(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 103858097 B
(45)授权公告日 2017.06.13

(21)申请号 201280042344.8
(22)申请日 2012.08.28
(65)同一申请的已公布的文献号
申请公布号 CN 103858097 A
(43)申请公布日 2014.06.11
(30)优先权数据
13/223064 2011.08.31 US
(85)PCT国际申请进入国家阶段日
2014.02.28
(86)PCT国际申请的申请数据
PCT/US2012/052626 2012.08.28
(87)PCT国际申请的公布数据
WO2013/033072 EN 2013.03.07
(73)专利权人 迈可菲公司
地址 美国加利福尼亚州
(72)发明人 P.M.斯图格斯
(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 徐予红 马永利
(51)Int.Cl.
G06F 9/06(2006.01)
G06F 9/44(2006.01)
G06F 17/00(2006.01)
(56)对比文件
US 5655077 A,1997.08.05,
US 2005091213 A1,2005.04.28,
US 2010132019 A1,2010.05.27,
US 2002112062 A1,2002.08.15,
CN 101167304 A,2008.04.23,
审查员 魏兰

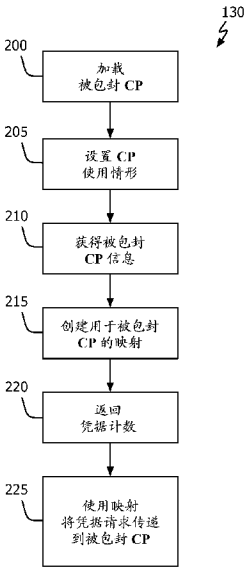
权利要求书3页 说明书8页 附图6页

(54)发明名称

封装其它凭据提供者的凭据提供者

(57)摘要

本文中描述了用于在单个包封CP内封装多个基于Windows®的凭据提供者(CP)的系统、方法和计算机可读媒体。通常,来自两个或更多个被封装或包封CP的CP凭据和字段可以这样的方式枚举和聚集使得保持来自每个CP的字段的顺序,识别并只呈现一次只可使用一次的字段,以及赋予字段新的唯一字段标识符。所有此类字段的联合(减去任何仅一次使用字段的复本)可用于生成映射,以便包封CP和CP凭据可将来自操作系统的登录接口的调用"传递"到正确的被包封CP和CP凭据。公开的技术提供例如可用于其中可使用多个登记凭据(例如,用户名/密码和智能卡PIN)的单点登记功能性。



CN 103858097 B

1.一种可编程装置,包括:

一个或多个可编程处理单元;

存储器,耦合到所述一个或多个可编程处理单元,在所述存储器上存储有指令,所述指令包含当执行时促使所述一个或多个可编程处理单元进行以下操作的指令:

对于多个原始凭据提供者创建包封凭据提供者,其中每个原始凭据提供者具有特定数量的凭据、字段的有序列表,其中每个字段具有原始凭据提供者特定标识符,并且每个字段具有描述符;

指派唯一提供者索引到所述多个原始凭据提供者的每个原始凭据提供者;

从来自每个原始凭据提供者的字段的有序列表生成映射列表,其中在所述映射列表中保持来自单个原始凭据提供者的字段的顺序;

识别所述映射列表中的仅一次使用字段;

指派唯一标识符到所述映射列表中每个仅一次使用字段的第一实例;

为所述映射列表中仅一次使用字段的每个随后实例指派与指派到所述映射列表中所述仅一次使用字段的第一实例相同的唯一标识符;以及

指派唯一标识符到所述映射列表中每个非仅一次使用字段。

2.如权利要求1所述的可编程装置,其中在执行时促使所述一个或多个可编程处理单元对于多个原始凭据提供者创建包封凭据提供者的指令包括在执行时促使所述一个或多个可编程处理单元基于原始凭据提供者的静态列表对于所述多个原始凭据提供者创建所述包封凭据提供者的指令。

3.如权利要求1所述的可编程装置,其中在执行时促使所述一个或多个可编程处理单元对于多个原始凭据提供者创建包封凭据提供者的指令包括在执行时促使所述一个或多个可编程处理单元基于原始凭据提供者的运行时标识对于所述多个原始凭据提供者创建所述包封凭据提供者的指令。

4.如权利要求1所述的可编程装置,其中所述指令还包括在执行时促使所述一个或多个可编程处理单元执行以下操作的指令:

从所述多个原始凭据提供者的每个原始凭据提供者获得指示每个原始凭据提供者的指定数量的凭据的数目;以及

将来自所述多个原始凭据提供者的每个原始凭据提供者的所述数目相加以确定凭据的总数。

5.如权利要求4所述的可编程装置,其中所述指令还包括在执行时促使所述一个或多个可编程处理单元执行以下操作的指令:

为登录接口过程提供指派到所述映射列表中字段的唯一标识符的数量;以及

为所述登录接口过程提供凭据的总数。

6.如权利要求1所述的可编程装置,其中所述指令还包括在执行时促使所述一个或多个可编程处理单元为登录接口过程提供足以使所述登录接口过程在显示装置上的单个窗口中显示多个块片的信息的指令。

7.如权利要求6所述的可编程装置,其中所述指令还包括在执行时促使所述一个或多个可编程处理单元执行以下操作的指令:

接收来自所述登录接口过程的对用于具有指定索引值的字段的字段描述符的请求;

识别所述映射列表中具有等于所述指定索引值的唯一标识符的条目；

基于所述映射列表中的所述条目，获得所述字段描述符；以及

为所述登录接口过程提供所述字段描述符。

8.如权利要求6所述的可编程装置，其中所述指令还包括在执行时促使所述一个或多个可编程处理单元执行以下操作的指令：

接收来自所述登录接口过程的更新具有字段标识符的字段的请求；

基于所述请求识别所述多个原始凭据提供者之一；

基于所述映射列表中的条目，识别用于所述一个原始凭据提供者的字段描述符的凭据提供者特定标识符；以及

向所述一个原始凭据提供者发送更新所述一个原始凭据提供者中由所述凭据提供者特定标识符识别的字段的请求。

9.如权利要求1所述的可编程装置，其中在执行时促使所述一个或多个可编程处理单元生成映射列表的指令包括在执行时促使所述一个或多个可编程处理单元在存储器中生成多个列表的指令。

10.一种用于控制计算机登录环境的方法，包括：

使用处理器对于多个原始凭据提供者创建包封凭据提供者，其中每个原始凭据提供者具有特定数量的凭据、字段的有序列表，其中每个字段具有原始凭据提供者特定标识符，并且每个字段具有描述符；

