(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 104364792 B
(45)授权公告日 2017.11.14

(21)申请号 201380018421.0
(22)申请日 2013.01.30
(65)同一申请的已公布的文献号
申请公布号 CN 104364792 A
(43)申请公布日 2015.02.18
(30)优先权数据
13/363675 2012.02.01 US
13/363681 2012.02.01 US
13/363685 2012.02.01 US
13/363664 2012.02.01 US
13/363654 2012.02.01 US
(85)PCT国际申请进入国家阶段日
2014.09.30
(86)PCT国际申请的申请数据
PCT/US2013/023818 2013.01.30
(87)PCT国际申请的公布数据
WO2013/116319 EN 2013.08.08

(73)专利权人 亚马逊科技公司
地址 美国内华达州
(72)发明人 D.W.希奇科克 B.L.坎贝尔
(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 蒋骏 徐红燕

(51)Int.Cl.
G06F 21/41(2013.01)
H04L 29/06(2006.01)
(56)对比文件
US 2007/0078785 A1,2007.04.05,
US 6182131 B1,2001.01.30,
CN 101286847 A,2008.10.15,
审查员 崔成东

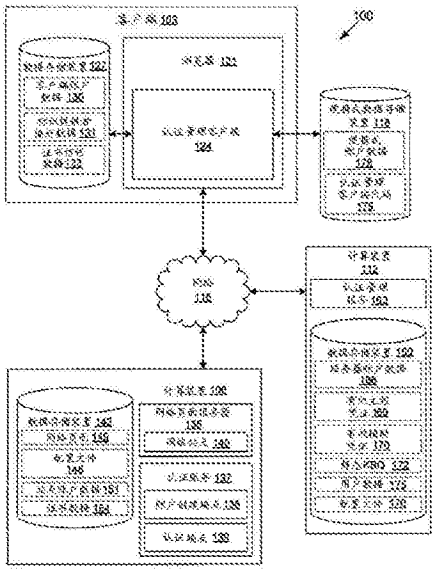
权利要求书3页 说明书37页 附图12页

(54)发明名称

用于多个网络站点的账户管理系统

(57)摘要

本发明公开了用于多个网络站点的账户管理的各种实施方案。在计算装置中维护用户的用于多个网络站点的多个账户。所述计算装置将要访问网络站点的受保护资源。响应于确定所述账户不能够访问所述受保护资源，创建新账户，或者升级现有账户。将关于所述用户的一组信息提供给所述网络站点以创建或升级所述账户。



CN 104364792 B

1.一种账户管理系统,其包括:

计算装置;以及

可在所述计算装置中执行的认证管理客户端应用程序,所述认证管理客户端应用程序包括:

维护用户的用于多个网络站点的多个账户的逻辑;

确定所述计算装置将要访问网络站点的受保护资源的逻辑;

确定所述多个账户是否能够访问所述受保护资源的逻辑;以及

响应于确定所述多个账户不能够访问所述受保护资源,受制于从用户获得对分享为创建能够访问受保护资源的新的账户所需的一组信息的同意,借助关于所述用户的所述一组信息或新提供的信息而用所述网络站点来自动创建新账户的逻辑,其中将关于所述用户的所述一组信息自动提供给所述网络站点以创建所述新账户;并且

其中,创建所述新账户的逻辑进一步包括为所述新账户自动建立安全凭证的逻辑。

2.如权利要求1所述的系统,其中所述创建所述新账户的逻辑进一步包括根据安全凭证规范自动生成用于所述新账户的安全凭证的逻辑。

3.如权利要求1所述的系统,其中所述维护所述账户的逻辑被配置来:

维护处于加密状态的与所述账户有关的数据;以及

响应于从所述用户获得的主控安全凭证对与所述账户有关的所述数据进行解密。

4.如权利要求1所述的系统,其中所述一组信息包括所述用户的姓名、所述用户的实际地址、所述用户的出生日期或所述用户的联系信息中的一个或多个。

5.如权利要求1所述的系统,其进一步包括:

确定所述用户是否具有将被所述计算装置访问的用于所述网络站点的现有账户的逻辑;以及

响应于确定所述用户具有用于所述网络站点的现有账户且所述账户不能够访问所述受保护资源而升级所述多个账户中的一个的逻辑,其中将关于所述用户的所述一组信息提供给所述网络站点以升级所述账户中的一个。

