步骤 (II)，由请求实体发起，用来从客户端应用请求相应于具有身份相关信息的位置实体的位置信息；

重定向步骤 (III)，用来将客户端应用连接到位置实体，以指令位置实体将身份相关信息传送给请求实体；以及

获取步骤 (IV)，用来获得身份相关信息，所述获取步骤包含：

联系步骤 (IVa)，其中位置实体联系请求实体；

请求步骤 (IVc)，其中请求实体请求身份相关信息；以及

响应步骤 (IVe)，其中请求实体从位置实体接收身份相关信息。

2. 根据权利要求1的方法，其中所述获取步骤 (IV) 只包含重定向子步骤 (IVg)，该子步骤借助客户端应用将位置实体重定向到请求实体，并且由此向请求实体传送身份相关信息。

3. 根据权利要求1的方法，还包括确定步骤：用来根据在 URL 中承载的信息的长度确定是否执行联系步骤 (IVa)。

4. 根据权利要求1的方法，其中在请求实体与客户端应用之间以及在位置实体与客户端应用之间使用的传输协议为安全超文本传送协议。

5. 根据权利要求1的方法，其中位置信息为相对于客户端应用的位置。

6. 根据权利要求1的方法，还包括：由请求实体与验证一起，从位置实体假名之下的位置实体接受身份相关信息，其中身份相关信息对应于个人的个人假名。

7. 根据权利要求1的方法，还包括：由请求实体发送使用身份相关信息的服务器策略。

8. 一种向请求实体传送位于位置实体的身份相关信息的方法，所述方法包含在所述请求实体向客户端应用请求传送相应于所述位置实体的位置信息时执行以下步骤：

重定向步骤 (III)，用来从客户端应用接收指令信息，以将身份相关信息传送给请求实体；以及

传送步骤 (IV)，用来向请求实体传送身份相关信息，包含：

联系步骤 (IVa)，其中位置实体联系请求实体；

请求步骤 (IVc), 其中请求实体请求身份相关信息; 以及

响应步骤 (IVe), 其中位置实体向请求实体发送身份相关信息。

9. 根据权利要求 8 的方法, 其中所述传送步骤 (IV) 还包含: 由位置实体根据预定策略确定传送在请求步骤 (IVc) 中请求的身份相关信息的哪个部分。

10. 根据权利要求 9 的方法, 其中所述响应步骤 (IVe) 还包含: 由位置实体传送预定策略的一部分。

11. 根据权利要求 8 至 10 中任一项的方法, 其中位置实体使用在重定向步骤 (III) 中建立的从客户端应用至位置实体的连接, 以在传送步骤 (IV) 期间进行与个人的交互。

12. 根据权利要求 8 至 10 中任一项的方法, 其中向请求实体释放个人信息包含以下步骤:

呈现有关请求实体的信息;

呈现位置实体已知的预先授权的属性值和/或非预先授权的属性值, 和/或为未知属性值呈现分配给用于输入相应属性值的空字段的属性名称;

请求编辑属性值; 以及

向请求实体发送编辑后的属性值。

13. 根据权利要求 12 的方法, 其中不同的属性值以不同方式呈现。

14. 根据权利要求 8 至 10 中任一项的方法, 其中所述传送步骤 (IV) 还包含以下步骤:

由位置实体生成随机值 (k);

在与身份相关信息相同的连接上, 将随机值 (k) 发送给请求实体;

将随机值 (k) 发送给客户端应用, 以使客户端应用能够针对身份相关信息向请求实体证明其真实身份。

15. 一种提供身份相关信息的系统, 所述系统包含:

具有身份相关信息的位置实体;

可连接到位置实体的客户端应用; 以及

用来从客户端应用请求相应于具有身份相关信息的位置实体的位置信息的请求实体, 其中, 根据对于请求的响应, 客户端应用被重定向到位置实体, 以指令位置实体将身份相关信息传送给请求实体, 其中位置实体联系请求实体, 请求实体请求身份相关信息, 并且请求实体从位置实体接收身份相关信

息。

16. 根据权利要求 15 的系统，其中一个客户端应用与几个位置实体交互。

17. 根据权利要求 15 的系统，其中身份相关信息由另一位置实体提供，并且可以由请求实体借助位置实体获得，所述另一位置实体的位置信息存储在位置实体上。

向请求实体传送身份相关信息的方法和系统

技术领域

本发明涉及一种向请求实体提供关于个人的身份相关信息的方法与系统。另外，本发明涉及一种向请求实体传送位于本地实体（也称为钱包）上的身份相关信息的方法。

背景技术

身份管理，就其最宽泛的意义来说，指关于一个人的所有个人信息的管理，这些信息至少包含该人的所有数字关系。在下个十年，这种宽泛意义上的身份管理可能会得到发展。短期来说，身份管理一般指网络单一注册（single sign on），以传送关于个人的少量数据。

主要的商业原因是对电子商务的总体促进：身份管理是基础结构问题，其中像因特网与网络标准那样的标准可能对几乎所有方都有利。

单一注册使个人或用户能够登录不同的组织，同时只要记住一个口令，而不允许所有这些组织相互之间冒充该人，简单地直接对所有组织使用同一口令就会造成这种情况。

最近，已知身份管理，尤其是单一注册，例如有 Liberty Alliance([URL: http://www.projectliberty.org](http://www.projectliberty.org))或者 Microsoft 公司的 Passport 系统（[URL: http://www.passport.com](http://www.passport.com)）。Microsoft 公司的所谓 Passport 系统或者简称为 Passport 是一种网络服务，其由 Microsoft 公司独家运行，允许用户登录网站并且进行电子商务交易。虽然已经许诺有不那么排他的运营，但是这样的运营仍没有公开。Passport 当前包含验证服务（不太有用的专门验证服务）以及快速购买服务。

与身份管理有关的老一些的系统类型为传统的单一注册产品、公开密钥基础结构以及表单填写器。

然而，已知的产品或建议中没有一个能够以全球信息社会尤其是一般电子商务所需的可互操作方式适应该信息社会与电视商务的各种参与者具有的所有不同需求。具体地讲，所有现有产品与建议都不能实现以后还会详细描

述的以下需求中的至少一种:

1、适合于自由选择持有关于个人的身份相关信息的位置实体,包括在各个用户自己的物理控制之下的位置实体,即所谓的本地钱包,并且还包括多个位置实体持有一个人的信息。

2、适合于只有浏览器的客户端以及甚至通过各种不同浏览器访问系统的用户,同时不需要他们以代理角色浏览通过位置实体,这就使位置实体能够看到该用户的所有消息内容。显然,只有浏览器的用户与具有本地钱包的用户是不同的——需求是服务器的方法与两者都要互操作。

3、适合于传送验证信息以及其他身份相关信息两者,其中后者可以由用户自由选择诸如偏好或者第三方确认所需的这样的两者。

4、适合于希望保持匿名的用户,同时仍然允许传送某些身份相关信息,例如偏好或者人口统计信息。

5、对于身份相关信息释放的灵活的隐私策略。

讨论满足这些需求(此后简称为 Req.)的身份管理系统的益处可能是有帮助的: Req.1 由雇主与银行这样的公司提出,它们希望至少在与其业务有关的关系中担当其雇员或者顾客的位置实体。另外,现在人们是否会自愿地采纳身份管理还没有如人们可能被引导地认为的那样清楚。当前,对于大多数人来说,对于“将所有鸡蛋都放在一个篮子里”的恐惧以及隐私与信任的担忧超过了单一注册以及简化表单填写两者所觉察的益处。再一次地, Req.1 中的自由选择可能有助于(尤其是)允许关于用户的真正个人信息的“本地”位置实体。这后几种担心还促进了 Req.4。Req.2 出于实际考虑,既因为不能让用户安装附加软件,也因为某些用户从各种因特网公用设施等使用信息社会基础结构。因特网公用设施被认为是例如在网吧中的公用计算机。Req.3 针对一般应用性与用户友好性,例如,只使用一个系统就允许对于特定信息的访问限制以及只对特定用户的特定操作,以及还有向商务伙伴传送地址、送货信息等等。Req.3 与 Req.5 最后部分的益处可以从以下看出: 传送少量数据针对的是标准电子商务应用,其中经常需要像送货与收费信息这样的数据,并且这些信息不大依赖于通信伙伴。对诸如预定与旅行偏好这类的更具体的数据的扩展中,人们必须更好地区分伙伴。长期的综合解决方案将包括需要第三方确认的数据,并且这些方案将与诸如使用这些收据的税务申报之类的其他个人应用集成。另外,长期的解决方案将集成诸如日历共享等个

