



(12) 发明专利申请

(10) 申请公布号 CN 102171984 A

(43) 申请公布日 2011. 08. 31

(21) 申请号 200880131426. 3

H04L 29/08 (2006. 01)

(22) 申请日 2008. 10. 06

(85) PCT申请进入国家阶段日
2011. 04. 06

(86) PCT申请的申请数据
PCT/EP2008/063333 2008. 10. 06

(87) PCT申请的公布数据
W02010/040378 EN 2010. 04. 15

(71) 申请人 诺基亚西门子通信公司
地址 芬兰埃斯波

(72) 发明人 刘进

(74) 专利代理机构 中国专利代理(香港)有限公
司 72001

代理人 王岳 卢江

(51) Int. Cl.
H04L 29/06 (2006. 01)
G06F 21/00 (2006. 01)

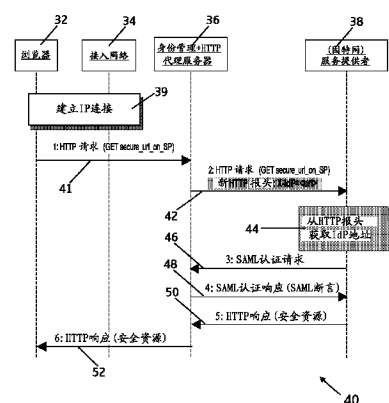
权利要求书 2 页 说明书 6 页 附图 5 页

(54) 发明名称

服务提供者访问

(57) 摘要

描述了一种用于使得用户能够访问服务提供者的方法和设备。用户从浏览器向代理服务器发送请求。代理服务器通过添加关于能够为用户提供用户证书的身份提供者的位置的数据(诸如 URL)来修改请求并将经修改的请求转送至服务提供者。访问请求的修改可以在请求被发送到服务提供者之前或响应于来自服务提供者的认证请求而发生。可以将关于身份提供者的位置的数据作为报头(例如 http 报头)来提供。



1. 一种方法,包括以下步骤:
从用户接收对访问服务提供者的请求;
通过添加关于能够为用户提供用户证书的身份提供者的位置的数据来修改所述请求;
以及
将经修改的请求转送到服务提供者。
2. 如权利要求 1 所述的方法,其中,响应于用户对访问服务提供者的请求来执行修改所述请求的步骤。
3. 如权利要求 1 所述的方法,其中,响应于服务提供者请求用户授权来执行修改所述请求的步骤。
4. 如权利要求 1 至 3 中的任一项所述的方法,其中,被添加到请求的关于身份提供者的位置的数据被作为报头提供。
5. 如任何前述权利要求所述的方法,其中,被添加到请求的关于身份提供者的位置的数据被作为统一资源定位符提供。
6. 如任何前述权利要求所述的方法,其中,由身份提供者响应于请求来提供关于身份提供者的位置的数据。
7. 如任何前述权利要求所述的方法,其中,由代理服务器来执行修改步骤。
8. 如任何前述权利要求所述的方法,还包括响应于从用户接收到对访问服务提供者的请求来设置用户身份的步骤。
9. 如权利要求 8 所述的方法,其中,基于由用户提供的设置来确定用户身份。
10. 一种方法,包括以下步骤:
在服务提供者处从用户接收服务请求,该请求包括报头,该报头包含关于能够为用户提供证书的身份提供者的位置的数据;
从所述报头获取关于身份提供者的位置的数据;以及
向身份提供者请求用户的证书。
11. 一种设备,包括:
第一输入,适合于从用户接收服务访问请求;以及
第一输出,适合于向服务提供者发送经修改的服务访问请求,其中,
所述设备适合于通过向从所述用户接收到的服务访问请求添加关于能够为用户提供用户证书的身份提供者的位置的数据来生成所述经修改的服务访问请求。
12. 如权利要求 11 所述的设备,其中,所述设备适合于在从所述用户接收到服务访问请求时添加关于身份提供者的位置的所述数据。
13. 如权利要求 11 所述的设备,还包括适合于从所述服务提供者接收信号的第二输入,其中,所述设备适合于响应于服务提供者请求用户授权来添加关于身份提供者的位置的所述数据。
14. 如权利要求 11 至 13 中的任一项所述的设备,其中,关于身份提供者的位置的数据被作为报头提供。
15. 如权利要求 11 至 14 中的任一项所述的设备,其中,所述设备是代理服务器。
16. 如权利要求 11 至 15 中的任一项所述的设备,还包括身份提供者。
17. 一种包括服务提供者和代理服务器的系统,其中:

所述代理服务器适合于从用户接收服务访问请求；

所述代理服务器适合于通过添加关于能够为用户提供用户证书的身份提供者的位置的数据来修改所述请求并将经修改的服务访问请求发送到服务提供者；

所述服务提供者适合于出于用户认证的目的使用户重定向至身份提供者。

18. 一种计算机程序产品,包括:

输入,适合于从用户接收服务访问请求;以及

输出,适合于向服务提供者发送经修改的服务访问请求,其中,

所述计算机程序产品适合于向从所述用户接收到的服务访问请求添加关于能够为用户提供用户证书的身份提供者的位置的数据。

19. 一种数据结构,包括为用户提供对服务提供者的访问的请求,其中,所述请求包括报头,该报头提供关于能够为用户提供证书的身份提供者的位置的数据。

20. 如权利要求 19 所述的数据结构,其中,关于身份提供者的位置的所述数据是统一资源定位符。

服务提供者访问

技术领域

[0001] 本发明涉及身份(identity)管理,并且更具体地涉及对身份管理信息的访问。

背景技术

[0002] 联合身份管理或身份的“联合”描述了用于实现身份信息跨越另外的自主安全域的可携带性的技术。身份联合的目的是在不需要冗余用户管理的情况下使得一个域的用户能够无缝地且安全地访问另一域的数据或系统。消除每当访问新应用程序或帐户时的重复登录过程的需要能够大大改善用户体验。

[0003] 图 1 是举例说明身份管理的概念的方框图。图 1 示出一般用附图标记 2 指示的系统,包括最终用户 4、服务提供者(provider)6 和身份提供者 8。当系统 2 的最终用户 4 想要访问服务提供者 6 处的安全资源且服务提供者 6 要求对用户的身份进行认证时,可以使用身份提供者 8 来向服务提供者提供所需的认证信息。

[0004] 图 2 示出一般由附图标记 10 指示的算法,示出如何能够使用系统 2 来为最终用户 4 提供对由服务提供者 6 提供的安全服务的访问。

[0005] 算法 10 在步骤 12 处开始,在该步骤处,最终用户 4 向服务提供者 6(例如使用 web 浏览器)发送请求访问由服务提供者提供的特定应用程序的消息。该服务要求用户证书,在请求中未提供该证书。

[0006] 算法 10 移动至步骤 13,在该步骤处,执行发现过程。发现过程 13 确定身份提供者 8 的位置。接下来,算法 10 移动至步骤 14,在该步骤处,服务提供者使用户重定向至身份提供者 8。然后,算法 10 移动至步骤 16,在那里,身份提供者 8 向服务提供者 6 提供用户证书数据。响应于接收到用户证书,服务提供者 6 允许用户访问所请求的服务(步骤 18)。

[0007] 算法 10 的发现步骤(步骤 13)涉及确定服务提供者的位置并以能够被传送给用户的形式来提供该信息。服务提供者通常还要求关于与该身份提供者通信所需的协议的信息,包括诸如所要求数据内容和该数据的格式之类的信息。

[0008] 克服对发现过程的需要的一种方法是定义必须使用以便使用服务提供者 6 的单个身份提供者;然而,这种方法是不灵活的,因为其要求所有用户在该身份提供者有帐户。一种替换方法是要求用户手动地输入由该用户使用的身份提供者的地址。这对于用户而言是不方便的,并且易受用户错误的影响。

发明内容

[0009] 本发明设法解决上述问题中的至少某些问题。

[0010] 根据本发明的一方面,提供了一种方法,包括步骤:从用户接收对访问服务提供者的请求;通过添加关于能够为用户提供用户证书的身份提供者的位置的数据来修改请求;以及将经修改的请求转送给服务提供者。位置数据可以是身份提供者的地址的形式。该位置数据可以例如是统一资源定位符(URL)、网际协议(IP)地址、可扩展资源指示符(XRI)、OpenID 身份的形式,或者使得服务提供者能够找到身份提供者的任何其它形式。可以由代

理服务器来实施修改用户的请求的步骤。

[0011] 本发明的另一方面提供了一种设备(诸如代理服务器),包括:第一输入,其适合于从用户接收服务访问请求;以及第一输出,其适合于向服务提供者发送经修改的服务访问请求,其中,所述设备适合于通过向从所述用户接收到的服务访问请求添加关于能够为用户提供用户证书的身份提供者的位置的数据(例如为诸如 http 报头之类的报头的形式)来生成所述经修改的服务访问请求。位置数据可以是身份提供者的地址的形式。该位置数据可以例如是统一资源定位符(URL)、网际协议(IP)地址、可扩展资源指示符(XRI)、OpenID 身份的形式,或者使得服务提供者能够发现身份提供者的任何其它形式。

[0012] 本发明的另一方面提供了一种包括服务提供者和代理服务器的系统,其中:代理服务器适合于从用户接收服务访问请求;代理服务器适合于通过添加关于能够为用户提供用户证书的身份提供者的位置的数据(常常是地址,诸如统一资源定位符(URL)、网际协议(IP)地址、可扩展资源指示符(XRI)、OpenID 身份,或使得服务提供者能够找到身份提供者的任何其它形式)来修改请求并将经修改的服务访问请求发送到服务提供者;以及服务提供者适合于出于用户认证的目的使用户重定向至身份提供者。可以将位置数据作为报头来提供,诸如 http 报头。

[0013] 因此,本发明的某些形式使得服务提供者能够接收关于能够为用户提供用户证书的身份提供者的位置的数据。可以在不要求来自用户的任何输入的情况下执行此步骤。特别地,不要求用户记住并输入用于其身份提供者的位置信息(诸如 URL)。

[0014] 因此,可以将依照本发明的方面的服务提供者布置为提供更好的用户体验,因为用户的焦点不需要在服务提供者和身份提供者之间转移。此外,可以将依照本发明的方面的系统配置为使得用户不需要在访问特定服务提供者之前登录到身份提供者,从而进一步改善用户体验。

