(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 102792311 A
(43)申请公布日 2012.11.21

(21)申请号 201180013569.6

(22)申请日 2011.02.22

(30)优先权数据
12/723,049 2010.03.12 US

(85)PCT申请进入国家阶段日
2012.09.12

(86)PCT申请的申请数据
PCT/US2011/025641 2011.02.22

(87)PCT申请的公布数据
WO2011/112345 EN 2011.09.15

(71)申请人 阿尔卡特朗讯公司
地址 法国巴黎

(72)发明人 I·凡博格 H-L·陆

(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.
G06F 21/00(2006.01)
H04L 29/06(2006.01)

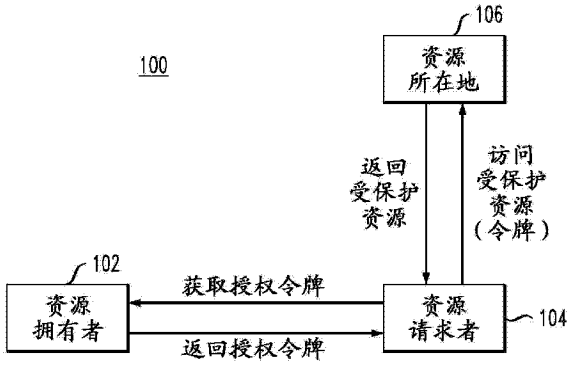
权利要求书 2 页 说明书 7 页 附图 9 页

(54)发明名称

安全动态权力委派

(57)摘要

在通信网络中，其中第一计算设备代表资源拥有者而第二计算设备代表资源请求者，该资源拥有者检测事件发生，其中该事件发生代表请求访问存储于资源所在地中的所述资源拥有者的一个或多个资源。所述资源拥有者响应于所述事件发生而发送授权令牌至所述资源请求者，所述授权令牌用作由所述资源拥有者所委派的授权的证明，该证明由所述资源请求者出示给所述资源所在地以允许该资源请求者访问存储于该资源所在地中的一个或多个所请求资源。



CN 102792311 A

1. 一种方法，包括：

- 在通信网络中，其中第一计算设备代表资源拥有者而第二计算设备代表资源请求者，该资源拥有者检测事件发生，其中该事件发生代表请求访问存储于资源所在地中的所述资源拥有者的一个或多个资源；

- 所述资源拥有者响应于所述事件发生而发送授权令牌至所述资源请求者，所述授权令牌用作由所述资源拥有者所委派的授权的证明，该证明由所述资源请求者出示给所述资源所在地以允许该资源请求者访问存储于该资源所在地中的一个或多个所请求资源。

2. 根据权利要求 1 所述的方法，其中，所述事件发生是由所述资源拥有者从所述资源请求者接收资源请求以使得该资源请求者和该资源拥有者能够通过拉通信方法交换请求和响应。

3. 根据权利要求 1 所述的方法，其中，所述事件发生是关联于应用程序的触发事件的发生以使得所述资源请求者与所述资源拥有者之间的通信方法是推通信方法。

4. 根据权利要求 1 所述的方法，其中，对于由所述资源拥有者所委派的授权的证明从所述资源请求者到至少另一个资源请求者是可传送的，以使得该另一个资源请求者能够出示另一个授权令牌给所述资源所在地从而允许该另一个资源请求者访问存储于该资源所在地中的一个或多个所请求资源。

5. 根据权利要求 1 所述的方法，其中，获得所述授权令牌并出示该授权令牌以获得对所述一个或多个所请求资源的访问是绑定到现有应用协议的。

6. 一种用于实现代表资源拥有者的第一计算设备的装置，该装置包括存储器和处理器，该处理器耦合到该存储器并且被配置成执行权利要求 1 中的各步骤。

7. 一种方法，包括：

- 在通信网络中，其中第一计算设备代表资源拥有者而第二计算设备代表资源请求者，并且其中，该资源拥有者检测事件发生并且该事件发生代表请求访问存储于资源所在地中的所述资源拥有者的一个或多个资源；

- 所述资源请求者接收由所述资源拥有者响应于所述事件发生而发送的授权令牌，该授权令牌用作由所述资源拥有者所委派的授权的证明，该证明由所述资源请求者出示给所述资源所在地以允许该资源请求者访问存储于该资源所在地中的一个或多个所请求资源。

8. 根据权利要求 7 所述的方法，还包括所述资源所在地在至少一个以下情况中认证所述资源请求者：在所述资源请求者出示所述授权令牌给所述资源所在地之前，和在所述资源请求者出示所述授权令牌给所述资源所在地之后。

9. 根据权利要求 7 所述的方法，还包括所述资源所在地在作用于所述一个或多个所请求资源之前验证由所述资源请求者出示的所述授权令牌。

10. 一种方法，包括：

- 在通信网络中，其中第一计算设备代表资源拥有者而第二计算设备代表资源请求者，并且其中，该资源拥有者检测事件发生并且该事件发生代表请求访问存储于资源所在地中的所述资源拥有者的一个或多个资源，并且其中，所述资源请求者接收由所述资源拥有者响应于所述事件发生而发送的授权令牌；

- 所述资源所在地接收所述授权令牌，该授权令牌用作由所述资源拥有者委派给所述资源请求者的授权的证明以允许该资源请求者访问存储于该资源所在地中的一个或多个

所请求资源。

安全动态权力委派

技术领域

[0001] 本发明一般地涉及通信网络，更具体地涉及用在通信网络中的技术，该技术用于安全动态地委派授权以实现涉及由不同于资源拥有者的实体访问受保护资源的应用。

背景技术

[0002] 这个部分介绍可能有助于更好地理解本发明的方面。相应地，这个部分的陈述是以该目的来阅读的并且不应当被看作是作为现有技术或非现有技术的认定。

[0003] 可经由通信网络获得的各种不同的工具，例如万维网，允许用户创建他们自己的应用或网页。一个例子称作“mashup（聚合）”，其是使用或组合来自两个或更多源的数据或功能性以创建新服务或应用的网页或应用。然而，当用户被要求针对不同的源而给出他/她的证书(用户名和密码)时，出现了问题，这暴露了源之间的信息并且给予一个源对另一个源的完全访问。这可能不是用户所期望的。

[0004] 称作 OAuth 的协议尝试提供对该问题的解决方案。一般地，OAuth 协议(参见 http://oauth.net/) 使得用户能够提供对他们的 web 资源的第三方访问而不必共享他们的密码。然而，该协议存在几个限制和缺陷。首先，由于协议与超文本传输协议(HTTP)有关，它不适用于非 web 应用。其次，由于该协议依赖于对 HTTP 重定向的使用，因此它容易受到网络钓鱼攻击。该协议也需要多个往返来获得所委派的授权，并且它对于应用性能而言不是最佳的。最后，由于该协议使用不止一种委派证据和涉及重复的加密签名的证明机制，它过于复杂。因此，需要一种克服了所述和其他缺点的关于权利委派的改进方法。

发明内容

[0005] 本发明的实施例提供用于动态地委派授权以实现通信网络(例如万维网或下一代网络)上的应用(例如 mashups 和第三方应用)的一般、有效且安全的方法，所述应用涉及由不同于资源拥有者的实体访问受保护资源。

[0006] 在第一方面中，一种方法包括下列步骤。在通信网络中，其中，第一计算设备代表资源拥有者，而第二计算设备代表资源请求者，该资源拥有者检测事件发生，其中该事件发生代表请求访问存储于资源所在地中的资源拥有者的一个或多个资源。该资源拥有者响应于事件发生而发送授权令牌至资源请求者，该授权令牌用作由资源拥有者所委派的授权的证明，该证明要由资源请求者出示给资源所在地以使得资源请求者能够访问存储于该资源所在地中的一个或多个所请求资源。

