(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 101785243 A
(43)申请公布日 2010.07.21

(21)申请号 200880105206.3
(22)申请日 2008.08.17
(30)优先权数据
11/848,464 2007.08.31 US
(85)PCT申请进入国家阶段日
2010.02.25
(86)PCT申请的申请数据
PCT/US2008/073411 2008.08.17
(87)PCT申请的公布数据
WO2009/032511 EN 2009.03.12
(71)申请人 微软公司
地址 美国华盛顿州
(72)发明人 R·L·迪金森 E·A·马丁内斯
D·J·普赞 J·S·格里沃
M·J·奥特
(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 张政权 钱静芳
(51)Int.Cl.
H04L 9/32(2006.01)

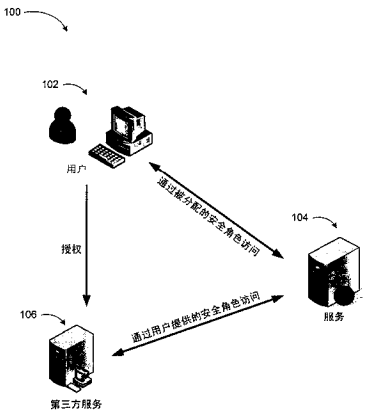
权利要求书 2 页 说明书 8 页 附图 9 页

(54)发明名称

可传递受限安全令牌

(57)摘要

在基于web的服务环境中,第三方提供者为其补充服务需要具有对用户数据的不同程度的访问权。为防止第三方提供者具有比所需更宽泛的访问权或不足的访问级别,采用可传递受限安全权证来确定用于第三方的访问的合适级别。具有有效期和限制角色的权证定义用于第三方的访问的有效期和级别。通过使系统中定义的授权用户的安全角色和限制角色相交来确定限制。



CN 101785243 A

1. 一种用于安全地处理对基于web的服务环境(104)中的用户数据的第三方访问请求的至少部分在计算设备(800)中执行的方法,所述方法包括:

从第三方提供者(106)处接收(902)访问请求,其中所述请求与补充基于web的服务的进程的子进程相关联;

从所述请求提取(904)权证(218)和声明,其中所述权证(218)包括有效期参数和限制角色(324,326);

验证(908)所述权证(218)未过期;

加载(910)与所述权证(218)相关联的至少一个用户角色(322);

基于使所述限制角色(324,326)与所述至少一个用户角色(322)相交来确定(912,914)用于所述请求的访问限制;以及

基于所述被确定的访问限制来允许(916)所述第三方访问所述用户数据。

2. 如权利要求1所述的方法,其特征在于,所述权证(218)与所述第三方提供者(106)的域名相关联。

3. 如权利要求1所述的方法,其特征在于,还包括:

在确定所述访问限制之前认证(906)所述权证(218)。

4. 如权利要求3所述的方法,其特征在于,采用数字签名来认证所述权证(218)。

5. 如权利要求4所述的方法,其特征在于,使用所述数字签名来验证所述声明。

6. 如权利要求3所述的方法,其特征在于,采用散列消息认证码(HMAC)来认证所述权证(218)。

7. 如权利要求6所述的方法,其特征在于,所述权证(218)还包括密钥指示符和组织标识符中的至少一个。

8. 如权利要求6所述的方法,其特征在于,还包括:

通过将一位添加到所述权证(218)的所述HMAC部分来将所述权证(218)限制于具体动作。

9. 如权利要求1所述的方法,其特征在于,所述权证(218)还包括定义可使用所述权证(218)多少次来访问所述用户数据的重复参数。

10. 如权利要求1所述的方法,其特征在于,使所述限制角色(324、326)与所述至少一个用户角色(322)相交(914)包括选择在所述角色中定义的限制中较严格的一个。

11. 如权利要求1所述的方法,其特征在于,还包括:

应用除选择在所述角色中定义的限制中较严格的一个之外的预定义规则。

12. 一种用于安全地处理对基于web的CRM服务环境中的用户数据的第三方访问请求的系统,包括:

至少一个CRM web服务器(772),其被配置成:

从第三方提供者(106)处接收(902)访问请求,其中所述请求与补充基于web的CRM服务的进程的子进程相关联;

从所述请求中提取(904)权证(218),其中所述权证(218)与所述第三方提供者(106)的域名相关联并包括有效期参数和限制参数;

验证(908)所述权证(218)未过期;

基于所述限制参数确定(910,912,914)用于所述请求的访问限制,其中所述访问限制

与正为其执行所述子进程的用户 (102) 的访问限制不同 ;以及

基于所述被确定的访问限制来允许 (916) 所述第三方访问所述用户数据。

13. 如权利要求 12 所述的系统,其特征在于,所述至少一个 CRM web 服务器 (772) 还被配置成 :

基于所述限制参数创建具有相关联的限制角色 (324、326) 的受限用户 / 域 ;以及

基于使所述相关联的限制角色 (324、326) 与用户角色 (322) 相交 (914) 来确定所述访问限制。

14. 如权利要求 12 所述的系统,其特征在于,所述至少一个 CRM web 服务器 (772) 还被配置成 :

从所述权证 (218) 中检索限制角色 (324、326) 的列表 ;

加载与所述子进程相关联的用户角色 (322) ;以及

基于使所述限制角色 (324、326) 与所述被加载的用户角色 (322) 相交 (914) 来确定所述访问限制。

15. 如权利要求 14 所述的系统,其特征在于,每一限制角色 (324、326) 和所述用户角色 (322) 包括定义对所述用户数据的访问许可级别的特权深度,且通过选择所述相交角色的特权深度中较严格的一个来确定所述访问限制。

16. 如权利要求 12 所述的系统,其特征在于,所述 CRM web 服务器 (772) 还被配置成提供用于配置所述限制角色 (324、326) 和所述用户角色 (322) 的所述特权深度的图形用户界面 (GUI)。

17. 如权利要求 12 所述的系统,其特征在于,基于所述基于 web 的 CRM 服务的客户组织的分层结构来定义被分配到与所述子进程相关联的用户角色 (322) 的至少一个限制。

18. 一种其上存储有用于安全地处理对基于 web 的服务环境 (104) 中的用户数据的第三方访问请求的指令的计算机可读存储介质,所述指令包括 :

从第三方提供者 (106) 处接收 (902) 访问请求,其中所述请求与补充基于 web 的服务的进程的子进程相关联 ;

从所述请求中提取 (904) 权证 (218) 和声明,其中所述权证 (218) 与所述第三方提供者 (106) 的域名相关联并包括有效期参数、限制角色 (324、326)、以及重复参数 ;

在确定所述访问限制之前认证 (906) 所述权证 (218)

验证 (908) 所述权证 (218) 未过期 ;

加载 (910) 与所述权证 (218) 相关联的至少一个用户角色 (322)

基于使所述限制角色 (324,326) 与所述至少一个用户角色 (322) 相交来确定 (914) 用于所述请求的访问限制 ;

基于所述被确定的访问限制来允许 (916) 所述第三方访问所述用户数据。

19. 如权利要求 18 所述的计算机可读存储介质,其特征在于,确定 (914) 所述限制角色 (324、326) 和所述至少一个用户角色 (322) 包括选择在所述角色中定义的限制中较严格的一个并应用预定义规则。

20. 如权利要求 18 所述的计算机可读存储介质,其特征在于,所述访问包括下组中的至少一个 :创建新记录、删除现存记录、修改现存记录、更新现存记录、检索与执行所述子进程相关联的操作参数、以及修改与所述用户数据相关联的模式。

可传递受限安全令牌

[0001] 背景

[0002] 基于 web 的服务包括服务提供者、其用户、以及可提供诸如用于提供指定服务的集成内容等补充服务的第三方之间的交互。此类集成内容可采取嵌入框架、表单、或脚本的形式。例如，商业记录服务可基于其用户的商业联系人为该用户执行各种进程（例如，历史数据收集、统计数据分析、事件的调度等）。换言之，用户和 / 或服务提供者指定的第三方可执行补充所提供的服务的子进程，如基于记录上的地址为商业联系人提供地图。

[0003] 客户关系管理 (CRM) 解决方案是提供通常在被主存的计算机应用程序环境中创建并维护从第一次联系到购买和售后的客户的清楚写照所需的工具和能力的基于 web 的商业服务的示例。对复杂组织而言，CRM 系统可提供帮助改善销售和营销组织瞄准新客户、管理营销活动、以及推动销售活动的方式的特征和能力。CRM 系统可包括由组织内部或外部的用户以及第三方提供者独立或以共享方式利用的许多硬件和软件的组件。