使用所述处理器指派唯一提供者索引到所述多个原始凭据提供者的每个原始凭据提供者；

使用所述处理器从来自每个原始凭据提供者的字段的有序列表生成映射列表，其中在所述映射列表中保持来自单个原始凭据提供者的字段的顺序；

使用所述处理器识别所述映射列表中的仅一次使用字段；

使用所述处理器指派唯一标识符到所述映射列表中每个仅一次使用字段的第一实例；

使用所述处理器为所述映射列表中仅一次使用字段的每个随后实例指派与指派到所述映射列表中所述仅一次使用字段的第一实例相同的唯一标识符；以及

使用所述处理器指派唯一标识符到所述映射列表中每个非仅一次使用字段。

11.如权利要求10所述的方法，其中对于多个原始凭据提供者创建包封凭据提供者的动作包括基于原始凭据提供者的静态列表对于所述多个原始凭据提供者创建所述包封凭据提供者。

12.如权利要求10所述的方法，其中对于多个原始凭据提供者创建包封凭据提供者的动作包括基于原始凭据提供者的运行时标识对于所述多个原始凭据提供者创建所述包封凭据提供者。

13.如权利要求10所述的方法，还包括：

使用所述处理器从所述多个原始凭据提供者的每个原始凭据提供者获得指示每个原始凭据提供者的指定数量的凭据的数目；以及

使用所述处理器将来自所述多个原始凭据提供者的每个原始凭据提供者的所述数目相加以确定凭据的总数。

14.如权利要求13所述的方法，还包括：

使用所述处理器为登录接口过程提供指派到所述映射列表中字段的唯一标识符的数量;以及

使用所述处理器为所述登录接口过程提供凭据的总数。

15.如权利要求10所述的方法,还包括使用所述处理器为登录接口过程提供足以使所述登录接口过程在显示装置上的单个窗口中显示多个块片的信息。

16.如权利要求15所述的方法,还包括:

使用所述处理器接收来自所述登录接口过程的对用于具有指定索引值的字段的字段描述符的请求;

使用所述处理器识别所述映射列表中具有等于所述指定索引值的唯一标识符的条目;

使用所述处理器,基于所述映射列表中的条目,获得所述字段描述符;以及

使用所述处理器为所述登录接口过程提供所述字段描述符。

17.如权利要求15所述的方法,还包括:

使用所述处理器接收来自所述登录接口过程的更新具有字段标识符的字段的请求;

使用所述处理器,基于所述请求识别所述多个原始凭据提供者之一;

使用所述处理器,基于所述映射列表中的条目,识别用于所述一个原始凭据提供者的字段描述符的凭据提供者特定标识符;以及

使用所述处理器,向所述一个原始凭据提供者发送更新所述一个原始凭据提供者中由所述凭据提供者特定标识符识别的字段的请求。

18.如权利要求10所述的方法,其中生成映射列表的动作包括在存储器中生成多个列表。

19.如权利要求10所述的方法,其中所述处理器包括多个可编程处理单元。

20.一种计算机系统,包括:

显示器;

存储器,以通信方式耦合到所述显示器;以及

可编程处理单元,以通信方式耦合到所述存储器,所述存储器存储用于促使所述可编程处理单元执行如权利要求11所述的方法的指令。

21.如权利要求20所述的计算机系统,其中所述计算机系统包括便携式计算机系统。

22.如权利要求20所述的计算机系统,其中所述计算机系统还包括以通信方式耦合到所述存储器和所述可编程处理单元的网络接口。

封装其它凭据提供者的凭据提供者

技术领域

[0001] 本公开内容一般涉及自动化登录过程领域。更具体但非限制性地说，它涉及用于在共同凭据提供者对象内包封多个凭据提供者的技术。

背景技术

[0002] 在使用Microsoft Windows XP®或Windows Server® 2003操作系统的计算机系统启动期间，Winlogon可执行文件加载并且执行图形标识和鉴权(GINA)动态链接库(DLL)。(WINDOWS XP和WINDOWS SERVER是Microsoft 股份有限公司的注册商标。) 一旦加载后，GNINA便提供可自定义用户标识和鉴权过程，并且负责渲染(rendering)登录操作/过程的图形方面。

[0003] 通过使用GINA，软件开发人员能够通过确保在其它GINA的加载和执行之前加载和执行其定制的GINA，定制登录过程用户体验。软件开发人员也能够通过利用称为“GINA链”的技术，“再使用”以前开发的登录功能性的功能性。由于存在必须调用的第一或“排头”GINA，并且通过其可提供所有其它GINA，因此，GINA链是可能的；链式的GINA形成分层结构。

[0004] 从Windows Vista®中开始，LogonUI过程变得负责渲染登录窗口的图形方面，而全部登录过程通过凭据提供者(CP)的使用进行调和。(WINDOWS VISTA是Microsoft 股份有限公司的注册商标。) 要在此新环境中输送GINA链提供的功能性，需要有“排头”CP。然而，Windows Vista和Windows 7的登录体系结构使得所有注册CP是彼此的对等体；不存在必须调用并且通过其可传递通信到其它CP的“排头”CP。Microsoft提供有关在称为“包封”的过程中一个CP能够如何调用和再使用/扩展正好一个其他CP的功能性的指导。也就是说，Microsoft允许仅一个CP的封装或包封。因此，即使只允许一个CP在登录时在活动状态(因此必须使用它) - 它只能够是一个其他CP的排头CP。在此类设置中，GINA链的全部功能性不可能实现。有鉴于此，提供允许一个CP同时封装或包封两个或更多个其它CP的机制将是有益的。

发明内容

[0005] 在一个实施例中，提供了一种在计算机登录操作期间控制用户体验的方法。方法包括创建(例如，实例化)包封凭据提供者，该凭据提供者又创建多个凭据提供者，其中，每个凭据提供者具有指定数量的凭据和字段的有序列表。另外，每个字段具有凭据提供者特定标识符和描述符。一旦创建凭据提供者，或者在凭据提供者创建期间，每个凭据提供者可指派有或获得唯一提供者索引。随后，可基于来自每个凭据提供者的字段的有序列表，生成映射列表，其中，在映射列表中保持来自单个凭据提供者的字段的顺序。识别映射列表中的仅一次使用字段，并且指派唯一标识符到每个仅一次使用字段的第一实例，为仅一次使用字段的每个随后实例指派赋予相同仅一次使用字段的第一实例的标识符。所述方法也可为登录接口过程(例如，Windows LongonUI过程)提供足够的信息，使得登录接口过程能够在显示装置上的单个窗口中显示多个块片(tile)，其中，多个被包封凭据提供者的每个凭据

提供者支持显示的块片至少之一。在另一实施例中，实现所述方法的计算机可执行程序可存储在可由计算机处理器读取和执行的任何非暂时性媒体中。此外，此类计算机处理器和计算机可执行程序可在计算机系统中体现。此类计算机系统可以是独立系统，或者它可以耦合到通信网络。

