(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 104871168 A
(43)申请公布日 2015.08.26

(21)申请号 201380068358.1
(22)申请日 2013.12.31
(30)优先权数据
13/732,526 2013.01.02 US
(85)PCT国际申请进入国家阶段日
2015.06.26
(86)PCT国际申请的申请数据
PCT/US2013/078397 2013.12.31
(87)PCT国际申请的公布数据
WO2014/107443 EN 2014.07.10
(71)申请人 微软技术许可有限责任公司
地址 美国华盛顿州
(72)发明人 M·门德洛维奇 R·玛取洛
(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 杨丽
(51)Int.Cl.
G06F 21/33(2006.01)

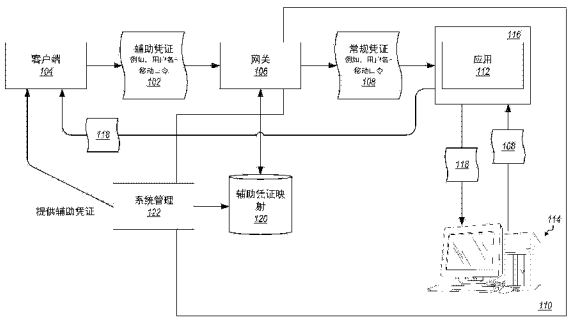
权利要求书1页 说明书5页 附图2页

(54)发明名称

不受信任的设备上的资源保护

(57)摘要

向第一服务认证用户以允许该用户访问由该第一服务所提供的资源。资源是要求通用凭证(例如,用户名和/或口令)才能访问该资源的受保护的资源。该方法包括在第二服务处从设备接收自组织凭证。自组织凭证是为该设备所特有的凭证。自组织凭证可用于认证用户和设备两者,但是不能直接用作第一服务处对用户访问资源的认证。该方法还包括在第二服务处用通用凭证替换自组织凭证,以及将通用凭证转发到第一服务。如此,第一服务可以向该设备处的用户提供资源。



CN 104871168 A

1. 一种在计算环境中向第一服务认证用户以允许所述用户访问由所述第一服务所提供的资源的方法，其特征在于，所述资源是要求第一用户凭证来访问所述资源的受保护的资源；所述方法包括：

在第二服务处从所述设备接收第二用户凭证，其中所述第二用户凭证是为所述设备所特有的凭证，并可用于认证所述用户和所述设备两者，但是不能直接用作所述第一服务处对所述用户访问所述资源的认证；以及

在所述第二服务处用所述第一用户凭证替换所述第二用户凭证，并将所述第一用户凭证转发到所述第一服务，以便所述第一服务能够向所述设备处的所述用户提供所述资源。

2. 如权利要求 1 所述的方法，其特征在于，所述第二用户凭证是为给定通信信道所特有的凭证。

3. 如权利要求 1 所述的方法，其特征在于，所述第二用户凭证在时间上受限，以便所述第二用户凭证在给定时间段之后期满。

4. 如权利要求 1 所述的方法，其特征在于，所述第二用户凭证在所述第二服务处的使用是受策略限制的。

5. 如权利要求 4 所述的方法，其特征在于，所述策略按时间来限制所述第二用户凭证的使用。

6. 如权利要求 4 所述的方法，其特征在于，所述策略通过限制什么资源可以使用所述第二用户凭证来访问来限制所述第二用户凭证的使用。

7. 如权利要求 4 所述的方法，其特征在于，所述策略根据用户角色来限制所述第二用户凭证的使用。

8. 如权利要求 1 所述的方法，其特征在于，所述第二用户凭证通过使用所述第一用户凭证和由所述第二服务维护的秘密计算所述第二用户凭证来生成。

不受信任的设备上的资源保护

[0001] 背景

[0002] 计算机和计算系统已经影响了现代生活的几乎每个方面。计算机通常涉及工作、休闲、保健、运输、娱乐、家政管理等。

[0003] 此外，计算系统功能还可以通过计算系统经由网络连接互连到其他计算系统的能力来增强。网络连接可包括，但不仅限于，经由有线或无线以太网的连接，蜂窝式连接，或者甚至通过串行、并行、USB 或其它连接的计算机到计算机的连接。这些连接允许计算系统访问其他计算系统上的服务，并快速且有效地从其他计算系统接收应用数据。