人至个人的应用，以及诸如某人的雇主已经订阅的访问服务之类的企业至企业。

传统的单一注册方案以及产品包含许多登录脚本或者对于许多应用的口令。例如，US 5944824 公开了一种对于多个网络元素的单一注册系统与方法。这不允许只有浏览器的客户端，除非使用代理（参看 Req.2）。另外，其只覆盖了验证信息，却没有覆盖其他身份相关信息（参看 Req.3），因此也没有隐私策略（Req.5）。

传统的公开密钥基础结构（PKI），最有名的有 X509，实际上只考虑了验证信息（参看 Req.3）。因为信息是通过固定证书传送的，所以如果该证书包含了其他身份相关信息，则该信息是固定的，这与 Req.5 矛盾。对于专门用途的客户端软件，可以容易地设计一种分离地发送其他属性的方法，例如，用属性证书的方法，但是这与只有浏览器的客户端不兼容（Req.2），并且尤其是没有使用各种浏览器的可以互操作的方法（还是 Req.2）。

在电视商务中传送个人数据的传统产品为表单填写器。它们与浏览器密切交互，以拖曳属性到表单字段中，或者使用功能强大的工具来解释表单中的这些字段。它们一般只作为复杂客户端工作，否则作为代理工作，这与 Req.2 矛盾。另外，它们没有提供完全的互操作性，这是因为没有相应的方法使服务器请求该信息。

Microsoft 的 Passport 假定一个固定位置实体或者至少一组都具有有关特定域内用户的信息的实体，即没有用户的选择或者基于其他商业关系的选择，例如，选择用户的银行作为位置实体，从而其与 Req.1 冲突。这是该系统的固有性质，而不是可以通过不同的使用方法或者实施方式而加以改变的，这是因为假定服务器实现知道应该连接到哪个位置实体。虽然正在考虑对所谓联盟的扩展，但是这些扩展可能会保留某些其他不足，像以下系统一样。Passport 也不区分需要第三方确认的信息（参看 Req.3）。另外，其不允许真正匿名：存在全局用户标识符，用户只能通过具有多个帐户并因此不太容易的管理来避免这一点，另外，位置实体了解用户的通信模式（参看 Req.4）。还不具备灵活的隐私策略（Req.5）。另外，Passport 不允许服务器与位置实体之间的直接接触，而这对于较长数据的安全传送至关重要，并且在满足所有上述要求的联盟的范围（context）中作到这一点也不是简单的事情。

US 6226752 公开了一种验证的方法与装置。其不允许用户对于位置实体

的选择,原因与 Passport 相同(参看 Req.1)。其只考虑了验证信息(参看 Req.3),因此没有隐私策略(Req.5)以及对于匿名性的方法(Req.4)。

Shibboleth(<http://middlewqre.internet2.edu/shibboleth>),即 Internet2/MACE(教育中间件体系结构委员会)的项目,是正在开发支持机构内共享访问控制影响的网络资源的体系结构、框架以及技术。Shibboleth 包含找到所谓的大学实体的方法,因此部分满足了 Req.1:服务器请求用户提供所关心的大学实体的用户友好名称,并且使用称为 WAYF 的另一实体转换该名称,该 WAYF 实体“知道每个大学实体的名称与位置”。向该位置进行重定向只是为了验证,然后大学实体用该大学实体的第二地址将用户重定向回到服务器。服务器使用这另一个地址来建立至大学实体的直接联系,通过该直接联系,服务器发送请求并获得响应。该协议不允许本地钱包(Req.1)与匿名性(Req.4),具体是因为第二地址标识对于本地钱包为用户位置的大学实体位置。没有已知方法来使该地址变为相对的,即只是说“在我的机器上”。第一地址也无法是相对的,因为知道本地钱包的所有名称与位置将使这一目的无法实现。与本地钱包与匿名性的结合不兼容的另外一点是在 Shibboleth 中所有“断言”,即发送的身份相关信息,必须包含大学实体的域名。另外,虽然 Shibboleth 包含隐私策略,但是其并不如所希望的那样灵活(参看 Req.5),这是因为请求不包含服务器作出的隐私承诺。最后,对于其中用户没有向大学实体预先授权的信息释放的请求,Shibboleth 具有不充分的流动,这是因为浏览器焦点(即询问用户的方式)必须由另一重定向来重新建立,随后还有至服务器的另一个重定向。

根据以上所述,可以看到本领域仍然存在对于改进的身份管理系统的需要,其包括个人与组织之间的交换协议。

发明内容

本发明允许可靠高效的身份管理,其可以在完全互操作性下满足参与者的各种需求,尤其是验证与其他身份相关信息的传送,在这些版本中用户只具有浏览器或者持有有关用户以及匿名与已标识的用户的信息的不同的位置实体(也称为钱包)的功能更强大的软件,以及隐私策略的集成。换言之,本发明使基于网络的服务(例如电子商务)的终端用户能够进行单一注册以及对于与服务供应者的简档信息的受控交换。有利地是,本发明使用标准 HTTP

(超文本传输协议)浏览器工作,该浏览器通常提供主要用户界面。所公开的方法与系统支持零足迹(fingerprint)版本,即不需要其他软件,甚至不需要诸如 Javascript、Java 或 ActiveX (Javascript 与 Java 为 Sun Microsystems 公司的商标,ActiveX 为 Microsoft 公司的商标)之类的活动内容。另外,本发明允许多个权威方以避免任何单一故障点。这也意味着支持多个权威方,从而为用户提供自由在其间选择而不需要信任其他的机会。另外,权威方不需要相互信任,从而与像 Passport 或 Kerberos 那样的已知解决方案不同。Kerberos 是一种通过使用保密密钥加密为客户端/服务器应用提供验证的网络验证协议。

根据本发明提供了一种向请求实体提供身份相关信息的方法,所述方法包含:

位置请求步骤,由请求实体发起,用来从客户端应用请求相应于具有身份相关信息的位置实体的位置信息;

重定向步骤,用来将客户端应用连接到位置实体,以指令位置实体将身份相关信息传送给请求实体;以及

获取步骤,用来获得身份相关信息,所述获取步骤包含:

联系步骤,其中位置实体联系请求实体;

请求步骤,其中请求实体请求身份相关信息;以及

响应步骤,其中请求实体从位置实体接收身份相关信息。

该方法允许位置实体是远程的或者位于有关其身份的个人或用户的本地控制之下,并且还允许该个人的位置对于请求实体保持未知,请求实体可能是服务器。当从位置实体或者(a)借助客户端应用或者(b)当位置实体联系请求实体时直接从位置实体发送身份相关信息时,这一点仍然成立。

所述获取步骤还可以只包含重定向步骤,该步骤借助客户端应用将位置实体重定向到请求实体,并且由此向请求实体传送身份相关信息。这样做的优点在于:其比上述子步骤快,但是这样做只对简短身份相关信息安全。

该方法还可以包括确定步骤:用来根据在 URL (统一资源定位符)中承载的信息的长度确定是否执行联系步骤。这就允许在传送路径上具有 HTTP 1.0 路由器与代理。一般地,此时应该能够毫无困难地使用导致多达 255 字节长度的总体 URL 的身份相关信息。该确定步骤可以由请求实体进行,该请求实体在知道其请求的身份相关信息足够短的情况下,已经在重定向步骤中没有