[0004] 为执行子进程，第三方通常需要具有对服务提供者处的用户记录的访问权。在以上示例中，第三方将需要访问商业联系人的地址以生成地图并将其集成到服务提供者的网页中。给出对用户数据用于读取、修改、创建、并删除该数据的访问权可带来安全挑战，尤其在第三方提供者不是可信实体时。

[0005] 概述

[0006] 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。该概述并非旨在标识所要求保护的主题的关键特征或必要特征，也不旨在用于帮助确定所要求保护的主题的范围。

[0007] 各实施例涉及通过采用可传递受限安全令牌来控制第三方提供者对用户数据的访问而提供基于 web 的服务提供者处的用户记录的增强安全性。生成具有除被分配给用户的那些安全限制之外的安全限制以及权证有效期的权证形式的可传递受限安全令牌。

[0008] 通过阅读以下详细描述并查阅相关联的附图，这些和其它特征和优点将是显而易见的。可以理解，前述一般描述和以下详细描述均仅是说明性的，且不限制所要求保护的各方面。

[0009] 附图简述

[0010] 图 1 是示出基于 web 的服务的用户、服务提供者、以及第三方提供者之间的典型数据访问交互的图示；

[0011] 图 2 示出根据实施例基于 web 的服务的用户、服务提供者、以及第三方提供者之间的示例交互；

[0012] 图 3 是示出用户和限制角色在确定要被分配给基于 web 的服务的第三方提供者的安全限制中的使用的概念图；

[0013] 图 4 是用于将访问限制分配给基于 web 的服务的用户的软件程序的屏幕截图；

[0014] 图 5 是用于将访问限制分配给基于 web 的服务的第三方提供者的软件程序的屏幕截图；

[0015] 图 6 示出根据实施例的三个示例受限安全权证；

[0016] 图 7 是其中可以实现各实施例的示例联网环境的图示；

[0017] 图 8 是其中可以实现各实施例的示例计算操作环境的框图；以及

[0018] 图 9 示出使用用于允许由基于 web 的服务中的第三方提供者访问用户数据的受限安全权证的过程的逻辑流程图。

[0019] 详细描述

[0020] 如上简述，可通过使用用于允许第三方提供者对数据的访问的受限安全权证来增强基于 web 的服务中的用户数据安全。在以下详细描述中，参考了构成其一部分并作为说明示出了各具体实施例或示例的附图。可组合这些方面，可利用其它方面并且可以做出结构上的改变而不背离本发明的范围。由此，以下详细描述并不旨在限制，本发明的范围由所附权利要求及其等效方案所定义。

[0021] 虽然在结合在个人计算机上的操作系统上运行的应用程序执行的程序模块的一般上下文环境中描述了各实施例，但是本领域的技术人员会认识到各方面也可以结合其它程序模块实现。

[0022] 一般而言，程序模块包括执行特定任务或实现特定的抽象数据类型的例程、程序、组件、数据结构和其它类型的结构。而且，如本领域的技术人员理解的，各实施例可以用其它计算机系统配置来实施，包括手持式设备、多处理器系统、基于微处理器或可编程消费者电子产品、小型机、大型机等等。各实施例还能在其中任务由通过通信网络链接的远程处理设备来执行的分布式计算环境中实现。在分布式计算环境中，程序模块可以位于本地和远程存储器存储设备中。

[0023] 各实施例可被实现为计算机过程（方法）、计算系统、或者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了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。计算机程序产品还可以是计算系统可读并编码了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。

[0024] 参考图 1，示出基于 web 的服务的用户、服务提供者、以及第三方提供者之间的典型数据访问交互的图示。

[0025] 如前所述，第三方提供者可为服务的用户执行该服务的 web 服务补充进程内内的子进程。之前所述的一个示例是第三方为处理用户的联系人的基于 web 的服务提供联系人的地图。另一示例是用于计算 CRM 系统内的信用得分的第三方服务。可定制 CRM 联系人表单以执行调用第三方的脚本，以传递联系人标识符。第三方可随后回调 CRM 服务以检索各种联系人和定单信息以计算所选联系人的信用得分。第三方可返回可在联系人表单的字段中显示的信用评级分数。第三方还可直接使用其它有用的统计数据来更新联系人记录。

[0026] 因此，第三方提供者可能需要具有对基于 web 的系统内的用户数据的访问权以进行收集、修改、删除、或创建操作。适应此类第三方操作中的挑战包括如何控制要对这些操作允许哪些第三方、以哪种许可级别、持续时间多长等。

[0027] 在常规的基于 web 的服务环境中，如图 1 的图示 100 所示，每一用户 102 在基于 web 的服务 104 内可具有被分配的安全角色并按该角色所允许地访问该服务。用户 102 可通过例如向第三方服务 106 提供其安全权证在某一点处授权第三方服务 106 执行操作。在此情况下，第三方服务 106 将如用户 102 的安全角色所允许地对与用户 102 相关联的数据具有完全访问权并执行其操作。此类设置的缺点是用户可能不想要第三方对用户本身拥有

的全部数据具有完全访问能力。

[0028] 进一步复杂化此问题的是，组织可能具有多个具有不同安全角色的内部用户。如果其中之一要授权第三方，该用户的安全角色可能不足以执行所需的操作或相反，该安全角色可能比所需的更宽泛。例如，公司的接待员可能具有诸如“读取”仅商业联系人信息的受限访问权。如果该接待员尝试激活用于计算信用分数的第三方服务，则该第三方可能由于接待员的受限安全角色而不能更新 web 服务处的数据。

[0029] 另一方面，具有宽泛的访问特权的高层经理可能希望激活用于商业联系人的地图服务，这通常将需要用于第三方的受限访问特权。然而，因为经理具有宽泛的访问特权，所以无论是否需要，第三方都将通过经理的安全权证取得相同的特权。

[0030] 控制第三方对用户数据的访问的另一方法可以是向第三方服务提供者分配 web 服务处的受限安全角色，但这可能严重限制了基于 web 的服务允许用户使用他们选择的第三方服务的灵活性，使得用户服务的定制成为非常有挑战性的任务。

[0031] 图 2 示出根据实施例基于 web 的服务的用户、服务提供者、以及第三方提供者之间的示例交互。

[0032] 如上所述，对基于 web 的服务提供者的挑战是如何控制允许哪些第三方回调服务、采用哪种许可级别、以及精确的持续时间。例如，如果服务管理者正在查看 CRM 服务中的联系人表单，向半受信第三方传递连接用户的整个安全上下文可意味着第三方现在可访问超出其执行预期服务真正需要的记录。可授权管理员删除任何类型的记录、创建任何类型的记录、或使得方案改变（例如，创建新实体、属性等）。向被期望仅提供指定服务的狭小集合的半受信第三方传递连接用户的整个安全上下文可能导致严重的风险。

[0033] 根据一实施例，可为第三方提供者生成权证。该权证可指定附加的安全限制和权证有效期。可使用基于 web 的服务角色基础结构来定义附加安全限制。可随后将第三方提供者的特定域名与限制角色相关联。例如，可为第三方域“http://accuratecreditinfo.com”定义限制角色以给出 :[本地范围的活动读取许可]+[当前商业单位的范围的引导创建和读取许可]。然而，万一连接用户不具有创建引导的许可，可通过使连接用户（及其角色）的许可与由限制角色定义的许可相交来评估安全性以确保不存在提升。限制角色还可指定当前商业单位的范围。

[0034] 在图示 200 中，基于 web 的服务由服务器 204 表示，其为用户 202 执行用户指定进程 210。可采用权证验证进程 (208) 认证用户并确定其访问特权。可将认证信息包括在权证中。在根据实施例的服务中，第三方服务 206 可执行子进程 212 以补充用户指定进程 210。为访问基于 web 的服务处的用户数据和定单，第三方服务 206 可向基于 web 服务 204 提供受限安全权证 218。第三方服务 206 还可与其它系统 214 交互。

[0035] 受限安全权证 218 还可由基于 web 的服务认证。该认证可通过众多方式执行。一个此类方法是散列消息认证码 (HMAC)。基于包括在消息（在此情况中是权证）中的密钥生成一“MAC 标签”，以使得攻击者难以生成有效配对（消息，标签）。