[0004] 当前网络允许许多新的以及不同类型的设备被联网。另外，还期望使联网设备具有移动性。随着智能电话和平板在商业企业网络上越来越流行，移动性持续发展。希望利用机会来提高雇员生产力的许多组织正在拥抱移动工作方式，允许信息工作人员从他们的移动设备访问企业资源。

[0005] 尽管这一趋势带来了提高雇员效率的新的机会，但是，它也为 IT 管理员造成了新的安全风险，因为在很多情况下，雇员会将企业凭证（例如，用户名和口令对）存储在他们的移动设备上。例如，使用由位于美国华盛顿州雷德蒙市的微软公司所提供的Active Sync的大多数移动电子邮件客户端都要求企业凭证。可以轻松地从移动设备中提取这些凭据。例如，设备可能会被偷，设备可能主存结果是收集保存的口令或记录击键的特洛伊木马的移动应用。这会是特别危险的，假定企业用户常常使用相同凭证来访问对该企业用户可用的大多数，如果并非全部资源。

[0006] 在此要求保护的主题不限于解决任何缺点或仅在诸如上述环境中操作的各个实施例。相反，提供该背景仅用以示出在其中可实践在此描述的部分实施例的一个示例性技术领域。

发明内容

[0007] 在此所示的一个实施例包括可以在计算环境中实施的方法。该方法包括向第一服务认证用户以允许该用户访问由第一服务所提供的资源的动作。资源是要求通用凭证（例如，用户名和 / 或口令）才能访问该资源的受保护的资源。该方法包括在第二服务处从设备接收自组织 (ad-hoc) 凭证。自组织凭证是为该设备所特有的凭证。自组织凭证可用于认证用户和设备两者，但是不能直接被用作第一服务处对用户访问资源的认证。该方法还包括，在第二服务处用通用凭证来替换自组织凭证以及将通用凭据转发到第一服务。如此，第一服务可以向该设备处的用户提供资源。

[0008] 提供本概述是为了以精简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出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。

[0009] 将在以下的描述中阐述另外的特征和优点，并且部分特征和优点可从该描述中显而易见，或者可从本文教导的实践中获知。本发明的特征和优点可以通过在所附权利要求中特别指出的手段和组合来实现并获取。本发明的特征将从以下描述和所附权利要求书中

变得完全显而易见，或者可通过如下所述对本发明的实践而获知。

[0010] 附图简述

[0011] 为了描述可获得本主题的上述和其它优点和特征的方式，将通过参考附图中示出的本主题的具体实施例来呈现以上简要描述的本主题的更具体描述。应该理解，这些附图仅描绘了各典型实施例，因此其不应被认为是对范围的限制，各实施例将通过使用附图用附加特征和详情来描述并解释，在附图中：

[0012] 图 1 示出了用于管理用户主要和辅助凭证的系统；以及

[0013] 图 2 示出了用于向第一服务认证用户以允许用户访问由第一服务所提供的资源的方法。

具体实施方式

[0014] 各实施例可包括通过发出将只从特定上下文，诸如特定企业接口、特定协议、特定邮箱，等等的和 / 或设备使用的并且可以具有单独的预期的生命周期的专用辅助凭证（例如，凭证只能从位于美国华盛顿州雷德蒙市的微软公司所提供的 ActiveSync 接口使用）来保护通用主要凭证的功能。如果这些辅助凭证被破坏，则损害是有限的。具体而言，损害可能仅限于辅助凭证应用到的设备，仅限于辅助凭证应用到的那些某些企业接口，和 / 或仅限于辅助凭证有效的有限的时段。如此，与当允许对整个企业系统或企业系统的大部分进行访问的主要企业凭证被破坏的情况相比，损毁会是有限的。

