[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 21/20 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200880012470.2

[43] 公开日 2010 年 3 月 3 日

[11] 公开号 CN 101663670A

[22] 申请日 2008.3.18
[21] 申请号 200880012470.2
[30] 优先权
[32] 2007. 4.20 [33] US [31] 60/912,986
[32] 2008. 2. 1 [33] US [31] 12/024,901
[86] 国际申请 PCT/US2008/057375 2008.3.18
[87] 国际公布 WO2008/130760 英 2008.10.30
[85] 进入国家阶段日期 2009.10.19
[71] 申请人 微软公司
地址 美国华盛顿州
[72] 发明人 C·迈克默特里 A·T·韦纳特
V·梅列舒克 M·E·贾巴拉
[74] 专利代理机构 上海专利商标事务所有限公司
代理人 顾嘉运 钱静芳

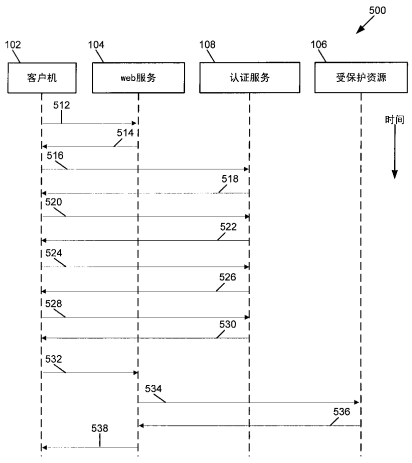
权利要求书 4 页 说明书 16 页 附图 6 页

[54] 发明名称

对访问 web 服务资源的请求专用认证

[57] 摘要

访问 web 服务资源的请求基于接收到的请求的类型来评估。 除非提供授权请求的认证的足够证明，否则不授权该请求。 认证服务评估一个或多个因素以确定是否认证客户机。 在得到认证服务的认证后，向 web 服务提供授权对 web 服务资源的访问的认证的证明。



1. 一种用于控制对受保护 web 服务资源（106）的访问的计算系统（104），所述计算系统（104）包括：

用于跨通信网络（110）进行通信的通信设备（612）；

通信地耦合到所述通信设备（612）的处理器（602）；以及

存储程序指令的存储器（604），所述指令在由所述处理器（602）执行时使所述计算系统（604）执行一种控制对受保护 web 服务资源（106）的访问的方法。所述方法包括：

(i) 从客户机接收从所述通信网络（110）访问所述受保护 web 服务资源（106）的第一请求；

(ii) 确定所述客户机已根据第一因素来认证；

(iii) 基于根据所述第一因素的认证来授权访问所述受保护 web 服务资源（106）的第一请求；

(iv) 从所述客户机（102）接收从所述通信网络（110）访问所述受保护 web 服务资源（106）的第二请求；

(v) 基于根据不足以授权所述第二请求的第一因素的认证来拒绝访问所述受保护 web 服务资源（106）的第二请求；

(vi) 确定所述客户机（102）已根据第二因素来认证；以及

(vii) 基于根据所述第二因素的认证来授权访问所述受保护 web 服务资源（106）的第二请求。

2. 如权利要求 1 所述的计算系统，其特征在于，所述第一因素选自包括以下各项的组：口令、对安全问题的回答、生物测定标识符、对象以及客户机专用信息。

3. 如权利要求 1 所述的计算系统，其特征在于，所述第二因素不同于所述第一因素。

4. 如权利要求 1 所述的计算系统，其特征在于，所述方法还包括在所述客户机已根据所述第一因素来由认证服务认证后从所述客户机接收第一认证令牌并且使用该第一认证令牌来确定所述客户机已根据所述第一因素来认证。

5. 如权利要求 4 所述的计算系统，其特征在于，确定所述客户机已被认证

包括：

用所述认证服务的公钥来解密所述第一认证令牌；以及

确定所述第一认证令牌中的由所述认证服务作出的声明满足访问条件。

6. 如权利要求 1 所述的计算系统，其特征在于，拒绝所述第二请求包括向所述客户机发送消息以将所述客户机定向到认证服务以便根据第二因素来认证。

7. 如权利要求 6 所述的计算系统，其特征在于，确定所述客户机已根据第二因素来认证包括在根据所述第二因素来由所述认证服务认证后从所述客户机接收认证令牌。

8. 如权利要求 6 所述的计算系统，其特征在于，授权访问所述受保护 web 服务资源的第二请求基于对认证令牌的评估。

9. 一种授权客户机（102）访问 web 服务资源（106）的方法，所述方法包括：

(i) 从所述客户机（102）接收要认证的请求（516）；

(ii) 向所述客户机（102）发送质询消息（518）；

(iii) 从所述客户机（102）接收对所述质询消息（518）的确认响应（520）；

(iv) 确定所述确认响应满足预定准则；

(v) 确定所述要认证的请求需要进一步认证；

(iv) 以第二质询消息（522）、第二确认响应（524）和第二预定准则来重复(ii)到(iv)；以及

(v) 向所述客户机（102）发送认证消息（530）；

10. 如权利要求 9 所述的方法，其特征在于，确定所述要认证的请求需要进一步认证包括从所述请求中读取数据并将来自所述请求的数据与同所述质询消息相关联的认证级别进行比较。

11. 如权利要求 9 所述的方法，其特征在于，向所述客户机发送所述认证消息包括向所述客户机发送认证令牌。

12. 如权利要求 11 所述的方法，其特征在于，所述认证令牌包括来自认证服务的关于用于认证所述客户机的因素的声明。

13. 如权利要求 9 所述的方法，其特征在于，还包括在向所述客户机发

送所述认证消息之前以第三质询消息、第三确认响应和第三预定准则来重复(ii)到(iv)。

14. 一种包含计算机可执行指令的计算机可读存储介质（608），所述指令在由计算机（104）执行时执行一种控制对受保护资源（106）的访问的方法，所述方法包括：

从客户机（102）接收标识 web 服务（104）的受保护资源（106）的请求（512）；

向所述客户机（102）发送向认证服务（108）请求认证的响应（514）；

在向所述认证服务（108）认证后从所述客户机（102）接收认证（532）；

确定所述认证是否足以授权所述请求；

如果所述认证足以授权所述请求，则授权所述请求；以及

如果所述认证不足以授权所述请求，则拒绝所述请求。

15. 如权利要求 14 所述的计算机可读介质，其特征在于，所述认证是认证令牌。

16. 如权利要求 15 所述的计算机可读介质，其特征在于，所述认证令牌使用公钥密码来加密。

17. 如权利要求 14 所述的计算机可读介质，其特征在于，所述方法还包括如果所述认证足以授权所述请求，则在授权所述请求后授权对所述 web 服务的受保护资源的访问。

18. 如权利要求 14 所述的计算机可读介质，其特征在于，拒绝所述请求包括用消息来将向所述客户机传达所述拒绝，所述消息包括关于被配置成认证所述客户机的认证服务的信息。

19. 如权利要求 14 所述的计算机可读介质，其特征在于，所述方法还包括：

从所述客户机接收标识所述 web 服务的受保护资源的第二请求，所述第二请求包括所述认证；

确定所述认证是否足以授权所述第二请求；

如果所述认证足以授权所述第二请求，则授权所述第二请求；以及

如果所述认证不足以授权所述第二请求，则拒绝所述第二请求。

20. 如权利要求 14 所述的计算机可读介质，其特征在于，拒绝所述请求包括发送根据简单对象访问协议的故障消息，并且其中接收认证包括接收根据 web 服务信任规约的 web 服务信任请求安全令牌响应消息。

对访问 web 服务资源的请求专用认证

背景

当用户试图通过诸如因特网等网络来访问受保护的远程资源时，该用户通常遵照由控制该资源的服务器发出的策略陈述。该策略陈述提供发起与资源的通信所需的认证和授权规则集。例如，策略陈述可能要求用户在访问资源之前提供口令。如果该用户提供正确的口令，则认证该用户的身份并允许访问该资源。