传送联系地址，或者在具有长的请求或者期望长的响应的情况下，只发送联系地址。如果对于两种情况请求实体都发送信息，则可以由位置实体执行确定步骤。

如果请求实体与客户端应用之间以及客户端应用与位置实体之间使用的传送协议为安全超文本传送协议（HTTPS），则是有利的，这是因为此时可以保障信息的安全传送。使用这样的安全信道防止所谓的中间人类型的攻击。

所返回的位置信息可以相对于客户端应用的位置。如果其为相对的，则在重定向步骤中的位置信息表示“localhost”，并且如果其为绝对的，则其可以为 URL（统一资源定位符）或者其他标识请求实体通过本地正常地址转换或者借助远程目录从其导出 URL 的位置实体的信息。标识关于个人的信息也可以用来由请求实体通过列出个人与其位置实体的特定目录导出适当位置实体的 URL。

重定向步骤可以通过超文本传送协议重定向或者简称为 HTTP 重定向进行，至 localhost 或者所导出的 URL，从而向位置实体传送实际的传送指令与返回地址或者联系地址与可能的已有的传送指令与返回地址。这使具有更灵活的传送协议的获取步骤成为可能，并且不需要要求客户端应用（如果其为浏览器的话）打扰用户来按压“提交”按钮从而开始推式操作或者使能脚本。

该方法还可以包括：由请求实体从在位置实体假名之下的位置实体，与验证一道接受身份相关信息，其中身份相关信息对应于个人的个人假名。这样的益处在于：可以可靠地保护个人的匿名性。显然，本发明还包括正常的、非匿名位置实体身份以及个人身份。

该方法还可以包括：由请求实体发送对于使用身份相关信息的服务器策略。具体地，请求实体或者服务器可以（例如）在传送指令中通过引用或者直接包含对于所请求的身份相关信息的、所承诺的隐私策略或者隐私偏好，例如隐私偏好纲领（P3P）。其还可以包含另一安全相关策略，例如有关安全存储的。来自位置实体的身份相关信息还可以包含或者引用预定隐私或者其他安全策略。这样的益处在于：请求实体可以优化方式与个人以及位置实体按不同策略交互，例如此时提供不同程度的个性化。请求实体完全可以拒绝继续依赖于应用的交互，除非提供了最少量的信息。这可以在请求中指示，还可以指示对信息或者其指令的其他要求，例如由一定级别权威方的确认，

新鲜度，或者确认者可靠性。

根据本发明的第二方面，提供了一种向请求实体传送位于位置实体的身份相关信息的方法，所述方法包含：

重定向步骤，用来从客户端应用接收指令信息，以将身份相关信息传送给请求实体，其中在重定向步骤之前请求实体在位置请求步骤从客户端应用请求相应于具有身份相关信息的位置实体的位置信息以及

传送步骤，用来向请求实体传送身份相关信息，包含：

联系步骤，其中位置实体联系请求实体；

请求步骤，其中请求实体请求身份相关信息；以及

响应步骤，其中位置实体向请求实体发送身份相关信息。

所述传送步骤还可以包含：由位置实体根据预定策略确定传送在请求步骤中请求的身份相关信息的哪个部分。这样的益处在于：请求实体可以对可能对其有用的所有信息进行一般请求，但是允许位置实体根据其自身或者用户的策略确定其实际上希望提供这些信息的哪些部分，（例如）以用于营销、个性化或者统计目的。

所述响应步骤还可以包含：由位置实体传送预定策略的部分。这样的益处在于：位置实体可以指令请求实体在有关身份相关信息方面以特定方式动作，从而（例如）不将其进一步发送，或者一段时间后将其删除，或者对于一特定时段不删除它。

位置实体可以使用在重定向步骤中建立的从客户端应用至位置实体的连接，以在传送步骤进行与个人的交互。与个人交互的益处在于：可以验证该个人的身份，并且该个人可以对预定策略进行添加，并且复用所述连接（与在获取步骤之前释放该连接相比）的益处在于：可能无延迟的进行交互。

向请求实体释放个人信息可以包含以下步骤：呈现有关请求实体的信息；呈现位置实体已知的预先授权的属性值，其中预先授权指预定策略允许向请求实体释放，和/或呈现位置实体已知的非预先授权的属性值，和/或呈现未知属性值的、分配给用于输入相应属性值的空字段的属性名称；请求编辑属性值；以及向请求实体发送编辑后的属性值。通过这样做，只要求用户填写未知属性值，并且对非预先授权的属性值进行是与否的判定。这简化了程序，并且允许用户对请求实体所请求的其个人的信息进行完全控制。

不同的属性值可以不同方式呈现，最好以不同颜色呈现。这允许向用户

清楚地呈现信息，然后用户可以确定输入、删除、修改或者不加修改地发送哪些信息。

所述传送步骤还可以包含以下步骤：由位置实体生成随机值 k ，在与身份相关信息相同的连接上，将随机值 k 发送给请求实体，将随机值 k 发送给客户端应用，以使客户端应用能够针对身份相关信息向请求实体证明其真实身份。这样的益处在于：在传送身份相关信息之后，请求实体可以给予在用户处运行的客户端应用附加特权。

根据本发明的第三方面，提供了一种提供身份相关信息的系统，所述系统包含：具有身份相关信息的位置实体；可连接到位置实体的客户端应用；以及用来从客户端应用请求相应于具有身份相关信息的位置实体的位置信息的请求实体，其中，根据对于请求的响应，客户端应用被重定向到位置实体，以指令位置实体将身份相关信息传送给请求实体，其中位置实体联系请求实体，请求实体请求身份相关信息，并且请求实体从位置实体接收身份相关信息。

该系统有利于为用户标识相关权威方，即位置实体，而不需要联系任何第三方，从而避免了在某些现有技术解决方案中的隐私与性能问题。

该系统使用标准具有 SSL 功能的 HTTP 浏览器运行，即具有安全套接字层功能的超文本传送协议浏览器，并且不要求任何需要用户接受在其机器上安装某些附加的信息的功能，所述附加信息例如 cookie 或者类似软件的活动内容：Javascript、Java、ActiveX 等等。同时，在可以存储附加信息的情况下，该系统可以使效率得到提高。

与已知解决方案相比，该系统提供了防止特定攻击的更高的安全性，例如中间人攻击。

在另一例子中，客户端应用与几个位置实体交互。这意味着用户在不同位置或者在同一位置上具有多个位置实体，并且作为对位置信息请求的回应，客户端应用与个人或者用户一道选择适当的一个位置实体。因此，位置实体可以是本地的或者是远程的。这样安排的益处在于：对于该个人，其避免了单一故障点，并且使不同位置实体之间的隐私成为可能。

身份相关信息可以由另一位置实体提供。然后，可以由请求实体借助位置实体获得身份相关信息。所述另一位置实体的位置信息存储在位置实体上。这样安排的益处在于：其避免了客户端应用或者个人必须在位置实体之间选

择，同时仍然允许不同类型的身份相关实体存储在不同的位置实体中。

附图说明

以下将参照以下示意图详细描述仅作为例子的本发明的优选实施方式。

图 1 显示根据本发明的系统的示意图。

图 2 显示根据本发明第一实施方式的消息流的示意图。

图 3 显示第二实施方式的消息流的示意图。

图 4 显示第三实施方式的消息流的示意图。

图 5 显示具有在图 4 步骤 II 中发送的位置查询的、向潜在用户呈现的表单的图。

图 6 显示图 4 所示第三实施方式的扩展的示意图。

图 7 显示完成一半的、向用户呈现的另一表单的图。

图 8 显示允许验证客户端应用身份的、第一或第三实施方式的扩展的示意图。

图 9 显示一个客户端与几个位置实体交互的系统的示意图。

图 10 显示身份信息由另一实体提供并且可以由请求实体借助位置实体获得的系统的示意图。

附图只用于解释目的，而不一定表示缩小了的本发明的实际例子。

具体实施方式

词汇表：

以下非正式定义用来帮助理解本说明书。

个人：其身份被管理的实体。如果个人行动，则其变为用户。个人或用户一般为单个人，但是至少小企业经常如同单个人那样与其他企业交互，例如，在旅行预定与信息收集中。

请求实体：希望知道个人的名称或者属性的实体，例如由服务器表示的组织。因为对于任何容易部署的注册系统没有什么保证，所以起始组织将主要是因特网商店。从长远看，组织包括所有个人的、诸如银行、医生、同事以及家庭之类的通信伙伴。如果希望在身份管理中包含联系或位置信息（例如消息与日历），则作为“组织”的同事与家庭尤其有意义。