[0015] 如此，并参考图 1，一些实施例为不受信任的设备（诸如设备 104）实现辅助凭证 102（诸如口令）。例如，设备 104 可以是移动设备。

[0016] 各实施例可以实现将辅助凭证 106 替换为主要凭证 108（例如，主要企业范围的凭证）的网关 106。通过实现网关 106，可以在不改变企业网络 110 上的设备 104 内部系统或各种服务或系统的情况下，实现主要凭证 108 和辅助凭证 102 的共存。网关 106 可以和客户端 104 分离。网关 106 能够代理与企业网络 110 中的应用 112 相关的话务，并将利用主要凭证 108 更换辅助凭证 102 以允许对企业资源进行访问。

[0017] 在很多情况下，此网关 106 驻留在企业网络 110 的边缘。网关 106 可以以这样的方式实现，以便所有外部话务都必须经过网关 106 才能进入企业网络 110。如此，从企业网络 110 内对应用 112 进行访问将要求使用主要凭证 108。例如，图 1 示出了用户可以使用驻场公司系统 114，诸如台式机或膝上型计算机，它们位于企业的建筑物中，并通过在企业网络 110 管理员的直接控制下硬件和通信线路连接到企业网络 110。在此情况下，如图所示，可以从公司系统 114 向服务 116 发送主要凭证 108 以访问应用 112 的资源 118。

[0018] 可另选地，当用户希望在远程连接时访问由应用 112 所提供的资源 118 时，可以通过客户端系统 104 向网关 106 发送辅助凭证 102 来使用特殊辅助凭证 102，它用于替换主要凭证 108 以允许资源 118 被返回到客户端系统 104。值得注意的是，可以实现并非所有的话务都被发送到网关 106 的实施例。相反，在某些实施例中，只向网关 106 发送某些类型的话务，或计划用于某些应用的话务。例如，可以向网关 106 发送电子邮件和日历数据，而其他话务不通过网关 106 路由。

[0019] 辅助凭证 102 可以服从与主要凭证 108 不同的策略。例如，辅助凭证 102 可以比主要凭证在时间上更受限。例如，辅助凭证可以比主要凭证 108 有效达更短的时间段。另

选地或另外地，辅助凭证 102 可以比主要凭证 108 在何时可以使用它方面具有限制性更强的时间限制。例如，主要凭证 108 可以在白天或夜间的任何时间使用，而辅助凭证 102 可以仅限于，例如，5:00PM 和 9:00AM 之间。这些策略可以通过网关 106 实施。

[0020] 网关 106 能够实施关于辅助凭证 102 的服务或应用级别的限制。例如，主要凭证 108 可以被用来访问对主要凭证 108 所属的给定用户可用的几乎任何资源，网关 106 可以将通过设备 104 并使用辅助凭证 102 来访问企业资源的相同用户限制到有限的应用或资源的集合。例如，当作出对电子邮件资源的请求时，网关可以替换主要凭证 108，但是，对于从客户端 104 作出的对敏感数据库资源的请求，可以拒绝替换主要凭证。某些这样的实施例可以是基于角色的。例如，网关 106 可以对 CEO 或企业的主要网络管理员实施较少的（或没有）限制，而对数据输入职员施加较多的限制。

[0021] 网关 106 可以基于将由管理系统 122 管理的主要凭证 108 和辅助凭证 102 进行相关的数据库 120 来执行辅助凭证 102 和主要凭证 108 的凭证交换。

[0022] 此管理系统 122 可以基于向用户界面提供的输入或 / 和其内部逻辑来分配辅助凭证。管理系统 122 也可以定义使用和期满策略。此管理系统通常将实现额外的认证逻辑来生成辅助认证并将其提供到用户和设备（诸如设备 104）。在说明性示例中，用户使用 Web UI 来访问管理系统 122。使用智能卡或其他认证来认证用户。然后，用户通过 Web UI 以自组织口令的形式接收辅助凭证，该自组织口令对于 ActiveSync 有效达一周。如此，用户能够获取可以与不受信任的设备 104 一起使用的辅助凭证 102，其中，辅助凭证在关于它有效期多长时间方面受限制以及限于某些应用。