虽然策略陈述认证方法在其中单一的认证形式足以发起与受保护资源的通信的情形中起到很好的作用，但策略陈述在动态环境中无法起到很好的作用。在动态环境中，在客户机和受保护资源之间的通信开始时的单个认证实例可能不够。例如，当用户试图访问具有受保护资源的网站时，对于该用户而言通过输入口令来提供认证在最初可能是足够的。然而，一旦用户可访问该网站，该用户就可尝试改变他或她的口令，更新目录、访问高度受保护资源或请求诸如系统管理员组等提升的访问组的特权。在这种情况下，该用户正在请求执行不止简单地查看信息的动作。这些动作具有对受保护资源造成大量破坏的可能性。

某些认证方法在使得能够与资源进行通信之前需要认证。然而，在动态环境中，在接收到请求访问受保护资源的实际请求之前难以确定要应用什么认证和认证规则。

概述

本发明的各实施例涉及用于消息专用认证的系统、方法和数据结构。一方面是用于控制对受保护 web 服务资源的访问的计算系统。该计算系统包括通信设备、处理器和存储器。该通信设备跨通信网络进行通信。该处理器通信地连接到该通信设备。该存储器存储程序指令，该指令在由该处理器执行时使该计算系统执行一种控制对受保护 web 服务资源的访问的方法。该方法包括从客户机接收从通信网络访问受保护 web 服务资源的第一请求；确定该客户机已根据

第一因素来认证；基于根据该第一因素的认证来授权该访问受保护 web 服务资源的第一请求；从客户机接收从通信网络访问受保护 web 服务资源的第二请求；基于根据不足以授权该第二请求的第一因素的认证来拒绝该访问受保护 web 服务资源的第二请求；确定客户机已根据第二因素来认证；以及基于根据该第二因素的认证来授权该访问受保护 web 服务资源的第二请求。

另一方面是一种认证客户机以便访问 web 服务资源的方法。该方法包括：(i) 从要认证的客户机接收请求；(ii) 向该客户机发送质询消息；(iii) 从该客户机接收对该质询消息的确认响应；(iv) 确定该确认响应满足预定准则；(v) 确定要认证的请求需要进一步认证；(iv) 以第二质询消息、第二确认响应和第二预定准则来重复(ii)到(iv)；以及(v) 向该客户机发送认证消息。

又一方面涉及一种包含计算机可执行指令的计算机可读存储介质，所述指令在由计算机执行时执行一种控制对受保护资源的访问的方法，所述方法包括：从客户机接收标识 web 服务的受保护资源的请求；向客户机发送向认证服务请求认证的响应；在向该认证服务认证后从该客户机接收认证令牌；确定该认证令牌是否足以授权该请求；如果该认证令牌足以授权该请求，则授权该请求；以及如果该认证令牌不足以授权该请求，则拒绝该请求。

各实施例可被实现为计算机进程、计算系统、或者诸如计算机程序产品或计算机可读介质等制品。计算机程序产品可以是计算机系统可读并编码用于执行计算机进程的指令的计算机程序的计算机存储介质。计算机程序产品也可以是计算系统可读并编码用于执行计算机进程的指令的计算机程序的载波上的传播信号。

提供本概述是为了以简化的形式介绍将在以下详细描述中进一步描述的一些概念。本概述并不旨在标识所要求保护的主题的关键特征或必要特征，也决不旨在用于限制所要求保护的主题的范围。

附图简述

图 1 是被配置成执行动态认证的示例系统的框图。

图 2 是示出用于动态确定是否需要认证的示例方法的流程图。

图 3 是示出用于认证客户机的示例方法的流程图。

图 4 是示出用于动态控制对受保护资源的访问的示例方法的流程图。

图 5 是示出用于控制对受保护资源的访问的示例方法的流程图。

图 6 是用于实现本发明的各方面的示例性计算系统的框图。

详细描述

本发明现将参考其中示出了各具体实施例的附图来更完整地描述各示例性实施例。然而，其它方面能以许多不同的形式来实现，并且在本发明中包括具体实施例不应被解释为将这些方面限于在此所述的各实施例。相反，包括附图中描绘的各实施例是为了提供全面和完整且将预期的范围完全地传达给本领域技术人员的公开。在参考附图时，使用相同的附图标记来指示所有附图所示的相同的结构和元素。

本发明的某些实施例涉及用于消息专用认证的系统和方法。一方面是在允许客户机访问受保护资源之前确定是否需要认证的方法。

一般而言，认证是验证由诸如计算系统、客户机、系统或人等某物作出的身份声明的真实性的过程。认证计算系统通常包括确认其来源或源。对来源或源的确认通常通过将诸如制造地点和时间、网络上的位置、物理位置、标识号等关于声明特定身份的计算系统的信息与关于该特定身份的已知信息进行比较来实现。

然而，认证一个人的动作涉及例如，确认这个人的身份。存在可用于认证的许多不同的标识特性。一种标识人的方法涉及检测生物测定标识符。该认证方法要求声明一身份的人提供诸如 DNA、指纹图案、视网膜图案等声明该身份的人的唯一特征形式的验证。能够验证一个人的身份的另一种方式是通过这个人所知道的某样东西。该认证方法要求声明一身份的人提供诸如口令、pin 号等个人信息形式的验证。能够验证一个人的身份的另一种方式是通过这个人所具有的某样东西。该认证方法要求声明一身份的人提供诸如钥匙、安全卡、安全令牌、信用卡等对象形式的验证。这些认证方法可在被称为多因素认证的过程中单独或一起使用。

一般而言，在认证客户机时，该过程包括认证客户机或认证使用该客户机的人的身份。在一个实施例中，该客户机可以是 web 浏览器。在另一实施例中，

该客户机可以是被配置成作出远程过程调用的程序，或者与受保护资源进行通信的任何其他应用程序或程序。

在动态环境中，各种类型的认证以及用于认证客户机的规则取决于所作出的各种类型的访问受保护资源的请求而变化。例如，请求查看受保护资源的消息可能需要比请求修改该受保护资源的消息较不费力的认证。在一个实施例中，受保护资源是仅特定用户可访问的专用网站。在另一实施例中，受保护资源可以是私人电子邮件组、受保护数据、受保护方法、受保护过程、受保护操作或者应被限于特定用户或客户机的任何其他类型的受保护信息或功能。

图 1 是被配置成执行请求专用动态认证的示例系统 100 的框图。在所示实施例中，系统 100 包括客户机 102、web 服务 104 和认证服务 108。web 服务 104 包括受保护资源 106。在该实施例中，客户机 102 期望获取对受保护资源 106 的访问权。然而，受保护资源 106 被保护以免被未经认证的客户机访问。客户机 102、web 服务 104 和认证服务 108 被配置成跨网络 110 进行通信。网络 110 是数据通信路径。在一个实施例中，网络 110 是因特网。在其他实施例中，网络 110 是局域网、内联网、无线网络或者被配置成将数据从一个计算设备传递到另一个计算设备的任何其他通信路径。

在一个实施例中，客户机 102 是计算系统。在其他实施例中，客户机 102 是被配置成跨网络 110 传递数据的任何计算系统。客户机 102 的一个示例是图 6 所示的计算系统 600。客户机 102 通过网络 110 来与 web 服务 104 和认证服务 108 通信地连接。在某些实施例中，客户机 102 可通过向 web 服务 104 发送消息来访问受保护资源 106。在另一实施例中，客户机 102 直接向受保护资源 106 发送消息。

在一个实施例中，web 服务 104 是诸如 web 服务器等操作 web 服务的计算系统（例如，图 6 所示的计算系统 600）。一般而言，web 服务 104 提供可使用数据通信协议来通过网络 110 访问的有用功能。web 服务可用于提供无数种有用功能。在一个实施例中，web 服务 104 是服务器。在另一实施例中，web 服务 104 是在通信地连接到网络 110 的计算系统上操作的计算系统应用程序。在某些实施例中，web 服务 104 是 web 服务消息可被定址到的可引用实体、处理器或资源。

一般而言，web 服务 104 的某些实施例监视网络 110 以查找发自客户机 102 的关于受保护资源 106 的消息。当接收到一消息时，web 服务 104 确定该消息是否包含需要认证客户机 102 的请求。对客户机 102 的认证有时在准许客户机 102 访问受保护资源 106 之前是必需的，以便控制对受保护资源 106 的访问。如果 web 服务 104 确定需要认证，则 web 服务 104 将客户机 102 定向到认证服务 108。