位置实体：存储个人的身份相关信息的实体。位置实体也称为钱包。位置实体或者钱包指为个人存储并处理个人信息的组件，一般为软件。位置实体持有者可以是个人自己，或者是其信任的一方。成为职业位置实体持有者可能需要前提条件，例如隐私与安全承诺以及适当的预防措施。首要位置实体持有者持有个人的单一注册口令，更具体地讲，其在没有另一实体干预的前提下可以识别个人。因此，如果个人能够记住几个口令，则他或她可以具有持有不同类型信息的几个首要位置实体持有者。本地位置实体位于该个人的计算机上。远程位置实体位于分离的位置实体持有者（一般为职业位置实体持有者）的计算机或服务器上。其可以与位于该持有者处的其他位置实体集成。

联盟：联盟一般指一组职业位置实体持有者与位置实体制造者。该组还可以包含个人或组织的代表，以协助大家都满意的标准，但是个人或组织可以成百上千万，而对职业位置实体持有感兴趣的实体可能几万，例如银行、CA（证书权威方）、ISP（因特网服务提供商）以及大的雇主。

法律实体或者组织可以担当上述的几种角色。

术语“计算机”包含诸如 PC 之类的设备，还包含具有浏览设施的数字助理以及移动电话。

详细描述

参照图 1，显示了可以使用本发明的通信环境的一般布局。在附图中，相同的标号表示相同的部件。图 1 显示作为用户 20 的个人 P。用户 20 在其机器上执行客户端应用 30，例如网络浏览器。客户端应用 30 为了依赖于应用的交互而连接到请求实体 50，例如提供服务的公司或银行的服务器。客户端应用 30 与请求实体 50 通过通信线路 5 连接，如现有技术所知。通信线路 5 一般通过网络例如互联网提供。客户端应用 30 还连接到位置实体 40，也称为钱包，其中位置实体 40 可以是本地的，即在用户 20 的计算机处，或者是远程的，即在外部服务器等等之上。位置实体 40 还可以连接到请求实体 50 以传送身份相关信息 IRI。作为术语“身份相关信息”，IRI 被理解为与个人或用户有关的任何信息。身份相关信息 IRI 包括名称、地址、组成员、授权证书、人口数据、个人偏好、日历项目、医疗与财务信息以及可以数字地存储的关于个人的或者在用户名下的其他任何信息。请求实体可能希望得到它

用于访问控制、授权、个性化、验证、登录、商务、医疗或政府事务，或者依靠身份相关信息 IRI 运行的任何其他应用。显示图 1 中的场景是为了有利于对于以下向请求实体 50 提供身份相关信息 IRI 的流程的描述。

图 2 显示第一实施方式的消息流的示意图。此处，客户端应用 30、位置实体 40 以及请求实体 50 之间的流利用标注箭头显示，向这些标注箭头分配了罗马数字。进一步的步骤或者子步骤由圆圈内的罗马数字指示。该流程理解为自顶向下依次进行，如递增的罗马数字所示。在步骤 I，在客户端应用 30 与请求实体 50 之间进行依赖于应用的交互。在位置请求步骤 II，该步骤由请求实体 50 启动（子步骤 IIa），请求实体 50 从客户端应用请求相应于具有身份相关信息 IRI 的位置实体 40 的位置信息 LI。在子步骤 IIc，位置信息 LI 发送到请求实体 50。可选地，子步骤 IIb 允许客户端应用 30 以不同的方式导出位置信息 LI，例如通过询问用户或者内部地导出。其后，重定向步骤 III 具有重定向指令（子步骤 IIIa），其中客户端应用 30 最终连接到位置实体 40（子步骤 IIIb）。通过这样做，位置实体 40 被指令传送身份相关信息 IRI 给请求实体 50。在获取步骤 IV，请求实体 50 如下获得身份相关信息 IRI。进行联系步骤 IVa，其中位置实体 40 联系请求实体 50。然后，进行请求步骤 IVc，其中请求实体 50 从位置实体 40 请求身份相关信息 IRI。最后，响应步骤 IVe，请求实体 50 从位置实体 40 接收身份相关信息 IRI。可以以不同的已知方式检索请求，如子步骤 IVb 所示，例如通过请求实体 50 在重定向步骤 III 中包含的以及位置实体 40 在联系步骤 IVa 中包含的会话标识符。另外，位置实体 40 可以（例如）根据用户验证、策略等等决定是否响应，以及响应什么，如子步骤 IVd 所示。可以使用内部的或者可能的外部的信息来准备响应。子步骤 IVf 指示请求与响应步骤 IVc 与 IVe 的可能重复，以获得更多的身份相关信息 IRI，或者解决错误，以及可能的对于该交换的结束消息。如子步骤 IVg 所示，可能在回连步骤 IVgii 中进行从位置实体 40（重定向返回步骤 IVgi）通过客户端应用 30 到请求实体 50 的重定向。然后，客户端应用 30 与请求实体 50 之间依赖于应用的交互再次成为可能，如步骤 V 所示。

图 3 显示第二实施方式的示意图，与第一实施方式相比，第二实施方式具有相似的消息流，不同之处在于进行获取步骤 IV 而不用联系、请求以及响应步骤 IVa、IVc、IVe。相反，现在进行重定向步骤 IVg，使得位置实体 40 传送身份相关信息 IRI，其中位置实体 40 通过客户端应用 30 连接到请求实

体 50。在该场景中，在子步骤 IVd，位置实体 40 与用户 20 交互，以使用户 20 验证自己的身份。在某些情况下，用户 20 还应该在子步骤 IVd 确认请求实体 50 的身份，这是因为位置实体 40 自身无法识别请求实体 50。

图 4 显示第二实施方式的示意图，其中假定安全信道，如可以由安全超文本传送协议 (HTTPS) 提供。假定在请求实体 50 与客户端应用 30 之间有安全信道 (未显示)。第三实施方式是浏览器特有的。这意味着客户端应用 30 此处为由用户 20 控制的浏览器 30。因此在图 4 中的左侧引入另一列，标注有个人 20，即指行动用户 20。用户 20 被请求与浏览器 30 交互。在步骤 I，用户 20 正浏览到请求实体 50。如果浏览器 30 以前访问过请求实体 50 并且仍然有一打开放的会话或者请求实体 50 设置并且浏览器 30 接受 cookie，或者浏览器 30 自动传送特定用户设置，则位置请求步骤 II 有时可以省略，如在现有的解决方案中一样。在子步骤 IIa，从请求实体 50 向浏览器 30 传送具有位置查询的表单，并且呈现给用户 20。可以以图 5 所示的方式进行该呈现，其中用户 20 使用选项来提交具有身份相关信息 IRL 的位置信息 LI。在子步骤 IIc，向请求实体 50 发送像 “localhost” (其指位置实体 40 位于本地) 或者地址的位置信息 LI。子步骤 IIa 与子步骤 IIc 定位位置实体 40 以准备重定向步骤 III。如果所有的位置实体 40 (此处只显示一个) 都是本地的，则可以将重定向指向 “localhost” 处的固定端口。类似地，当只有一个远程位置实体持有者时，可以将重定向直接指向该远程位置实体持有者。然而，必须区分不同的远程位置实体 40，即使一个用户也可能具有多个位置实体 40。为这些步骤建立总体用户交互的最简单方法是在屏幕上向用户显示上述表单，如图 5 所示。重定向步骤 III 包含子步骤 IIIa，现在为 HTTP 重定向，其中从请求实体 50 向浏览器 30 发送联系地址，以及子步骤 IIIb，其中浏览器 30 连接到位置实体 40。所述联系地址包含协议绑定，其可以是 HTTP 绑定，但也可以是另一协议，诸如 SOAP (简单对象访问协议) 绑定。另外，还传送会话标识符 SID 以在子步骤 IIIb 中使用。传送其他信息 (例如在步骤 I 中请求的最后的 URL) 是可能的，但并不推荐，因为其可能侵犯用户对于本地实体 40 的隐私。如果请求实体 50 猜测所希望的身份相关信息 IRI 太短，则其可以立即包含该确切请求以及返回地址 (可在子步骤 IVg 中使用)。如果其确定，甚至可以省略联系信息。对 “太短” 的稳妥定义为在子步骤 IVg 中的结果总体 URL 不超过 255 字节。通过在子步骤 IIIb 获得连接消息，位置实