附图说明

[0006] 图1A和1B以流程图形式示出根据一个实施例的单点登记(single sign-on)操作。

[0007] 图2以流程图形式示出根据一个实施例的凭据提供者包封操作。

[0008] 图3以流程图形式示出根据一个实施例的字段映射操作。

[0009] 图4以框图形式示出根据一个实施例的计算机网络。

[0010] 图5以框图形式示出可用于实现根据本公开的一个或多个操作的说明性计算机系统。

具体实施方式

[0011] 本公开涉及用于在单个“包封”凭据提供者(CP)对象内包封或在功能上封装多个基于Windows®的凭据提供者(CP)的系统、方法和计算机可读媒体。(WINDOWS是Microsoft股份有限公司的注册商标。) 概括而言，公开了其中单个CP对象实例识别、枚举和分类来自两个或更多个其它CP的字段的技术，以便这些“被包封”CP凭据的每个凭据“属于”包封CP并且能够由包封CP控制，并且可在共同显示窗口中显示和由用户以与其“解封”操作一致的方式选择。更具体地说，可枚举来自两个或更多个CP的字段，并且识别仅可使用一次的那些字段。所有此类字段的联合(减去仅可使用一次的那些字段的复本)可用于生成映射，以便包封CP可将调用从例如操作系统的登录接口“传递”到正确的被包封CP(例如，Windows Vista和Windows 7中的LongonUI)。在本文中使用时，短语“包封CP”或“被包封CP”指包含两个或更多个其它凭据提供者的功能性的凭据提供者。类似地，短语“被包封CP”指其功能性已包含在包封CP内的CP。

[0012] 在单个CP内提供多个CP功能性的另一方案是单点登记(SSO)能力的一些提供者采用的方案，是创建将所有目标CP的功能性编码的单个CP(最重要CP(über alles CP))。使用此方案的实现通常必须将其能力要包含在最重要CP(例如，Microsoft智能卡CP)内的每个CP的行为“反向工程”。这不但是个困难的任务，而且从软件管理的角度而言是一个难以维护的任务。将现有CP反向工程的任务可特别困难，这是因为单个CP能够供应多个异类凭据，并且控制何时显示它们。本文中描述的方案避免了这些困难。

[0013] 在下面的描述中，为便于解释，陈述了许多特定细节以便提供本发明概念的详尽理解。作为此描述的一部分，本公开的一些附图以框图形式表示结构和装置以便避免混淆本发明。因此，应理解的是，对无相关联标识符的编号附图元素的引用(例如，900)指带有标识符的附图元素的所有实例(例如，900a和900b)。另外，在本公开中使用的语言主要选择用于实现可读性和指导目的，并且可未选择以描述或限定发明性主题，借助于确定此类发明性主题需要的权利要求。说明书对“一个实施例”或“实施例”的引用指结合该实施例描述的特定特性、结构或特征包括在本发明的至少一个实施例中，并且对“一个实施例”或“一实施例”的多次引用不应理解为必需全部引用相同实施例。

[0014] 将领会的是，在任何实际实现的开发中(如在任何开发项目中一样)，必须做出许多决定以实现开发人员的特定目标(例如，符合系统和业务有关约束)，并且这些目的将从一个实现到另一实现不同。也将领会的是，此类开发工作可能复杂并耗时，但仍然会是从本公开受益的计算机数据保护领域技术人员进行的日常工作。

[0015] 本文中将描述公开系统、方法和计算机可读媒体的实施例，这是因为它们可用于为Windows Vista和Windows 7操作系统(OS)提供SSO能力。例如，为实现SSO功能性，可包封密码和智能卡CP。在另一实施例中，SSO功能性也可包括指纹CP的使用。在一些实施例中，可静态(例如，通过用户设置或系统文件，例如Windows注册表文件)确定要包封的CP。在其它实施例中，可动态确定(即，在运行时)被包封CP的标识。在还有的其它实施例中，可静态确定一些被包封CP，并且可动态确定其它被包封CP。

[0016] 例如，以下描述教导将CP包封技术包含到来自McAfee有限公司的端点加密产品(通常，McAfee端点加密产品使用预引导鉴权过程提供完全磁盘加密和数据保护)。另一说明性使用能够是通过在现有例如用于特定凭据提供者的凭据上放置图像，将公开的技术用于产品“品牌标示”。在仍有的另一实施例中，基于例如时间、系统策略或谁已使用“第一”凭据登录到系统，可限制可用于登录的Windows凭据。

[0017] 参照图1A，在加载计算机系统的预引导OS时可开始根据一个实施例的SSO系统设置操作100(方框105)。也如本领域技术人员认识到的一样，可通过计算机系统的BIOS或引导固件提供预引导环境以提供在计算机系统的操作系统外部的安全环境。在预引导期间，用户可登录到目标系统上利用本文中所述包封技术的应用(例如，端点加密)(方框110)。预引导完成时，可启动Windows OS(方框115)。在Windows启动期间，LogonUI过程加载多个CP过滤器 - 一般情况下每个注册的CP一个(方框120)。在Windows Vista和Windows 7中，LogonUI过程实现在要求用户登录到本地机器时示出的图形用户接口。与包封CP相关联的过滤器可配置成使得它阻止加载除包封CP外的所有CP(方框125)。一旦加载后，包封CP便加载两个或更多个其它CP(方框130)。在一个实现中，要包封的CP的列表可与字段的标识符一起提供以用于SSO“秘密”(例如，分别在密码和智能卡CP中的密码和PIN字段标识符)。另一实现能够动态发现要包封的CP(例如，在运行时通过“.ini”或系统注册表文件)。如果用户的登录凭据(例如，密码或智能卡PIN)已知(方框135的“是”分叉)，则操作100在图1B中的方框140继续。如果用户的凭据不可用(方框135的“否”分叉)，则操作100在图1B的方框150继续。

[0018] 现在参照凭据可用情况下的图1B，包封CP将那些凭据传递到被包封CP，并且请求它使用那些凭据使用户登录(方框140)。接收/被包封CP正常执行以完成请求的任务。如果登录成功(方框145的“是”分叉)，则操作100在方框165继续(在下面讨论)。如果登录不成功(方框145的“否”分叉)，则LogonUI过程显示被包封CP的块片(方框150)。术语“块片”以其习惯性意义使用，并且指凭据的视觉表示，通常呈现为LogonUI窗口内的图标或小图像。在Windows环境中，每个块片/凭据后面是CP凭据对象，由CP创建，并且实现ICredentialProviderCredential接口。要注意的是，一个CP可创建多个块片。

[0019] 用户可选择块片，这随后造成调用块片的相关联CP。如果在选择显示的块片之一后，用户未能成功登录(方框155的“否”分叉)，则操作100返回到方框150。如果用户成功登录到目标系统(方框155的“是”分叉)，则用户的“秘密”被以安全的方式捕捉和存储(方框

160)。在一个实施例中,用户的秘密能够是其用户名和密码。在另一实施例中,用户的秘密能够是智能卡的PIN标识符。例如,用户的名称和/或密码可在McAfee端点加密应用内以加密形式存储。在成功登录后,在主机的操作系统中启动用户的会话(方框165)。