6.如权利要求5所述的系统,其中所述一组信息先前没有提供给所述网络站点用来创建所述账户中的一个。

7.如权利要求1所述的系统,其中所述受保护资源是第一受保护资源,所述认证管理客户端应用程序进一步包括:

确定所述计算装置将要访问所述网络站点的第二受保护资源的逻辑;

确定所述账户是否能够访问所述第二受保护资源的逻辑;

响应于确定所述账户能够访问所述第二受保护资源而将与所述账户中的一个相关联的所存储安全凭证自动提供给所述网络站点的逻辑;以及

从所述网络站点访问所述第二受保护资源的逻辑。

8.如权利要求1所述的系统,其进一步包括:

借助网络使用于所述账户的经加密安全凭证与认证管理服务同步的逻辑;以及

响应于确定所述账户不能够访问所述受保护资源而使用旧账户对所述网络站点进行认证的逻辑,其中从所述用户获得用于所述旧账户的至少一个安全凭证。

9.如权利要求1所述的系统,进一步包括:

根据所述网络站点的域名来识别所述多个账户中的一个的逻辑，所述多个账户中的一个与具有与所述域名不同的域名的不同网络站点相关联；以及

使用与所述账户中的一个相关联的安全凭证对所述网络站点进行自动认证的逻辑。

10.如权利要求1所述的系统，其进一步包括：

至少部分基于所述网络站点的域名和从所述网络站点获得的所支持的第三方认证提供者的列表而识别被所述网络站点接受的多个所述账户以便对所述受保护资源进行认证的逻辑；

使得显示被配置来获得对多个所述账户中的一个的用户选择的用户界面的逻辑；

存储对与所述网络站点的所述域名相关联的多个所述账户中的一个的所述用户选择的逻辑；以及

使用与多个所述账户中通过所述用户选择所选择的一个账户相关联的安全凭证对所述网络站点进行自动认证的逻辑。

11.如权利要求1所述的系统，其进一步包括：

向认证管理服务发送对账户数据的请求的逻辑，所述请求指定用于访问所述账户数据的安全凭证，所述账户数据包括用户用于访问所述多个网络站点的多个安全凭证；

响应于对所述账户数据的所述请求而从所述认证管理服务获得所述账户数据的逻辑；

获得主控安全凭证的逻辑；

使用所述主控安全凭证对所述账户数据进行解密的逻辑；以及

将所述安全凭证中的每一个自动重置为相应的新安全凭证的逻辑。

12.如权利要求1所述的系统，其进一步包括：

维护用于所述用户的用于所述多个网络站点的所述多个账户的账户数据的逻辑，所述账户数据包括用于所述账户中的每一个的相应安全凭证；

响应于所述用户访问所述多个所述网络站点中的每一个而使用相应的多个所述账户来对与多个所述网络站点对应的多个认证服务进行自动认证的逻辑，其中为所述网络站点中的每一个建立相应会话；

确定将要执行注销的逻辑；以及

通过结束所述会话中的每一个而执行所述注销的逻辑。

13.一种账户管理系统，其包括：

至少一个计算装置；以及

可在所述至少一个计算装置中执行的认证服务，所述认证服务包括：

借助认证协议从在第一客户端计算装置中执行的第一认证管理客户端获得第一认证请求的逻辑，所述第一认证请求指定与第一用户账户相关联的第一安全凭证；

响应于所述第一认证请求而在所述第一客户端计算装置处对所述第一用户账户进行认证以便访问网络站点的至少一个受保护资源的逻辑；

借助所述认证协议从在第二客户端计算装置中执行的第二认证管理客户端获得第二认证请求的逻辑，所述第二认证请求指定与第二用户账户相关联的第二安全凭证；以及

响应于所述第二认证请求而在所述第二客户端计算装置处对所述第二用户账户进行认证以便访问所述网络站点的所述至少一个受保护资源的逻辑，

其中所述第一认证管理客户端和所述第二认证管理客户端是由认证管理服务的不同

提供者部署，并且受制于用户对分享为创建能够访问至少一个受保护资源的第一用户账户或第二用户账户所需的信息的同意，由所述第一认证管理客户端和所述第二认证管理客户端提供所述认证请求，并且