在所示实施例中，web 服务 104 包括受保护资源 106。受保护资源包括例如，只可由经认证的客户机来访问、使用或修改的由 web 服务 104 执行的功能以及由 web 服务 104 存储的数据。例如，如果 web 服务 104 提供维护组分发列表的服务，则该组分发列表是只可由经认证的客户机访问、使用或修改的受保护资源。作为另一示例，受保护资源 106 是目录中的条目。在另一实施例中，受保护资源 106 是数据库中的记录。在另一实施例中，受保护资源 106 是存储在存储器存储设备上的文件或文件的一部分。其他实施例使用其他形式的受保护资源 106。

在一个实施例中，认证服务 108 是诸如服务器等通信地连接到网络 110 的计算系统（例如，图 6 所示的计算系统 600）。在另一实施例中，认证服务 108 是运行位于网络上的软件应用程序的计算系统。认证服务 108 被配置成认证客户机 102。认证服务 108 的一个示例是安全令牌服务端点。尽管所示实施例示出认证服务 108 的一个示例与 web 服务 104 分开且不同，但在其他实施例中，认证服务 108 和 web 服务 104 在同一服务器上操作。

如果客户机 102 得到认证以执行其消息中对受保护资源 106 的请求，则 web 服务 104 向客户机 102 传递所请求的操作的结果。然后，在其他可能的实施例中，认证服务 108 跨网络 110 直接与 web 服务 104 进行通信，诸如以便从 web 服务 104 接收对认证的请求，或者向 web 服务 104 发送认证证明。

除了认证之外，有时期望通过要求不仅认证客户机而且授权客户机来控制对受保护资源的访问。认证在由 Craig V. McMurtry、Alexander T. Weinert、Vadim Meleshuk 和 Mark E. Gabarra 在 2008 年 2 月 1 日提交的题为“AUTHORIZATION FOR ACCESS TO WEB SERVICE RESOURCES（对 web 服务资源的访问的授权）”的美国专利申请第 12/024,896 号中描述，该申请的

全部公开内容通过引用结合于此。

图 2 是示出用于动态确定是否需要认证的示例方法 200 的流程图。方法 200 包括操作 202、204、206、208 和 210。方法 200 开始于操作 202，在其间作出资源请求。在一个实施例中，操作 202 涉及将包括访问受保护资源 106 的请求的消息从客户机 102 传递至 web 服务 104。在某些实施例中，该消息是远程过程调用。在另一实施例中，该请求可采取电子邮件或客户机和资源之间的任何其他类型的电子通信的形式。在另一实施例中，操作 202 涉及客户机 102 向 web 服务 104 发送诸如在 web 服务通信中常用的 Create（创建）、Get（获取）、Delete（删除）、Enumerate（枚举）请求。

在作出该资源请求后，执行操作 204 以评估该请求并确定认证是否是必需的。在一个实施例中，web 服务分析从客户机发送到受保护资源的消息以确定该消息是否包含要求该客户机提供认证的请求。在一个实施例中，如果试图访问受保护资源的客户机先前已经提供了对于请求所必需的认证，则该客户机将不必提供认证。在另一实施例中，如果资源是对请求该资源的任何人可用的公共资源，则客户机将不必提供认证。在另一实施例中，即使资源可能是受保护的，但如果消息包含不需要认证的请求，诸如如果该消息是无法破坏该受保护资源的类型，则认证并非必需。如果 web 服务 104 在操作 204 中确定认证并非必需，则执行操作 206。如果认证是必需的，则执行操作 208。

在一个示例中，web 服务 104 通过评估多个考虑事项来确定认证是否是必需的。这些考虑事项包括用于传达请求的介质（诸如是局域网还是远程访问）、请求所涉及的对象的类型、请求所涉及的对象的特性、以及已经与请求包括在一起的凭证的质量。例如，对于凭证的质量，如果凭证是对应于来自另一组织的用户，则取决于该用户正试图访问的资源，可能需要附加凭证。

如果认证并非必需，则执行操作 206 以授权对所请求的资源的访问。web 服务通过例如向客户机发送资源的表示、通过对受保护资源执行所请求的操作或通过向客户机发送所请求的操作的结果来授权对该受保护资源的访问。

然而，如果认证是必需的，则执行操作 208 以执行该认证。认证客户机将参考图 3 进一步讨论。要求客户机提供认证的情形的示例包括其中客户机试图访问或修改专用网站、私人电子邮件组、受保护数据、受保护方法、受保护过

程、受保护操作或任何其他类型的受保护信息或功能的情况。在某些实施例中，web 服务 104 质询客户机 102 以使其提供认证。或者，web 服务 104 将该客户机定向到认证服务（如认证服务 108）。认证服务 108 可位于 web 服务 104 处，位于来自该 web 服务的其他地方，或者在分布式网络的情况下位于两者处。认证客户机的示例方法参考图 3 示出并描述。

在认证客户机后，执行操作 206 以授权该客户机访问该 web 服务的受保护资源。在一个实施例中，在该客户机将来自认证服务的认证令牌提供给 web 服务后授权该访问。该 web 服务例如通过向客户机发送资源、通过对受保护资源执行所请求的操作、通过指示受保护资源执行所请求的操作或通过向客户机发送所请求的操作的结果来授权访问。

如果确定客户机不应当得到认证，则执行操作 210，在其间拒绝对受保护资源的访问。在一个示例中，由于认证服务 108 未提供获取对受保护资源的访问权所需的认证令牌而拒绝访问。

图 3 是示出用于认证客户机的示例方法 300 的流程图。在一个实施例中，方法 300 与图 2 所示的操作 208 相对应。方法 300 开始于操作 302，在其间作出对认证的请求。在一个实施例中，操作 302 涉及将消息从客户机 102 发送到认证服务 108 以及认证服务 108 接收对认证的请求。

在所示实施例中，在接收到该对认证的请求后，执行操作 304 以传递认证质询。在一个实施例中，认证服务 108 向客户机 102 传递质询以测试该客户机或用户身份的真实性。在某些实施例中，该质询采取以下形式：请求口令；请求对安全问题的回答；请求 DNA 样本、指纹图案、视网膜图案、其他形式的生物测定标识符、使用客户机的人的其他唯一标识符；请求诸如钥匙、安全卡、安全令牌、信用卡或对于使用客户机的人是唯一的某一其他对象等对象形式的验证；请求诸如制造地点和时间、网络上的位置、物理位置、标识号等客户机专用信息；或者请求可用于认证目的的任何其他类型的信息。

在所示实施例中，一旦已传递质询，就执行操作 306 以接收对该质询的确认响应。操作 306 涉及提供操作 304 中所请求的信息、样本、标识符等，并将其传递给认证服务 108。在一个实施例中，客户机 102 的用户使用输入设备（例如，图 6 所示的输入设备 614）来向客户机 102 提供标识信息，该客户机 102

然后将该信息传递给认证服务 108。在某些实施例中，使用传感器（其也是一种形式的输入设备）。例如，用户将手指放在指纹扫描仪上，该扫描仪扫描该指纹。该指纹数据然后被传送到认证服务 108。可使用各种类型的输入设备，包括键盘、鼠标、触摸垫、话筒、笔、生物测定传感器、扫描仪、读卡器、化学检测器等。在其他实施例中，将数据输入到客户机 102 中，该客户机 102 然后将该数据传递给认证服务 108。

在所示实施例中，一旦已传递确认，就执行操作 308 以验证该确认响应。在一个实施例中，认证服务将其从客户机 102 接收到的确认响应与关于所声明的身份的已知信息进行比较。例如，认证服务 108 取得存储在数据库中的数据，并将该数据与确认响应数据进行比较。认证服务 108 然后确定该确认响应是否匹配先前存储的数据。如果是，则该确认响应通过验证，并且执行操作 312。如果否，则该确认响应未通过验证，并且执行操作 310。

如果所接收到的确认响应不匹配已知信息，则执行操作 310，其中拒绝对所请求的资源的访问。在另一实施例中，认证服务 108 改为返回至操作 304 以再次重试认证。在这一实施例中，可准许多次重试，诸如三次重试。如果重试不成功，则执行操作 310 以拒绝对受保护资源的访问。