[0020] 将认识到的是,SSO操作100提供到Windows的自动化登录,但未去除如方框110中所述用户最初登录到包封应用的要求。在操作100的上下文中,用户体验是一旦它们成功登录到在预引导期间加载的应用(例如,端点加密),则该应用在启动期间将其登录凭据传递到Windows OS - 结果是用户自动登录到Windows中。

[0021] 参照图2,通过加载为包封识别的那些CP,开始根据方框130的包封操作(方框200)。例如,在Windows环境中,根据方框200的动作创建被包封CP COM对象的集合。一旦加载后,用于被包封CP的使用情形便可设成例如登录或解锁(方框205)。包封CP随后可查询每个被包封CP以获得凭据的数量和与其各自相关联的字段(方框210)。如下面更详细所述,包封CP使用此信息生成一个或多个映射表(方框215)。在被要求时,包封CP将总凭据计数传递到LogonUI过程(方框220)。实际上,每个被包封CP生成其自己的凭据(一个或多个),将它们传递回包封CP。包封CP随后将每个凭据返回到LogonUI过程。此信息允许LogonUI显示被包封CP的凭据,好象被包封CP实际上在活动状态(即,未被包封)。

[0022] 包封CP使用根据方框215生成的映射信息以充当在LogonUI过程与每个被包封CP之间的中间人(方框225)。也就是说,用户选择在显示的登录窗口中显示的块片时,包封CP使用一个或多个映射表(或列表),以便用户的动作可转发到适当的被包封CP。

[0023] 参照图3,映射操作215识别要包封的第一CP,并且确定其凭据中的每个包含的字段数量,随后枚举通过每个字段以获得其相关联的字段描述符(方框300)。在Windows环境中,字段描述符可包含字段的字段标识符和字段类型。说明性字段包括标签(例如,在编辑框旁的提示符)、编辑框(例如,通过其可输入用户数据的字段,如用户名或密码)、复选框和单选按钮。已确定的是,一些CP字段只能够在实现ICredentialProvider接口的CP中出现一次;即,与LogonUI过程交互(例如,包封CP)。在Windows Vista和Windows 7环境内,这类仅一次使用字段包括类型CPFT_SUBMIT_BUTTON和CPFT_TILE_IMAGE的字段。相应地,可识别仅一次使用字段(方框305)。

[0024] 第一CP的字段列表可放置到包封CP的聚集字段列表中,该列表到现在已为空(方框310)。也已发现的是,在Windows环境中,在包封CP的聚集字段列表内保持单独被包封CP的字段的顺序是重要的(除对于仅一次使用字段外,参阅下述讨论)。如果当前CP不是要包封的最后CP(方框315的“否”分叉),则识别要包封的下一CP,并且如上相对于方框300所述获得其字段信息(方框320)。之后,操作215继续到方框305,其中,如果当前CP有任何仅一次使用字段,则识别当前CP的仅一次使用字段(方框305)。象以前一样,识别所有仅一次使用字段,并且从当前CP的字段列表删除以前识别的那些仅一次使用字段的复本。一旦已询问要包封的所有CP,并且在包封CP的聚集字段列表中已包括其字段(方框315的“是”分叉),则可为其聚集字段列表中的每个字段生成对包封CP唯一的新字段标识符(方框325)。此映射以此类方式进行,使得包封CP能够将其聚集字段列表(其中带有仅一次使用字段的单次出现)中的字段反向与来自来源被包封CP的字段相关;从包封CP的字段标识符(其用于与LogonUI过程进行有关字段的通信)转换回(被包封CP理解的)被包封CP的字段标识符。根据本公开,包封CP的聚集字段列表在逻辑上由来自每个被封装CP的所有字段的联合减去仅一

次使用字段的复本形成。

[0025] 在上述实施例中，包封CP实现ICredentialProvider接口并且包含被包封CP的实例。从包封CP可用的凭据的数量是从被包封CP可用的凭据的数量之和。包封CP赋予每个凭据唯一索引号，并且将此索引映射到被包封CP实例和凭据索引，从而使它能够将调用从LogonUI过程“传递”到在被包封CP的自己唯一凭据索引号的上下文中的特定被包封CP。包封CP中凭据(在特定索引号)的每个实例实现ICredentialProviderCredential接口，并且将来自被包封CP的对应凭据的实例“包封”。具体而言，包封CP的广告方法将其到ICredentialProviderCredentialEvents接口的指针包封(在其事件对象中)，并且将此对象赋予被包封CP的广告方法。(在Windows Vista和Windows 7中，CP对象的广告方法的目的是赋予CP用于异步通知LogonUI关于CP的可见UI元素的任何所需更改的机制。)在被包封CP调用LogonUI时，包封CP的事件对象使用字段映射信息(参阅上面有关图2在元素225的讨论)将字段索引号从被包封CP的上下文映射回包封CP的上下文。

[0026] 为说明一些上述操作，考虑将其凭据和字段信息在表1中示出的两个CP包封。作为初步事项，应注意的是，两个CP均利用仅一次使用字段(例如，提交按钮和图像块片)。

[0027] 表1 要包封的说明性凭据提供者

被包封 CP-1（2 个凭据）		
索引	ID	类型
0	10	标签
1	20	标签
2	30	编辑框
3	40	提交按钮
4	50	块片图像

被包封 CP-2（1 个凭据）		
索引	ID	类型
0	10	标签
1	20	编辑框
2	30	提交按钮
3	40	块片图像

[0028] 通过询问要包封的每个CP，包封CP的初始映射表可如表2中所示。要注意的是，包封CP的凭据计数是被包封CP的凭据之和。还要注意的是，CP-2列为只具有2个字段，在表1中时它示为具有4个字段。这是因为CP-2字段的两个字段是在与CP-1一起工作时先发现的仅一次使用字段。表2中的信息允许包封CP告诉LogonUI过程包封CP具有的凭据块片数量和字段数量。它也将索引与每个CP相关联(“提供者索引”)。实际上，提供者索引可以只是表2中CP条目的索引(例如，在行0的CP具有隐式提供者索引0)。因此，用于示例包封CP的聚集字段列表包含7个字段。

[0029] 表2 被包封提供者映射表

提供者	凭据数量	字段数量	CP 索引
CP-1	2	5	0
CP-2	1	2	1
总计：	3	7	

[0030] 在一个实施例中，包封CP随后生成字段索引映射表，如表3所示的字段索引映射表。此表提供为用于包封CP的用于在其聚集字段列表中每个字段（第一列）的唯一字段索引。第二列（“被包封CP索引”）通过唯一被包封CP识别每个包封CP的字段。第三列（“被包封字段索引”）将用于包封CP的聚集字段列表中每个字段的索引与被包封CP的环境中对应字段索引相关联。例如，包封CP中具有索引5的字段（第一列）与CP-2（第二列）相关联，并且CP-2的环境本身中的字段索引为0（第三列）。