[0036] 代替 HMAC，还可根据其它实施例使用数字签名。使用数字签名，组件可验证声明，但可能不具有生成有效权证的能力（仅验证密钥可为其使用）。使用 HMAC，组件可验证声明，但随后还具有创建有效权证的能力，因为它们具有对所需对称密钥的访问权。使用数字签名对允许进一步委托是有用的。例如，第三方可向其它第三方传递基于 web 的服务权证，

这可在采取某些行动之前验证对基于 web 的服务的访问权。还可使用此处所述的原理来采用其它认证方法。

[0037] 因此，示例权证是如下形式的：{用户标识 + 有效期 + 受限角色标识 +HMAC(用户标识 + 有效期 + 受限角色标识)}。权证还可包括密钥指示符（以知道使用哪个密钥，如果使用各自在一定时间之后过期的旋转密钥）以及组织标识 (Id)(以防止其中可重用相同用户标识的交叉组织攻击)。

[0038] 根据另一实施例，可允许基于 web 的服务管理员指定应该将权证限制于诸如只读动作等具体动作。这可通过例如向权证的 HMAC 添加一位并随后阻塞平台中的写动作来达成。

[0039] 根据其它实施例，可在系统中创建受限用户 / 域而不是将受限角色的列表包括在权证中。受限用户 / 域可具有与它们相关联的角色且这些角色可被用作受限角色。可如上所述确定用户角色和受限角色的相交。在此场景中，权证可以是以下形式的：{用户标识 + 有效期 + 受限用户标识 +HMAC(用户标识 + 有效期 + 受限用户标识)}。

[0040] 在其中受限权证包含角色列表的版本中，关联到域的角色可能改变了，但是安全限制是基于权证中的角色组的，虽然可独立改变角色中的特权。在受限用户 / 域方式中，服务器维护受限角色的控制。因此，可独立于已经授予的权证来添加 / 改变 / 移除仅具有受限域 / 用户的版本中的角色。

[0041] 虽然根据具有动态地重新评估可能改变的用户特权且不处理从未由第三方使用的权证（节省系统资源）的一个实施例可在权证从 web 服务（例如，CRM) 服务返回时执行特权相交，但是使用此处所述的原理还可在权证被第一次发放时执行同样的相交。

[0042] 图 3 是示出用户和限制角色在确定要被分配给基于 web 的服务的第三方提供者的安全限制中的使用的概念图。

[0043] 在基于角色的访问特权系统中，可基于用户与记录的关系定义不同层次的特权深度。例如，可为由用户拥有的记录定义“基本”深度；可为用户所属的商业单位的记录定义“本地”深度；可为用户的商业单位或任何子商业单位的记录定义“深”深度；以及可为伞状组织的任何商业单位中的记录定义“全局”深度。

[0044] 基于这些示例特权深度，可向用户分配定义如下的单个角色：具有基本深度的“读活动”；具有深深度的“写引导”；以及具有深深度的“创建联系人”。可向第三方提供者分配定义如下的单个角色：具有本地深度的“写引导”以及具有全局深度的“创建联系人”。

[0045] 在根据各实施例的服务中，这些角色（例如，用户角色 322 与限制角色 324 和限制角色 326 的）的相交 320 将得到具有本地深度的“写引导”角色以及具有深深度的“创建联系人”角色（在每一情况下选择深度中较小的一个）。

[0046] 以上的限制角色、特权深度、以及相交场景仅为说明性目的提供且不构成对各实施例的限制。可使用任何定义的特权深度、组织结构、以及限制角色来实现各实施例。此外，可定义确定用户角色和限制角色除两者中较小的一个之外的相交的其它规则。此外，在此处将 CRM 服务用作示例的基于 web 的服务。使用此处所述的原理，可使用任何应用程序安全限制来实现各实施例。

[0047] 图 4 是用于将访问限制分配给基于 web 的服务的用户的软件程序的屏幕截图 (400)。

[0048] 如上所述，可向组织的每一用户分配安全角色以及各种访问许可级别。例如，如屏幕截图所示，web 服务程序的访问管理模块可允许管理者定义每一用户的安全角色。为接待员创建示例角色 (432)。诸如帐户、联系人、电子邮件模板等不同类型的记录在一列中列出 (434)。将诸如创建、读、写、删除等访问操作 (438) 列在对应列中，以允许管理员为矩阵中的每一类型的记录上的每一操作设置许可级别 (430)。

[0049] 可设置用户界面使得为选项表所示为组织子划分而对记录分组 (436)。安全角色可由用户分配并被传送到基于 web 的服务、由用户在由基于 web 的服务生成的默认角色的模板上修改、或由用户以基于 web 的服务的管理程序的配置模式分配。

[0050] 图 5 是用于将访问限制分配给基于 web 的服务的第三方提供者的软件程序的屏幕截图。第三方提供者可执行补充该基于 web 的服务的各种任务。屏幕截图 500 中示出的示例进程是联系人分析。

[0051] 屏幕截图 500 中的配置用户界面类似于图 4 的用户界面，其中记录类型 (544) 被列为矩阵中的第一列，访问类型被列为第一行 (548)。将每一记录类型和访问类型的访问限制显示为用户界面矩阵 540 的元素。重要的是，根据各实施例的用户界面包括用于启用伙伴访问限制的控制，伙伴由与第三方提供者相关联的 URL 定义。

[0052] 此外，还可基于组织分层结构来确定限制。例如，可基于第三方服务是为个别用户执行、为商业单位执行、为商业子单位执行、或为整个组织执行来定义限制角色。

[0053] 图 6 示出根据实施例的三个示例受限安全权证。根据各实施例的受限安全权证可包括除在图中示出的那些以外的元素。有效期和限制也不限于所示示例。

[0054] 如上所述，第三方的角色限制可与基于 web 的服务中的具体域名相关联。第一示例权证 652 与域名 http://accuratecreditinfo.com（虚构域名）相关联。该权证具有 60 秒的有效期以及仅联系人分析角色的限制。因此，一旦接受权证 652，被分配该权证的第三方就具有 60 秒来执行其进程，且其仅可为执行联系人分析来访问基于 web 的服务处的用户数据。

[0055] 第二权证 654 与域名 http://productimages.com 相关联，该域名可以是用于处理具体企业的产品图像的第三方提供者服务。该权证具有 10 秒的有效期且限制是受限产品访问角色。可在基于 web 的服务的访问管理部分中定义此角色。除有效期和限制之外，权证 654 可任选地包括重复参数。重复参数可基于重复参数的值来允许第三方提供者重复地使用其安全权证。在图 6 的示例中，将重复参数设置为“否”以表示该权证是单次使用权证。

[0056] 示例权证 656 与域名 http://analyzeleads.com 相关联，该域名可提供 CRM 服务的业务引导的分析。权证的有效期被设置为 60 分钟而限制是“读所有引导”。因此，具有此权证的第三方可读取 CRM 服务中的所有业务引导数据，但不执行任何其它访问操作。在此情况下将可任选的重复参数设置为 10 次，以表示第三方提供者可使用相同权证至多十次以访问用户数据。

[0057] 根据某些实施例，可按其它方式实现时间戳有效期，诸如代替定义有效时间期限范围的有效期期限（日期和时间）。此外，可将更复杂的表达式包括在权证中以表达相对更为灵活的限制。例如，可使用类似 &（时间．小时＜ 8)（用户．开始于（“a*”)（用户．角色．包括 (CEO)) 的表达式来提供时间有效期、用户标识（或名称）类别、以及用户角色。

[0058] 根据一个实施例，可向第三方提供在将权证移交给另一第三方之前进一步限制该

权证的能力。因此，如果一个第三方需要使用来自另一第三方的某些服务，则它们可选择创建进一步受限的令牌（或该服务可这样做）以使得权证包括多个受限用户标识、或源自超过一个域的受限角色标识。

[0059] 出于说明的目的，在图 2、4、5、以及 6 中所述的示例系统、服务、权证、以及操作是示例性的。使用此处所述的原理，可使用额外或较少的组件和元件来实现在基于 web 的服务环境中提供可传递受限安全权证的系统。