体 40 被指令向请求实体 50 传送身份相关信息 IRI。在获取步骤 IV，请求实体 50 如下获得身份相关信息 IRI。在联系步骤 IVa，如果不是如参照图 3 所述地进行，则通过使用在联系地址中包含的协议，将位置实体 40 连接到联系地址，即请求实体 50。进行请求步骤 IVc，其中借助在联系步骤 IVa 建立的连接，通过根据会话标识符 SID 检索适当的请求，请求实体 50 从位置实体 40 请求身份相关信息 IRI。所述请求可以是任意已知形式，例如达成一致的扩展标记语言（XML）模式。在响应步骤 IVe，请求实体 50 接收来自位置实体 40 的身份相关信息 IRI。该响应将是对应于请求的格式的已知格式，例如，来自相应的响应 XML 模式。位置实体 40 可以确定是否响应以及响应什么，例如，通过评估用户验证、策略、带请求的请求实体 50 提交的验证与证书、用户 20 的实时释放（release）等。如子步骤 IVd 所示。子步骤 IVf.i 指示返回地址可能依赖于所收到的响应，例如原来所请求的资源的不同的个人化了的版本。然后，由请求实体 50 向位置实体 40 发送返回地址，如子步骤 IVf.ii 所示。然后，进行重定向，如子步骤 IVg 所示。此处，返回地址在子步骤 IVg.i 从位置实体 40 发送到客户端应用 30，客户端应用 30 进而连接到该返回地址，即连接到请求实体 50，如回连步骤 IVg.ii 所示。该步骤可以承载其他信息，例如，用来验证浏览器 30 的信息，如下参照图 6 所述。子步骤 IVh 允许请求实体 50 以任何已知方式查找在响应步骤 IVe 接收的适当响应用于正在连接的浏览器 30，并因此将该响应用于与该浏览器 30 的进一步交互。为此，使用 HTTPS 提供了安全会话，这些安全会话可以通过其他已知会话维护机制得到改进。然后，由用户 20 执行的、浏览器 30 与请求实体 50 之间的浏览可以再次进行，如步骤 V 所示。

图 5 显示向潜在用户呈现的表单或者示例屏幕的图，其具有可以在图 4 的位置请求步骤 II 中呈现的位置查询。为了使该表单或者示例屏幕看起来真实，还显示了拒绝标识以及借助用户名称与口令的遗留验证，以及到有关请求实体 50（例如组织）的信息的链接，该信息可能帮助用户 20 确定填写什么。“o”为单选按钮，字段用户输入文本。词“联盟身份”可以表示待选择的品牌。选择“我自己的钱包”给出至“localhost”的重定向，即位于本地的位置实体 40。查找选择使请求实体 50 在全局目录中查找在“我的名称是”之后输入的名称；该选项降低了隐私，但是某些人可能会忘记自己位置实体的地址。用户 20 可以在“我们是谁”之下了解请求实体 50，以及在“隐私

策略”之下了解这些策略。借助“提交”按钮可以提交信息。如参照图 4 所述，如果用户总是允许联系其位置实体 40，则有几种方法允许用户避免这样的屏幕。

图 6 显示如图 4 所示的第三实施方式的扩展的示意图，具体地为子步骤 IVd，响应导出的实施方式。只显示了相关的流程。在子步骤 IIIb，浏览器 30 连接到位置实体 40。在获取步骤 IV，请求实体 50 获取身份相关信息 IRI。此处，在子步骤 IVd.i，进行个人的验证。该子步骤 IVd.i 也可以在执行联系步骤 IVa 与请求步骤 IVc 时并行进行。如果具有根据已知机制的安全会话，则该步骤可以省略。然后，在子步骤 IVd.iii，向用户 20 呈现完成一半的表单。IVd.ii 表示当使用预定策略时尽可能地准备响应，以及从请求响应格式转换到用户友好格式。在释放子步骤 IVd.v 从浏览器 30 向位置实体 40 传送作为表单的、完成后的响应之前，用户可以在子步骤 IVd.iv 改变该表单，位置实体 40 最终在响应步骤 IVe 将该响应转发给请求实体 50，现在再次为请求响应格式。

图 7 显示在图 6 子步骤 IVd.iii 中呈现给用户 20 的完成一半的表单的图。开头的文本解释该表单，并且指出谁请求该信息，即<名称>为请求实体 50 的名称，就像位置实体 40 在联系步骤 IVa 期间验证请求实体 50 的身份时获得的那样。如果在另一实施方式中在响应步骤 IVe 之前没有该验证，则在这种表单中的该行应该相应地以不同方式形成，例如，应该在来自步骤 I 的 HTTPS 连接中要求用户 20 检查服务器证书。“名称”、“送货地址”、“身份证号”以及“你的收入”是属性或者属性名称的例子。为“名称”、“送货地址”以及“身份证号”已经输入了各自的属性值，这是因为在该例子中假定这些对于位置实体 40 来说是已知。位置实体 40 不知道“你的收入 (income)”，因此为空。在已知的属性中，“名称”与“送货地址”假定被预先授权，但是“身份证号”不被预先授权。因此，它们的属性值以不同的用户界面风格呈现，例如以不同的颜色，以使用户 20 可以容易地看出哪些信息是敏感的，哪些不是。用户 20 掌握编辑或者删除给定属性值以及添加缺失属性值的完全的灵活度。可选地，用户 20 通过诸如“*”等提示来获得哪些是必须提交或者确认的提示。这意味着该呈现还包含将属性表征为从接收实体 50 的观点看为必须或者自愿的元素。在我们例子中，在以“红色:”以及“*”开始的行中解释了这些用户界面元素与指示符的含义。“提交”按钮允许提交该表单中的

信息。在另一例子中，可以重复执行子步骤 IVd.iii 到 IVd.v，其中在子步骤 IVd.iii 的重复中呈现属性，其具有位置实体 40 的附加注释，例如错误信息，并且只有在子步骤 IVd.v 中释放最后一次重复之后，才进行对请求实体 50 的响应。该呈现可以作为具有属性的可编辑字段的正常网络表单执行。在另一例子中，在用户 20 的编辑阶段或者适当重复具有必要属性缺失的特定注释的步骤之后，如果不是所有必要属性都可用并且已授权，则不释放任何属性。