其中，为能够访问所述至少一个受保护资源的第一用户账户或第二用户账户自动建立安全凭证。

14.如权利要求13所述的系统，其进一步包括：

至少部分基于所述第一认证管理客户端的密切度来确定是否支持所述第一认证管理客户端的逻辑；以及

响应于所述第一认证请求且响应于支持所述第一认证管理客户端而在所述第一客户端计算装置处对所述第一用户账户进行认证以便访问所述网络站点的所述至少一个受保护资源的逻辑。

15.如权利要求13所述的系统，其中所述第一认证管理客户端被配置来：

响应于从用户获得主控安全凭证对由所述第一认证管理客户端所存储的与所述第一用户账户相关联的所述第一安全凭证进行解密；

使用所述第一认证管理客户端借助所述认证协议将所述第一认证请求发送给与所述网络站点的所述至少一个受保护资源相关联的所述认证服务，所述第一认证请求指定与所述第一用户账户相关联的所述第一安全凭证；

在响应于所述第一认证请求而被所述认证服务认证之后访问所述至少一个受保护资源；以及

将所述第一安全凭证从所述第一认证管理客户端导入到在所述第一客户端计算装置中执行的第三认证管理客户端中。

16.如权利要求13所述的系统，其进一步包括：

存储包括与用户的多个网络站点相关联的多个安全凭证的账户数据的逻辑，所述账户数据以加密形式来存储；

从第三客户端获得对所述账户数据的请求的逻辑，所述请求指定用于访问所述账户数据的第三安全凭证；以及

响应于确定所述第三客户端对应于预先授权的客户端且响应于确定用于访问所述账户数据的所述第三安全凭证是有效的而向所述第三客户端发送所述账户数据的逻辑。

17.如权利要求13所述的系统，其进一步包括：

在认证之后获得更换用于所述第一用户账户的所述第一安全凭证的请求的逻辑，所述更换所述第一安全凭证的请求是在所述第一认证管理客户端中自动发出；以及

响应于所述更换所述第一安全凭证的请求而建立用于所述第一用户账户的新安全凭证的逻辑。

18.如权利要求13所述的系统，其进一步包括：

在认证之后从所述第一认证管理客户端获得账户升级请求的逻辑，所述账户升级请求指定关于用户的一组信息；

根据所述账户升级请求来升级所述第一用户账户的逻辑；以及

在升级之后在所述第一客户端计算装置处对所述第一用户账户进行认证以便访问所述网络站点的另一受保护资源的逻辑。

用于多个网络站点的账户管理系统

[0001] 相关申请的交叉引用

[0002] 本申请请求以下各案的优先权和利益:2012年2月1日提交的发明名称为“用于多个网络站点的账户管理(ACCOUNT MANAGEMENT FOR MULTIPLE NETWORK SITES)”的美国专利申请第13/363,654号;2012年2月1日提交的发明名称为“认证管理服务(AUTHENTICATION MANAGEMENT SERVICES)”的美国专利申请第13/363,664号;2012年2月1日提交的发明名称为“向网络站点呈现受管理的安全凭证(PRESENTING MANAGED SECU RITY CREDENTIALS TO NETWORK SITES)”的美国专利申请第13/363,675号;2012年2月1日提交的发明名称为“受管理的安全凭证的恢复(RECOVERY OF MANAGED SECURITY CREDENTIALS)”的美国专利申请第13/363,681号;以及2012年2月1日提交的发明名称为“从多个网络站点注销(LOGOUT FROM MULTIPLE NETWORK SITES)”的美国专利申请第13/363,685号,上述各案以全文引用的方式并入本文中。

技术领域

[0003] 本发明涉及一种账户管理系统,其包括计算装置。

背景技术

[0004] 许多网站要求用户用用户名和密码登录,使得可以安全地识别用户。然而,用户经常会忘记他们需要用来登录到网站的用户名和/或密码。用户通常还会将相同的用户名和/或密码用于多个网站。管理数十或甚至数百用户名和密码是用户苦恼的主要原因且导致过大的放弃率,其中如果新服务需要新账户,那么用户完全无法注册新服务。