[0023] 进一步，在某些实施例中，辅助凭证 102 可以以只允许它与某些设备（例如，设备 104）或某些信道一起使用的方式生成。例如，网关 106 能够实施允许辅助凭证 102 与特定设备 104 或设备组一起使用而排除其与其他设备一起使用的限制。网关 106 能够另选地或另外地限制辅助凭证 102 与某些通信信道一起使用。例如，辅助凭证能够和用户的特定家庭网络一起使用，但当设备连接到某些公众 Wi-Fi 网络或蜂窝网络时不能被使用。

[0024] 可以以各种不同的方式生成诸如凭证 102 之类的辅助凭证。例如，在某些实施例中，辅助凭证 102 可以通过使用在管理系统 122 处的秘密和主要凭证 108 来生成。可以使用管理系统处的秘密和主要凭证来执行散列或其他计算以生成辅助凭证 102。

[0025] 在另一个实施例中，在用户通过管理系统 122 的 Web UI 呈现主要凭证 108 之后，可以由用户选择或人工地生成辅助凭证 102。

[0026] 以下讨论现涉及可以执行的多种方法以及方法动作。虽然用特定次序讨论或用以特定次序发生的流程图示出了各个方法动作，但除非明确规定或因为一动作依赖于另一动作在执行该动作之前完成而需要特定次序，否则不需要特定次序。

[0027] 现在参考图 2，示出了方法 200。可以在计算环境中实施方法 200。方法 200 包括向第一服务认证用户以允许该用户访问由第一服务所提供的资源的动作。资源是要求通用凭证（例如，用户名和 / 或口令）才能访问该资源的受保护的资源。例如，如图 1 所示，用户能够通过呈现主要凭证 108 从服务 116 访问资源 108。

[0028] 该方法包括在第二服务处从设备接收自组织凭证（动作 202）。自组织凭证是为所述设备所特有的凭证，并可用于认证所述用户和所述设备两者，但是不能直接用作所述第一服务处对所述用户访问所述资源的认证。例如，设备 104 可以从管理系统 122 接收辅助

凭证 102。辅助凭证 102 可以是设备 104 特定的凭证，当凭证和设备 104 一起使用时，它可以被用作认证，但是当与其他设备一起使用时，它不能被用作认证。在某些实施例中，凭证必须和一个或多个特定信道一起使用，并且不能与其他信道一起使用。在某些实施例中，凭证可以只对于单一特定设备有效，在其他实施例中，它对预先指定的设备组有效。

[0029] 方法 200 还包括在第二服务处用通用凭证替换自组织凭证，以及将通用凭证转发到第一服务（动作 204）。例如，如图 1 所示，用主要凭证 108 代替辅助凭证 102。使用主要凭证 108 来为设备 104 处的用户获取资源 108。如此，可以执行动作 204，以便第一服务（例如，服务 116）可以向设备（例如，设备 104）处的用户提供资源。

[0030] 可以在所述自组织凭证是给定通信信道所特有的凭证的情况下实施方法 200。例如，一个辅助凭证可以用于与公众 Wi-Fi 网络一起使用，而不同的凭证可以用于与家庭网络一起使用，而再一个不同的凭证用于蜂窝网络，等等。

[0031] 可以在所述自组织凭证在时间上受限以便所述自组织凭证在给定时间段之后期满的情况下实施方法 200。如此，例如，辅助凭证 102 可以只在颁发之后或在其第一次使用之后的给定时间段内有用。

[0032] 可以在所述自组织凭证在所述第二服务处的使用受策略限制的情况下实施方法 200。例如，策略可以按时间来限制自组织凭证的使用。例如，凭证的使用可以仅限于白天的某些时间，有限的连续的时间或有限的时间总长度等等。在某些实施例中，策略通过限制什么资源可以使用自组织凭证来访问来限制自组织凭证的使用。例如，如上所述，网关 106 可以限制当使用辅助凭证 102 时可以访问什么应用、服务、或资源。可以实现其中策略根据用户角色来限制自组织凭证的使用的各实施例。如前面所述，网关 106 能够实施限制，从而有较大特权的用户能够利用辅助凭证来访问比有较少特权的用户较大的资源组。