图 8 显示在子步骤 IVg 中提供浏览器 30 的验证的第一或第三实施方式的扩展的示意图。考虑到位置实体 40，此处获取步骤 IV 称为传送步骤 IV。图 8 已经以重定向步骤 III 的第二部分开始，其中在子步骤 IIIb 客户端应用 30 连接到位置实体 40。进行联系步骤 IVa，其中位置实体 40 联系请求实体 50。然后，进行请求步骤 IVc，其中请求实体 50 从位置实体 40 请求身份相关信息 IRI。在子步骤 IVd，位置实体 40 生成随机值 k。在响应步骤 IVe，响应与随机值 k 一道被发送给请求实体 50。子步骤 IVf.ii 指示返回地址从请求实体 50 到位置实体 40 的传送。然后，如子步骤 IVg 所示，进行重定向。此处，在子步骤 IVg.i，从位置实体 40 向客户端应用 30 传送返回地址与随机值 k，客户端应用 30 还连接到返回地址，即连接到接收随机值 k 的请求实体 50，如回连步骤 IVg.ii 所示。在子步骤 IVh，请求实体 50 使用所接收的随机值 k 来查找发生同一随机值 k 的、在响应步骤 IV 收到的响应。然后，再次可以进行由请求实体 50 发起的、客户端应用 30 与请求实体 50 之间依赖于应用的交互，如步骤 V 所示。通过向客户端应用 30 发送随机值 k，使客户端应用 30 能够针对身份相关信息 IRI 向请求实体 50 证明其身份真实性。在另一例子中，值 k 只是伪随机的，甚或只是部分伪随机的。然而，在所有正确的例子中，其都应该是实际不可猜测的。

图 9 显示参照图 1 所述的通信环境的扩展的示意图。向图 1 附加地安排了第二位置实体 42。该第二位置实体 42 可以是本地或远程的，并且可以通过通信线路 5 连接到客户端应用 30 与请求实体 50。一般地，一个客户端应用 30，即一个浏览器 30，在此处与几个位置实体 40、42 交互，并且在位置请求步骤 II 选择适当的一个位置实体。

图 10 显示参照图 1 或图 9 所述的通信环境的另一种结构的示意图。此处身份相关信息 IRI 由另一个位置实体提供，即第二位置实体 42。请求实体 50 可以通过位置实体 40（此后也称为第一位置实体 40）获得身份相关信息 IRI。

因此，与对第二位置实体 42 持有哪些身份相关信息 IRI 的指示一道，将第二位置实体 42 的位置信息 LI 存储在第一位位置实体 40 上。因此，客户端应用 30 总是可以在位置请求步骤 II 选择一个第一位位置实体 40。该例子显示只连接到第一位位置实体 40 的第二位置实体 42，即表示这样的实施方式：在子步骤 IVd 内，第一位位置实体 40 直接从第二位置实体 42 检索身份相关信息 IRI。所述身份关系可以承载来自第二位置实体 42 的验证或者其他安全属性。在另一例子中，在子步骤 IVd 内，第一位位置实体 40 可以将客户端应用 30 重定向到第二位置实体 42，从而也允许第二位置实体 42 与用户 20 交互。在另一例子中，第二位置实体 42 可以将请求实体 50 的联系信息转发到第二位置实体 42，以便第二位置实体 42 可以将其身份相关信息 IRI 直接传送给请求实体 50。

在附图中显示的所有例子都假定请求实体 50 与位置实体 40（或 42）可以相互直接验证身份。这可以通过已知技术容易地达到，例如，通过使用具有在各自联盟中达成一致的根权威方（root authority）公共集合的公开密钥证书。例如，如果连接是通过 HTTPS 或者另一使用 TCP（传送控制协议）的协议，则在联系步骤 IVa，请求实体 50 可以使用安全套接字层（SSL）服务器证书来向位置实体 40 验证身份。为了使匿名性成为可能，位置实体 40 不应该总是使用这样的证书，例如，如果只请求可以自由选择的身份相关信息 IRI 的话。如果身份相关信息 IRI 需要已知权威方（其可能是图 10 中的第一位位置实体 40 或者第二位置实体 42）的确认，其可以（例如）由针对 X509 证书的 XML 签名给出。在另一例子中，请求实体 50 与位置实体 40（或 42）可能已经预先交换过特殊密钥并且使用这些特殊密钥。在另一例子中，可能希望只使用对称密钥（至少在 HTTPS 之外），但是请求实体 50 与位置实体 40 预先还没有交换过密钥。这也是可能的，但是某种程度上降低了匿名性，或者需要不同实体相互更强的信任。具体地讲，参照图 2，联系步骤 IVa 可以通过对于位置实体 40 与请求实体 50 借助中间方链（chain）的 Kerberos 密钥交换协议扩展。参照图 3，或者位置实体 40 可以开始同一协议，或者客户端应用 30 可以通过中间方链重定向，其中每个中间方根据先前的“票签（ticket）”授与其新的、具有身份相关信息（此处一般为验证信息）的票签，这与 Kerberos 类似，只是在 HTTP 之内，而不是作为密钥交换。

任一公开的实施方式都可能与所显示和/或描述的其他实施方式的一或多个组合。这对实施方式的一或多个特征也是可能的。

本发明可以以硬件、软件或者硬件与软件的组合实现。任何类型的计算机系统——或者适合于执行此处所述的方法的设备——都是适合的。硬件与软件的典型组合为具有计算机程序的通用计算机系统，所述计算机程序当被加载并执行时，控制所述计算机系统使其执行此处所述的方法。本发明还可以嵌入计算机程序产品，该产品包含所有使此处所述的方法的实施方式成为可能的特征，并且该产品当被加载到计算机系统中时，能够执行这些方法。

在当下的语境中，计算机程序部件或者计算机程序指一组指令的、任意语言、代码或者标记形式的任何表达，所述指令用来使具有信息处理能力的系统或者直接或者在以下一者或者两者处理之后执行特定功能：a) 转换为另一语言、代码或者标记；b) 以不同的物质形式再现。