[0060] 图 7 是其中可以实现各实施例的示例联网环境。可在多个物理和虚拟的客户机和服务器上以分布式方式实现提供第三方提供者的受限安全令牌的基于 web 的服务。该服务还可以在非群集系统或利用通过一个或多个网络（例如，网络 770）通信的多个节点的群集系统中实现。

[0061] 这种系统可以包括服务器、客户机、因特网服务提供者、以及通信介质的任何拓扑结构。同样，系统可以具有静态或动态拓扑结构。术语“客户机”可以表示客户机应用程序或客户机设备。尽管实现可传递受限安全权证可以涉及更多组件，但相关组件仍然结合此图来讨论。

[0062] 用户可使用各个客户机设备 761-763 来访问基于 web 的服务。可由诸如 web 服务器 772 等一个或多个服务器来管理基于 web 的服务。可将用于与基于 web 的服务相关联的各种目的的数据存储在数据存储 776 中，该数据存储 776 可被数据库服务器 774 直接访问或管理。补充由 web 服务器 772（以及相关联的服务器）提供的服务的第三方服务可使用如前所述的可传递受限安全权证来访问基于 web 的服务并执行被集成到基于 web 的服务中的子进程。

[0063] 网络 770 可以包括诸如企业网络等安全网络、诸如无线开放网络等非安全网络、或因特网。网络 770 提供此处描述的节点之间的通信。作为示例而非局限，网络 770 可以包括诸如有线网络或直接线连接等有线介质，以及诸如声学、RF、红外线和其它无线介质等无线介质。

[0064] 可以利用计算设备、应用程序、数据资源、数据分布系统的许多其它配置来实现基于 web 的服务环境中的可转移受限安全权证。此外，图 7 中所讨论的联网环境仅用于说明目的。各实施例不限于示例应用程序、模块、或过程。

[0065] 图 8 及相关联的讨论旨在提供对适于在其中实现各实施例的计算环境的简要概括描述。参考图 8，示出了诸如计算设备 800 等示例计算操作环境的框图。在基本配置中，计算设备 800 可以是服务器，其提供与允许第三方提供者通过受限安全权证访问数据的基于 web 的服务相关联的服务并通常包括至少一个处理单元 802 和系统存储器 804。计算设备 800 还可包括协作执行程序的多个处理单元。取决于计算设备的确切配置和类型，系统存储器 804 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。系统存储器 804 通常包括适于控制联网的个人计算机的运作的操作系统 805，诸如来自华盛顿州雷德蒙市的微软公司的 WINDOWS 操作系统。系统存储器 804 还可以包括一个或多个软件应用程序，诸如程序模块 808 和、web 服务 822、以及安全模块 824。

[0066] web 服务 822 可以是单独的应用程序或是向与计算设备 800 相关联的客户机应用程序提供数据和处理服务的主存的基于 web 的服务应用程序的整合模块。如前所述，安全模块 824 可提供与确保对由用户和 / 或第三方提供的数据的安全访问相关联的服务以实现

受限安全权证。该基本配置在图 8 中由虚线 806 内的组件示出。

[0067] 计算设备 800 可具有附加的特征或功能。例如，计算设备 800 还可包括附加的数据存储设备（可移动和 / 或不可移动），诸如例如磁盘、光盘或磁带。这些其它存储在图 8 中由可移动存储 809 和不可移动存储 810 示出。计算机存储介质可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实现的易失性和非易失性、可移动和不可移动介质。系统存储器 804、可移动存储 809 和不可移动存储 810 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设备 800 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设备 800 的一部分。计算设备 800 也可具有诸如键盘、鼠标、笔、语音输入设备、触摸输入设备等的输入设备 812。还可包括输出设备 814，如显示器、扬声器、打印机等。这些设备在本领域中公知且无需在此处详细讨论。

[0068] 计算设备 800 还可以包含允许该设备诸如在分布式计算环境中，例如在内联网或互联网中通过无线网络与其它计算设备 818 通信的通信连接 816。其它计算设备 818 可以包括执行与基于 web 的服务相关联的应用程序的服务器。通信连接 816 是通信介质的一个示例。通信介质通常由诸如载波或其它传输机制等已调制数据信号中的计算机可读指令、数据结构、程序模块或其它数据来体现，并包括任何信息传递介质。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。

[0069] 所要求保护的主题还包括各方法。这些方法可以用任何数量的方式，包括本文中所描述的结构来实现。一种此类方式是通过本文中描述的类型的设备的机器操作。

[0070] 另一可任选方式是结合一个或多个人类操作者执行该方法的各个操作中的某一些来执行该方法的一个或多个操作。这些人类操作者无需彼此同在一处，但是其每一个可以仅与执行程序的一部分的机器同在一处。

[0071] 图 9 示出使用用于允许由基于 web 的服务中的第三方提供者访问用户数据的受限安全权证的过程 (900) 的逻辑流程图。过程 900 可作为 CRM 服务的一部分来实现。

[0072] 过程 900 开始于操作 902，其中接收来自第三方提供者的对访问的请求。如前所述，第三方提供者可执行补充由基于 web 的服务提供的服务的子进程。处理从操作 902 前进至操作 904。

[0073] 在操作 904，从请求中提取安全权证和声明。声明定义所请求的访问的范围。权证包括有效期和限制。权证还可包括定义可使用该同一权证多少次的可任选的重复参数。处理从操作 904 移动至可任选操作 906。

[0074] 在可任选操作 906，认证该权证。可通过诸如受信第三方认证、公 / 私钥加密、散列消息认证码 (HMAC) 加密等各种机制来认证权证。在操作 906 之后，处理移动至操作 908。

[0075] 在操作 908，验证权证的时间戳。如果时间戳是无效的，则可异常终止该进程并拒绝第三方请求者的访问。处理从操作 908 移动至操作 910。

[0076] 在操作 910，由安全模块加载用户角色。处理从操作 910 前进至操作 912，在那里

还由安全模块加载限制角色。

[0077] 在操作 912 之后的操作 914 处，使用户角色和限制角色的相交以确定可应用到进行请求的第三方提供者的限制。处理从操作 914 前进至操作 916。

[0078] 在操作 916，基于根据限制角色和用户角色的相交确定的限制（以及在权证中定义的有效期）向进行请求的第三方提供者授予访问权。在操作 916 之后，处理移动至调用进程以进行进一步动作。

[0079] 包括在过程 900 内的各操作仅出于说明目的。可通过具有较少或额外步骤、以及按使用此处所述的原理的不同次序的操作的类似过程来实现使用用于允许在 web 服务中对第三方的访问的可传递受限安全权证。

[0080] 以上说明、示例和数据提供了对各实施例成分的制造和使用的全面描述。尽管用结构特征和 / 或方法动作专用的语言描述了本主题，但可以理解，所附权利要求书中定义的主题不必限于上述特定特征或动作。相反，上述具体功能部件和动作是作为实现权利要求和各实施例的示例形式而公开的。