[0015] 另一优点是根据本发明的方面,不需要在用户的前端处安装任何附加软件或硬件以便使用本发明。例如,具有 web 浏览器的任何终端能够访问依照本发明的方面适配的代理服务器。

[0016] 在本发明的某些形式中,用户不需要在服务提供者或身份提供者处输入用户证书。这不仅对用户方便,而且通过防止恶意程序根据由用户进行的按键寻找用户证书(所谓的“仿冒(phishing)”攻击)来增加安全性。

[0017] 在本发明的某些形式中,在不要求任何特定用户介入的情况下直接生成经修改的服务访问请求,使得对用户隐藏修改访问服务访问请求的过程。

[0018] 可以响应于用户访问服务提供者的请求来生成经修改的请求。在此类布置中,不要求服务提供者请求用户细节,因为那些细节是被自动添加的。事实上,可以在向服务提供者发送任何信息之前添加用户细节。

[0019] 可替换地,可以响应于服务提供者请求用户授权来生成经修改的请求。举例来说,可以响应于来自服务提供者的 HTTP 401 未授权响应来生成经修改的请求。

[0020] 在本发明的某些形式中,可以将被添加到该请求的关于身份提供者的位置的数据作为报头提供,诸如 http 报头。

[0021] 可以由身份提供者响应于请求来提供关于身份提供者的位置的数据。例如,代理服务器可以请求身份提供者提供适当的数据:身份提供者可以返回数据(诸如统一资源定

位符)以便插入报头中。

[0022] 在本发明的某些形式中,由诸如 http 代理服务器之类的代理服务器来执行修改步骤。还可以由代理服务器来执行接收和 / 或转送步骤。在本发明的使用中,用户可以经由代理服务器来配置他用来路由服务请求的浏览器。

[0023] 在本发明的某些形式中,响应于从用户接收到对访问服务提供者的请求的步骤来设置用户身份。可以基于由用户提供的设置(setting)来确定用户身份。例如,用户身份可以是公共身份、私有身份(private identity)或随机身份中的一个。当涉及高度可信任网站时,公共身份(诸如用户的名称)可能是适当的。当涉及不那么可信任网站时,随机身份可能是适当的。

[0024] 根据本发明的一方面,提供了一种方法,包括以下步骤:在服务提供者处从用户接收服务请求,该请求包括报头(诸如 http 报头),其包含关于能够为用户提供证书的身份提供者的位置的数据;从报头获取身份提供者的位置;以及向身份提供者请求用户的证书。位置数据可以是身份提供者的地址的形式。该位置数据可以例如是统一资源定位符(URL)、网际协议(IP)地址、可扩展资源指示符(XRI)、OpenID 身份的形式,或者使得服务提供者能够找到身份提供者的任何其它形式。

[0025] 根据本发明的一方面,提供了一种服务提供者,包括:输入,其用于从用户接收服务访问请求,该请求包括关于能够为用户提供证书的身份提供者的位置的数据(诸如地址);用于从所述报头获取关于身份提供者的位置数据的装置;以及用于向身份提供者请求用户的证书的装置。该位置数据可以例如是统一资源定位符(URL)、网际协议(IP)地址、可扩展资源指示符(XRI)、OpenID 身份的形式,或使得服务提供者能够找到身份提供者的任何其它形式。可以将位置数据作为报头提供,诸如 http 报头。

[0026] 根据本发明的一方面,提供了一种计算机程序产品,包括:输入,其适合于从用户接收服务访问请求;以及输出,适合于向服务提供者发送经修改的服务请求,其中,所述计算机程序产品适合于向从所述用户接收到的服务访问请求添加关于能够为用户提供用户证书的身份提供者的位置的数据。所述计算机程序产品可以适合于在不要求服务提供者请求用户证书的情况下响应于用户的请求来修改该请求。可替换地,所述计算机程序产品可以适合于响应于服务提供者请求用户授权来修改请求。所述计算机程序产品可以例如是代理服务器。所述计算机程序产品可以包括身份提供者。

[0027] 本发明的另一方面提供了一种包括为用户提供对服务提供者的访问的请求的数据结构,其中,所述请求包括报头,该报头提供关于能够为用户提供证书的身份提供者的位置的数据。关于身份提供者的位置的数据可以是地址,诸如统一资源定位符(URL)、网际协议(IP)地址、可扩展资源指示符(XRI)、OpenID 身份的形式,或者使得服务提供者能够找到身份提供者的任何其它形式。所述请求可以采取 http 请求的形式。

附图说明

[0028] 下面参考以下编号附图仅以示例的方式来描述本发明的实施例。

[0029] 图 1 是举例说明现有技术中的身份管理的使用的方框图;

图 2 是举例说明图 1 的布置的已知使用的流程图;

图 3 是依照本发明的方面的系统的方框图;

图 4 示出依照本发明的方面的消息序列；以及
图 5 示出依照本发明的方面的消息序列。

具体实施方式

[0030] 图 3 是依照本发明的方面的一般用附图标记 30 指示的系统的方框图。系统 30 包括用户浏览器 32、接入网络 34、代理服务器 36 和服务提供者 38。代理服务器 36 包括 http 代理 35 和身份提供者 37。可以在相同的位置处在物理上提供 http 代理 35 和身份提供者 37 作为代理服务器 36 的一部分，或者可以使其在物理上分离。此外，可以由相同的公司（诸如电信运营商）或由单独的公司来控制 http 代理 35 和身份提供者。