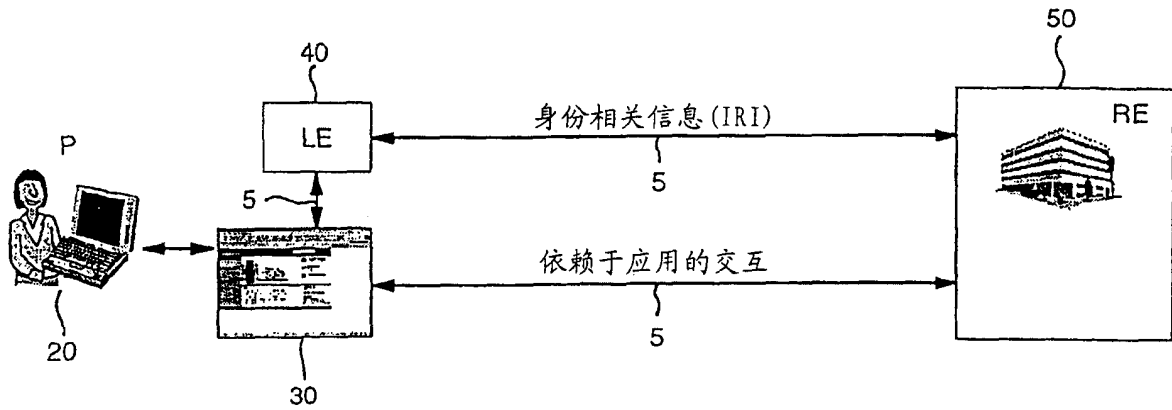


图 1

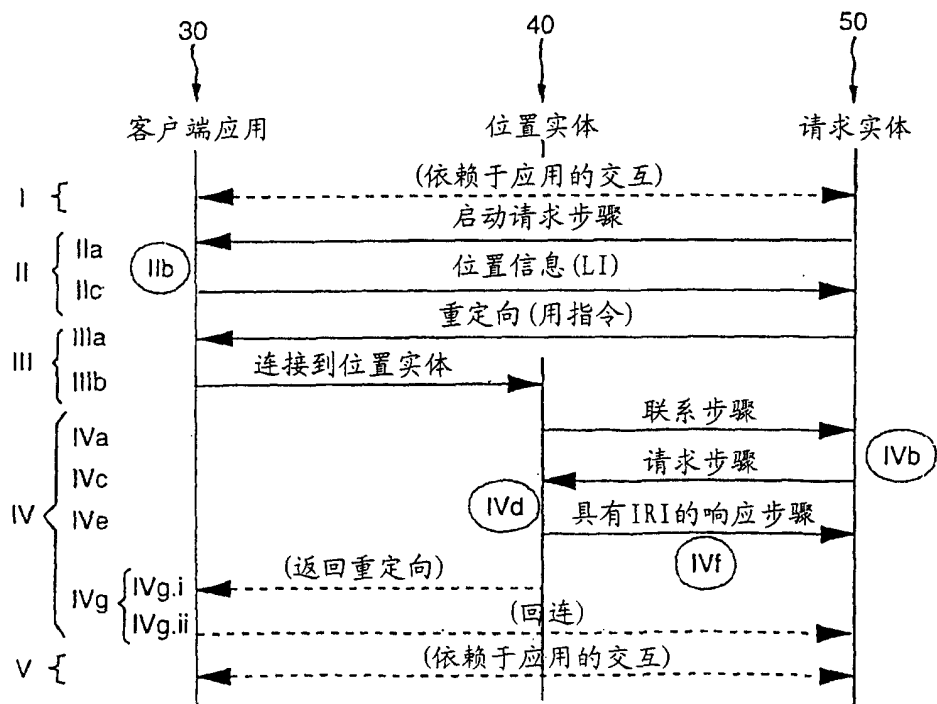


图 2

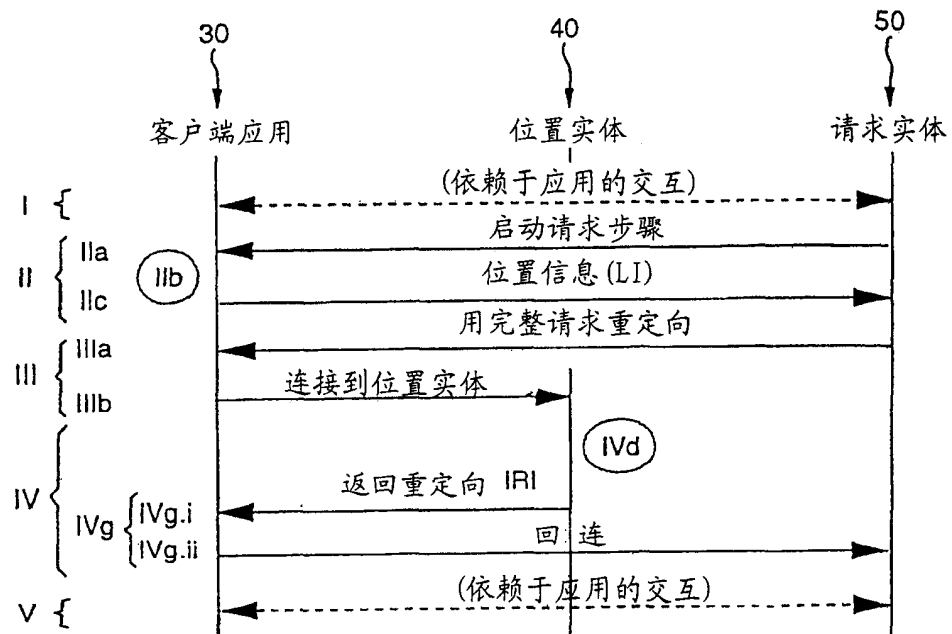


图 3

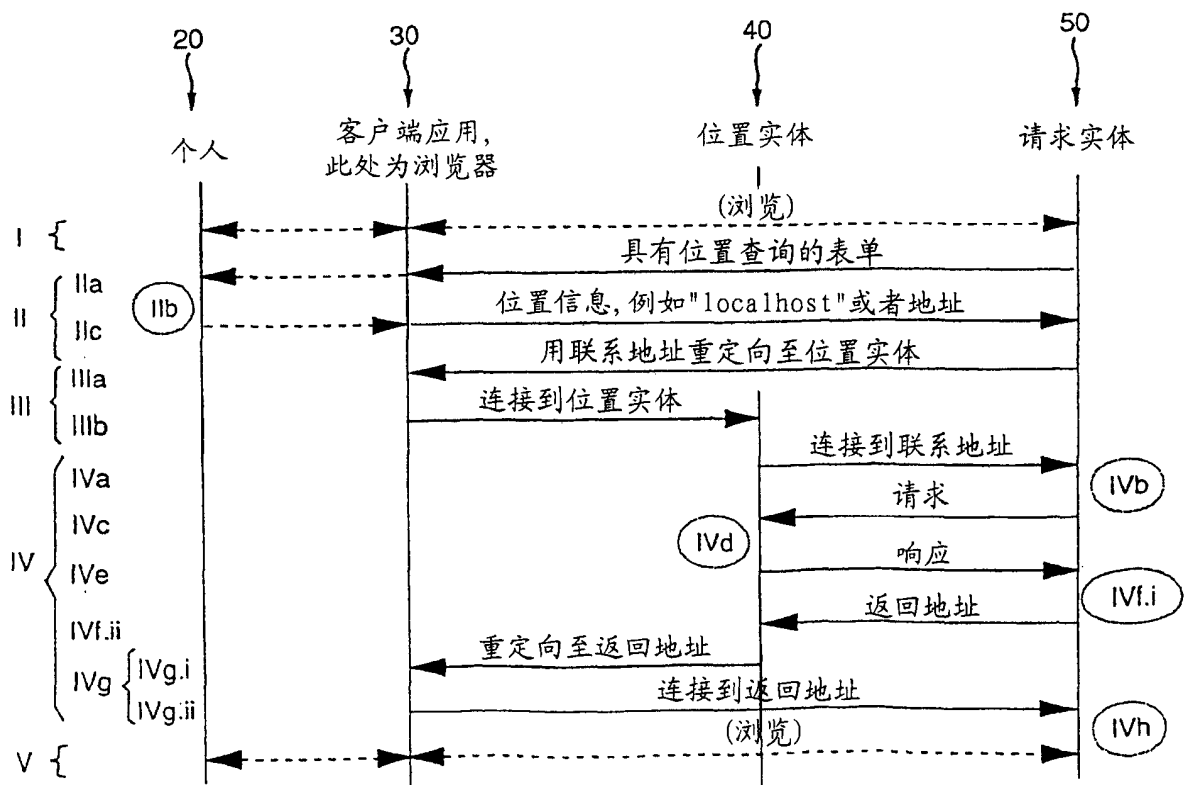


图 4

我们希望你进行了解。

我们怎样才能找到？

○ 不, 我不想泄露任何情况

○ 我具有你的用户名称/口令

○ 我具有联盟身份以及

○ ... 我自己的钱包

○ ... 我的钱包持有者

○ ... 查找我, 我的名称是

提交

你可以看到 我们是谁 以及我们的 隐私策略。

图 5

The diagram illustrates a sequence of interactions between four entities: 20 (个人 - Individual), 30 (客户端应用, 此处为浏览器 - Client application, here browser), 40 (位置实体 - Location entity), and 50 (请求实体 - Request entity).

Entity 20 (个人): Labeled with III and IV. Sub-steps include IIIb, IVd.i, IVa, IVc, IVd.iii, IVd.iv, IVd.v, and IVe.

Entity 30 (客户端应用, 此处为浏览器): Acts as the central interface.

Entity 40 (位置实体): Labeled with IVd.ii.

Entity 50 (请求实体): Labeled with IVb.

Sequence of Interactions:

- Entity 30 connects to Entity 40: 连接到位置实体 (Connect to location entity).
- Entity 30 sends a request to Entity 20: 验证个人身份 (Verify individual identity).
- Entity 30 connects to Entity 50: 连接到联系地址 (Connect to contact address).
- Entity 30 sends a request to Entity 50: 请求 (Request).
- Entity 40 sends a response to Entity 20: 完成一半的作为表单的响应 (Response for half of the form).
- Entity 20 sends a response to Entity 30: 完成的作为表单的响应 (Completed response for the form).
- Entity 30 sends a response to Entity 40: 完成的作为表单的响应 (Completed response for the form).
- Entity 40 sends a response to Entity 50: 响应 (Response).