[0007] 在一个或多个实施例中，该事件发生可以是由资源拥有者接收来自资源请求者的资源请求(例如拉方法)。可选地，该事件发生可以是关联于应用程序(例如推方法)的触发事件的发生。该资源所在地可以位于第三计算设备中或它可以位于第一计算设备中。该授权令牌可以具有一个或多个可验证结构、有限的寿命并且指定了用于认证资源请求者的方法或用于认证资源请求者的保证等级。该可验证结构可以包括资源拥有者的数字签名。该授权令牌可以指定一个或多个动作，该动作被许可按照一个或多个所请求资源而被执行。

该资源请求者可以在一个往返中获得来自资源拥有者的授权令牌。用于获得令牌的机制可以绑定到现有的应用协议。为获得对一个或多个所请求资源的访问而出示授权令牌也可以绑定到现有的应用协议。进一步地，由资源拥有者委派的授权的证明可以从资源请求者被传送到至少另一个资源请求者以使得该另一资源请求者能够出示另一个授权令牌给资源所在地以允许该另一资源请求者访问存储于该资源所在地中的一个或多个所请求资源。由该另一资源请求者所获得的另一授权令牌可以指定动作许可范围，该动作许可范围是由资源请求者直接从资源拥有者获得的授权令牌中所指定的动作授权范围的子集。在一个实施例中，由该另一资源请求者所获得的另一授权令牌没有更改用于认证资源请求者的方法或用于认证资源请求者的保证级别。进一步地，该另一授权令牌可以是初始接收的授权令牌的修改形式并且前一个资源请求者在发送该授权令牌的修改形式至该另一资源请求者之前执行修改。

[0008] 仍进一步地，该资源拥有者可以在发送授权令牌至资源请求者之前认证该资源请求者。

[0009] 在第二方面中，一种方法包括下列步骤。在通信网络中，其中第一计算设备代表资源拥有者而第二计算设备代表资源请求者，并且该资源拥有者检测事件发生并且该事件发生代表请求访问存储于资源所在地中的该资源拥有者的一个或多个资源，该资源请求者接收由该资源拥有者响应于该事件发生而发送的授权令牌，该授权令牌用作由该资源拥有者委派的授权的证明，该证明要由资源请求者出示给资源所在地以使得该资源请求者能够访问存储于该资源所在地中的一个或多个所请求资源。

[0010] 在一个或多个实施例中，该资源所在地可以在该资源请求者出示授权令牌给该资源所在地之前认证该资源请求者。该资源所在地在作用于一个或多个所请求资源之前验证由该资源请求者出示的授权令牌。进一步地，该资源所在地可以在该资源请求者出示授权令牌给该资源所在地之后认证该资源请求者。该资源请求者也可以将由该资源拥有者所委派的授权的证明传送至至少另一个资源请求者。这种传送可以包括该资源请求者发送另一个授权令牌给该另一个资源请求者以使得该另一资源请求者能够出示该另一授权令牌给该资源所在地从而许可该另一个资源请求者访问存储于该资源所在地中的一个或多个所请求资源。

[0011] 在第三方面中，一种方法包括下列步骤。在通信网络中，其中，第一计算设备代表资源拥有者而第二计算设备代表资源请求者，并且该资源拥有者检测事件发生并且该事件发生代表请求访问存储于资源所在地中的该资源拥有者的一个或多个资源，并且该资源请求者接收由该资源拥有者响应于该事件发生而发送的授权令牌，该资源所在地接收该授权令牌，该授权令牌用作由该资源拥有者委派给该资源请求者的授权的证明以许可该资源请求者访问存储于该资源所在地中的一个或多个所请求资源。

[0012] 有利地，本发明的动态授权委派技术适用于 web 和非 web 应用。本发明的技术不依赖于对 HTTP 重定向的使用并且不需要多次往返来获得所委派的授权。进一步地，本发明的技术不如现有的授权委派方案那样复杂。

附图说明

[0013] 参考附图，通过阅读下面对说明性实施例的详细描述，本发明的所述和其他目的、

特征和优点将变得明显，其中：

[0014] 图 1 示出了根据本发明一个实施例的参与安全动态授权委派的实体；

[0015] 图 2 示出了根据本发明一个实施例的授权令牌的基本结构；

[0016] 图 3 示出了根据本发明一个实施例的由资源请求者执行的用于请求授权令牌的方法；

[0017] 图 4 示出了根据本发明一个实施例的由资源拥有者响应于对授权令牌的请求而执行的方法；

[0018] 图 5A 和 5B 示出了根据本发明一个实施例的由资源请求者执行的用于访问受保护资源的方法；

[0019] 图 6A 和 6B 示出了根据本发明一个实施例的由资源所在地响应于对访问受保护资源的请求而执行的方法；

[0020] 图 7 示出了根据本发明一个实施例的另一个授权令牌的结构；

[0021] 图 8 示出了根据本发明一个实施例的适于实现安全动态授权委派的通信网络的硬件结构。

具体实施方式

[0022] 下面将结合示例性通信网络和示例性应用来说明本发明。然而，应当理解，本发明不限于使用任何特定类型的通信网络或应用。所公开的技术适于使用各种各样的通信网络，包括基于 web 的和基于非 web 的网络，以及多种应用。实际上，所公开的技术可以在任何合适的通信网络中利用任何合适的应用来实现，其中期望提供动态授权委派以实现通信网络上的涉及由不同于资源拥有者的实体对受保护资源的访问的应用。

[0023] 如这里使用的，“授权委派”一般是指能够访问某项目的一方允许另一方访问该项目。作为例子，在下面的实施例中，资源拥有者允许资源请求者利用授权令牌访问某资源。在委派是实时按需执行而不是通过提供来执行的意义下，该操作被看做是“动态的”。

[0024] 如这里所使用的，“令牌”一般是指一种代表可验证或能够被认证的访问控制准则和操作的数据对象或结构。如这里所使用的，“资源”一般是指能够通过通信网络访问的任何项目、数据、信息等。

[0025] 如这里所使用的，“应用”一般是指被设计用于辅助用户或实体至一个或多个指定任务的计算机软件。

[0026] 如这里将解释的那样，本发明的说明性实施例提供的技术使得资源请求者能够动态地从资源拥有者直接获得对访问其资源所在地中的资源的许可。如这里使用的“所在地”一般是指可经由通信网络访问的存储位置。资源请求者能够通过出示由资源拥有者委派的授权证明来访问资源所在地中的受保护资源。该证明(即授权令牌)具有可验证的结构和有限的寿命，并且还指定了用于认证资源请求者的方法和保证等级。资源请求者能够通过一种基于请求 - 响应并且能够绑定到现有应用协议的机制来在一个往返中从资源拥有者动态获得授权令牌。例如，资源令牌请求 / 响应能够作为消息报头或报体或二者的一部分，通过 HTTP 或会话起始协议(SIP)来承载。用于出示资源令牌以获得对受保护资源的访问的机制是基于请求 - 响应的并且能够绑定到现有应用协议。例如，令牌能够作为消息报头或报体的一部分，通过 HTTP 或 SIP 来承载。

[0027] 图 1 示出了根据本发明一个实施例的系统 100，其中实体参与安全动态授权委派。如所示，该系统涉及三种行为者：资源拥有者 102、资源请求者 104 和资源所在地 106。应当认识到，这三种行为者每个都能够被实现为一个或多个计算设备，如下面将进一步解释的那样。

[0028] 资源拥有者 102 能够体现为用户代理（在终端用户的情况下）或授权服务器（在服务提供商或组织的情况下）。类似地，资源请求者 104 能够体现为用户代理（在终端用户的情况下）或应用服务器（在服务提供商或组织的情况下）。在其中（操作计算设备 A 的）“爱丽斯”请求照片打印服务提供商打印她存储在服务器中的在莫斯科旅游时的照片这一使用情形中，资源拥有者 102（爱丽斯）将由用户代理（例如执行于计算设备 A 上的 web 浏览器程序）代表，而资源请求者 104（照片打印服务提供商）将由应用服务器代表。在另一使用情形中，其中（操作计算设备 B 的）“鲍勃”是在线电影服务的用户，资源拥有者 102（在线电影服务提供商）将由授权服务器代表，而资源请求者 104（鲍勃）将由用户代理（例如执行与计算设备 B 上的 web 浏览器程序）代表。