表 3 包封 CP 的字段索引映射

[0031]

包封字段索引	被包封 CP 索引	被包封字段索引
0	0	0
1	0	1
2	0	2
3	0	3
4	0	4
5	1	0
6	1	1

[0032] 通过将如表4所示的仅一次使用字段考虑在内，可完成根据此实施例的映射表的生成。如图所示，带有包封CP标识符3和4的仅一次使用字段（即，提交按钮和块片图像字段）由两个被包封CP（具有被包封CP索引0的CP-1和具有被包封CP索引1的CP-2）使用。表4所示映射允许包封CP将请求按字段标识符从LogonUI过程路由到正确的被包封CP；将包封CP字段标识符转换成被包封CP的标识符。

表 4 包封 CP 到被包封 CP 字段标识符映射

仅一次使用字段

映射

[0033]

字段类型	包封字段 ID
被支持的	3
映射表格	4

包封字段 ID	被包封 CP 索引	被包封字段 ID
0	0	10
1	0	20
2	0	30
3	0	40
4	0	50
5	1	10
6	1	20
3	1	30
4	1	40

[0034] 例如，比如说LogonUI过程请求在索引5的字段描述符。使用表3(“包封CP的字段索引映射”)时，可发现请求应作为对在索引零(“0”)的字段的请求传递到CP-2(在索引1的CP)。

[0035] 在另一示例中，比如说LogonUI过程与包封凭据交互，包封凭据将来自CP-2(在索引1的CP)的凭据包封以发生字段标识符3的某个更改。使用表4(“包封CP到被包封CP字段标识符映射”)时，能够发现用于CP-2的包封CP的字段标识符3映射到被包封CP(即，CP-2)的字段标识符30。在此转换完成时，包封CP能够将请求(其识别字段标识符30)传递到CP-2的凭据。

[0036] 在还有的另一示例中，比如说LogonUI过程请求在索引2的凭据。使用表2(“被包封提供者的映射”)时，由于表1-4中的编号从“0”开始，因此，可确定此请求应传递到第三凭据。由于前两个凭据来自CP-1，因此，这必须在CP-2引导。此外，由于CP-2只具有一个凭据，因此，这必须是在CP-2的索引0的凭据。因此，在LogonUI过程请求在索引2的凭据时，包封CP将此请求传递到在CP-2的索引“0”的凭据。

[0037] 现在参照图4，其内可实现公开技术的说明性网络体系结构400包括多个网络405(即，405a、405b和405c)，每个网络可采用任何形式，包括但不限于局域网(LAN)或诸如因特网等广域网(WAN)。此外，网络405可使用任何所需技术(有线、无线或其组合)和协议(例如，传送控制协议TCP)。耦合到网络405的有能够通过网络405进行通信的数据服务器计算机410(即，410a和410b)。耦合到网络405和/或数据服务器计算机410的还有最终用户计算机415(即，415a、415b和415c)。在一些实施例中，网络体系结构410也可包括诸如打印机420等网络打印机和诸如425等存储系统。为便于在不同网络装置(例如，数据服务器410、最终用户计算机415、网络打印机420和存储系统425)之间的通信，至少一个网关或路由器430可选

择性地耦合在其之间。

[0038] 参照图5，代表性计算机系统500(例如，数据服务器410或最终用户计算机系统415)包括处理器505、随机存取存储器(RAM) 510、只读存储器(ROM) 515、存储装置520、通信接口525(用于连接到数据网络，如网络405)、用户接口适配器530及显示适配器535 - 所有这些可经系统总线或背板540耦合。用户接口适配器530可用于连接键盘545、麦克风550、指针装置555、扬声器560和诸如触摸板和/或触摸屏(未示出)等其它用户接口装置。显示适配器535可用于连接显示器565。

[0039] 处理器505可包括任何可编程控制器装置，例如包括来自Intel 股份有限公司的Intel Atom®、Core®、Pentium®、Celeron®和Intel Core®处理器系列和来自ARM的Cortex和ARM处理器系列或定制设计的状态机中的一个或多个成员。(INTEL、INTEL ATOM、CORE、PENTIUM、CELERON和INTEL CORE是Intel 股份有限公司的注册商标。CORTEX是ARM 股份有限公司的注册商标。ARM是ARM 有限公司的注册商标。) 处理器505也可实现为定制设计的状态机，并且可在诸如专用集成电路(ASIC)和现场可编程门阵列(FPGA)等硬件装置中体现。

[0040] 计算机系统500其上可驻留有任何所需操作系统。将领会的是，本文中所述技术的各种实施例可在提及的那些平台和操作系统外的之外的平台和操作系统上实现。一个实施例可使用JAVA®、C和/或C++语言或其它编程语言编写。(JAVA是美国Oracle有限公司的注册商标。)

[0041] 如本文中所述实现凭据提供者允许几个异类CP包封在包封器CP的单个实例中。这允许一个CP实例(包封器CP)注册为实现ICredentialProvider接口。另外，包封器CP能够再使用LogonUI内多个(被包封)CP的行为和凭据。本方案的益处包括但不限于：静态或动态发现要包封的CP；包封无限制数量的CP的能力；扩展被包封CP的功能性而无需在包封CP的多个实例之间传递状态的能力；以及仅要求启动一个凭据并且允许转变到被包封凭据和被包封凭据的再使用的单点登记功能。

[0042] 在不脱离以下权利要求的范围的情况下，材料、组件、电路元件及所示操作方法的细节的各种更改也是可能的。例如，公开方法可由执行组织到一个或多个程序模块中的指令的可编程控制装置(例如，处理器505)执行。程序模块可存储在任何适合的非暂时性存储器/存储装置(例如，存储器510和/或515和/或520)中。最后，要理解的是，上述描述旨在说明而不是限制。例如，上述实施例可相互组合使用。在查看上述说明后，本领域的技术人员将明白许多其它实施例。因此，本发明的范围应参照所附权利要求以及此类权利要求被授权的等同体的完全范围来确定。在随附权利要求中，术语“包括”和“其中”用作相应术语“包含”和“之中”的日常英语等同体。