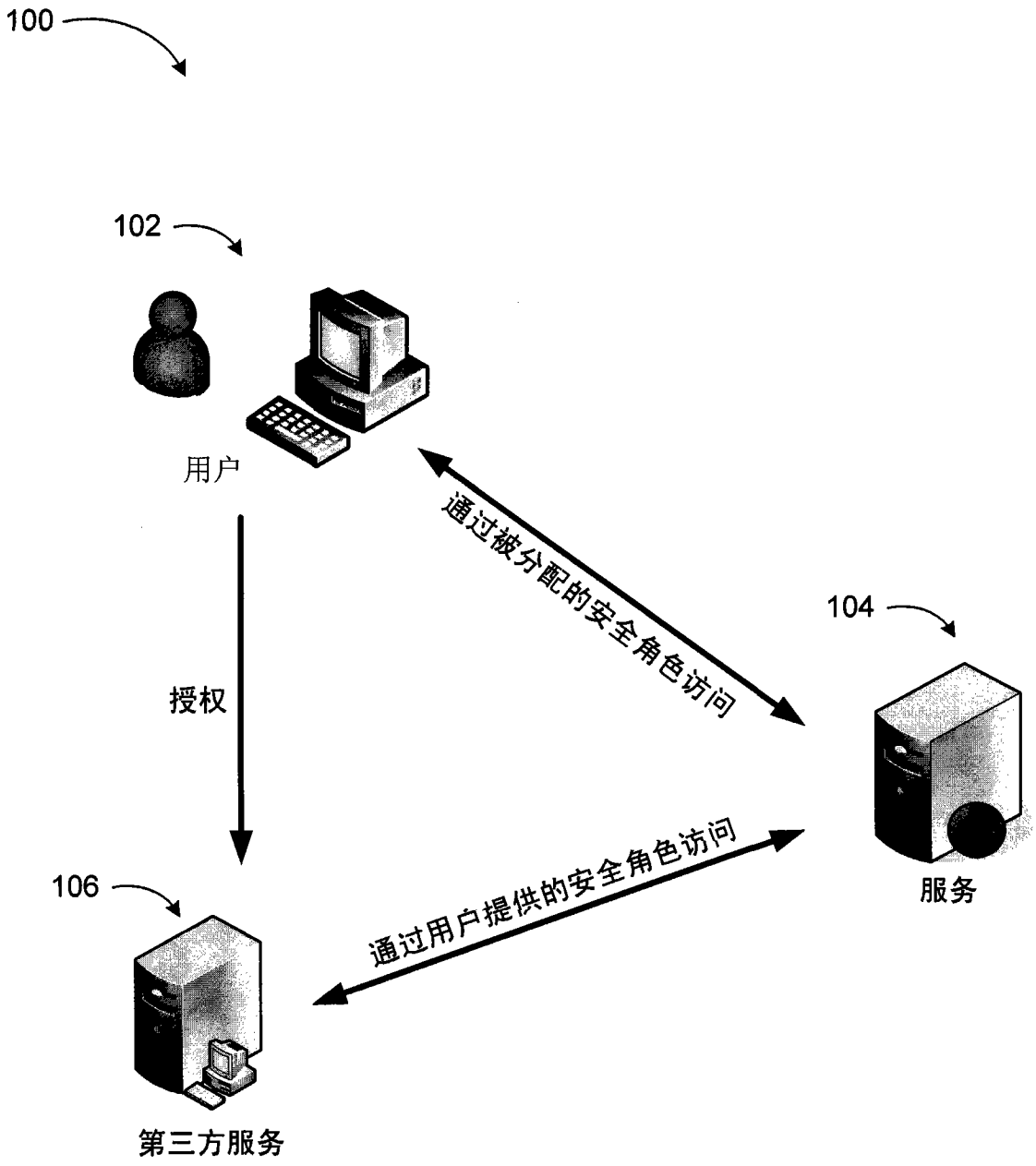


图 1

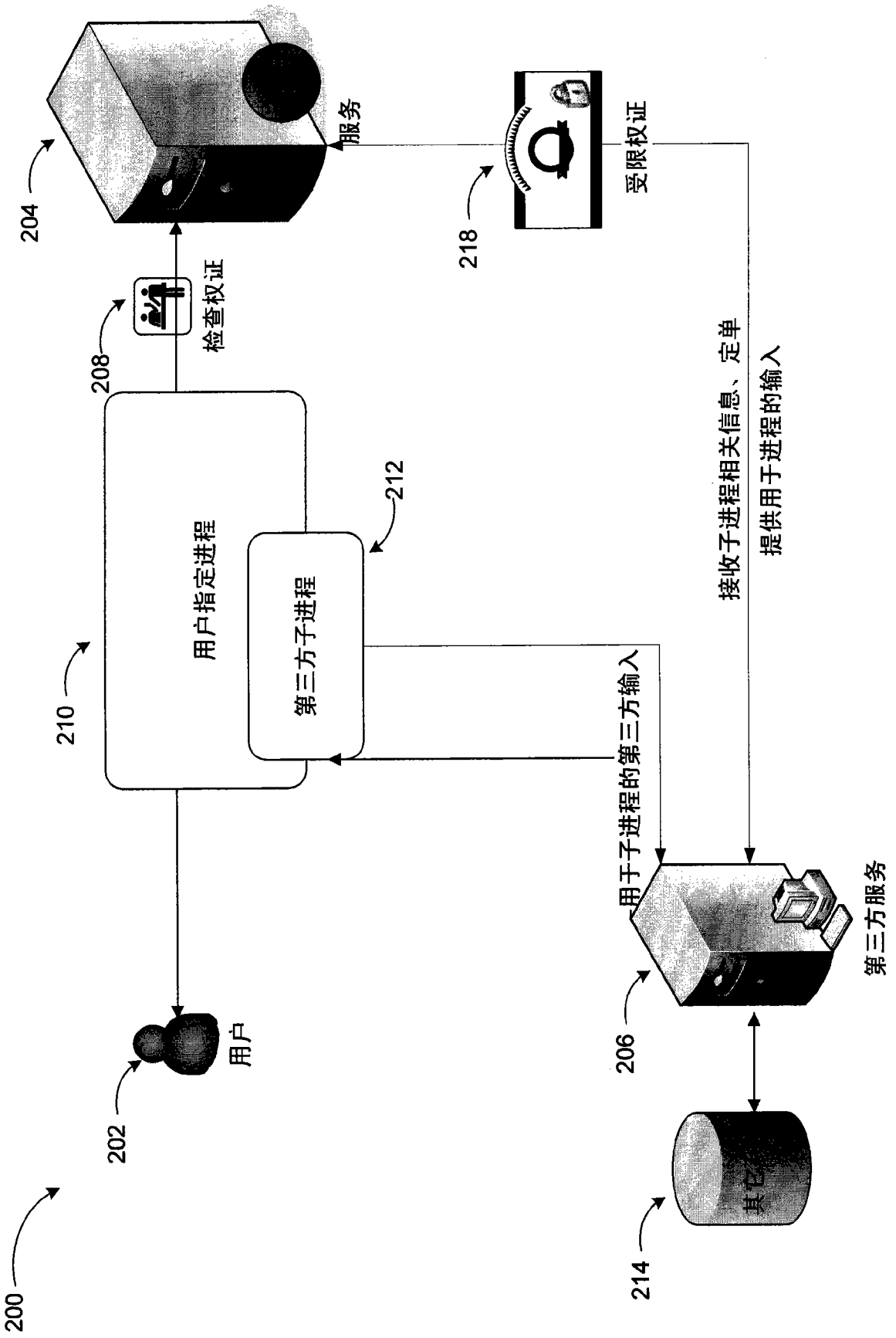

200
202
用户
204
服务
206
第三方服务
208
检查权证
210
用户指定进程
212
第三方子进程
214
其它
218
受限权证
接收子进程相关信息、定单
提供用于进程的输入
用于子进程的第三方输入