[0029] 为了获得对资源所在地 106 中的特定受保护资源的访问，资源请求者 104 需要从资源拥有者 102 直接获得授权令牌，该令牌具有如图 2 所示（将在下文进一步讨论）的基本结构 200。为此，两种方法是可行的：拉和推。在拉方法中，资源请求者 104 和资源拥有者 102 交换请求和响应。令牌请求将至少标识请求者以及目标资源和关联的动作。将在下文解释的图 3 和 4 分别从资源请求者 104 和资源拥有者 102 的角度示出了拉方法。在推方法中，作为应用触发的结果而不是作为来自资源请求者的明确请求的结果，资源拥有者 102 能够向资源请求者 104 发出授权令牌。

[0030] 图 3 示出了在资源请求者（例如图 1 中的 104）一侧的用于请求基本授权令牌的拉方法 300。在步骤 302 中，资源请求者生成并发送授权令牌请求给资源拥有者。在步骤 304 中，资源请求者检查从资源拥有者接收的第一响应并且在步骤 306 中确定该第一响应是否包括认证请求（由此资源拥有者在发送授权令牌给请求者之前请求认证该请求者）或该第一响应是否包括授权令牌。

[0031] 如果来自资源拥有者的第一响应不是认证请求而是包括授权令牌，并且因此步骤 308（即下文描述的检查失败令牌响应的接收）产生否定结果，则请求者在步骤 310 中保存该授权令牌（以随后发送至资源所在地）。

[0032] 然而，如果来自资源拥有者的第一响应是认证请求，则在步骤 312 中，资源请求者生成并发送认证响应给资源拥有者。在步骤 314 中，资源请求者检查从资源拥有者接收的第二响应并且确定该第二响应是否包括授权令牌（因此假设认证成功）。如果是，则步骤 308（失败令牌响应）产生否定结果，并且请求者在步骤 310 中保存该授权令牌（以随后发送至资源所在地）。然而，如果认证失败，则接收自资源拥有者的第二响应是失败令牌响应，即这意味着资源拥有者将不发出授权令牌给请求者。应当理解，用于认证请求者的技术可以包括任何常规的认证技术。

[0033] 图 4 示出了在资源拥有者（例如图 1 中的 102）一侧的用于处理令牌请求的拉方法 400。在步骤 402 中，资源拥有者检查资源请求者（已从其接收资源令牌）是否已经被认证。如果没有，则在步骤 404 中，资源拥有者生成认证请求并且发送它至资源请求者。在步骤 406 中，资源拥有者检查接收自资源请求者的认证响应。在步骤 408，进行检查以确定认

证是否成功。如果没有成功，则资源拥有者在步骤 410 发送失败令牌响应至请求者（即不发送授权令牌给请求者）。然而，如果认证成功，则拥有者在步骤 412 判定是否应当允许请求者访问拥有者的资源，并且如果是，则在步骤 414 中生成授权令牌并且发送它至请求者。然而，如果访问被拒绝，则在步骤 410 中发送失败令牌响应。

[0034] 由于拥有授权令牌，资源请求者 104 因而能够请求访问资源所在地 106 中的受保护资源。当接收资源请求（参见图 1）时，资源所在地 106 采取下列动作：

[0035] 1. 基于令牌中指定的数字签名方法来验证关联于该请求的数字签名有效；

[0036] 2. 验证该令牌在时间和最大使用数目方面还没有过期；

[0037] 3. 验证所请求的资源和要执行的动作是令牌中指定的关联权限和资源列表的一部分；

[0038] 4. 验证资源请求者的名称匹配于令牌中的请求者名称；和

[0039] 5. 利用令牌中指定的方法或强度等级方法来认证该资源请求者。

[0040] 图 5A 和 5B 示出了在资源请求者（例如图 1 中的 104）一侧的用于访问由资源所在地（例如图 1 中的 106）所保存的受保护资源（不必在初始请求中包括授权令牌）的方法 500。

[0041] 在步骤 502 中，资源请求者生成并发送资源请求给资源所在地。在步骤 504 中，资源请求者检查从资源所在地接收的第一响应并且在步骤 506 中确定该第一响应是否包括认证请求（由此资源所在地在允许请求者访问资源之前请求认证该请求者）或该第一响应是否请求授权令牌。

[0042] 如果来自资源所在地的第一响应不是认证请求而是请求授权令牌（下文所述的 514），并且因而步骤 508（即下文所述的检查失败响应的接收）产生否定结果，则该请求者发送授权令牌（下文所述的 516）。

[0043] 然而，如果来自资源所在地的第一响应是认证请求，则在步骤 510 中，资源请求者生成并发送认证响应给资源所在地。在步骤 512 中，资源请求者检查从资源所在地接收的第二响应并且确定该第二响应是失败响应（508）还是对于授权令牌的请求（514），这因而假定认证是成功的。如果是后者，则该请求者在步骤 516 中发送（根据上文在图 3 和图 4 的背景下所描述的协议而接收自资源拥有者的）授权令牌。

[0044] 在步骤 518 中，资源请求者检查接收自资源所在地的第三响应并且确定该第三响应是否是另一个认证请求，即由资源所在地进行下一个认证的请求以确保请求者利用令牌中规定的方法被认证。也就是说，为了增强的安全性，资源所在地可能需要每次接收令牌时重新认证请求者。如果是，则执行步骤 524、526 和 528，其类似于上面描述的步骤 510、512 和 508。在步骤 530 中，请求者处理响应，其通常包含所请求的资源。

[0045] 图 6A 和 6B 示出了在资源所在地（例如图 1 中的 106）一侧的用于处理来自资源请求者（例如图 1 中的 104）的资源请求的方法 600。在步骤 602 中，资源所在地检查资源请求者是否已经被认证。如果是，则在步骤 604 中，资源所在地确认该请求者是否是资源拥有者（在该情况下，该请求者不需要授权令牌）。如果是，则在步骤 606 中，资源所在地应用合适的资源动作并且发送响应（例如提供对所请求资源的访问）。

[0046] 然而，回到步骤 602，如果请求者还未被认证并且授权令牌还未由请求者提供（步骤 608），则在步骤 610（生成并发送请求至请求者）、612（检查认证响应）和 614（确认认证成功）执行认证过程。如果不成功，则在步骤 616 失败响应被发送至请求者。然而，如果认

证成功，则执行步骤 604（检查请求者是否是拥有者），并且如果是肯定的，则执行步骤 606（应用资源动作并发送响应）。然而，在（步骤 614 中的）成功认证以及（步骤 604 中的）对请求者是否是拥有者的验证之后，资源所在地在步骤 618 中向请求者请求授权令牌，并且在步骤 620 中检查它是否被请求者提供。如果不是，则在步骤 616 中发送失败响应。

[0047] 一旦令牌以及被接收，资源所在地就在步骤 622 验证该令牌。例如，执行验证以确定令牌签名是否有效，请求中的请求者名称与令牌是否匹配，令牌是否仍未过期，所请求的资源和动作是否在范围内（即针对请求者和 / 或所请求的资源而允许什么）。应当理解，根据令牌的结构，可以对令牌及其内容执行更少或更多的验证。如果令牌的一个或多个方面无法被验证，则在步骤 624 中发送失败响应给请求者，并且因而该资源对于该请求者而言不可用。然而，如果所接收令牌的所有方面都被验证，则根据令牌中所指定的验证需要（就方法或保证等级而言），可以由资源所在地请求另一个认证过程。这是通过步骤 626、628、630 和 632 来完成的，其类似于步骤 610、612 和 614。假定第二次认证成功，则在步骤 634 中应用资源动作并且发送响应（即访问所允许的资源）。如果未成功，则在步骤 624 中发送失败响应。