[0031] 为了访问由服务提供者 38 提供的服务，用户将其浏览器 32 指向代理服务器 36。经由接入网络 34 来实现此连接。代理服务器 36 如下文详细讨论的那样与服务提供者 38 通信。经由代理服务器 36 在服务提供者 38 与用户的浏览器 32 之间传输数据。

[0032] 图 4 示出依照本发明的方面的系统 30 的元件之间的一般由附图标记 40 指示的示例性消息序列。

[0033] 首先，用户浏览器 32 经由接入网络 34 来设立网际协议（IP）连接（如附图标记 39 所指示的）。

[0034] 一旦已经建立了 IP 连接，消息序列就从由用户浏览器 32 向代理服务器 36 发布的服务访问请求（消息 41）开始。例如，消息 41 可以采取 HTTP GET 请求的形式，诸如“GET secure_url_on_SP”。

[0035] 代理服务器 36 接收服务访问请求 41 并构造标识身份提供者 37 的位置的统一资源位置（URL，uniform resource location），在所述位置处能够获得用于用户的证书。URL 可以具有一般形式 <http://idp.operator.com>。可替换地，URL 可以具有用户特定形式，诸如 http://idp.operator.com/user_id，其中，基于由用户设定的偏好来生成用户 ID。

[0036] 由代理服务器 36 生成的 URL 被作为报头（X-IDP = <identity_provider_location>）插入由代理服务器 36 从浏览器 32 接收到的 GET 请求中。由附图标记 42 指示的包括新报头的新 GET 请求被转送到服务提供者 38。

[0037] 在接收到经修改的 GET 请求 42 时，服务提供者 38 在步骤 44 处从由代理服务器 36 插入的报头字段中获取身份提供者（IDP）地址。然后可以例如以上文参考图 2 所述的方式进行对用户进行认证的过程。

[0038] 因此，在步骤 46 处，服务提供者 38 向代理服务器 36 请求用于用户的认证细节。该请求被例如依照关于重定向的 HTTP 标准路由到在报头中给定的 URL（即到身份提供者 37）。响应于对认证细节的请求，身份提供者 37 例如以安全断言标记语言（SAML，Security Assertion Markup Language）断言的形式来提供用户证书（步骤 48）。接下来，服务提供者允许代理服务器 36 访问服务（步骤 50）且代理服务器将这些细节转送至浏览器 32（步骤 52）。然后，用户能够使用浏览器来访问由服务提供者 38 提供的服务。

[0039] 形成代理服务器 36 的 http 代理 35 和身份提供者 37 能够以多种方式合作。例如，http 代理 35 可以让身份提供者 37 提供用于插入 http 报头中的 URL。然后，身份提供者 37 可以抓住机会生成使得身份提供者能够以简单的方式查找用户的 URL。另外，如果身份提供者 37 由多个分布式机器组成，则可以选择 URL，使得其指向最小负载机器。

[0040] 如上文所讨论的,代理服务器 36 响应于从浏览器 32 接收到服务访问请求 41 来生成用户 ID。基于用户偏好来确定用户 ID。例如,用户 ID 可以是公共身份、持久性身份或随机身份。

[0041] 公共身份是直接和用户相关联的身份。公共身份的示例是用户的真实姓名(例如 John Smith 先生)、其通讯地址、社会保险号等。通常,用户将仅在访问诸如在线银行的高度可信任和安全网站时使用公共身份。

[0042] 持久性身份是与用户相关联的固定字符串(例如“clever_boy_007”)。在某些情况下,用户可能希望在其每次访问特定服务时使用相同的身份。这样,可以为该用户身份积累信誉。当然,可以使用公共身份,但是如果用户不希望这样做(出于安全原因,或出于保密原因),可以替代地使用持久性身份。

[0043] 随机身份是每当用户访问服务时被修改的字符串。例如,当用户第一次访问特定娱乐网站时,代理 36 可以生成用户 ID “anonymous_1234”。当用户访问不同的网站或重新访问相同的网站时,代理 36 可以生成新的用户 ID,诸如“anonymous_5678”。使用随机身份更加安全,因为更加难以识别用户的真实身份。此外,使用随机 ID 防止网站能够跟踪单独用户的活动。

[0044] 在随机、持久性和公共用户 ID 之间进行选择的主要目的是允许用户选择适当的隐私水平。可以根据被访问的服务的名称或性质来选择要使用的 ID 的类型。此外,用户将能够通过访问运营商的客户服务网页来修改用户偏好。

[0045] 在上文参考图 4 所述的协议中,由代理服务器 36 在第一次寻求访问服务提供者 38 时插入新 HTTP 报头 X-IDP = <identity_provider_location>。这不是必不可少的。

[0046] 图 5 示出依照本发明的方面的用户浏览器 32、接入网络 34、代理服务器 36 和服务提供者 38 之间的一般由附图标记 60 指示的示例性消息序列。

[0047] 如前所述,消息序列从用户浏览器经由接入网络 34 来建立网际协议(IP)连接开始,如附图标记 39 所指示的。

[0048] 一旦已经建立了 IP 连接,消息序列就从由用户浏览器 32 向代理服务器 36 发布的服务访问请求(消息 41)开始。如上文参考图 4 所述,消息 41 可以采取 HTTP GET 请求的形式,诸如“GET_secure_url_on_SP”。