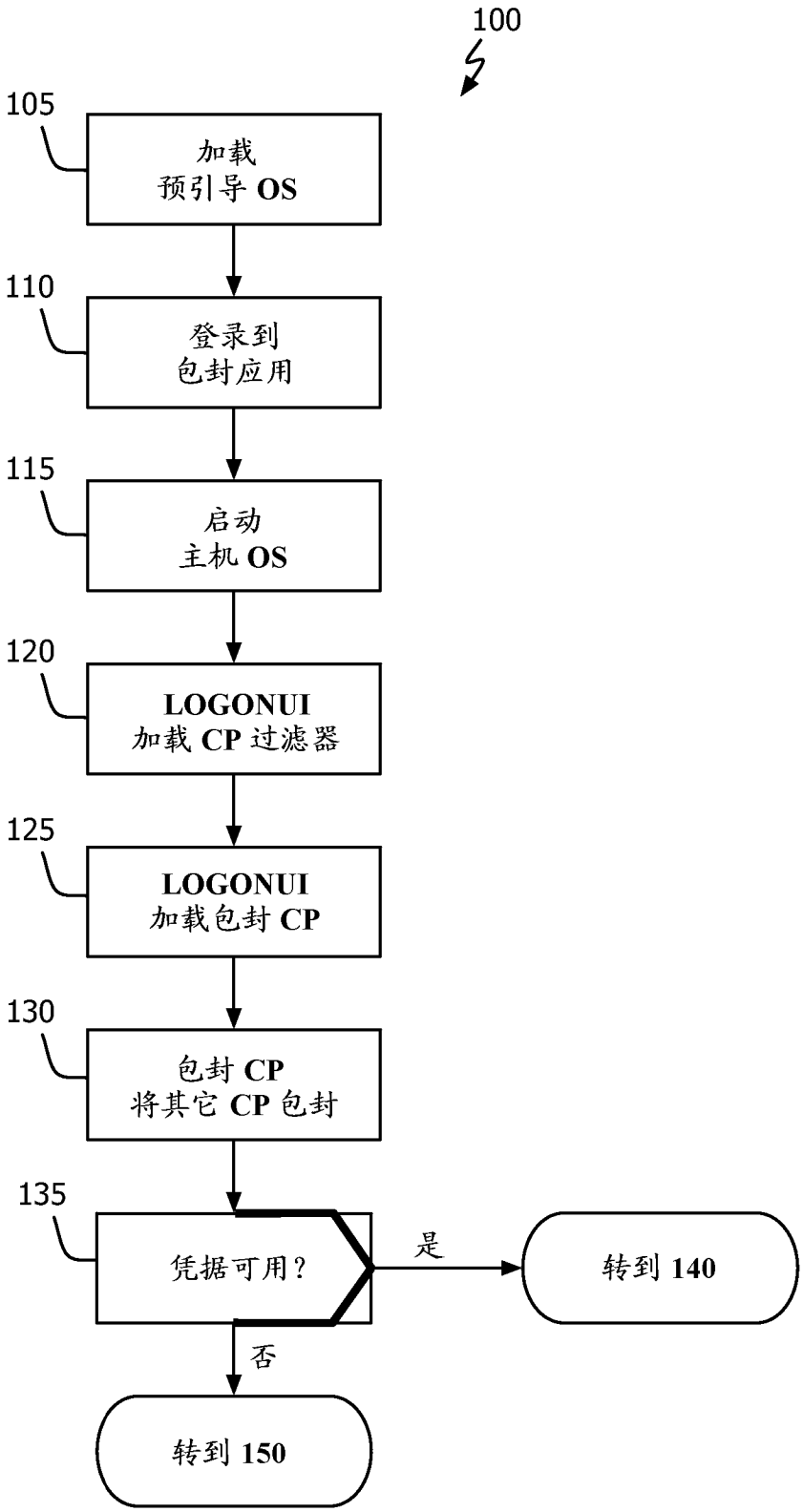

100
105
加载
预引导 OS
110
登录到
包封应用
115
启动
主机 OS
120
LOGONUI
加载 CP 过滤器
125
LOGONUI
加载包封 CP
130
包封 CP
将其它 CP 包封
135
凭据可用？
是
转到 140
否
转到 150

图 1A

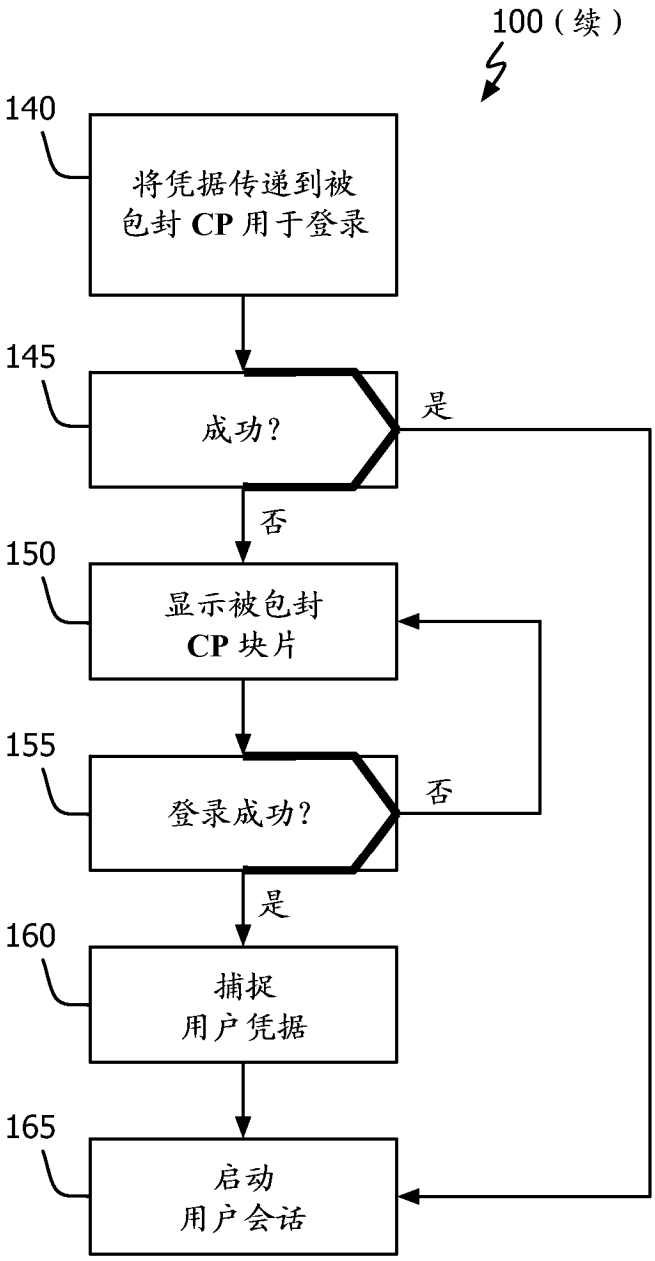

100（续）
140
将凭据传递到被包封 CP 用于登录
145
成功？
是
否
150
显示被包封 CP 块片
155
登录成功？
否
是
160
捕捉用户凭据
165
启动用户会话