发明内容

[0005] 根据本发明的一种账户管理系统,其包括:计算装置;以及可在所述计算装置中执行的认证管理客户端应用程序,所述认证管理客户端应用程序包括:维护用户的用于多个网络站点的多个账户的逻辑;确定所述计算装置将要访问网络站点的受保护资源的逻辑;确定所述多个账户是否能够访问所述受保护资源的逻辑;以及响应于确定所述多个账户不能够访问所述受保护资源,受制于从用户获得对分享为创建能够访问受保护资源的新的账户所需的一组信息的同意,借助关于所述用户的所述一组信息或新提供的信息而用所述网络站点来自动创建新账户的逻辑,其中将关于所述用户的所述一组信息自动提供给所述网络站点以创建所述新账户;并且其中,创建所述新账户的逻辑进一步包括为所述新账户自动建立安全凭证的逻辑。所述的系统中,所述创建所述新账户的逻辑进一步包括根据安全凭证规范自动生成用于所述新账户的安全凭证的逻辑。所述维护所述账户的逻辑被配置来:维护处于加密状态的与所述账户有关的数据;以及响应于从所述用户获得的主控安全凭证对与所述账户有关的所述数据进行解密。所述一组信息包括所述用户的姓名、所述用户的实际地址、所述用户的出生日期或所述用户的联系信息中的一个或多个。所述的系统进一步包括:确定所述用户是否具有将被所述计算装置访问的用于所述网络站点的现有账

户的逻辑；以及响应于确定所述用户具有用于所述网络站点的现有账户且所述账户不能够访问所述受保护资源而升级所述多个账户中的一个的逻辑，其中将关于所述用户的所述一组信息提供给所述网络站点以升级所述账户中的一个。所述一组信息先前没有提供给所述网络站点用来创建所述账户中的一个。所述受保护资源是第一受保护资源，所述认证管理客户端应用程序进一步包括：确定所述计算装置将要访问所述网络站点的第二受保护资源的逻辑；确定所述账户是否能够访问所述第二受保护资源的逻辑；响应于确定所述账户能够访问所述第二受保护资源而将与所述账户中的一个相关联的所存储安全凭证自动提供给所述网络站点的逻辑；以及从所述网络站点访问所述第二受保护资源的逻辑。所述的系统进一步包括：借助网络使用于所述账户的经加密安全凭证与认证管理服务同步的逻辑；以及响应于确定所述账户不能够访问所述受保护资源而使用旧账户对所述网络站点进行认证的逻辑，其中从所述用户获得用于所述旧账户的至少一个安全凭证。所述的系统进一步包括：根据所述网络站点的域名来识别所述多个账户中的一个的逻辑，所述多个账户中的一个与具有与所述域名不同的域名的不同网络站点相关联；以及使用与所述账户中的一个相关联的安全凭证对所述网络站点进行自动认证的逻辑。所述的系统进一步包括：至少部分基于所述网络站点的域名和从所述网络站点获得的所支持的第三方认证提供者的列表而识别被所述网络站点接受的多个所述账户以便对所述受保护资源进行认证的逻辑；使得显示被配置来获得对多个所述账户中的一个的用户选择的用户界面的逻辑；存储对与所述网络站点的所述域名相关联的多个所述账户中的一个的所述用户选择的逻辑；以及使用与多个所述账户中通过所述用户选择所选择的一个账户相关联的安全凭证对所述网络站点进行自动认证的逻辑。所述的系统，其进一步包括：向认证管理服务发送对账户数据的请求的逻辑，所述请求指定用于访问所述账户数据的安全凭证，所述账户数据包括用户用于访问所述多个网络站点的多个安全凭证；响应于对所述账户数据的所述请求而从所述认证管理服务获得所述账户数据的逻辑；获得主控安全凭证的逻辑；使用所述主控安全凭证对所述账户数据进行解密的逻辑；以及将所述安全凭证中的每一个自动重置为相应的新安全凭证的逻辑。所述的系统进一步包括：维护用于所述用户的用于所述多个网络站点的所述多个账户的账户数据的逻辑，所述账户数据包括用于所述账户中的每一个的相应安全凭证；响应于所述用户访问所述多个所述网络站点中的每一个而使用相应的多个所述账户来对与多个所述网络站点对应的多个认证服务进行自动认证的逻辑，其中为所述网络站点中的每一个建立相应会话；确定将要执行注销的逻辑；以及通过结束所述会话中的每一个而执行所述注销的逻辑。本发明还提供另一种账户管理系统，其包括：至少一个计算装置；以及可在所述至少一个计算装置中执行的认证服务，所述认证服务包括：借助认证协议从在第一客户端计算装置中执行的第一认证管理客户端获得第一认证请求的逻辑，所述第一认证请求指定与第一用户账户相关联的第一安全凭证；响应于所述第一认证请求而在所述第一客户端计算装置处对所述第一用户账户进行认证以便访问网络站点的至少一个受保护资源的逻辑；借助所述认证协议从在第二客户端计算装置中执行的第二认证管理客户端获得第二认证请求的逻辑，所述第二认证请求指定与第二用户账户相关联的第二安全凭证；以及响应于所述第二认证请求而在所述第二客户端计算装置处对所述第二用户账户进行认证以便访问所述网络站点的所述至少一个受保护资源的逻辑，其中所述第一认证管理客户端和所述第二认证管理客户端是由认证管理服务的不同提供者部署，并且受制于用户对