图 2

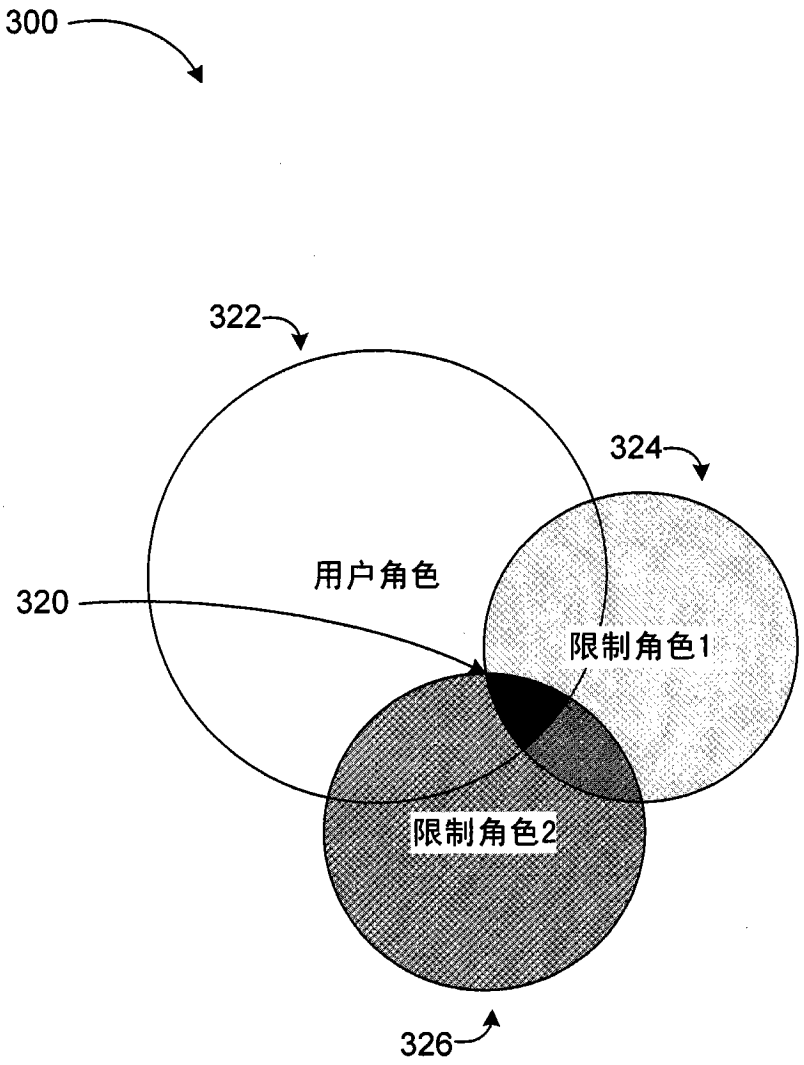


图 3

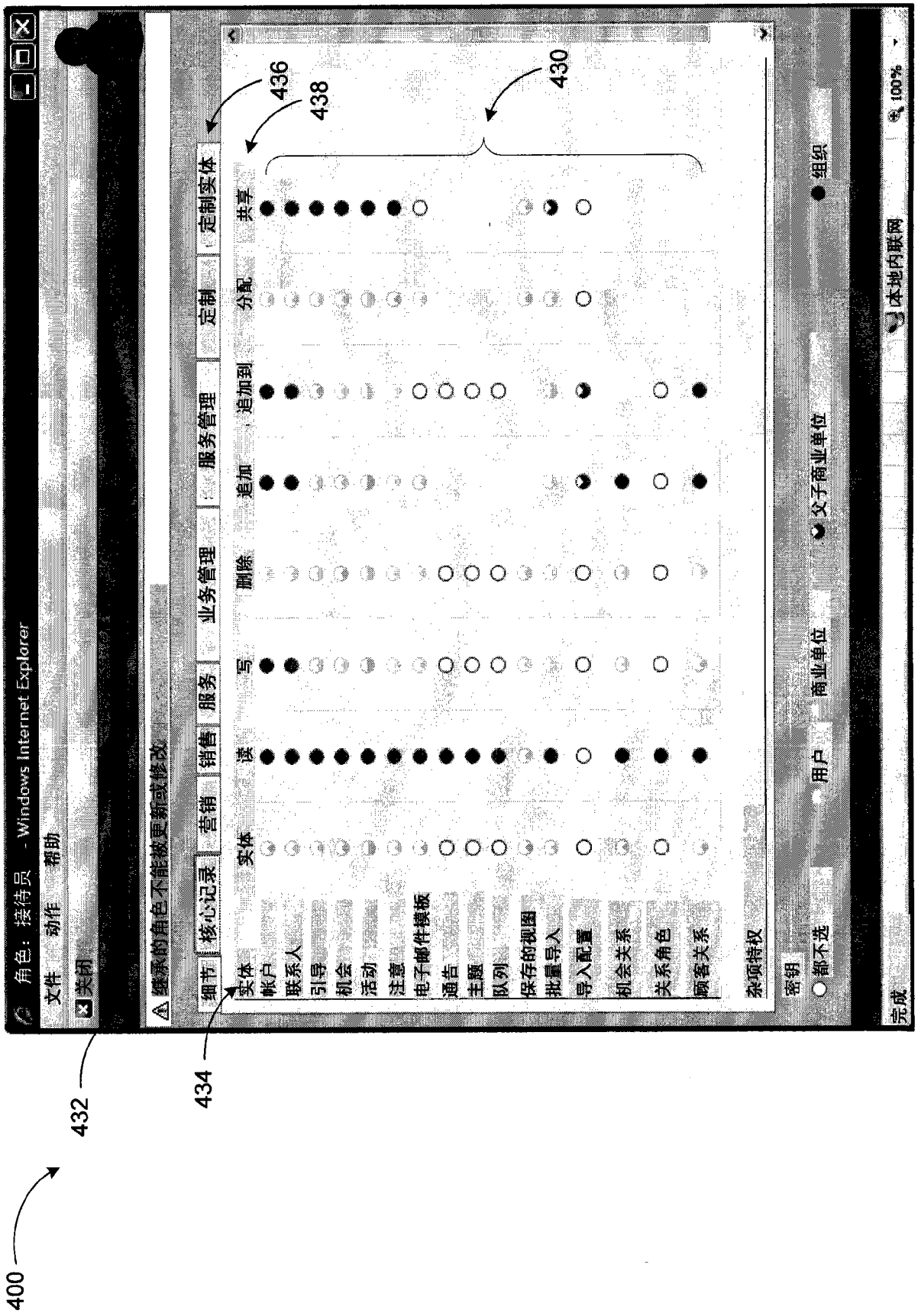

400
432
434
436
438
430
角色：接待员 - Windows Internet Explorer
文件 动作 帮助
关闭
继承的角色不能被更新或修改
细节 核心记录 营销 销售 服务 业务管理 服务管理 定制 定制实体
实体 读 写 删除 追加 追加到 分配 共享
帐户
联系人
引导
机会
活动
注意
电子邮件模板
通告
主题
队列
保存的视图
批量导入
导入配置
机会关系
关系角色
顾客关系
杂项特权
密钥
都不选
用户
商业单位
父子商业单位
组织
完成
本地内联网
100%