[0048] 再次返回图 2，授权令牌的基本结构包括字段列表（就姓名 - 值对而言）以及发出者的签名 202，该签名是利用基于发出者的私钥或共享密钥而指定的签名算法 210（例如 RSA-SHA1 和 HMAC-SHA256）而在字段上被计算的。唯一的令牌标识符 204 能够通过级联发出者名称 206 和时间标记来被构造。发出者的证书链或证书指针链 208 在令牌中被指定。注意，当用于计算发出者签名的算法是基于私钥时，该字段仅需要被包含在内以改进整体性能。字段 212 指定了资源请求者的名称（身份）。字段 214 指定了用于认证请求者的方法或该方法的强度。字段 216 指定了接收方的名称（身份），即用作资源所在地的设备或服务器。

[0049] 资源和权限的列表的组合字段 218、有效期时间 220 以及最大使用数目 222 设定了整个委派范围。可传送性等级 224 指示了由资源拥有者发出的令牌能够被向下转发至一组始于初始请求者的令牌请求者的等级。可以假设非负整数的值。可传送性的第零级令牌无法被转发。可传送性的第 N 级令牌能够被初始令牌请求者传送给第二令牌请求者、至第三令牌请求者等等，最多到第 N 个令牌请求者。

[0050] 在获得可传送的令牌后，请求者可以基于旧令牌而发出新的令牌给新的请求者。如图 7 所示，新令牌 700 指定了新请求者 708（其将通过与之前相同的方法被认证）的身份，以及可能地降级的委派范围 710。在一个实施例中，新令牌 700 也包括旧令牌 704（即图 2 所示的令牌结构），以及前一请求者（现在是发出者）的证书链或证书指针链 706。发出者的签名 702 是基于发出者的私钥或共享密钥利用签名算法（其可以与旧令牌中指定的签名算法相同）而在字段上被计算的。

[0051] 当验证转发的令牌时，资源所在地还需要检查：

[0052] 1. 可传送性等级大于新请求者存在的数量；

[0053] 2. 所有签名都有效；和

[0054] 3. 当令牌沿路径被转发时范围没有变宽。

[0055] 可传送令牌的使用情形如下：爱丽斯在内容服务器上公开特定的内容并且使得关联的内容管理器作为她的代理以处理其他人对她的内容的访问。注意，为了支持可传送的

或具有有限使用次数的令牌，资源所在地需要保持状态。

[0056] 最后，图 8 示出了根据本发明的上述原理的适于实现安全动态授权委派的通信网络 800 的一般化硬件结构。

[0057] 如所示，资源拥有者（例如图 1 中的 102）的计算设备 810、资源所在地（例如图 1 中的 106）的计算设备 820 和资源请求者（例如图 1 中的 104）的计算设备 830 经由通信网络介质 850 可操作地耦合。网络介质可以是计算设备期望穿过其进行通信的任何网络介质。作为例子，网络介质能够端到端地承载 IP 分组并且可能涉及接入网中的 UMTS（通用移动通信网络）或 WiFi 或 DSL（数字用户线）、城域网中的以太网以及骨干网中的 MPLS（多协议标签交换）。然而，本发明不限于特定类型的网络介质。通常，根据所执行的授权委派场景，每个计算设备可以用作客户端机器或服务器机器。还应当理解，尽管资源所在地被显示为分离的计算设备，然而它可以是与拥有者或请求者相同的计算设备的一部分。同样，尽管资源拥有者、请求者和所在地在图 8 中每个都显示为通过一个技术设备而实现，然而应当理解，每个都可以通过不止一个这种计算设备被实现。如对于本领域技术人员显而易见的那样，计算设备可以实现为在计算机程序代码控制下操作的编程计算机。计算机程序代码由计算机的处理器执行。给出本发明的公开，本领域技术人员能够容易地制造合适的计算机程序代码来实现这里描述的协议。

[0058] 然而，图 8 一般地示出了通过网络介质通信的每个设备的示例性结构。如所示，资源拥有者 810 包括 I/O 设备 812、处理器 814 和存储器 816。资源所在地 820 包括 I/O 设备 822、处理器 824 和存储器 826。资源请求者 830 包括 I/O 设备 832、处理器 834 和存储器 836。

[0059] 应当理解，这里使用的术语“处理器”旨在包括一个或多个处理设备，这包括中央处理单元（CPU）或其它处理电路，包括但不限于一个或多个信号处理器、一个或多个集成电路等等。同样，这里使用的术语“存储器”旨在包括关联于处理器或 CPU 的存储器，例如 RAM、ROM、固定存储设备（例如硬驱）或可移除存储设备（例如磁盘或 CDROM）。此外，这里使用的术语“I/O 设备”旨在包括用于输入数据至处理单元的一个或多个输入设备（例如键盘、鼠标），以及用于提供关联于处理单元的结果的一个或多个输出设备（例如 CRT 显示器）。

[0060] 相应地，用于执行这里描述的本发明方法的软件指令或代码可以被存储在一个或多个相关存储设备中，例如 ROM、固定或可移除存储器，并且当准备好被使用时被载入 RAM 并且由 CPU 执行。也就是说，图 8 所示的每个计算设备（810、820 和 830）可以被单独编程以执行图 1 和 7 所示的它们各自的协议步骤。

[0061] 尽管这里已经参考附图描述了本发明的说明性实施例，然而应当理解，本发明不限于这些明确的实施例，并且本领域技术人员可以在不背离本发明范围或精神的前提下实现各种不同的更改和修改。