图 1B

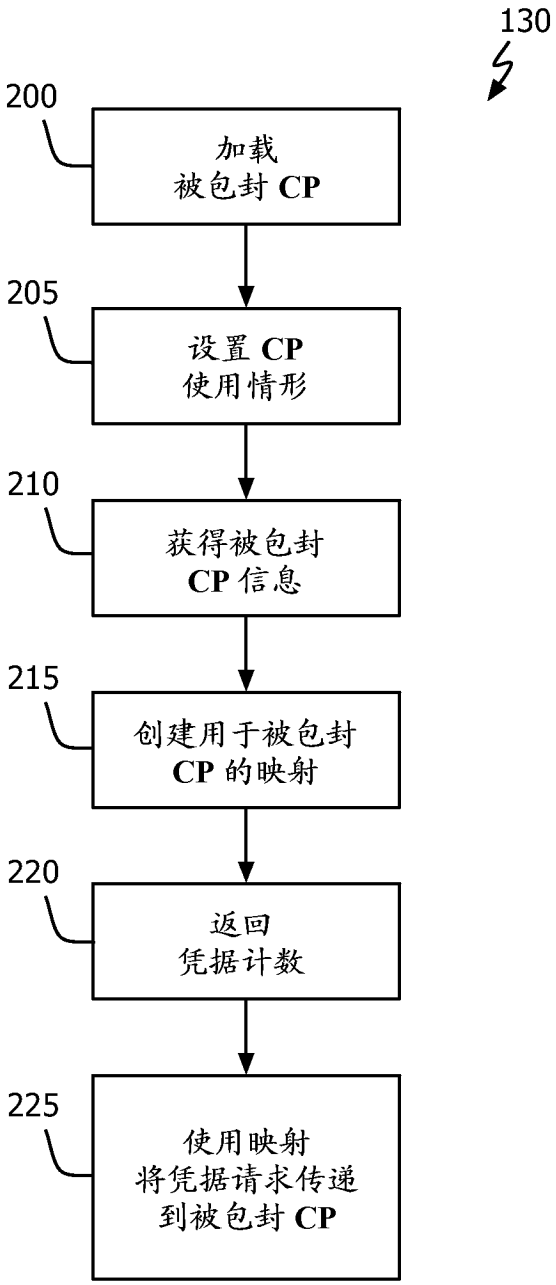

130
200
加载
被包封 CP
205
设置 CP
使用情形
210
获得被包封
CP 信息
215
创建用于被包封
CP 的映射
220
返回
凭据计数
225
使用映射
将凭据请求传递
到被包封 CP

图 2

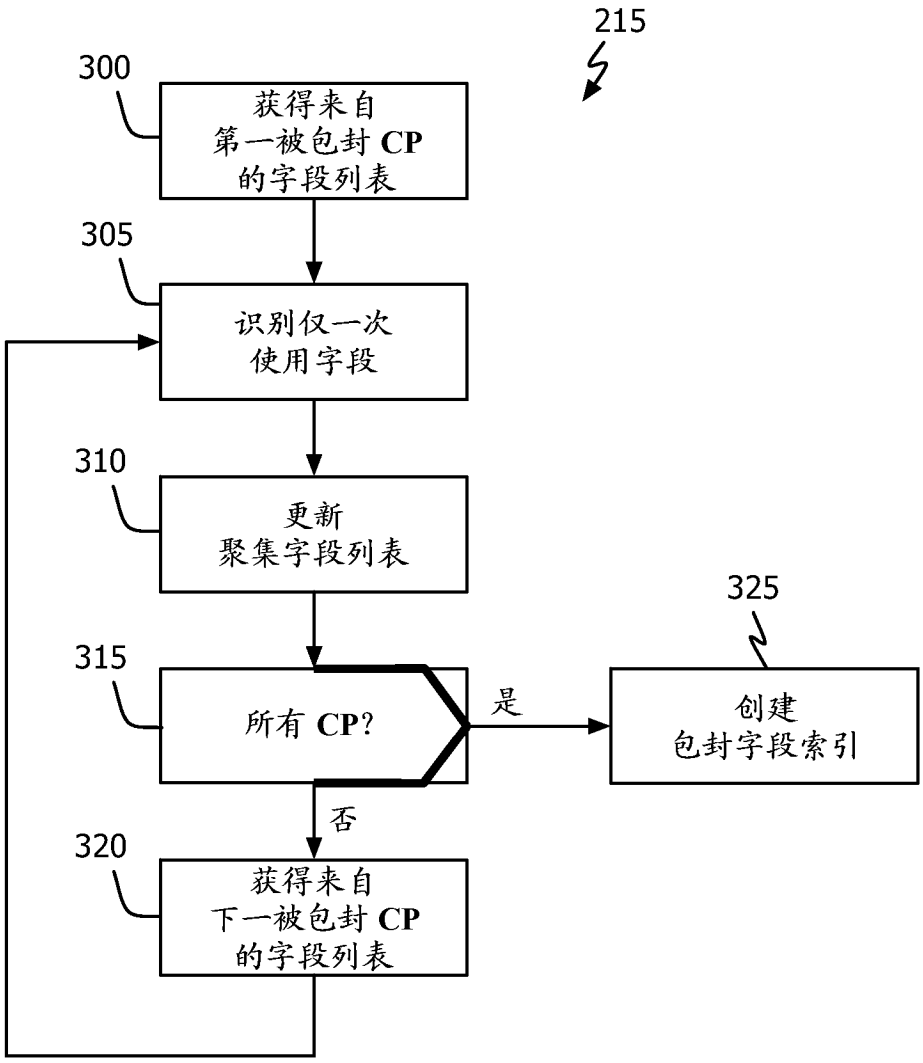

215
300
获得来自
第一被包封 CP
的字段列表
305
识别仅一次
使用字段
310
更新
聚集字段列表
315
所有 CP?
是
325
创建
包封字段索引
否
320
获得来自
下一被包封 CP
的字段列表