图 4

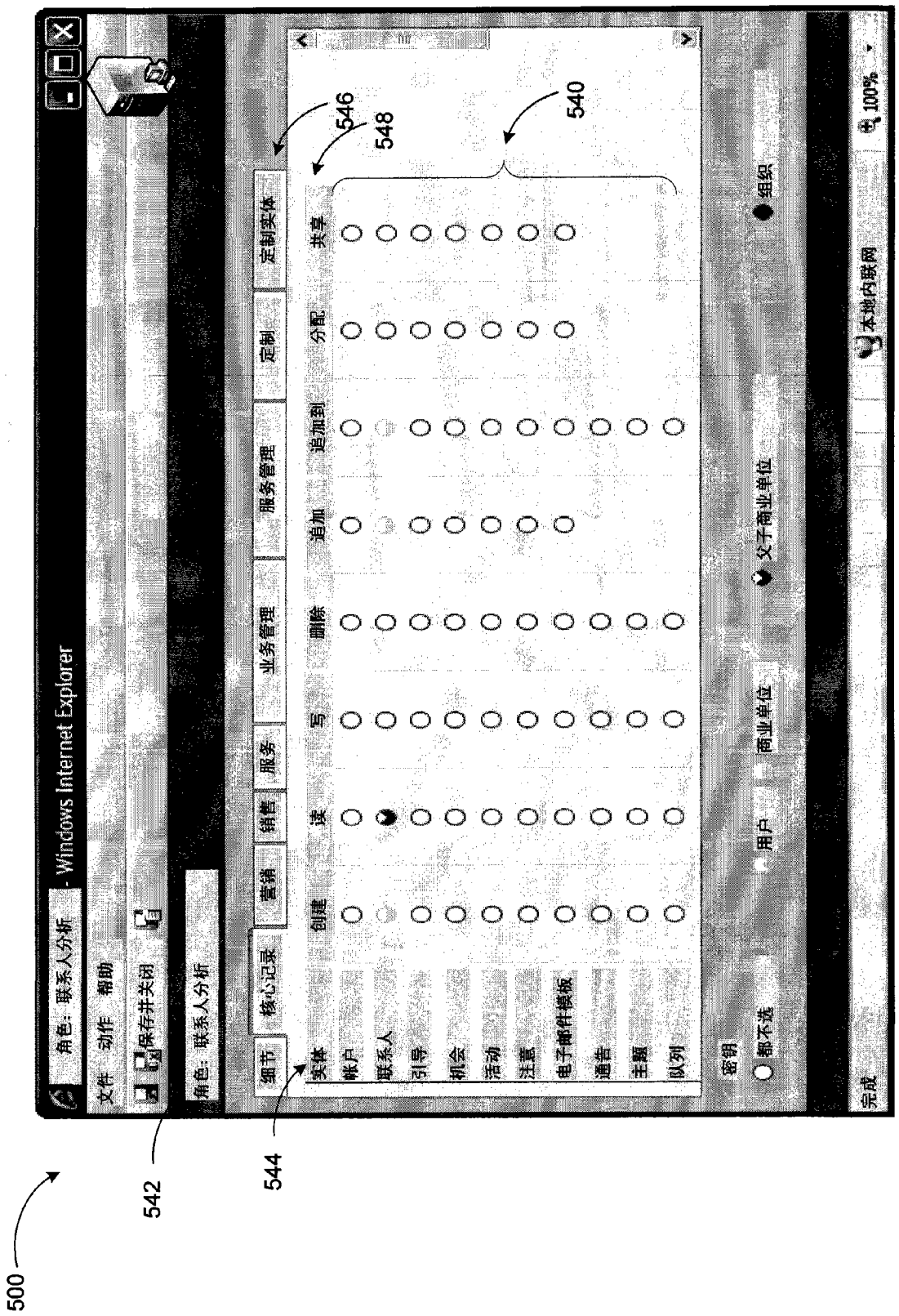

角色: 联系人分析 - Windows Internet Explorer
文件 动作 帮助
保存并关闭
角色: 联系人分析
细节
核心记录
营销
销售
服务
业务管理
服务管理
定制
定制实体
实体
帐户
联系人
引导
机会
活动
注意
电子邮件模板
通告
主题
队列
创建
读
写
删除
追加
追加到
分配
共享
密钥
都不选
用户
商业单位
父子商业单位
组织
完成
本地内联网
100%
500
542
544
546
548
540

图 5

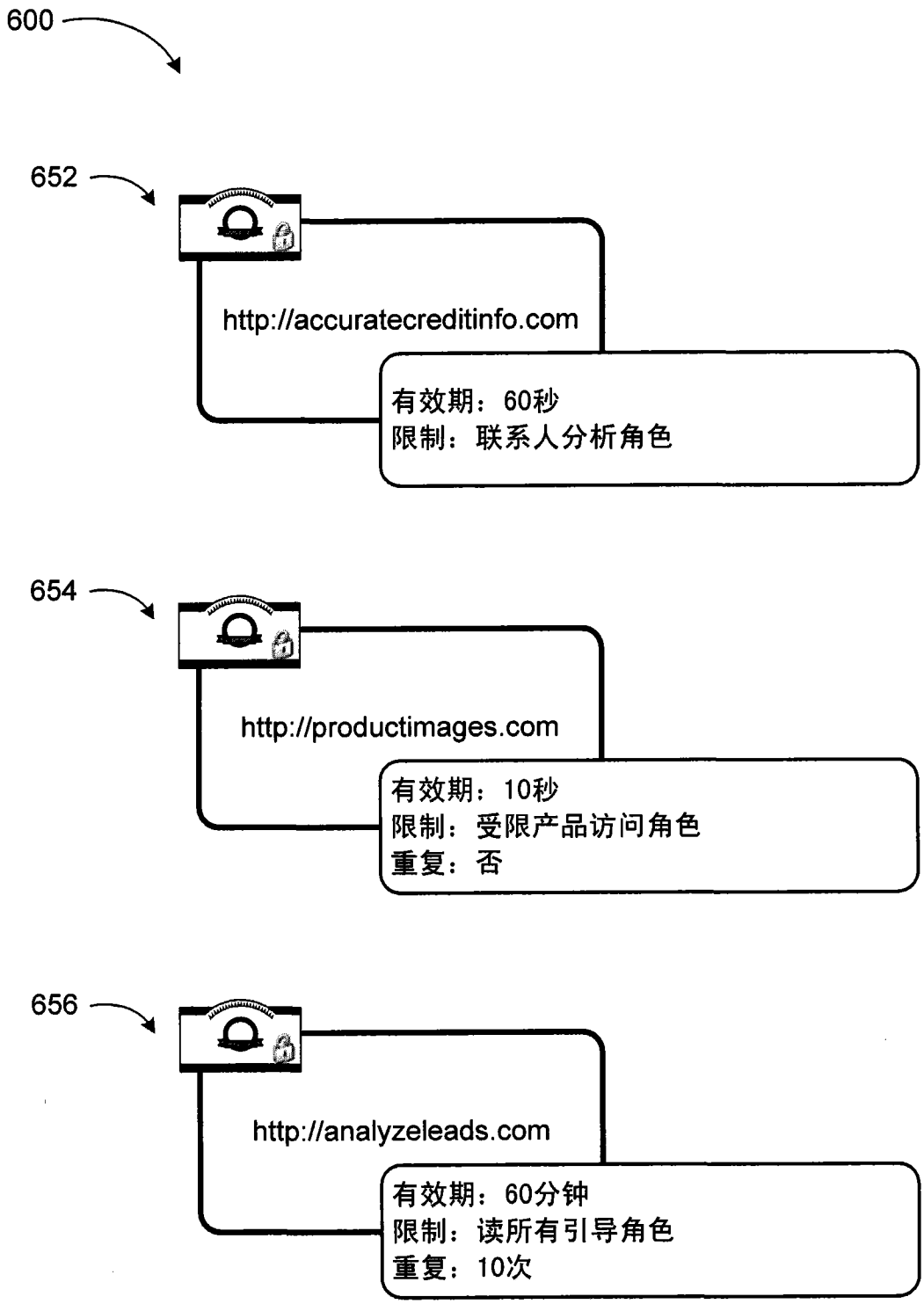

600
652
http://accuratecreditinfo.com
有效期：60秒
限制：联系人分析角色
654
http://productimages.com
有效期：10秒
限制：受限产品访问角色
重复：否
656
http://analyzeleads.com
有效期：60分钟
限制：读所有引导角色
重复：10次