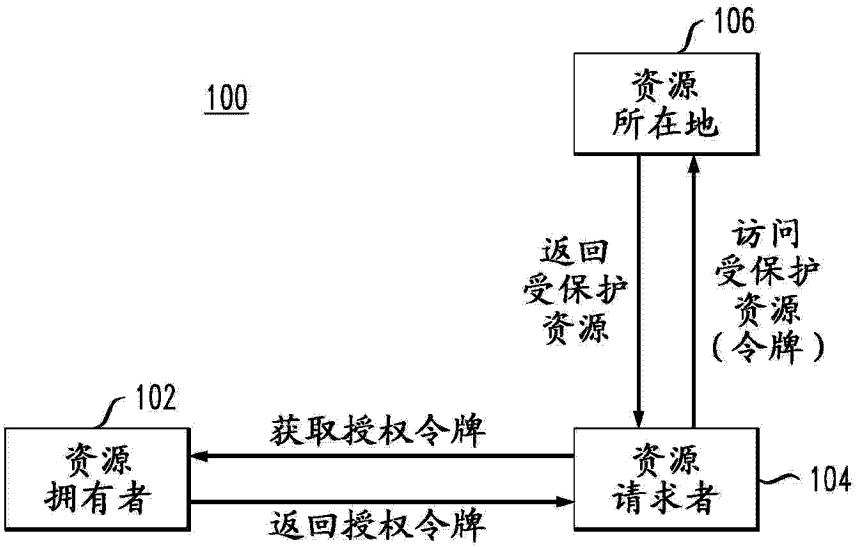

100
106
资源
所在地
返回
受保护
资源
访问
受保护
资源
(令牌)
102
资源
拥有者
获取授权令牌
返回授权令牌
资源
请求者
104

图 1

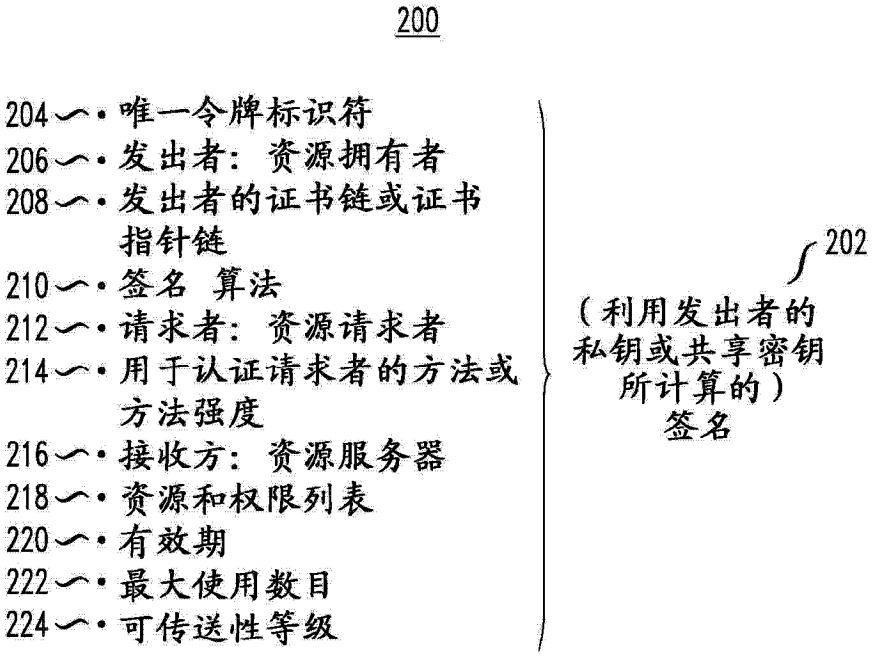

200
204 唯一令牌标识符
206 发出者: 资源拥有者
208 发出者的证书链或证书
指针链
210 签名 算法
212 请求者: 资源请求者
214 用于认证请求者的方法或
方法强度
216 接收方: 资源服务器
218 资源和权限列表
220 有效期
222 最大使用数目
224 可传送性等级
202
(利用发出者的
私钥或共享密钥
所计算的)
签名

图 2

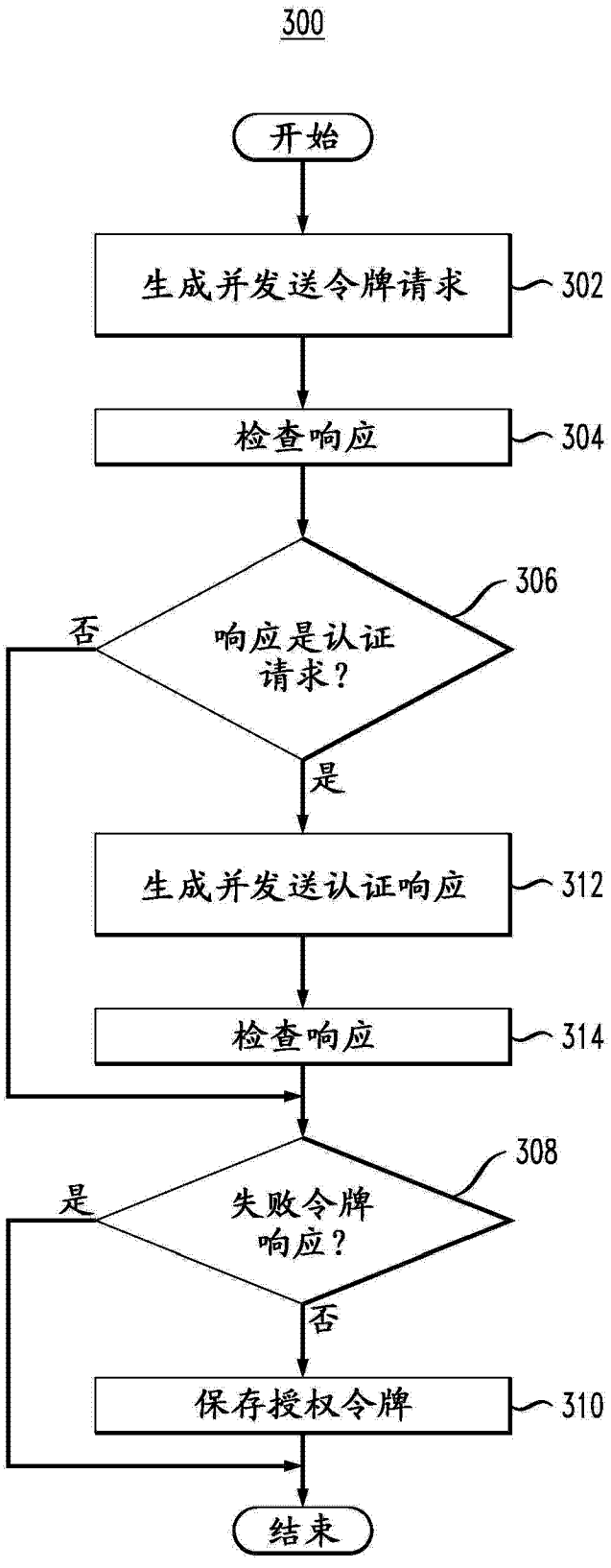

300
开始
生成并发送令牌请求
302
检查响应
304
响应是认证请求？
306
否
是
生成并发送认证响应
312
检查响应
314
失败令牌响应？
308
是
否
保存授权令牌
310
结束