如果所接收到的确认响应匹配已知信息，则然后执行操作 312 以确定进一步的认证是否是必需的。在一个实施例中，认证服务 108 确定是否需要更强形式的认证，即要求客户机提供多种形式的认证的多因素认证。如果多因素认证是必需的，则方法 300 返回到操作 304 以传递第二质询。然后如所需要地多次重复操作 304、306、308 和 310 或 312。然而，在重复时，认证质询将采取不同于先前从认证服务发出的质询的形式。例如，如果认证服务最初要求客户机提供口令，则它可能在第二或后几轮验证期间要求该客户机使用智能卡或生物测定扫描仪。在某些实施例中，可使用任何形式的认证，只要该认证形式以某种方式不同于先前所使用的形式，以使得认证服务 108 并非简单地反复请求相同的信息。在大多数情形中，重复请求相同信息将不会提供任何附加认证价值。然而，在某些情形中，诸如如果自从前一次质询以来已过去了大量时间，则可使用重复请求。

如果进一步的认证并非必需，则执行操作 314 以发放认证令牌。认证服务

108 将安全令牌返回给客户机，该客户机将该安全令牌用作该客户机已通过认证的证明。将该认证令牌从客户机 102 发送到 web 服务 104，并且 web 服务 104 然后授权客户机 102 访问最初请求的受保护资源。

图 4 是示出用于动态控制对受保护资源的访问的示例方法 400 的流程图。在一个实施例中，方法 400 由 web 服务 104 响应于从诸如试图获取对受保护资源 106 的访问权的客户机 102 接收到的消息来执行。方法 400 开始于操作 404，在其间接收请求消息。在一个实施例中，web 服务 104 从客户机 102 接收对受保护资源 106 的请求。作为一些示例，该请求是查看受保护资源、获取对受保护资源的访问权、修改受保护资源的请求。

在所示实施例中，然后执行操作 406 以确定该请求消息是否包含需要认证的请求。在一个实施例中，web 服务 104 分析该请求以确定该请求中所包含的请求是否需要认证客户机。在某些实施例中，例如，如果试图访问受保护资源的客户机先前已经提供了对于请求所必需的认证，如果资源是公共的并且对所有人可用，如果请求类型是包含不需要认证的请求的类型，或者如果请求类型及其相关联的请求无法对受保护资源造成破坏，则该客户机将不必提供认证。如果认证并非必需，则然后执行操作 414 以执行所请求的操作。

在所示实施例中，如果消息中所包含的请求需要认证，则然后执行操作 408 以传达需要认证。在一个实施例中，操作 408 涉及将消息从 web 服务 104 发送到客户机 102 以通知客户机 102 执行所请求的操作需要认证。在一个实施例中，web 服务 104 将客户机 102 定向到认证服务 108 以便进行认证，如参考图 3 所描述的。例如，消息包含认证提供者的地址。客户机使用该地址来定位该认证提供者以试图接收认证。在另一实施例中，方法 300 由 web 服务 104 来执行，以使得该消息包含请求客户机 102 提供认证信息的对客户机 102 的质询。

在所示实施例中，如果客户机成功地通过认证，则然后执行操作 410，其中接收认证令牌。如参考图 3 所描述的，成功认证的结果是接收到认证令牌。将该令牌传递给 web 服务 104 以提供认证证明。web 服务 104 评估该令牌并验证该令牌是有效的。

在某些实施例中，对令牌的验证涉及两个步骤。第一个步骤涉及公钥密码。如果 web 服务 104 能够使用认证服务 108 的公钥来解密令牌，则 web 服务 104

确定该令牌肯定是认证服务 108 发放的。第二个步骤包括判定认证服务 108 所作出的关于客户机 102 的声明是否满足一个或多个访问条件。

例如，为了使得能够访问特定受保护资源 106，web 服务 104 可能要求执行三个特定认证过程以便向认证服务 108 认证客户机 102。结果，web 服务 104 评估从客户机 102 接收到的令牌以验证该令牌包含认证服务 108 所作出的三个声明，从而断言客户机 102 已完成所有三个认证过程。在其他实施例中，可能需要任何数量的认证过程。在某些实施例中，所需认证过程的数量和类型与所做出的请求的类型相关。例如，涉及更高风险的请求通常将需要更严格的认证过程。

在某些实施例中，成功完成的认证过程的数量被称为认证级别。在某些实施例中，涉及受保护资源 106 的低风险操作只需要低认证级别，诸如一级或二级认证。在某些实施例中，高风险操作需要诸如三级认证和五级认证之间的高认证级别。单个受保护资源可取决于所作出的请求而与各个认证级别相关联。例如，从受保护资源中取得信息的请求在某些情形中可能只需要低认证级别，而从受保护资源中删除信息的请求可能需要中或高认证级别。在其他情形中，如果信息是敏感的或机密的，则从受保护资源中取得该信息的请求可能需要高认证级别。

在所示实施例中，如果未提供有效的认证证明或者如果所提供的认证被评估或确定为不足的，则执行操作 411 以拒绝对受保护资源的访问。在某些实施例中，向客户机 102 发送消息以将该拒绝通知给该客户机 102。在某些实施例中，该消息还包括关于如何获取适当的认证的信息，诸如将客户机 102 定向到认证服务 108。

在所示实施例中，如果提供认证证明并且该认证证明被验证为有效，则在操作 412 中执行所请求的操作。换言之，授权对受保护资源的访问。在某些实施例中，然后执行操作 414 以通知请求者请求已被处理。例如，web 服务 104 发送消息以通知客户机 102 对受保护资源的请求已被处理。在其他示例中，web 服务 104 通过向客户机 102 发送资源 106 的表示、通过对受保护资源 106 执行所请求的操作或通过向客户机 102 发送所请求的操作的结果来授权对该受保护资源的访问。

在所示实施例中，然后执行操作 416 以监视对其他消息的接收。例如，web 服务 104 监视来自客户机 102 的关于资源 106 的其他通信。如果客户机 102 发送对于资源 106 的其他消息，则方法 400 返回到操作 404 以便通过操作 404、406 和 408 来评估该新消息是否需要附加认证。尽管客户机此时可能已经进行了自我认证，但在动态环境中该客户机可能取决于它发送的消息和请求的类型而必须提供更强形式的认证，即多因素认证。如果再未接收到消息，则方法 400 结束。

图 5 是示出用于控制对受保护资源的访问的示例方法 500 的流程图。方法 500 涉及客户机 102、web 服务 104、认证服务 108 和受保护资源 106。尽管认证服务 108 被示为与 web 服务分开且不同的实体，但在某些实施例中，认证服务 108 和 web 服务 104 在同一计算系统上操作。在一个实施例中，受保护资源 106 位于 web 服务 104 上。在又一实施例中，受保护资源 106 位于另一 web 服务、服务器、计算机或其他计算系统上。在通信 512，客户机 102 提交对受保护资源 106 的请求。web 服务 104 接收该请求。在通信 514，web 服务 104 确定认证是必需的并且用指示为了能够处理该请求必须完成至少一个认证过程的故障来响应。在可能的实施例中，该故障可采取如简单对象访问协议（SOAP）1.2 规约中所定义的 SOAP 故障的形式。在其他实施例中，该故障可采取任何其他类型的数据通信协议的形式。在其他实施例中，来自 web 服务 104 的故障将包含诸如安全令牌服务端点等认证服务 108 的地址。

在通信 516，客户机 102 向认证服务 108 发送对安全令牌的请求以声明已完成必需的认证过程。在一个实施例中，该请求采取如 web 服务信任（WS-信任）规约所定义的 WS-信任请求安全令牌响应消息的形式。在其他实施例中，该请求可采取其他协议的形式。在通信 518，认证服务 108 用对身份确认的质询来响应客户机 102。在某些实施例中，该质询采取参考图 3 所描述的质询的形式。在通信 520，客户机 102 用身份确认来响应。在某些实施例中，该身份确认采取参考图 3 所描述的确认的形式。在通信 522，认证服务 108 用对身份确认的又一质询来响应客户机 102。在一个实施例中，该质询响应于失败的身份确认。在又一实施例中，该质询是执行多因素认证所必需的。在通信 524，客户机 102 用又一身份确认来响应认证服务 108。该过程可用通信 526 中的质