[0049] 代理服务器 36 接收服务访问请求并作为响应将 GET 请求转送到服务提供者 38(消息 62)。与在上述消息序列 40 中不同,消息 62 未被代理服务器 36 修改(在此阶段)。

[0050] GET 请求被服务提供者 38 接收到。由于 GET 请求不包括所需用户证书,所以服务提供者 38 返回指示该用户未被授权的消息 64。在图 5 的示例中,消息 64 采取 HTTP 401 未授权响应的形式。

[0051] 响应于未授权消息 64,代理服务器 36 基于由用户设定的偏好来生成用户 ID。例如,根据由用户指定的偏好,用户 ID 可以是随机的、持久性的和 / 或公共的。在这时生成用户 ID 不是必不可少的;然而,由于在接收到 HTTP 401 未授权消息之前不要求用户 ID,所以为了减少代理服务器上的负担,等待直至此时间以生成用户 ID 是方便的。

[0052] 接下来,代理服务器 36 为用户构造 URL;例如,URL 可以具有一般形式 <http://idp.operator.com> 或个人特定形式,诸如 http://idp.operator.com/user_id。由代理服务器生成的 URL 被作为报头(X-IDP = <identity_provider_location>)插入经修改的 GET

请求中。包括新报头的由附图标记 66 指示的经修改的 GET 请求被转送到服务提供者 38。

[0053] 在接收到经修改的 GET 请求 66 时,服务提供者 38 在步骤 44 处以与上文所述相同的方式从由代理服务器 36 在先前步骤中插入的报头字段中获取 IDP 地址。然后可以例如以上文参考图 4 所述的方式来进行对用户进行认证的过程。

[0054] 因此,在步骤 46 处,服务提供者 38 向身份提供者 / 代理服务器 36 请求用于用户的认证细节。该请求被路由到在报头中给定的 URL。响应于认证请求,身份提供者提供用户证书(步骤 48)。接下来,服务提供者允许代理服务器 36 访问该服务(步骤 50)且代理服务器将这些细节转送至浏览器 32 (步骤 52)。然后,用户能够使用浏览器来访问由服务提供者 38 提供的服务。

[0055] 在上述布置中,代理服务器 36 为用户构造统一资源位置(URL)并将该 URL 发送到服务提供者。在本发明的替换实施例中,由身份提供者 37 来生成 URL 且 http 代理 35 向身份提供者 37 发送询问以便获得该 URL,使得其能够被转送到服务提供者 38。

[0056] 本发明的上述实施例包括在报头中包括 URL,其中,该 URL 标识身份提供者的位置。这不是必不可少的。该报头可以包含使得服务提供者能够对身份提供者进行定位的任何信息。示例包括但不限于 IP 地址、可扩展资源标识符(XRI)和 OpenID 标识符。

[0057] 在上述实施例中,用户经由接入网络 34 使用浏览器 32 来与代理服务器 36 通信。接入网络的提供不是必不可少的。使得用户能够与代理服务器通信并使得代理服务器能够与服务提供者通信的任何布置是足够的。例如,可以在用户终端处提供代理服务器。

[0058] 上文已经使用 http 作为示例性协议描述了本发明。这不是必不可少的。可以由利用不同协议的代理来取代 http 代理 35。例如,可以使用能够转送数据分组的任何协议来代替 http。

[0059] 上文所述的本发明的实施例是说明性而不是限制性的。对于本领域的技术人员来说将显而易见的是在不脱离本发明的一般范围的情况下上述设备和方法可以结合许多修改。意图在本发明的范围内包括所有此类修改,只要其落在所附权利要求的范围内。