分享为创建能够访问至少一个受保护资源的第一用户账户或第二用户账户所需的信息的同意，由所述第一认证管理客户端和所述第二认证管理客户端提供所述认证请求，并且其中，为能够访问所述至少一个受保护资源的第一用户账户或第二用户账户自动建立安全凭证。所述的系统进一步包括：至少部分基于所述第一认证管理客户端的密切度来确定是否支持所述第一认证管理客户端的逻辑；以及响应于所述第一认证请求且响应于支持所述第一认证管理客户端而在所述第一客户端计算装置处对所述第一用户账户进行认证以便访问所述网络站点的所述至少一个受保护资源的逻辑。所述第一认证管理客户端被配置来：响应于从用户获得主控安全凭证对由所述第一认证管理客户端所存储的与所述第一用户账户相关联的所述第一安全凭证进行解密；使用所述第一认证管理客户端借助所述认证协议将所述第一认证请求发送给与所述网络站点的所述至少一个受保护资源相关联的所述认证服务，所述第一认证请求指定与所述第一用户账户相关联的所述第一安全凭证；在响应于所述第一认证请求而被所述认证服务认证之后访问所述至少一个受保护资源；以及将所述第一安全凭证从所述第一认证管理客户端导入到在所述第一客户端计算装置中执行的第三认证管理客户端中。所述的系统，其进一步包括：存储包括与用户的多个网络站点相关联的多个安全凭证的账户数据的逻辑，所述账户数据以加密形式来存储；从第三客户端获得对所述账户数据的请求的逻辑，所述请求指定用于访问所述账户数据的第三安全凭证；以及响应于确定所述第三客户端对应于预先授权的客户端且响应于确定用于访问所述账户数据的所述第三安全凭证是有效的而向所述第三客户端发送所述账户数据的逻辑。所述的系统进一步包括：在认证之后获得更换用于所述第一用户账户的所述第一安全凭证的请求的逻辑，所述更换所述第一安全凭证的请求是在所述第一认证管理客户端中自动发出；以及响应于所述更换所述第一安全凭证的请求而建立用于所述第一用户账户的新安全凭证的逻辑。所述的系统进一步包括：在认证之后从所述第一认证管理客户端获得账户升级请求的逻辑，所述账户升级请求指定关于用户的一组信息；根据所述账户升级请求来升级所述第一用户账户的逻辑；以及在升级之后在所述第一客户端计算装置处对所述第一用户账户进行认证以便访问所述网络站点的另一受保护资源的逻辑。

附图说明

[0006] 参看以下图式可以更好地理解本公开的许多方面。图式中的组件不一定按比例绘制，而是将重点放在清楚地说明本公开的原理。此外，在图式中，若干附图中的相同元件符号表示对应的部件。

[0007] 图1是根据本公开的各种实施方案的网络环境的图式。

[0008] 图2A到图2C是根据本公开的各种实施方案的由图1的网络环境中的客户端呈现的用户界面的实例的图式。

[0009] 图3到图6B是图示了根据本公开的各种实施方案的实施为在图1的网络环境中的客户端中执行的认证管理客户端的多个部分的功能性的实例的流程图。

[0010] 图7是图示了根据本公开的各种实施方案的实施为在图1的网络环境中的计算装置中执行的认证端点的多个部分的功能性的一个实例的流程图。

[0011] 图8是图示了根据本公开的各种实施方案的实施为在图1的网络环境中的计算装置中执行的认证管理服务的多个部分的功能性的一个实例的流程图。

[0012] 图9是提供了根据本公开的各种实施方案的在图1的网络环境中使用的客户端的一个实例图示的示意框图。

具体实施方式

[0013] 本公开涉及管理安全凭证，例如用户名、密码、安全密钥和/或其它安全凭证。尽管密码在恰当使用时可以是很强的安全凭证，但是它们通常被误用。举例来说，用户可能会设置相对较弱的密码，例如词典中的词语或者否则容易猜出的密码。用户还可能会为在多个网络站点上且具有不同安全要求的多个账户设置相同的密码。因此，如果一个账户受到威胁，那么使用相同密码的所有其它账户也是易受攻击的。