询和质询确认 528 来再次重复。尽管该组质询和确认被示为执行三次，但在其他实施例中，这些质询和响应通信重复任何次数。在认证服务 108 确认客户机 102 的身份后，认证服务 108 在通信 530 中向客户机 102 发放所请求的安全令牌。

在通信 532，客户机 102 连同该安全令牌一起重新提交对受保护资源的原始请求。web 服务 104 检查该请求以确保其与原始请求相同并验证该安全令牌以确保其有效。在通信 534，web 服务 104 处理客户机 102 所做出的请求。在某些实施例中，该处理涉及读取和/或更新受保护资源 106。在通信 536，将对受保护资源 106 的读取和/或更新的结果返回给 web 服务 104。在通信 538，web 服务 104 响应客户机 102 所做出的请求。

现在参考表 1：提供了认证质询架构，即用于指示需要消息专用认证过程来处理请求的数据结构。在某些实施例中，参考图 5 所描述的通信诸如在诸如 web 服务 104 等 web 服务确定对于认证发起请求的用户需要消息专用过程时以表 1 中所定义的数据结构的形式来传递。在一个实施例中，该服务将返回如 SOAP 1.2 规约中所定义的 SOAP 故障。在某些实施例中，与传统 SOAP 故障不同，用于指示需要消息专用认证协议的 SOAP 故障将包含上下文首部，该上下文首部包含 web 服务可用于取得原始请求以及被发现与该请求相关联的任何认证过程的细节的标识符。在另一实施例中，所返回的 SOAP 故障还将包含 Detail（细节）元素，该元素将表示代表其作出请求的用户的身份。这是将进一步认证的身份。在又一实施例中，该 Detail 元素还将或另选地提供诸如认证服务 108 等认证服务的地址，该认证服务可向用户发放安全令牌以确认该用户已成功完成与请求相关联的每一个认证过程。在某些实施例中，认证服务的地址与 web 服务的地址相同。在其他实施例中，认证服务的地址与 web 服务的地址不同。

表 1：认证质询架构

```
<?xml version='1.0' encoding='utf-8'?>
<xs:schema
  elementFormDefault='qualified'

targetNamespace='http://schemas.microsoft.com/2006/11/IdentityManag
ement'
```

```
    xmlns:xs='http://www.w3.org/2001/XMLSchema'
    xmlns:wsa=http://schemas.xmlsoap.org/ws/2004/08/addressing

  xmlns:idm='http://schemas.microsoft.com/2006/11/IdentityManagement
  '>
    <xs:import
      namespace='http://schemas.xmlsoap.org/ws/2004/08/addressing'/>
    <xs:complexType name='AuthenticationChallengeType'>
      <xs:sequence>
        <xs:element
        name='Challenge'
        nillable='true'
        minOccurs='0'>
          <xs:complexType>
            <xs:sequence>
              <xs:any
                minOccurs='0'
                processContents='lax' />
            </xs:sequence>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
    </xs:complexType>
    <xs:element
      name='AuthenticationChallenge'
      nillable='true'
      type='idm:AuthenticationChallengeType' />
  </xs:schema>
```

表 1 所示的架构包括 Challenge（质询）元素和 AuthenticationChallenge（认证质询）元素。该 Challenge 元素用于向客户机传送质询用户以使其提供所需认证数据所必需的信息。在某些实施例中，该客户机可以是 web 浏览器，该 web 浏览器将向用户显示质询数据，提示用户响应于该质询来提供数据。例如，Challenge 元素可指示客户机 102 显示提示用户输入口令的文本框。其他实施例将提示用户提供以下形式的认证：请求对安全问题的回答；请求 DNA 样本、指纹图案、视网膜图案或使用客户机的人的某一其他唯一标识符；请求诸如钥匙、安全卡、安全令牌、信用卡或对于使用客户机的人是唯一的某一其他对象等对象形式的验证，如参考图 3 所描述的。在可能的实施例中，该认证质询架构将包括用作该架构的包装器的 AuthenticationChallenge 元素。

现在参考表 2：提供了认证质询响应架构，即用于响应认证质询的数据结

构。诸如认证服务 108 等认证服务向用户发出质询以认证信息。在某些实施例中，质询根据 WS-信任规约的 10 节中所定义的质询框架来作出。如果认证服务需要附加信息来认证用户的身份，则它将用如 WS-信任规约所定义的响应来响应对安全令牌的请求。

表 2：认证质询响应架构

```
<?xml version='1.0' encoding='utf-8'?>
<xs:schema
  elementFormDefault='qualified'

targetNamespace='http://schemas.microsoft.com/2006/11/IdentityManag
ement'
  xmlns:xs='http://www.w3.org/2001/XMLSchema'
  xmlns:wsa=http://schemas.xmlsoap.org/ws/2004/08/addressing

xmlns:idm='http://schemas.microsoft.com/2006/11/IdentityManagement
'>
  <xs:import
    namespace='http://schemas.xmlsoap.org/ws/2004/08/addressing'/>
  <xs:complexType name='AuthenticationChallengeResponseType'>
    <xs:sequence>
      <xs:element
      name='Response'
      nillable='true'
      minOccurs='0'>
        <xs:complexType>
          <xs:sequence>
            <xs:any
              minOccurs='0'
              processContents='lax' />
          </xs:sequence>
        </xs:complexType>
      </xs:element>
    </xs:sequence>
  </xs:complexType>
  <xs:element
    name='AuthenticationChallengeResponse'
    nillable='true'
    type='idm:AuthenticationChallengeResponseType' />
</xs:schema>
```

该认证质询响应架构包括 Response（响应）元素和 AuthenticationChallengeResponse（认证质询响应）元素。该 Response 元素向

认证服务标识来自客户机的所需认证信息。该信息由认证服务例如用来确定应向客户机发送什么质询以认证该客户机。该 AuthenticationChallengeResponse 元素用作该架构的包装器。

图 6 是用于实现本发明的各方面的示例性计算系统 600 的框图。在一个实施例中，计算系统 600 是客户机 102。在另一个实施例中，计算系统 600 是 web 服务 104。在另一个实施例中，计算系统 600 是认证服务 108。在其最基本的配置中，计算系统 600 通常包括至少一个处理单元 602 和存储器 604。取决于计算系统系统的确切配置和类型，存储器 604 可以是易失性的（诸如 RAM）、非易失性的（诸如 ROM、闪存等）或是两者的某种组合。该最基本配置在图 6 中由虚线 606 来例示。另外，计算系统 600 还可具有附加特征/功能。例如，计算机系统 600 还可包含附加存储（可移动和/或不可移动），包括但不限于磁盘、光盘或磁带。这些其他存储在图 6 中由可移动存储 608 和不可移动存储 610 示出。计算机存储介质包括以用于存储诸如计算机可读指令、数据结构、程序模块或其它数据等信息的任何方法或技术来实现的易失性和非易失性、可移动和不可移动介质。存储器 604、可移动存储 608 和不可移动存储 610 都是计算机存储介质的示例。计算机存储介质包括，但不限于，RAM、ROM、EEPROM、闪存或其它存储器技术、CD-ROM、数字多功能盘（DVD）或其它光盘存储、磁带盒、磁带、磁盘存储或其它磁性存储设备、或能用于存储所需信息且可以由计算系统 600 访问的任何其它介质。任何这样的计算机存储介质都可以是计算系统 600 的一部分。

计算系统 600 还可包含允许该计算系统与其它设备进行通信的通信连接 612。通信连接 612 是通信介质的一个示例。通信介质通常以诸如载波或其它传输机制等已调制数据信号来体现计算机可读指令、数据结构、程序模块或其它数据，并包括任意信息传送介质。术语“已调制数据信号”指的是其一个或多个特征以在信号中编码信息的方式被设定或更改的信号。作为示例而非限制，通信介质包括有线介质，诸如有线网络或直接线连接，以及无线介质，诸如声学、RF、红外线和其它无线介质。如此处所使用的术语计算机可读介质包括存储介质和通信介质两者。

计算系统 600 还可具有输入设备 614，诸如键盘、鼠标、笔、语音输入设

备、触摸输入设备等。在某些实施例中，输入设备还（或另选地）包括例如，生物测定标识符、传感器、检测器、读卡器等。还可包括输出设备 616，如显示器、扬声器、打印机等。所有这些装置在本领域中都是众所周知的，因此不必在此详细讨论。