图 6

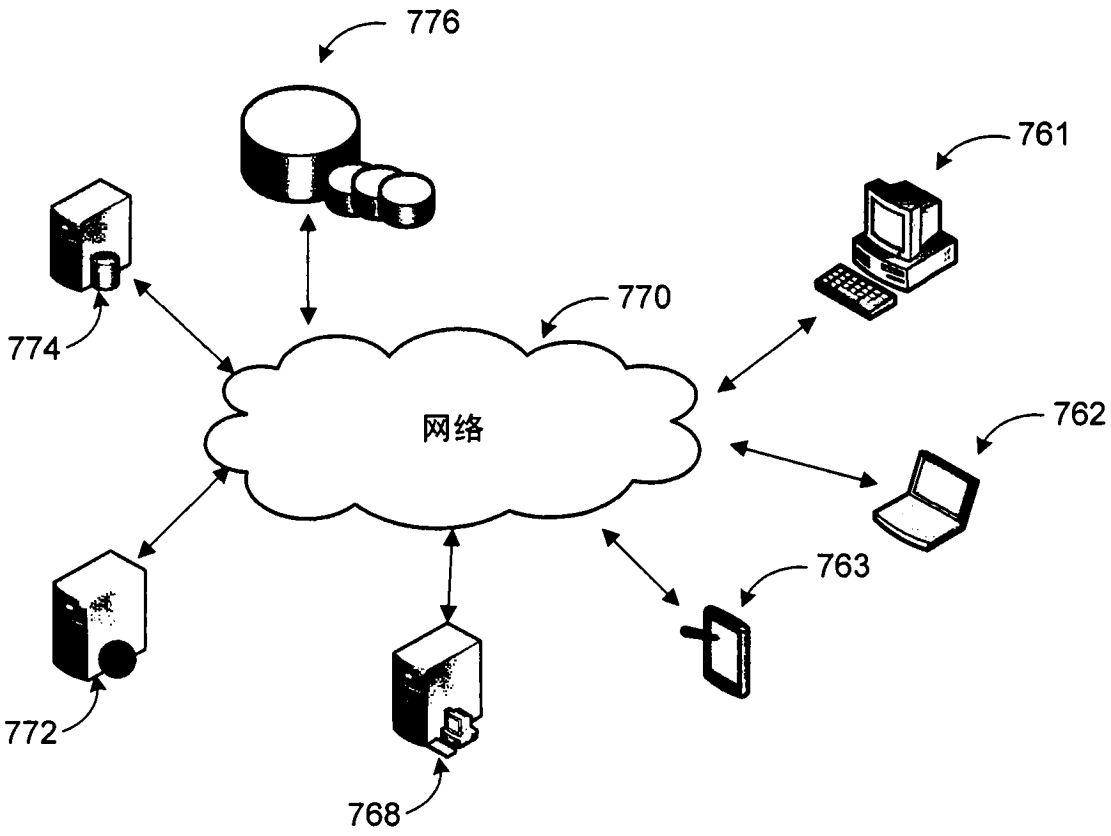


图 7

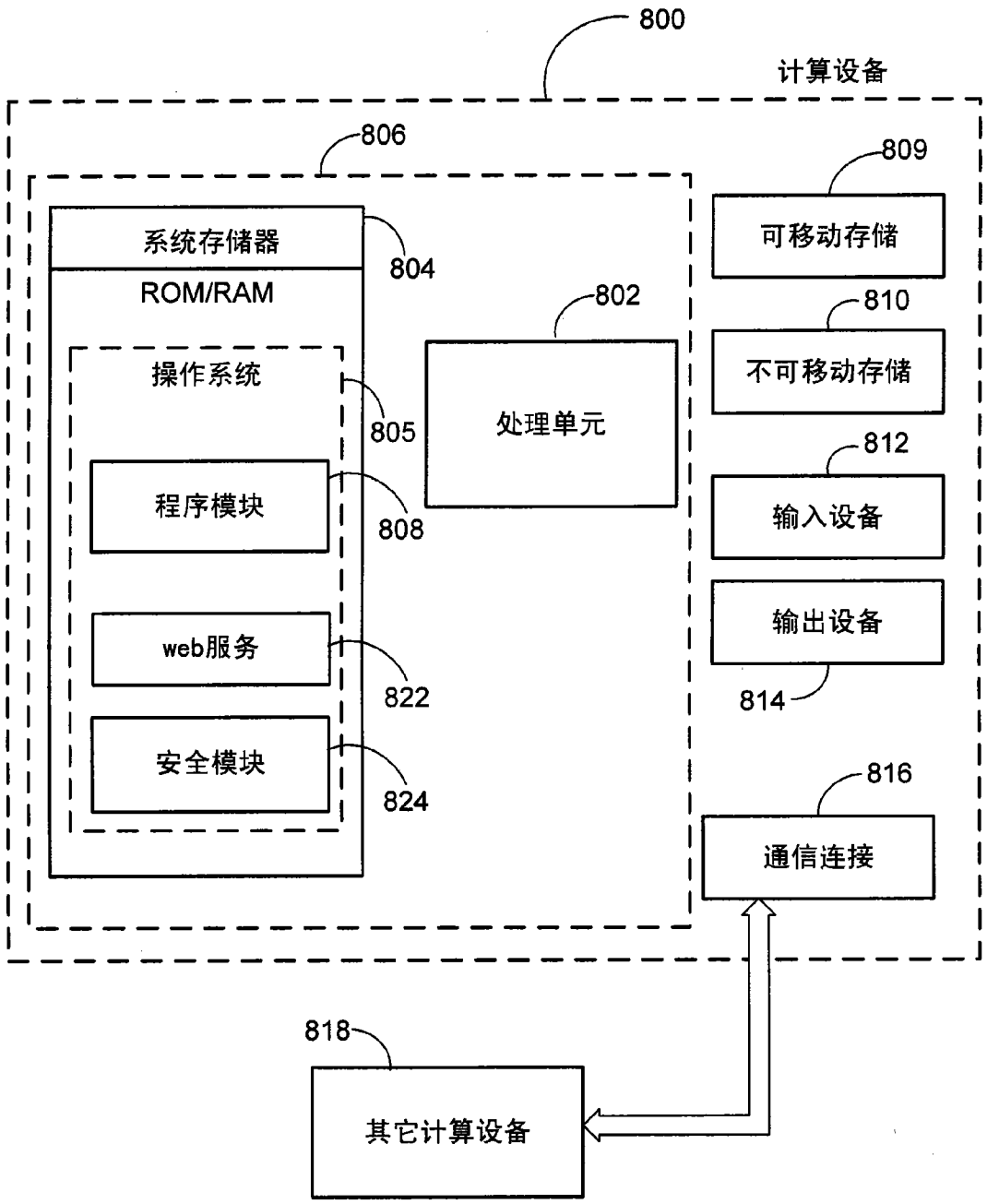

800
计算设备
806
系统存储器
804
ROM/RAM
操作系统
805
程序模块
808
web服务
822
安全模块
824
802
处理单元
809
可移动存储
810
不可移动存储
812
输入设备
输出设备
814
816
通信连接
818
其它计算设备

图 8

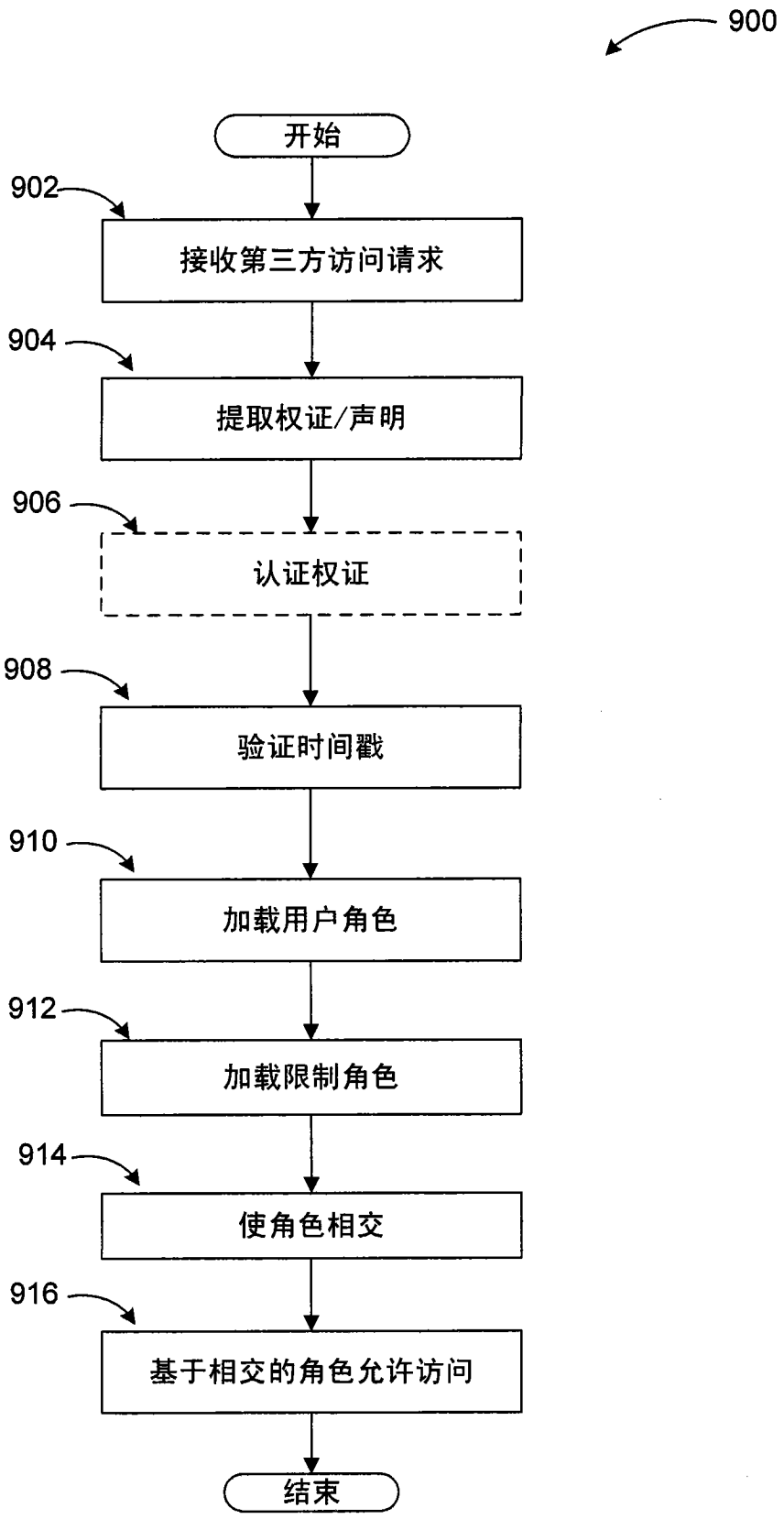

900
开始
902
接收第三方访问请求
904
提取权证/声明
906
认证权证
908
验证时间戳
910
加载用户角色
912
加载限制角色
914
使角色相交
916
基于相交的角色允许访问
结束

图 9