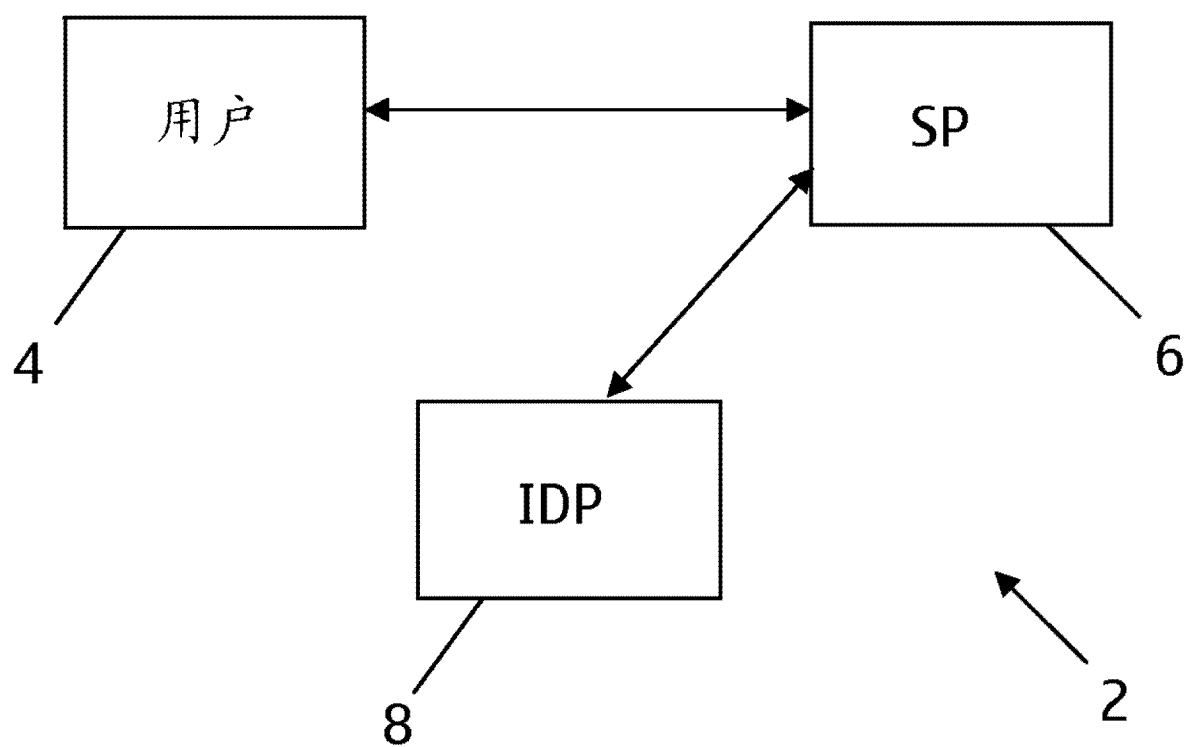


图 1

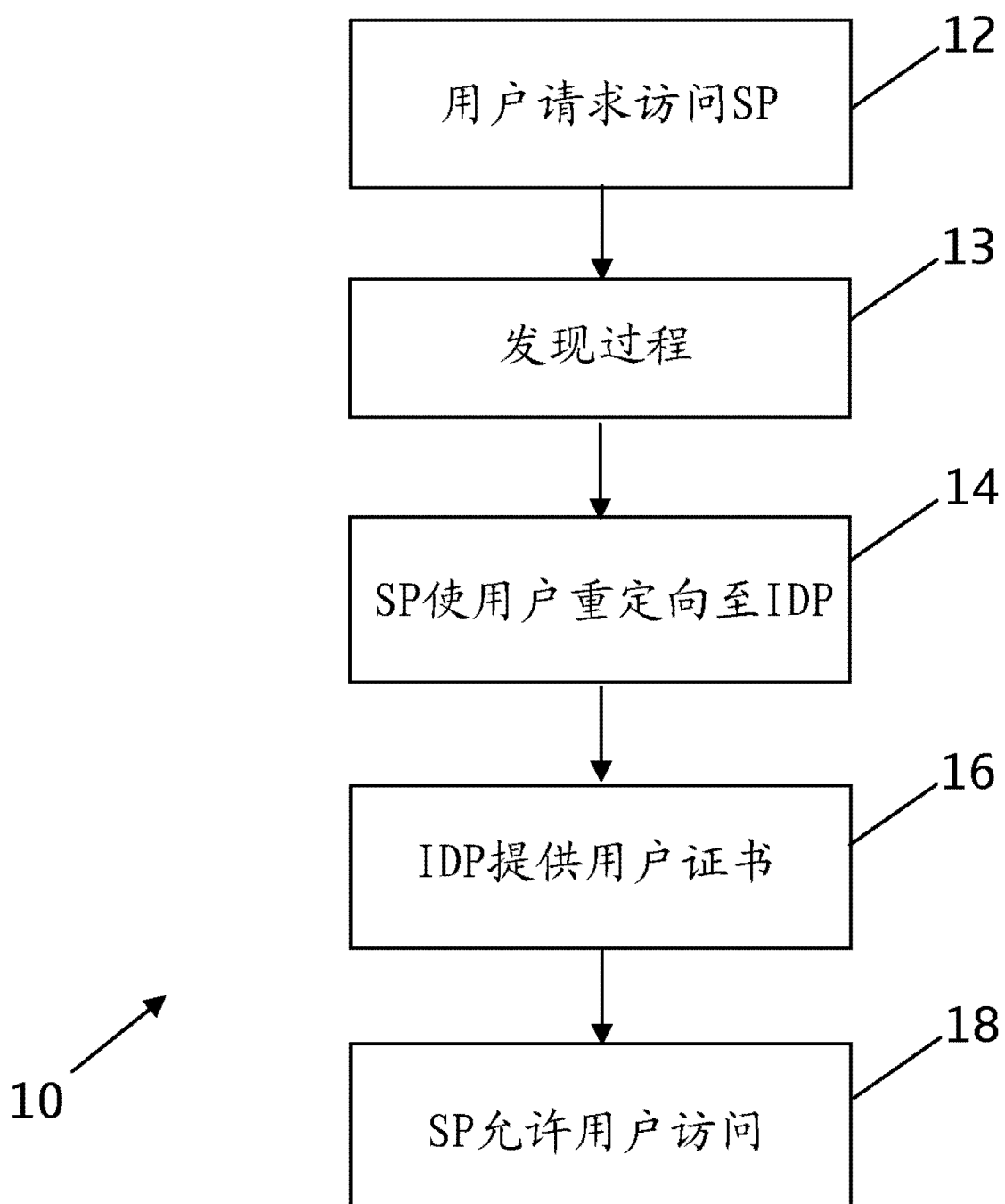