在某些实施例中，存储器 604 包括操作系统 620、应用程序 622、其他程序模块 624 和程序数据 626 中的一个或多个。在某些实施例中，全局数据、客户机专用数据和变换规则各自可被存储在存储器 604、可移动存储 608 和不可移动存储 610 或此处所描述的任何其他计算机存储介质中。

虽然已经用对结构特征、方法动作和包含这些动作的计算机可读介质专用的语言描述了各实施例，但是应该理解，如在所附权利要求中定义的可能的实施例不必限于所描述的具体结构、动作、或介质。 本领域技术人员将认识到本发明精神和范围中的其它实施例或改进。因此，这些具体结构、动作、或介质仅作为说明性实施例而公开。

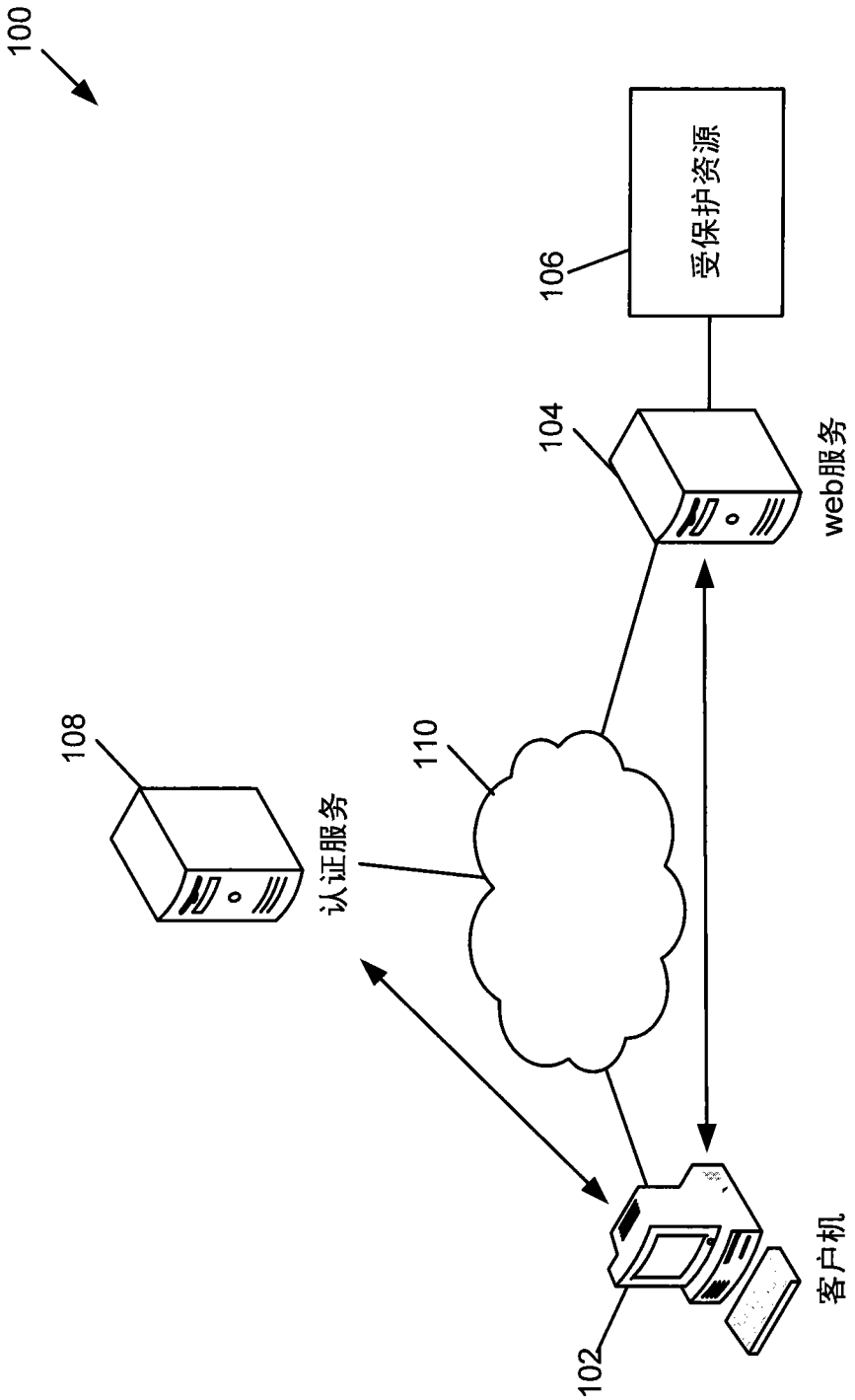