[0033] 可以在所述自组织凭证通过使用所述通用凭证和由所述第二服务维护的秘密计算所述自组织凭证来生成的情况下实施方法 200。如上所述，管理系统 122 可以通过使用管理服务器 122 处的秘密和主要凭证 108 来执行计算以生成辅助凭证 102。可另选地，管理系统可以随机地生成辅助凭证，然后将它们与主要凭证相关联。在再一个替代方案中，用户能够选择或提供他们自己的辅助凭证，然后可以通过管理系统 122 将辅助凭证与主要凭证相关联。

[0034] 此外，各种方法可由包括一个或多个处理器和诸如计算机存储器等计算机可读介质的计算机系统来实施。具体而言，计算机存储器可存储计算机可执行指令，这些指令在由一个或多个处理器执行时使得诸如各实施例中所述的各个动作等各种功能被执行。

[0035] 本发明的各实施例可以包括或利用包含计算机硬件的专用或通用计算机，这将在下文中更详细地讨论。本发明范围内的各实施例还包括用于承载或存储计算机可执行指令和 / 或数据结构的物理和其他计算机可读介质。这样的计算机可读介质可以是可由通用或专用计算机系统访问的任何可用介质。存储计算机可执行指令的计算机可读介质是物理存储介质。承载计算机可执行指令的计算机可读介质是传输介质。由此，作为示例而非限制，本发明的各实施例可包括至少两种显著不同的计算机可读介质 :物理计算机可读存储介质和传输计算机可读存储介质。

[0036] 物理计算机存储介质包括 RAM、ROM、EEPROM、CD-ROM 或其他光盘存储（如 CD、DVD 等）、磁盘存储或其他磁存储设备、或可用于存储计算机可执行指令或数据结构形式的所需

程序代码装置且可由通用或专用计算机访问的任何其他介质。

[0037] “网络”被定义为使得电子数据能够在计算机系统和/或模块和/或其它电子设备之间传输的一个或多个数据链路。当信息通过网络或另一个通信连接（硬连线、无线、或者硬连线或无线的组合）传输或提供给计算机时，该计算机将该连接适当地视为传输介质。传输介质可包括可用于携带计算机可执行指令或数据结构形式的所需程序代码装置且可由通用或专用计算机访问的网络和/或数据链路。以上介质的组合也被包括在计算机可读介质的范围内。

[0038] 此外，在到达各种计算机系统组件之后，计算机可执行指令或数据结构形式的程序代码装置可从传输计算机可读介质自动转移到物理计算机可读存储介质（或者相反）。例如，通过网络或数据链路接收到的计算机可执行指令或数据结构可被缓存在网络接口模块（例如，“NIC”）内的 RAM 中，然后最终被传送到计算机系统 RAM 和/或计算机系统处的较不易失性的计算机可读物理存储介质。因此，计算机可读物理存储介质可被包括在同样（或甚至主要）利用传输介质的计算机系统组件中。

[0039] 计算机可执行指令包括，例如使通用计算机、专用计算机、或专用处理设备执行某一功能或某组功能的指令和数据。计算机可执行指令可以是例如二进制代码、诸如汇编语言之类的中间格式指令、或甚至源代码。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征或动作。更具体而言，上述特征和动作是作为实现权利要求的示例形式而公开的。

[0040] 本领域的技术人员将理解，本发明可以在具有许多类型的计算机系统配置的网络计算环境中实践，这些计算机系统配置包括个人计算机、台式计算机、膝上型计算机、消息处理器、手持式设备、多处理器系统、基于微处理器的或可编程消费电子设备、网络 PC、小型计算机、大型计算机、移动电话、PDA、寻呼机、路由器、交换机等等。本发明也可在其中通过网络链接（或者通过硬连线数据链路、无线数据链路，或者通过硬连线和无线数据链路的组合）的本地和远程计算机系统两者都执行任务的分布式系统环境中实施。在分布式系统环境中，程序模块可以位于本地和远程存储器存储设备二者中。