[0014] 因此，与使用密码作为安全凭证相关联的许多问题是因为人类不能处理密码所表示的那类数据而造成。强的密码通常含有随机字符并且是长的，这使得它们难以记住。密码通常不是单块信息且可以延伸人类工作记忆的极限。本文中公开的系统使用户与密码在很大程度上分离，由此解决了许多所述问题。举例来说，所述系统可使用从网络站点可接受的整个字符集合中选出的字符来为每一网络站点自动生成独特的强密码。这可以使得从强力、彩虹表和/或其它攻击中得到极好恢复。在一般使用中，用户可能无需知道用于网络站点的密码。另外，所述系统可将密码存储在服务器上且使用户在多个客户端装置上、甚至在例如信息亭等公用客户端装置上可以使用所述密码。对集中存储的密码的访问可以通过基于知识的问题、主控密码和/或其它方法来保护。用于强凭证生命周期管理的各种技术由2011年7月29日提交的发明名称为“管理安全凭证(MANAGING SECURITY CREDENTIALS)”的美国专利申请第13/194,287号描述，所述申请以全文引用方式并入本文中。

[0015] 在各种实施方案中，可以通过认证管理客户端来自动地创建账户，所述认证管理客户端将关于用户的信息的基本集合提供给网络站点或标识提供者的账户创建端点。在必要时可以通过提供额外的信息以访问某些受保护资源来升级账户。多个用户可以能够登录到认证管理客户端，这样可以允许用户创建相应账户且通过使用认证管理客户端进行认证来访问网络站点的受保护资源。在一些实施方案中，多个认证管理服务可能是可用的，且可能可以由竞争实体提供。一些网络站点或标识提供者可支持所述认证管理服务中的一些但不支持另一些。用户可以从一个认证管理服务迁移到另一认证管理服务。

[0016] 在各种实施方案中，认证管理客户端使用域名匹配或其它分组根据网络站点的域名来向网络站点(或标识提供者)呈现安全凭证。一些网络站点可支持使用多个标识提供者进行认证。用户可存储对认证管理客户端将使用的优选标识提供者的偏好，其中多个标识提供者是可用的。在一些情形中，由认证管理服务管理的账户和安全凭证仅可以通过预先授权的客户端来恢复和使用。此外，可改变或导出凭证以方便在认证客户端外部使用。在一些实施方案中，在认证客户端方便使用多个账户登录到多个网络站点的情况下，认证客户端可被配置来提供用于所述多个网络站点的自动注销功能性。在以下论述中，提供对所述系统以及其组件的大体描述，之后再论述其操作。

[0017] 参看图1，示出了根据本公开的各种实施方案的网络环境100。网络环境100包括可借助网络115与计算装置106和计算装置112进行数据通信的客户端103。网络115包括(例如)互联网、内联网、外联网、广域网(WAN)、局域网(LAN)、有线网络、无线网络或其它合适网络等，或两个或两个以上此类网络的任何组合。客户端103还可借助(例如)本地接口、数据

总线或另一网络115与便携式数据存储装置118进行数据连接。

[0018] 客户端103可包括(例如)计算机系统,例如台式计算机、膝上型计算机、个人数字助理、移动电话、智能电话、机顶盒、音乐播放器、上网平板、平板计算机系统、游戏控制台、电子书阅读器、信息亭或具有类似能力的其它装置。另外,客户端103还可包括可经由网络115与计算装置106、112通信以执行各种功能的具有网络能力的任何装置。此类客户端103可包括(例如)具有处理器电路的基于处理器的装置,所述处理器电路包括处理器和存储器。