图 1

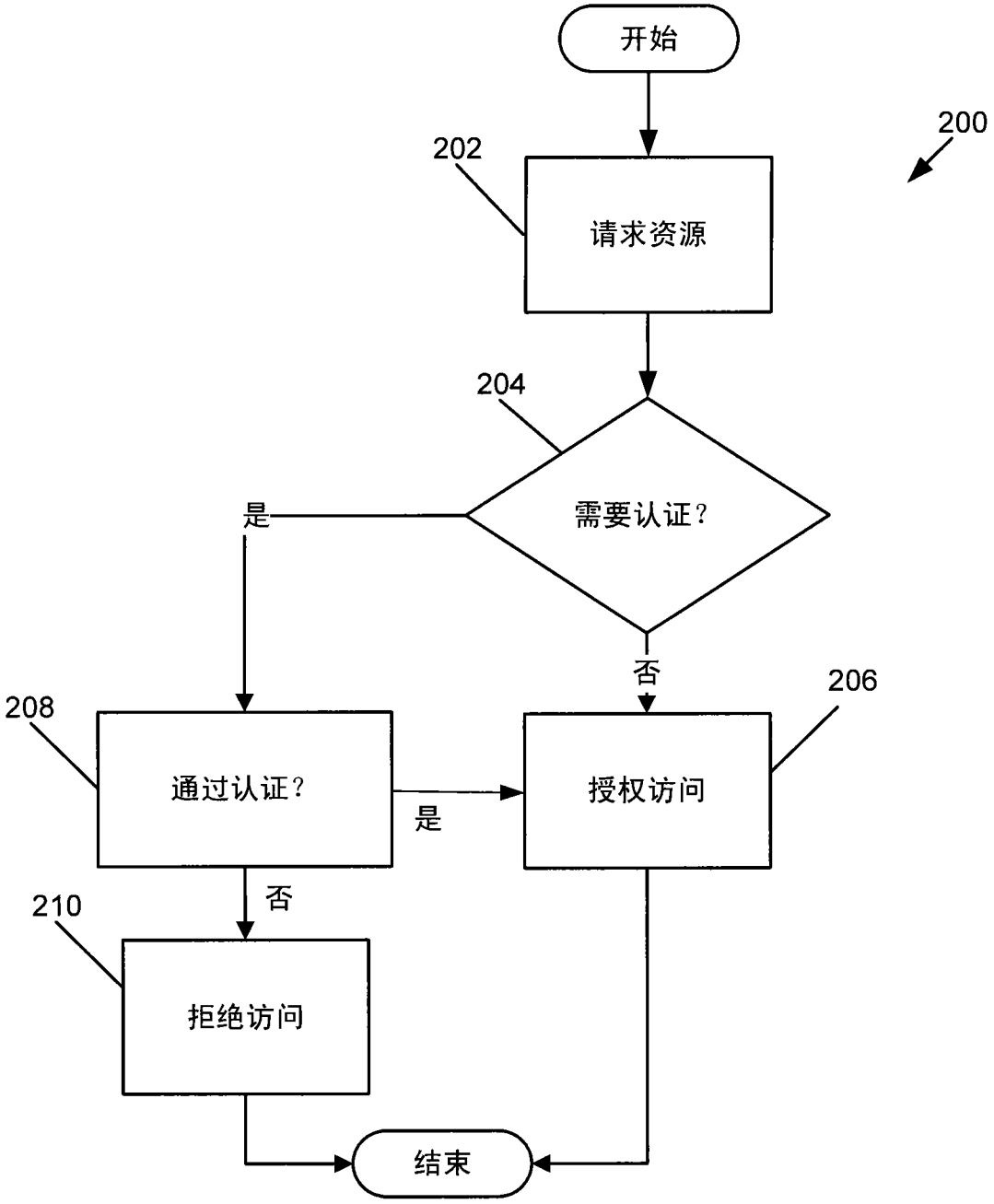


图 2

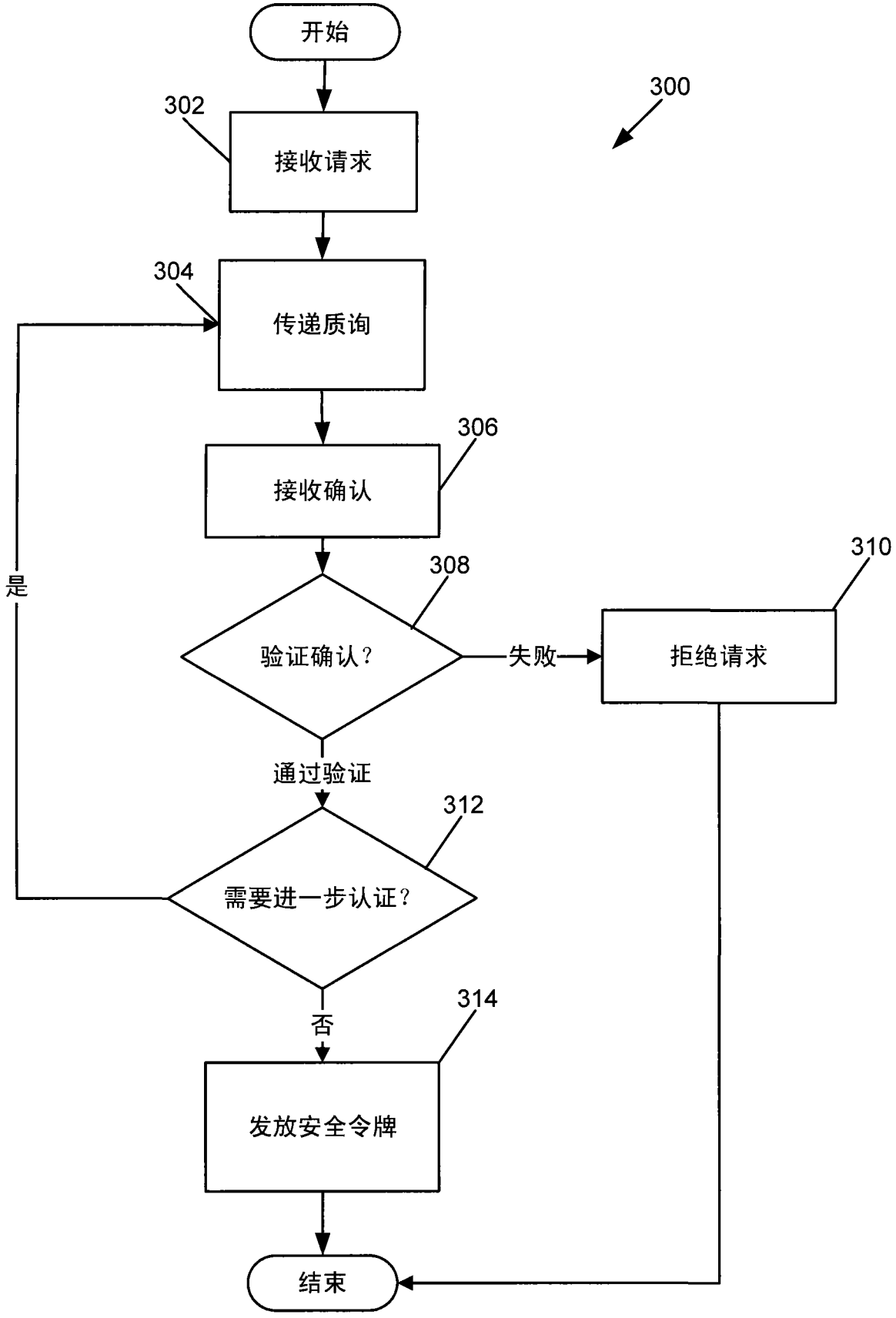

开始
300
302
接收请求
304
传递质询
306
接收确认
308
验证确认？
失败
310
拒绝请求
是
通过验证
312
需要进一步认证？
否
314
发放安全令牌
结束

图 3

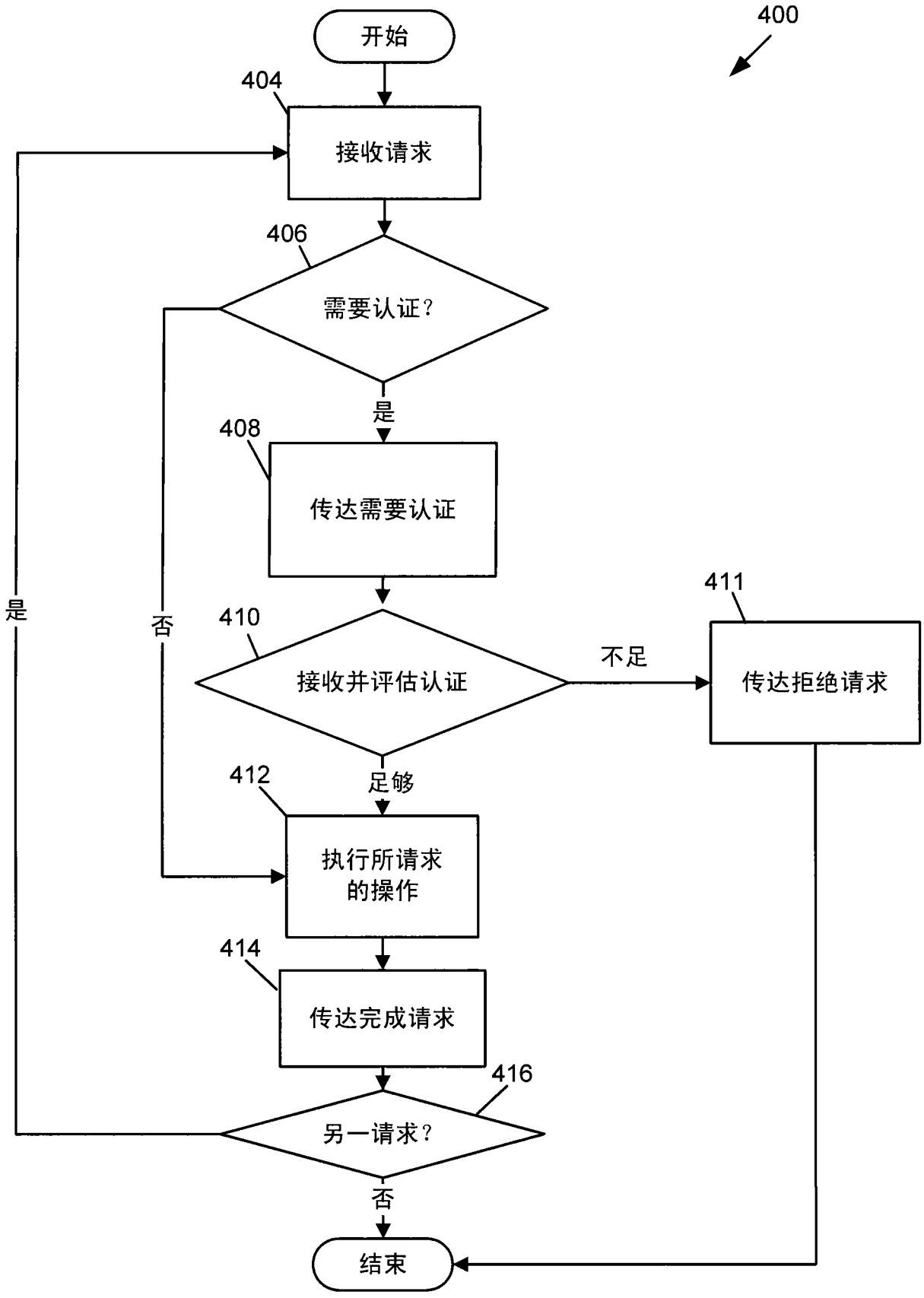

400
开始
404
接收请求
406
需要认证？
是
否
408
传达需要认证
410
接收并评估认证
不足
411
传达拒绝请求
足够
412
执行所请求的操作
414
传达完成请求
416
另一请求？
是
否
结束