图 3

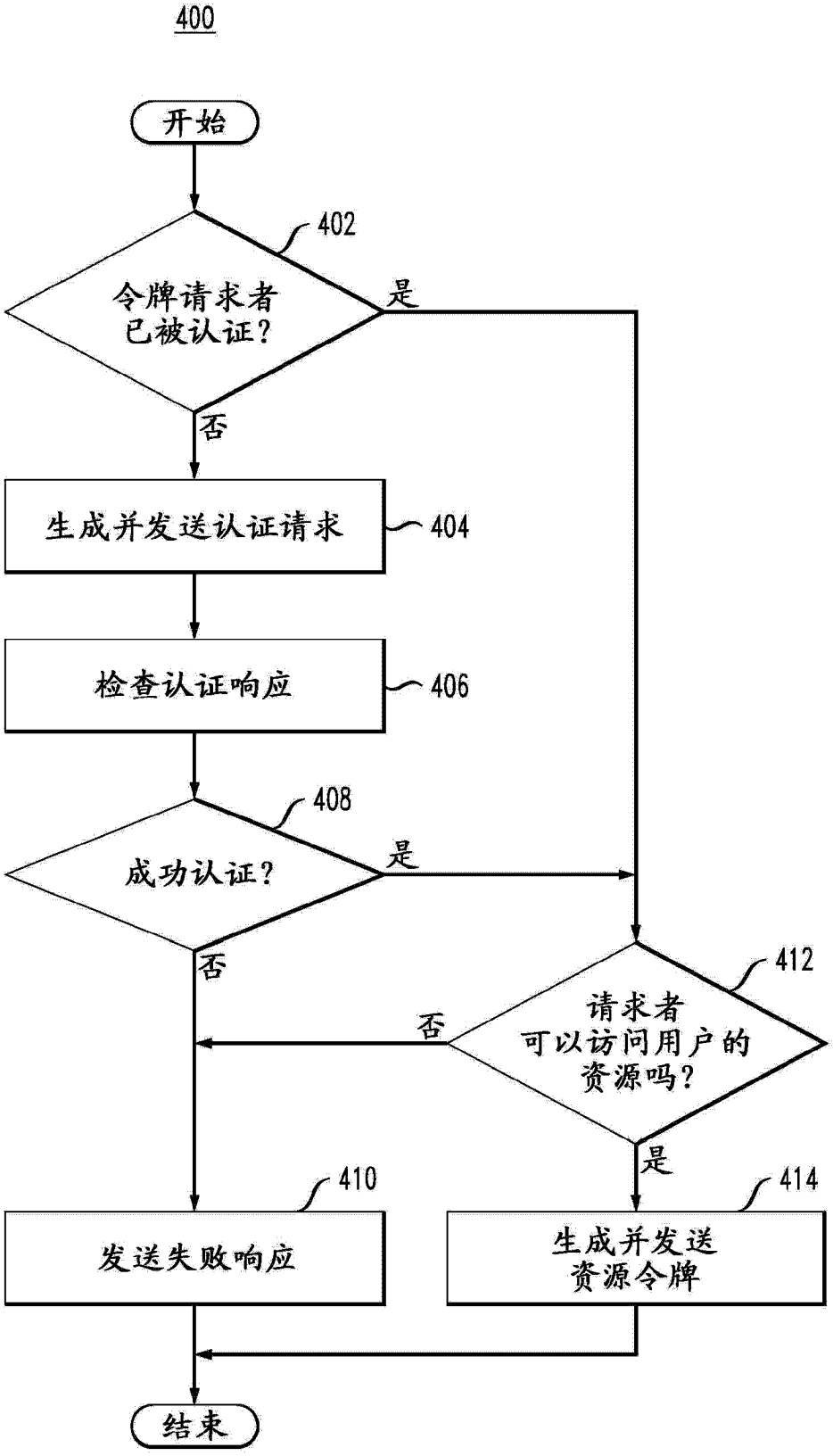

400
开始
402
令牌请求者
已被认证?
是
否
生成并发送认证请求
404
检查认证响应
406
408
成功认证?
是
否
412
请求者
可以访问用户的
资源吗?
否
是
410
发送失败响应
414
生成并发送
资源令牌
结束

图 4

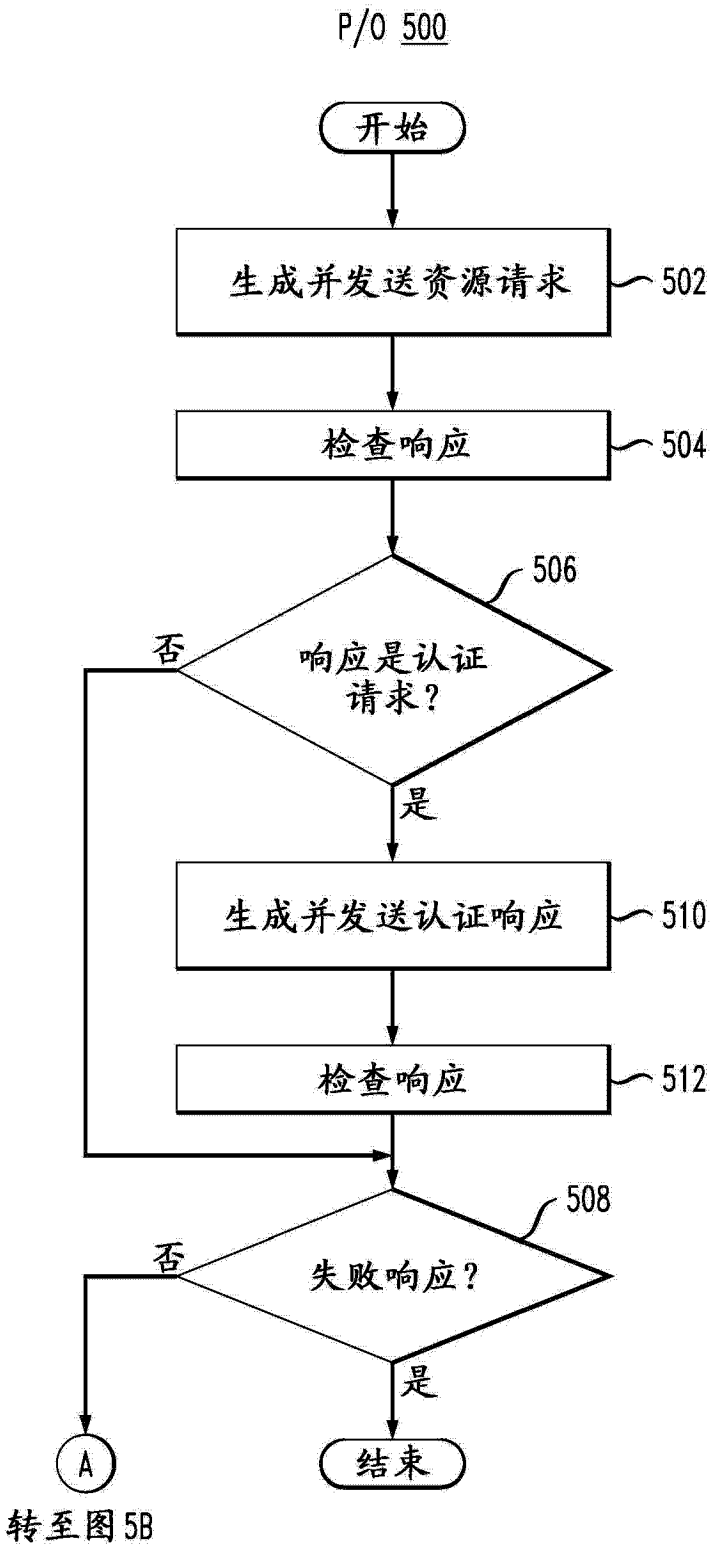

P/O 500
开始
生成并发送资源请求
502
检查响应
504
506
响应是认证请求？
否
是
生成并发送认证响应
510
检查响应
512
508
失败响应？
否
是
A
转至图 5B
结束