图 2

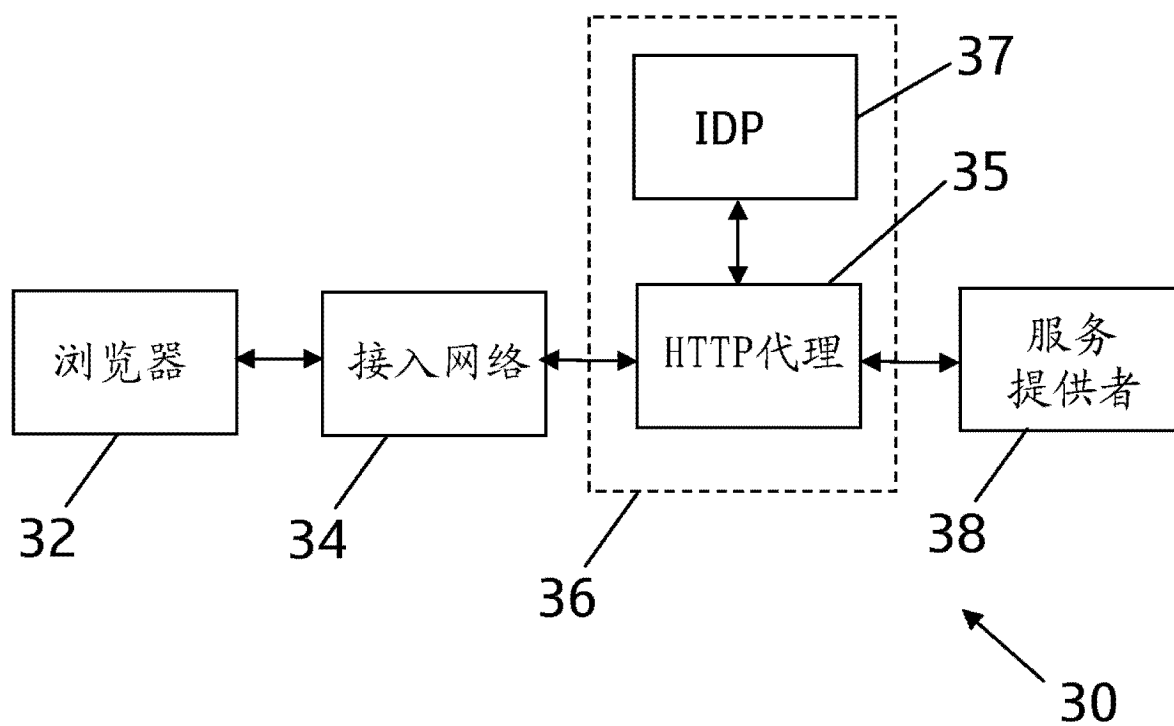


图 3