图 3

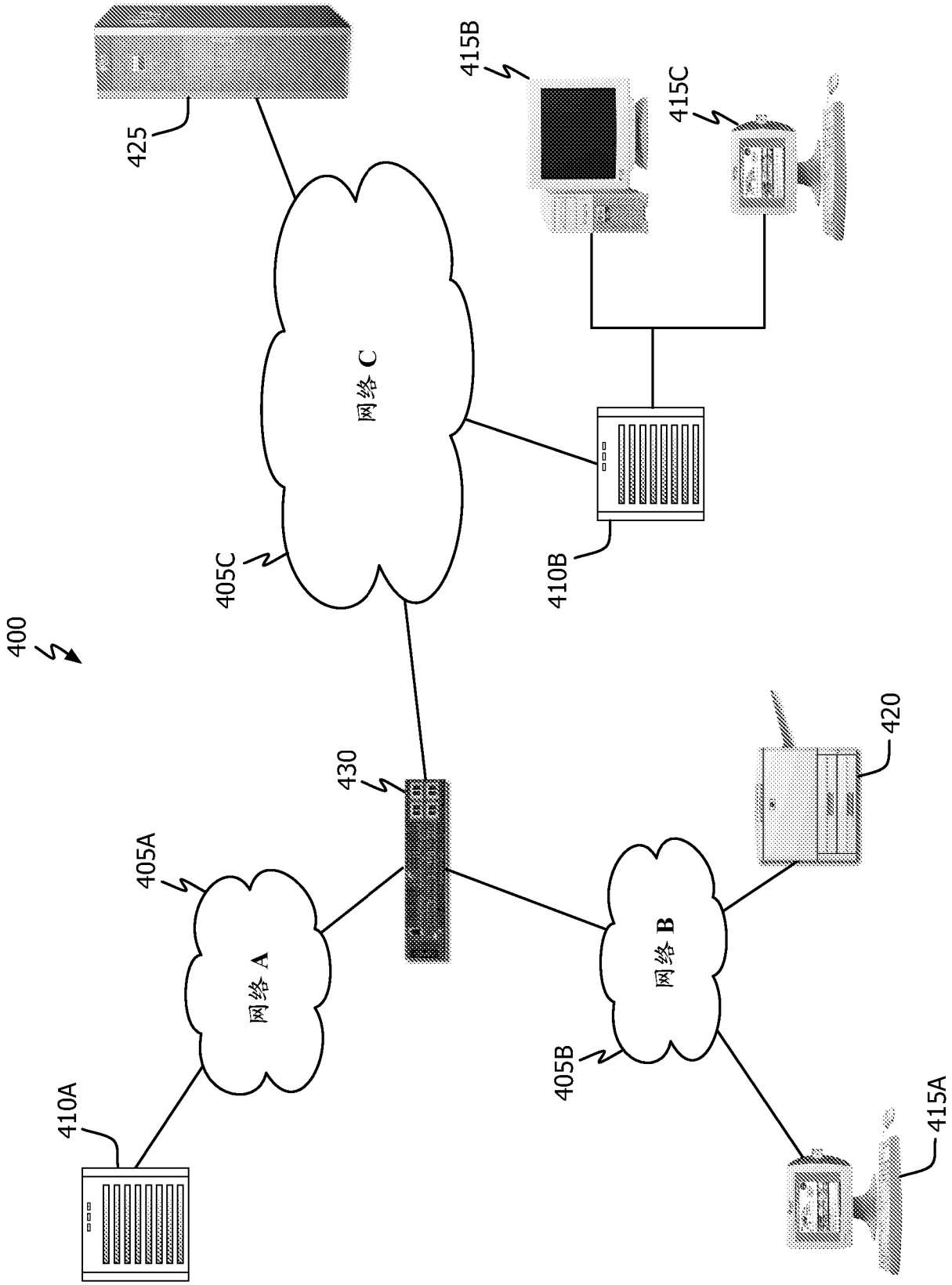

425
415B
415C
网络 C
405C
410B
400
430
420
405A
网络 A
网络 B
405B
410A
415A

图 4

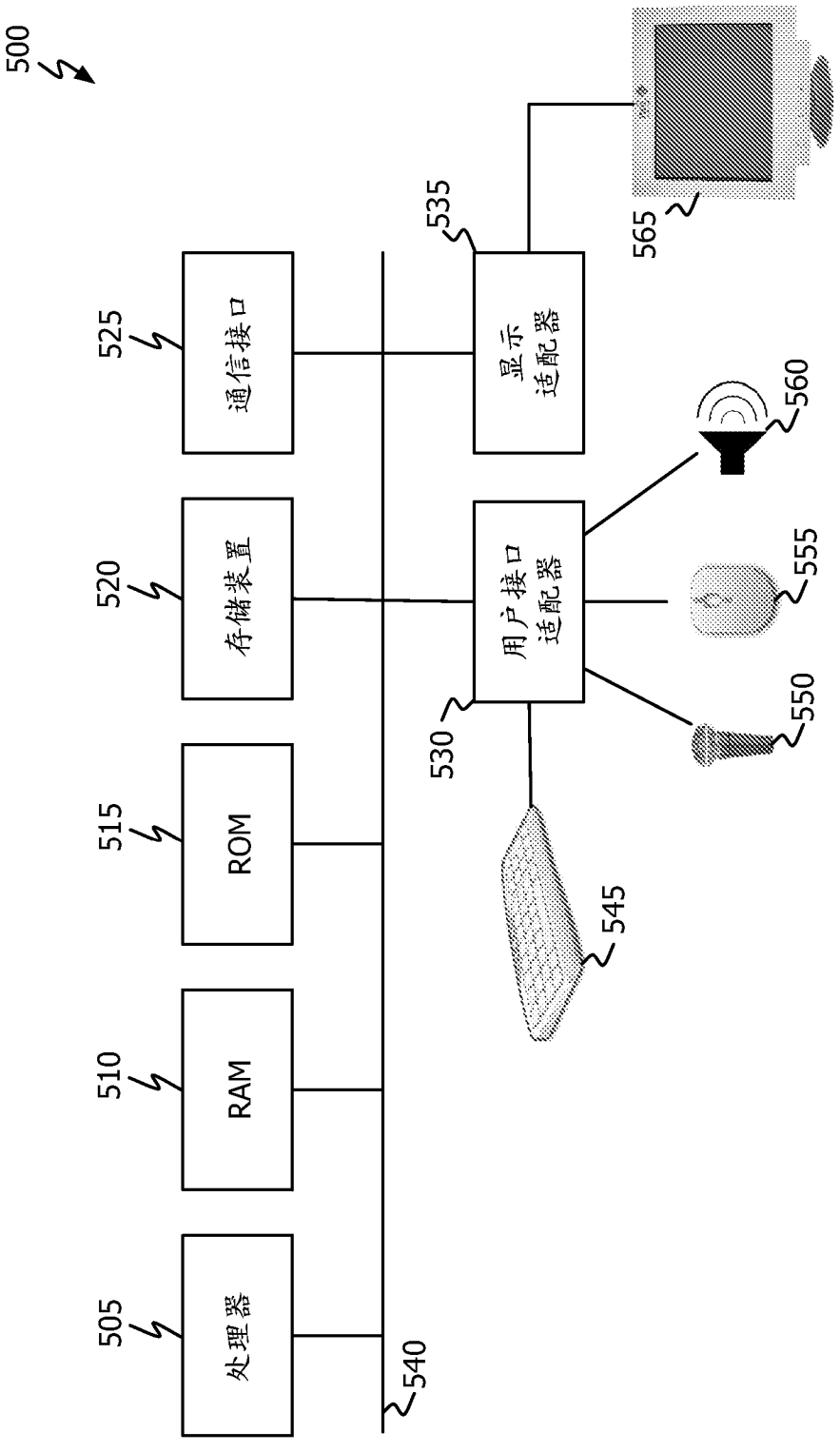

500
505
处理器
510
RAM
515
ROM
520
存储装置
525
通信接口
530
用户接口适配器
535
显示适配器
540
545
550
555
560
565

图 5