图 4

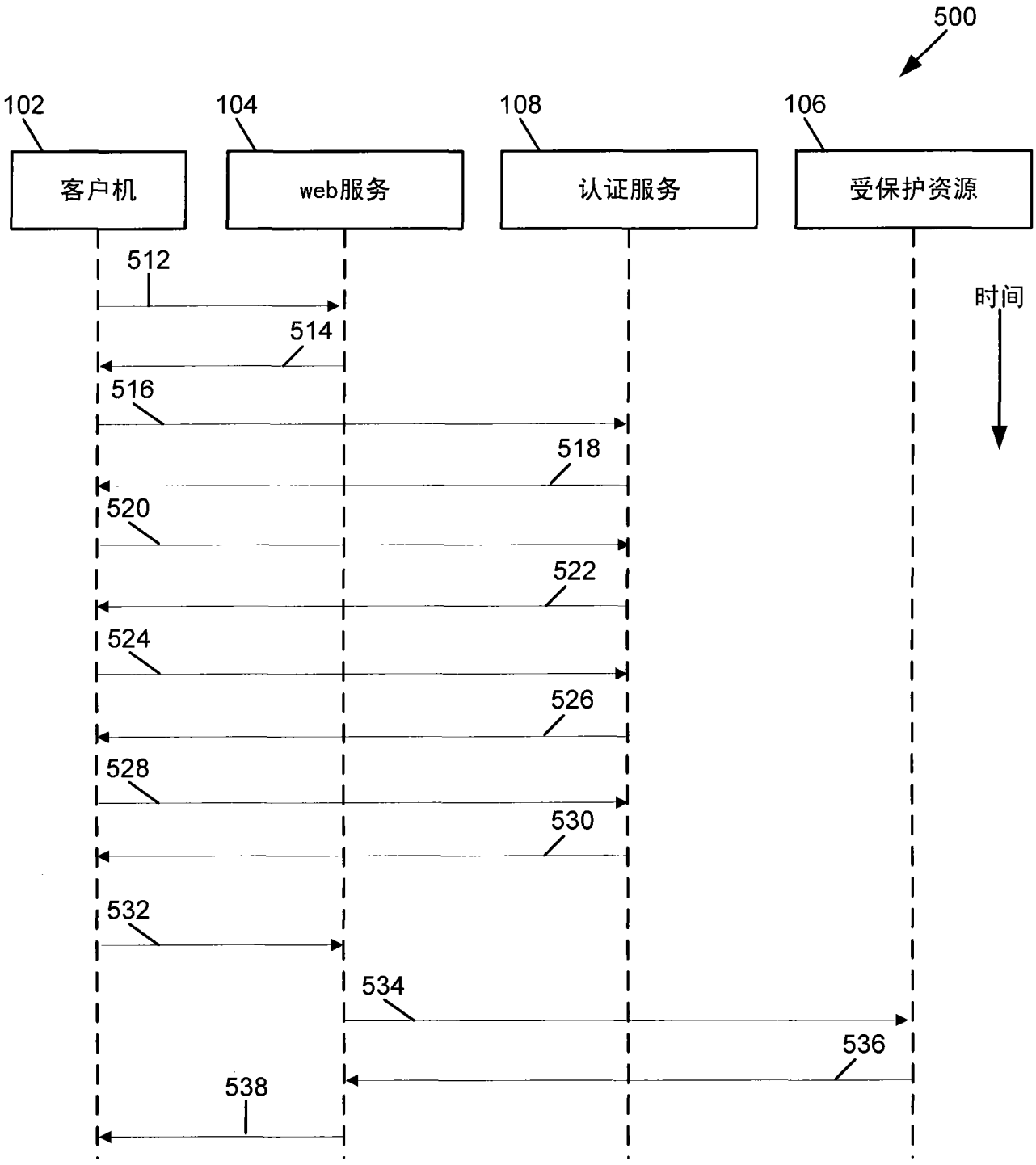

500
102
104
108
106
客户机
web服务
认证服务
受保护资源
时间
512
514
516
518
520
522
524
526
528
530
532
534
536
538

图 5

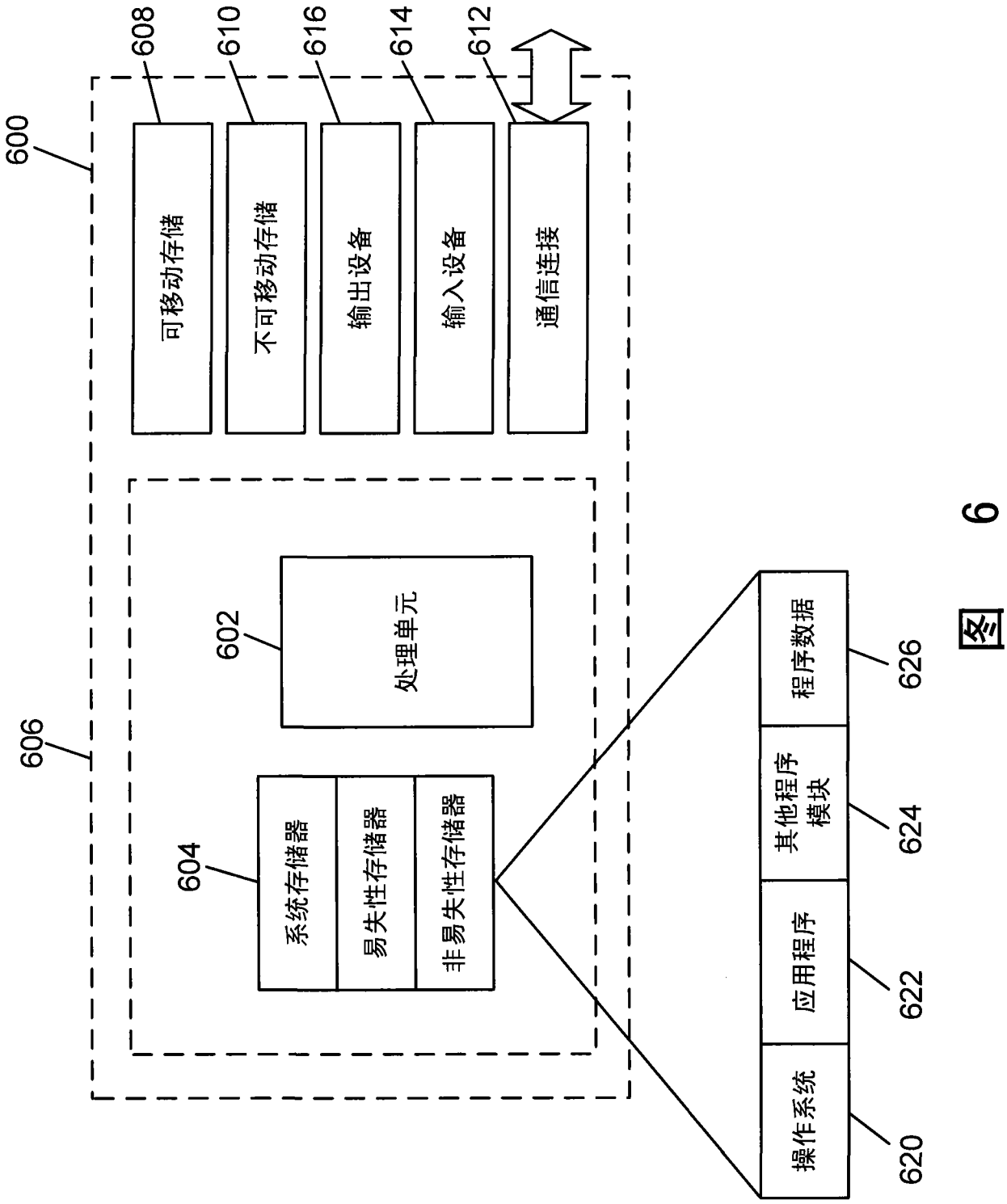

600
608
610
616
614
612
可移动存储
不可移动存储
输出设备
输入设备
通信连接
606
602
处理单元
604
系统存储器
易失性存储器
非易失性存储器
626
程序数据
624
其他程序模块
622
应用程序
620
操作系统

图 6