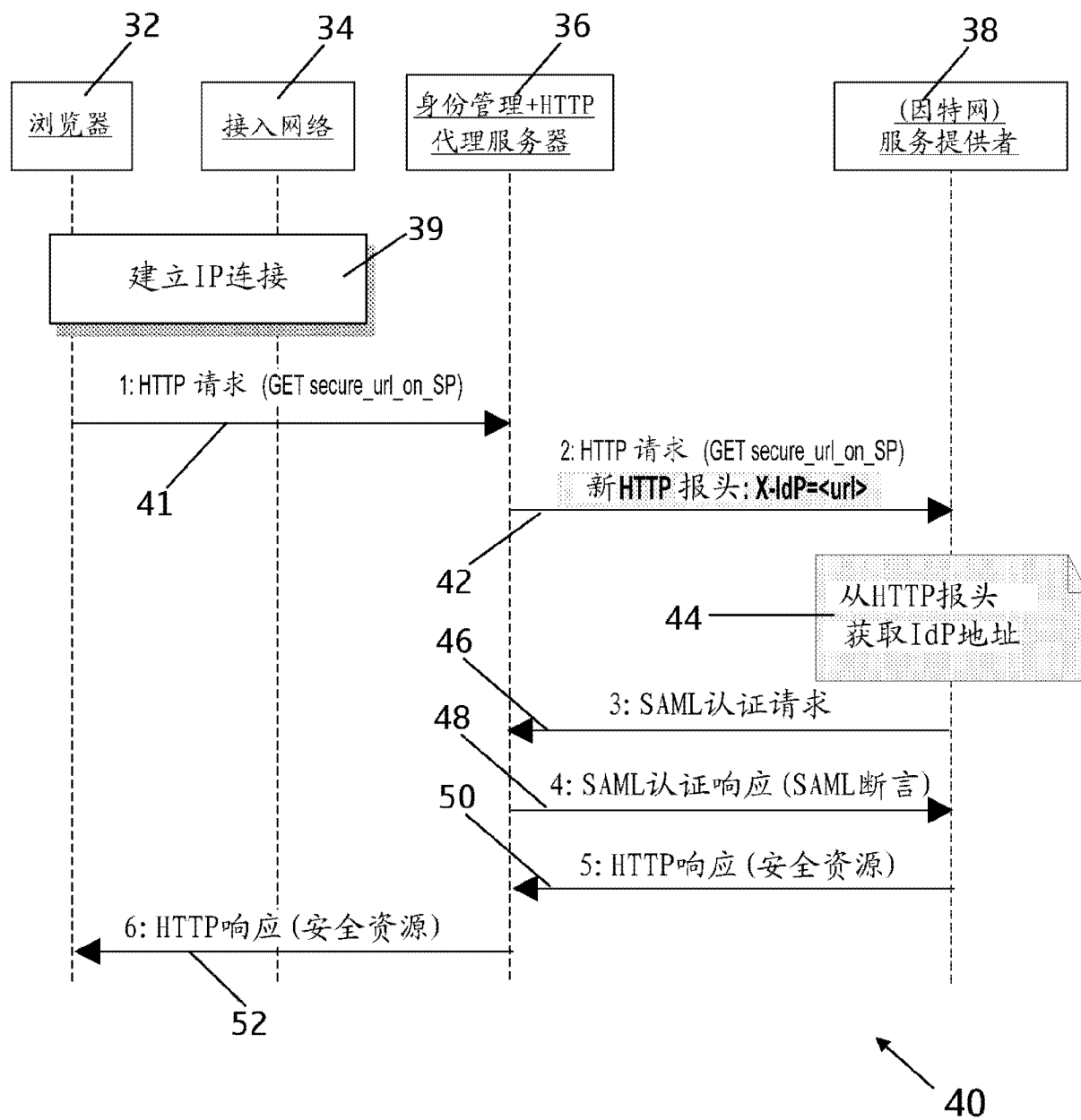


图 4

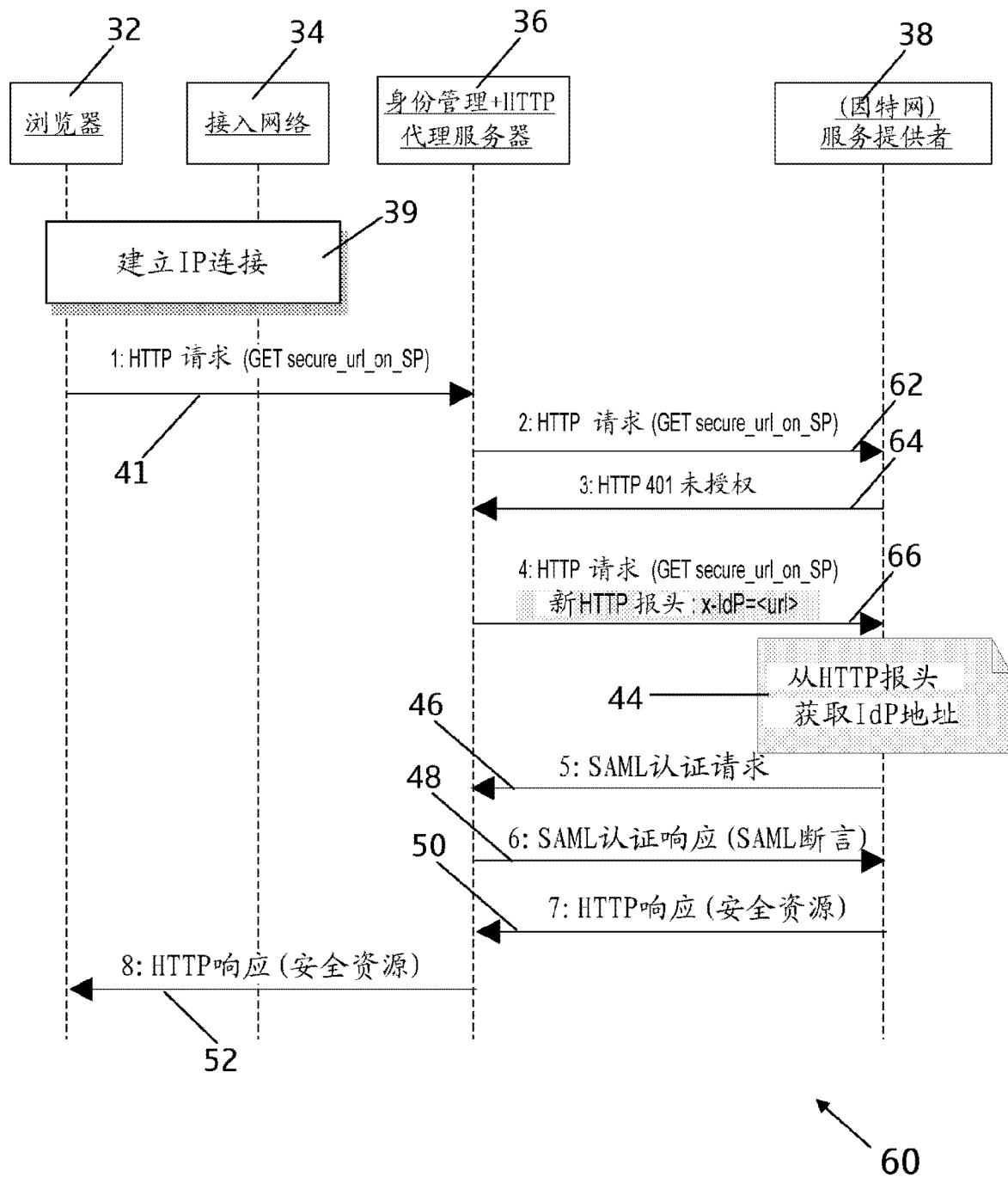


图 5