[0041] 作为替代或除此之外，本文所述的功能可至少部分地由一个或多个硬件逻辑组件来执行。例如，但非限制，可被使用的硬件逻辑组件的说明性类型包括现场可编程门阵列 (FPGA)、专用集成电路 (ASIC)、专用标准产品 (ASSP)、片上系统 (SOC)、复杂可编程逻辑器件 (CPLD) 等。

[0042] 本发明可具体化为其他具体形式而不背离其精神或特征。所描述的实施例在所有方面都应被认为仅是说明性而非限制性的。因此，本发明的范围由所附权利要求书而非前述描述指示。落入权利要求书的等效方案的含义和范围内的所有改变都被权利要求书的范围所涵盖。

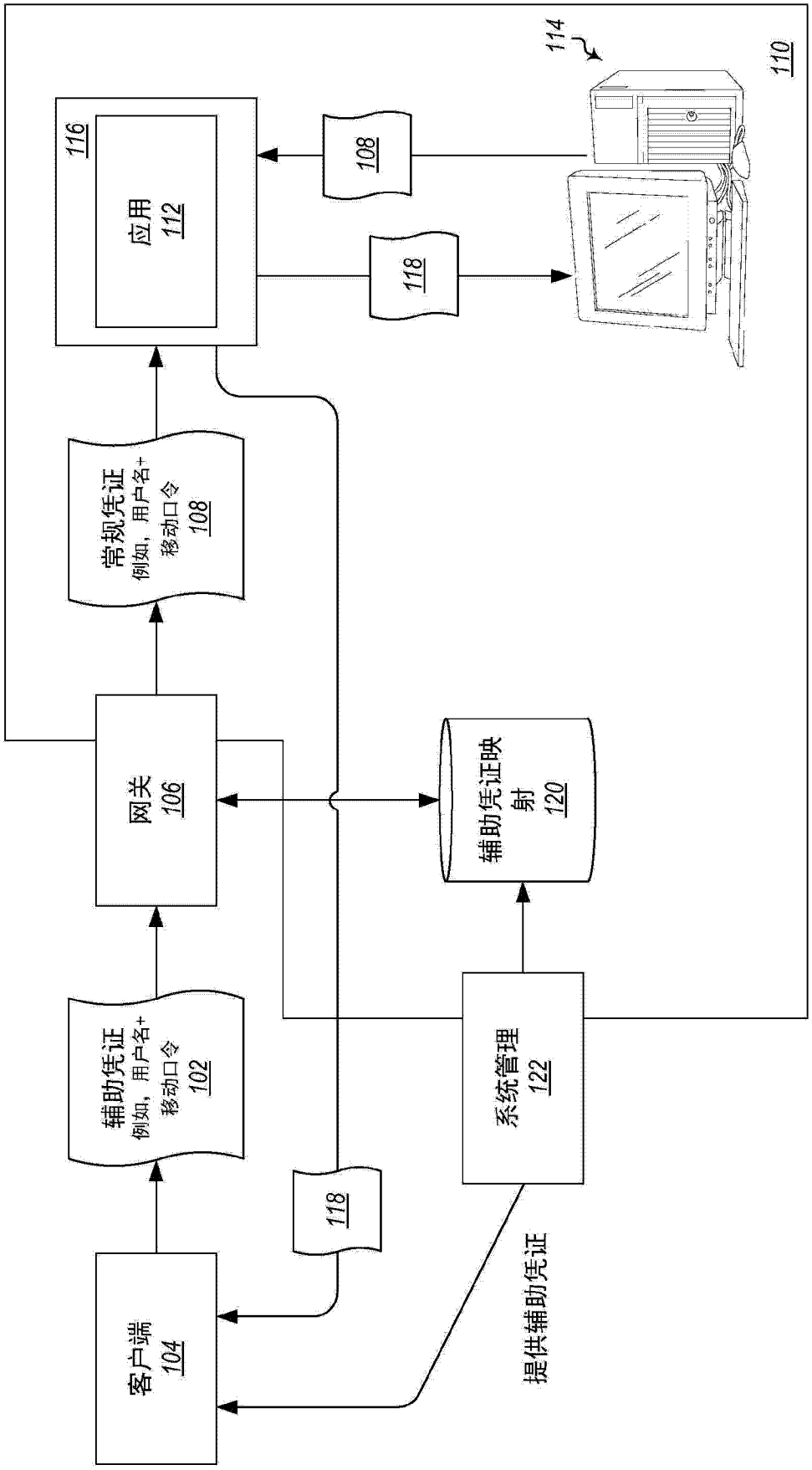

114
110