图 6

24

你的伙伴, <名称>, 希望得到有关你的以下数据

- 名称
- 送货地址
- 身份证号
- 你的收入

Mary Smith	★
1 Marystreet, Smithtown, GB	★
1111 2222 3333	

 你可能不希望发送这个数据
 * : 他们没有这个数据就不继续

提交

图 7

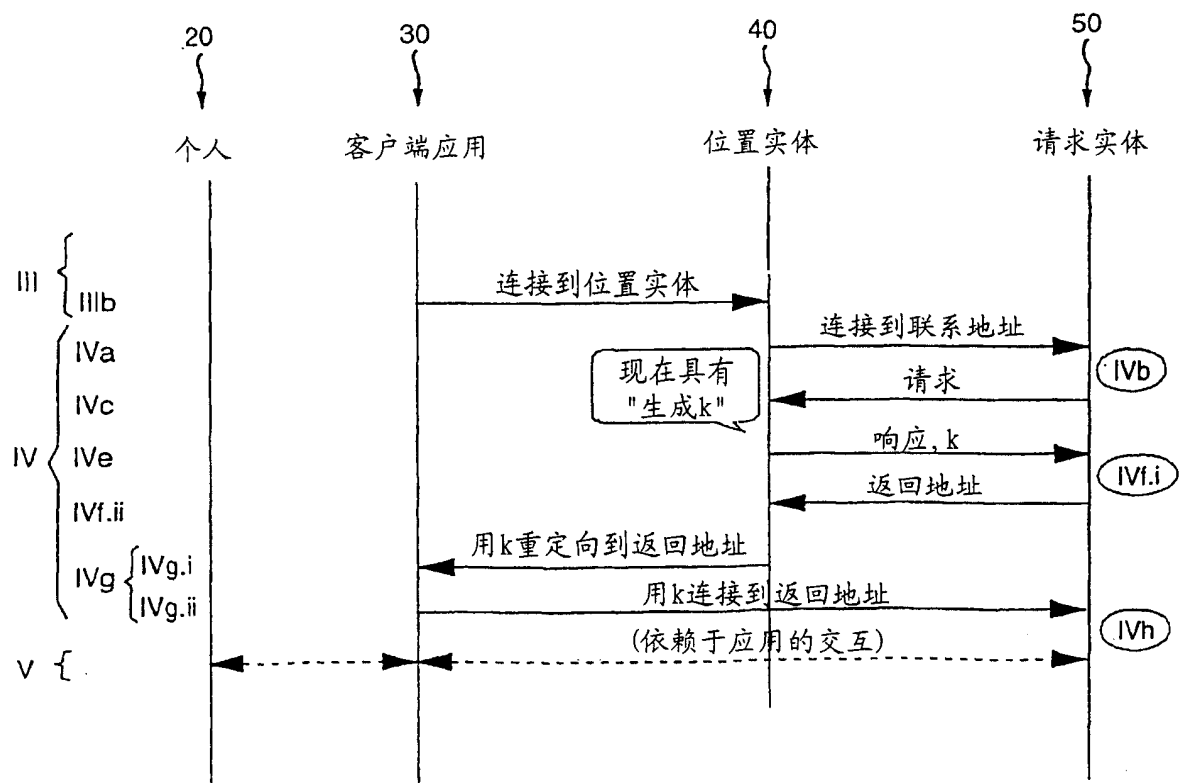


图 8

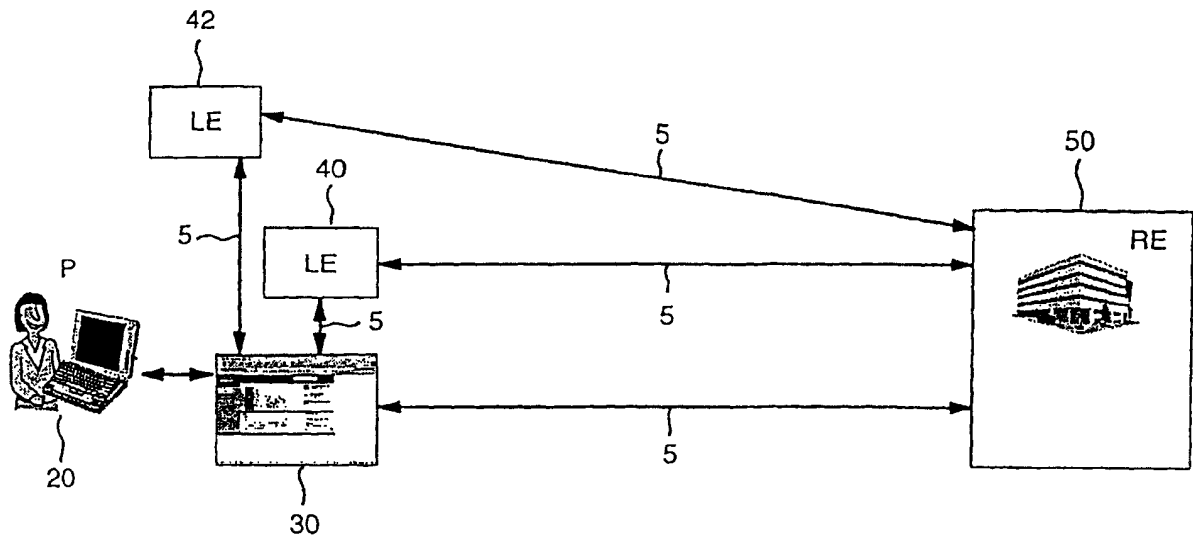


图 9

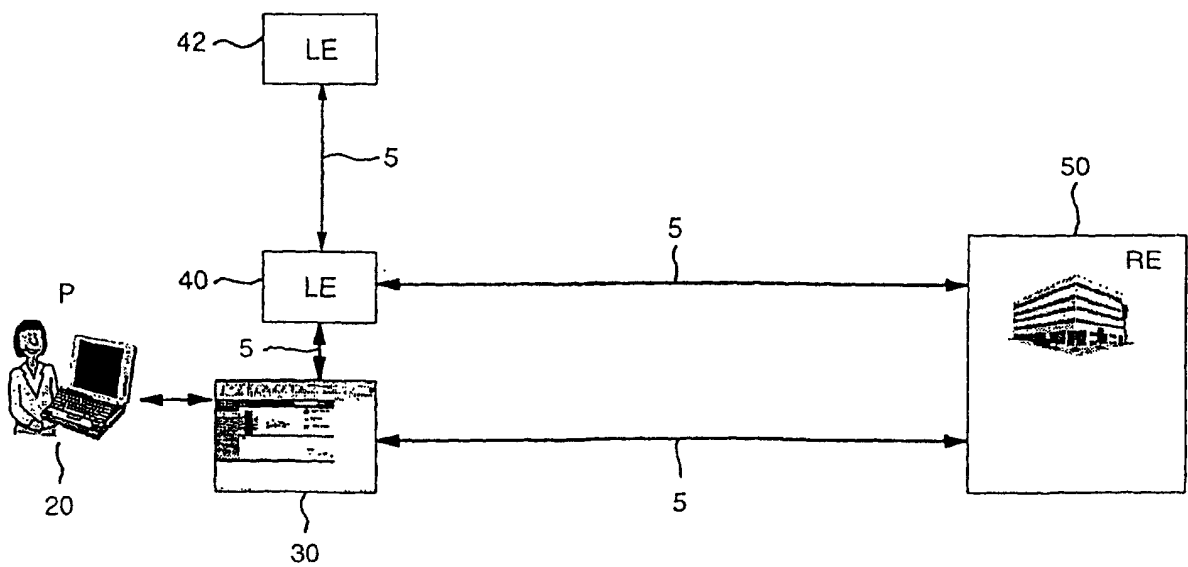


图 10