图 5A

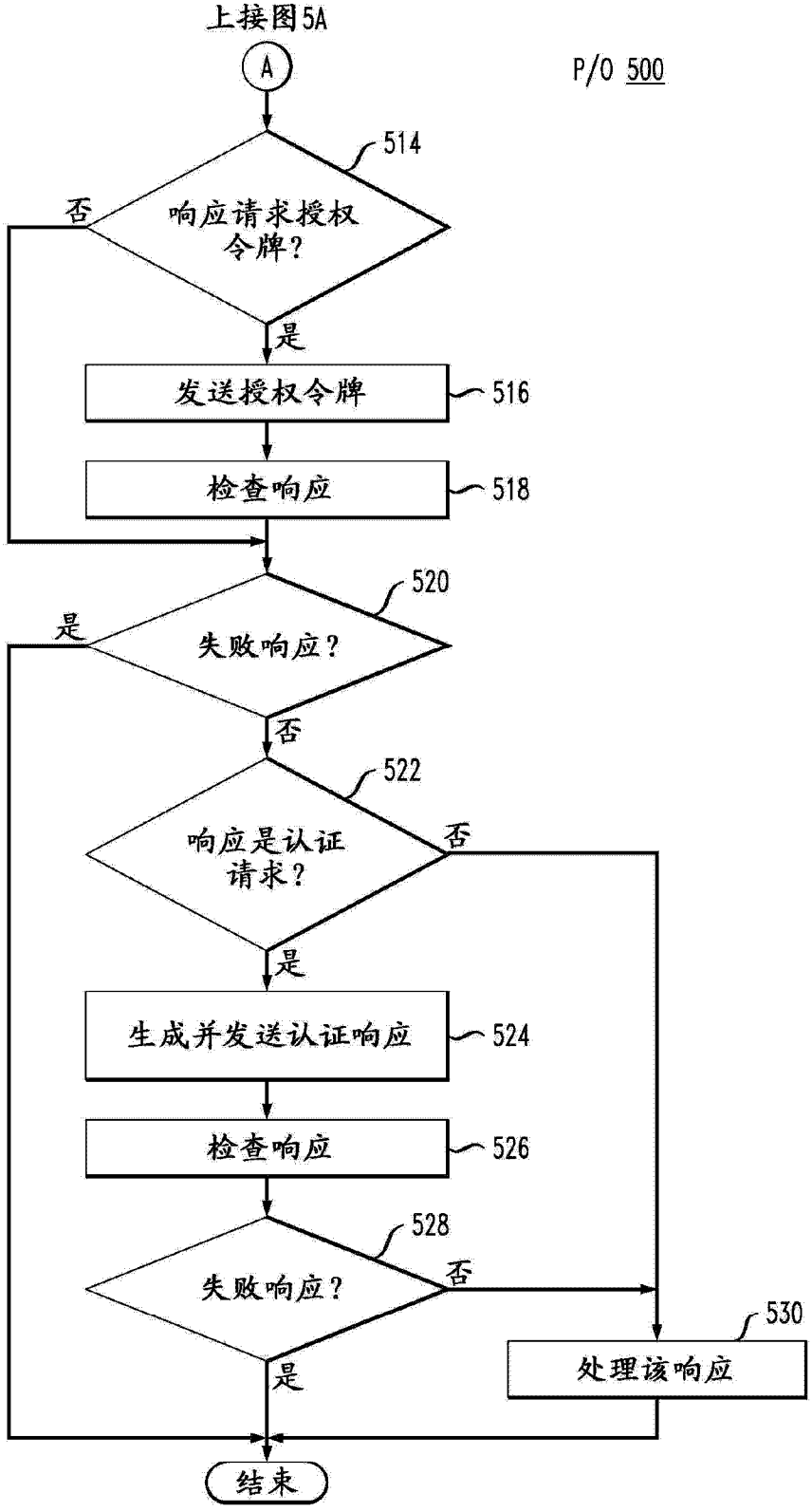

上接图5A
A
P/O 500
514
响应请求授权令牌？
否
是
发送授权令牌
516
检查响应
518
520
失败响应？
是
否
522
响应是认证请求？
否
是
生成并发送认证响应
524
检查响应
526
528
失败响应？
否
是
530
处理该响应
结束

图 5B

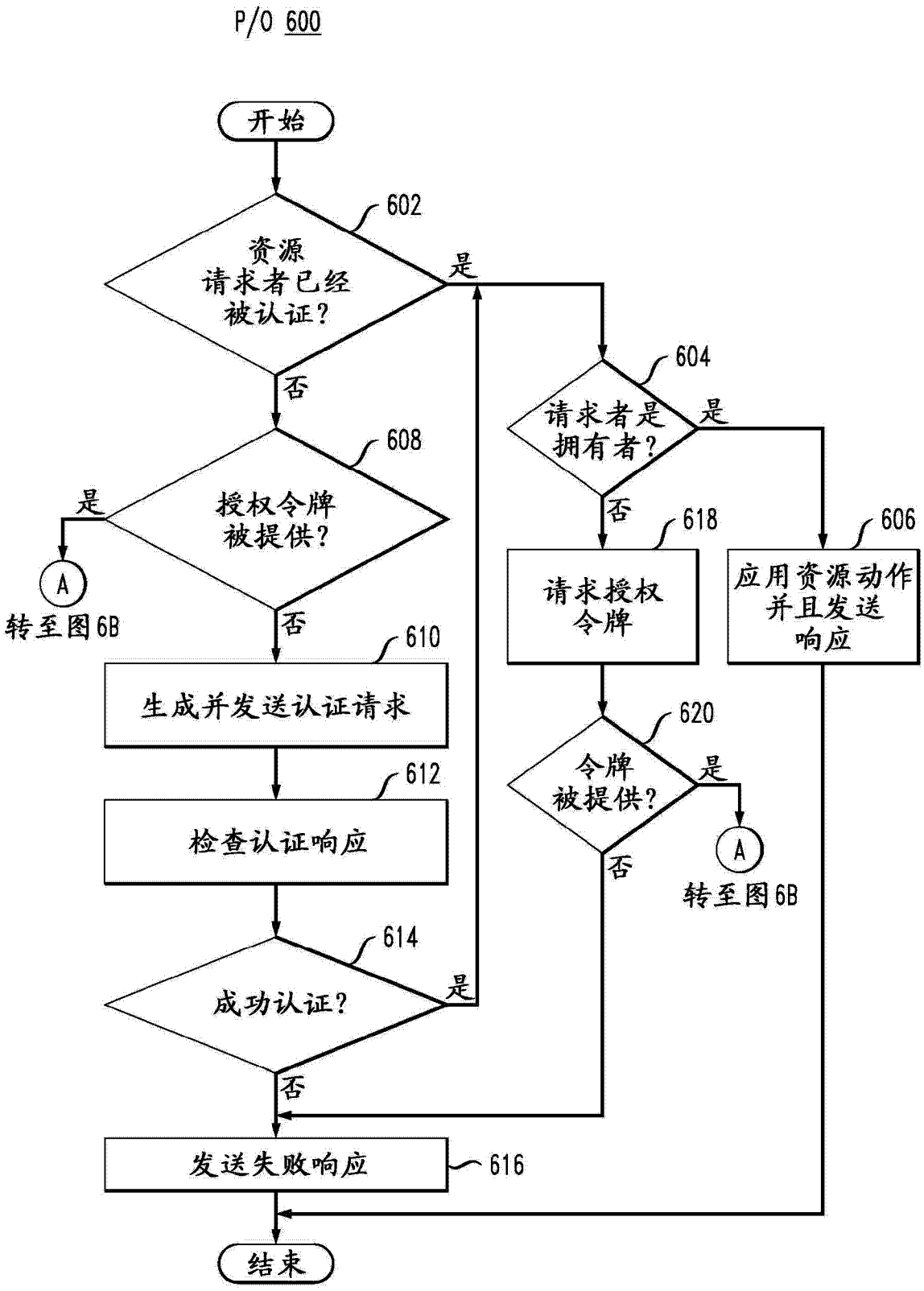

P/O 600
开始
602
资源请求者已经被认证？
是
否
604
请求者是拥有者？
是
否
606
应用资源动作并且发送响应
608
授权令牌被提供？
是
否
A
转至图 6B
610
生成并发送认证请求
612
检查认证响应
614
成功认证？
是
否
616
发送失败响应
618
请求授权令牌
620
令牌被提供？
是
否
A
转至图 6B
结束