116
应用
112
108
118
常规凭证
例如，用户名+
移动口令
108
网关
106
辅助凭证映
射
120
辅助凭证
例如，用户名+
移动口令
102
系统管理
122
118
客户端
104
提供辅助凭证

图 1

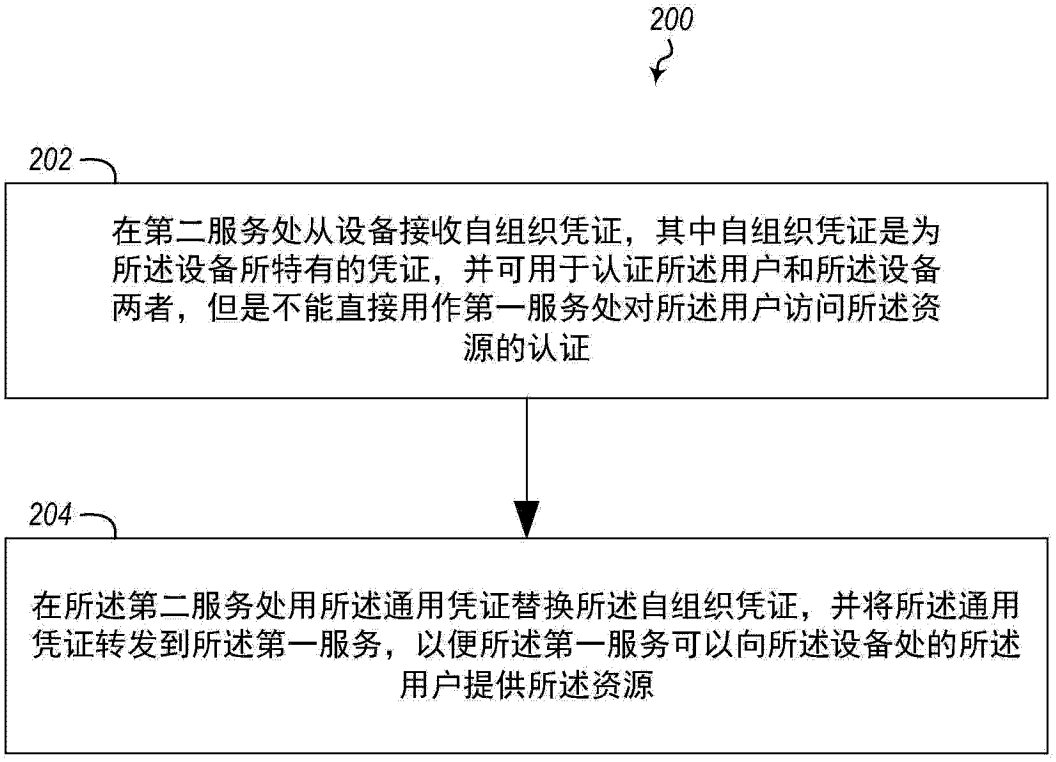

200
202
在第二服务处从设备接收自组织凭证，其中自组织凭证是为所述设备所特有的凭证，并可用于认证所述用户和所述设备两者，但是不能直接用作第一服务处对所述用户访问所述资源的认证
204
在所述第二服务处用所述通用凭证替换所述自组织凭证，并将所述通用凭证转发到所述第一服务，以便所述第一服务可以向所述设备处的所述用户提供所述资源

图 2