图 6A

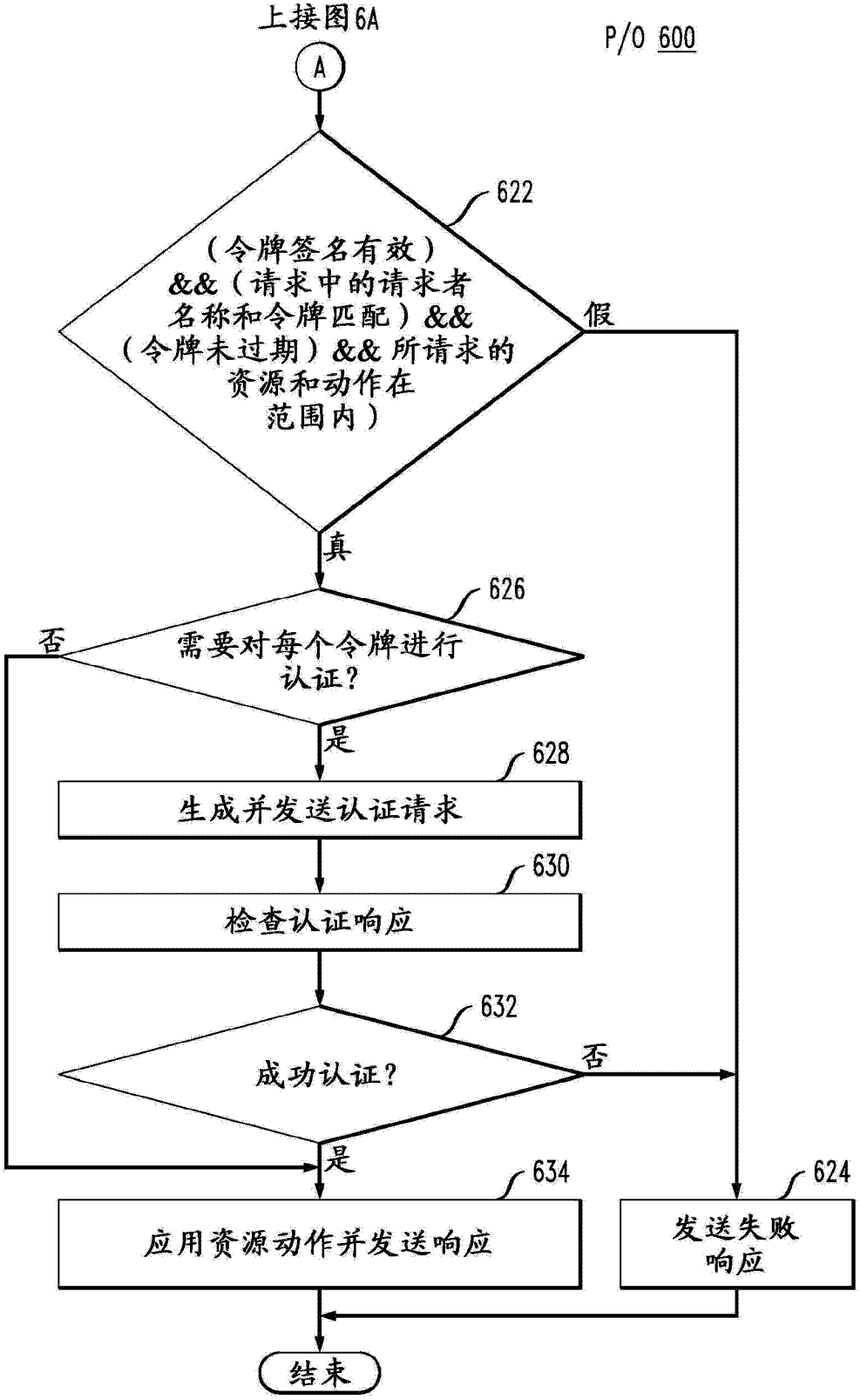

上接图6A
A
P/O 600
622
（令牌签名有效）&&（请求中的请求者名称和令牌匹配）&&（令牌未过期）&& 所请求的资源和动作在范围内）
假
真
626
需要对每个令牌进行认证？
否
是
628
生成并发送认证请求
630
检查认证响应
632
成功认证？
否
是
634
应用资源动作并发送响应
624
发送失败响应
结束

图 6B

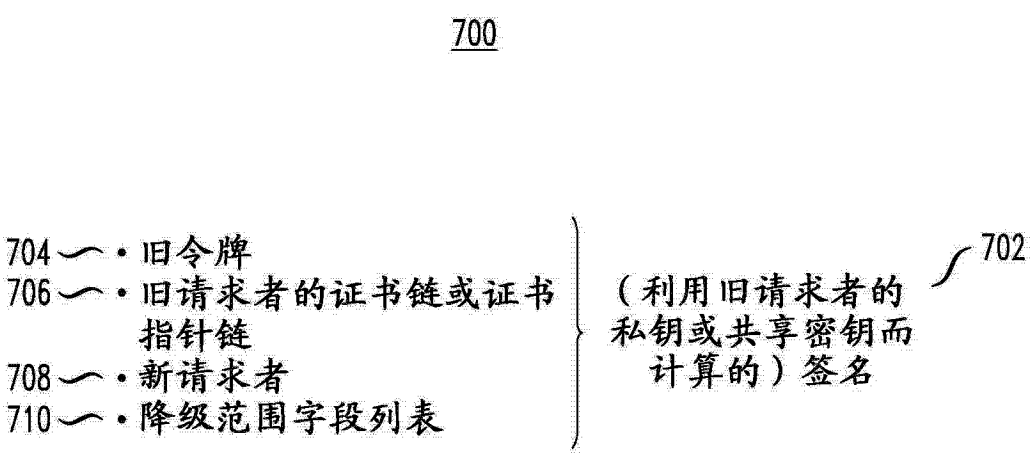

700
704 • 旧令牌
706 • 旧请求者的证书链或证书指针链
708 • 新请求者
710 • 降级范围字段列表
（利用旧请求者的私钥或共享密钥而计算的）签名
702

图 7

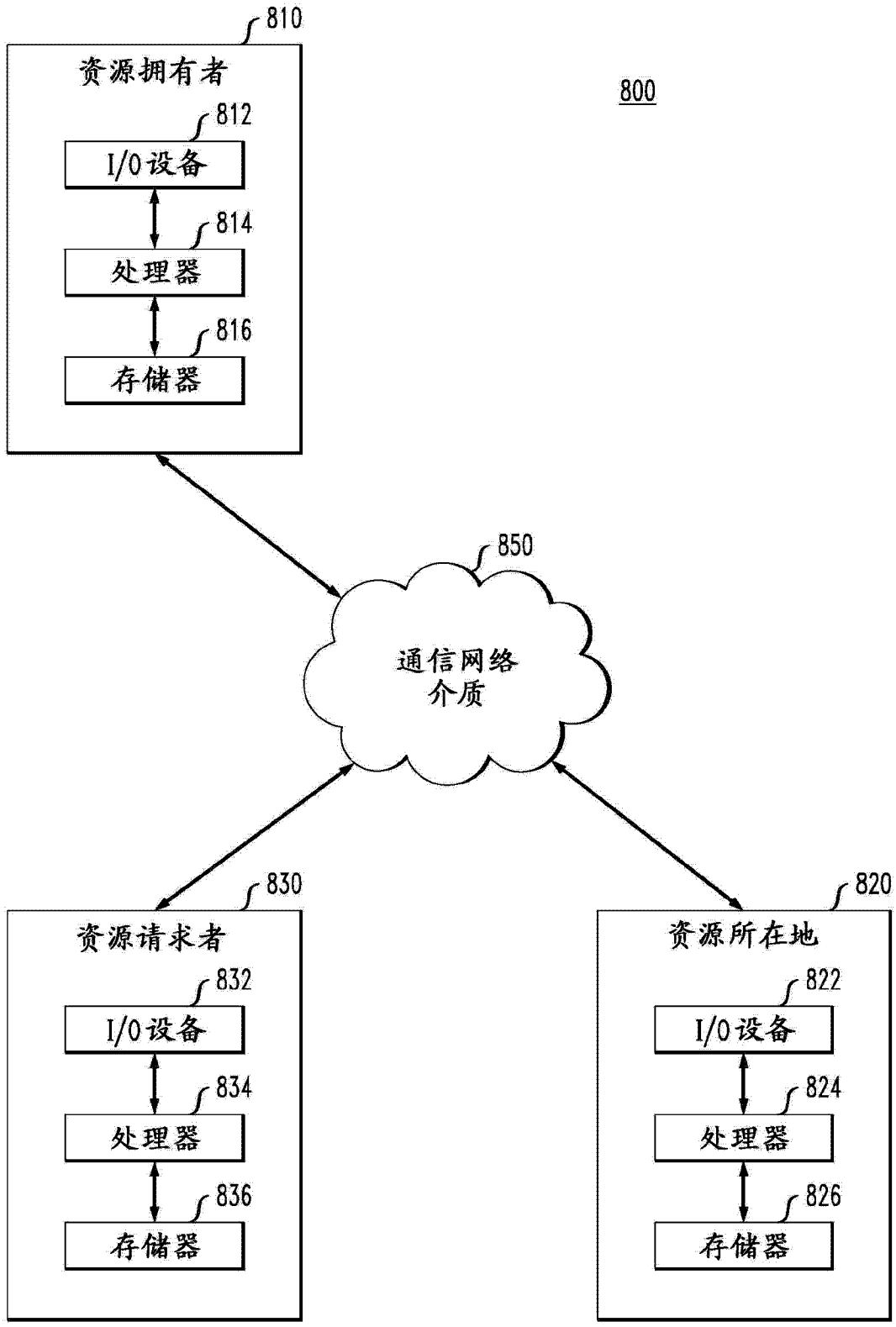

800
810
资源拥有者
812
I/O设备
814
处理器
816
存储器
850
通信网络
介质
830
资源请求者
832
I/O设备
834
处理器
836
存储器
820
资源所在地
822
I/O设备
824
处理器
826
存储器

图 8