[0019] 客户端103可被配置来执行各种应用程序,例如浏览器121、认证管理客户端124和/或其它应用程序。浏览器121可以在客户端103中执行,例如,以访问和呈现网络页面,例如网页、gopher页面、移动应用内容或由计算装置106和/或其它服务器提供的其它形式的网络内容。可执行认证管理客户端124以管理用于网络站点和标识提供者的用户账户,包括用户名、密码、私用和公开密钥、证书和/或其它安全凭证。

[0020] 在一些实施方案中,认证管理客户端124作为浏览器121的插件应用程序来运行。举例来说,认证管理客户端124可实施为浏览器121的工具栏。认证管理客户端124可用超文本标记语言(HTML)第5版或另一语言来实施。在其它实施方案中,认证管理客户端124可为与浏览器121、移动应用程序和/或要求认证管理的其它应用程序介接的独立应用程序。客户端103可被配置来执行浏览器121和认证管理客户端124以外的应用程序,例如电子邮件应用程序、即时消息应用程序和其它应用程序。

[0021] 客户端103包括数据存储装置127且可能的其它数据存储装置,所述数据存储装置可包括数据和被配置来提供对所述数据访问的应用程序。可使用数据存储装置127来存储客户端账户数据130、标识提供者偏好数据131、证书信任数据133和/或可能还有其它数据。客户端账户数据130可包括(例如)用以访问各种网络站点或网络页面的安全凭证、关于认证端点的信息和/或其它信息。在各种实施方案中,客户端账户数据130可以以加密格式来存储。在各种实施方案中,可暂时存储客户端账户数据130,使得在认证管理客户端124的会话终止时擦除安全凭证。在一个实施方案中,数据存储装置127可存储经加密密钥,所述经加密密钥可响应于从用户获得的主控安全凭证而解密。可接着使用经解密密钥来对客户端账户数据130进行解密。

[0022] 客户端账户数据130还可包括关于用户的一组信息,认证管理客户端124可使用所述信息来自动地创建或升级账户。此类信息可包括(例如)名字、姓氏、中间名缩写或中间名、电子邮件地址、电话号码、实际地址、出生日期和/或其它信息。所存储的用户信息可划分为较敏感的集合和较不敏感的集合,所述两个集合在用户同意分享所述信息时可突出显示。在一个实施方案中,可默认分享被视为较不敏感的信息以创建或升级账户。如果请求用户信息以进行账户创建或升级但所述用户信息并不存储在客户端账户数据130中,那么可呈现表单以便用户提供缺失信息。在一个实施方案中,信息的“基本”集合可通过标准来界定。

[0023] 标识提供者偏好数据131可指示对于认证管理客户端124将使用的标识提供者的用户偏好,其中对于一个网络站点,有多个标识提供者可用。证书信任数据133可描述发布网络站点所用的数字证书的受信任证书授权中心。证书信任数据133可包括(例如)与受信任证书授权中心相关联的公开密钥。可使用所述公开密钥来验证受信任证书授权中心在数

字证书上的数字签名。

[0024] 计算装置106可包括(例如)服务器计算机或提供计算能力的任何其它系统。替代地,可使用多个计算装置106,所述计算装置被布置成(例如)一个或多个服务器组或计算机组或其它布置。举例来说,多个计算装置106一起可包括云计算资源、网格计算资源和/或任何其它分布式计算布置。此类计算装置106可局限在单个装置中或可分布在许多不同地理位置间。出于方便起见,计算装置106在本文中以单数来提及。尽管计算装置106以单数来提及,但应理解,如上所述,可在各种布置中使用多个计算装置106。

[0025] 计算装置106被配置来执行各种应用程序,例如网络页面服务器136、具有账户创建端点138和认证端点139的认证服务137,以及其它应用程序。网络页面服务器136被配置来向各种客户端103提供网络页面(例如网页)和来自计算装置106的其它数据。网络页面服务器136可被配置来通过超文本传输协议(HTTP)、安全超文本传输协议(HTTPS)或某一其它协议来发送网络页面。网络页面服务器136可使用使用(例如)安全套接字层(SSL)、传输层安全性(TLS)和/或某一其它方法进行的加密。网络页面服务器136的非限制性实例包括Apache®HTTP服务器、Apache®Tomcat、Microsoft®互联网信息服务(IIS)和其它服务器应用程序。

[0026] 网络页面服务器136可被配置来提供一个或多个网络站点140。这样的网络站点140据称是由网络页面服务器136托管。网络站点140可包括与域名(例如规范名称)和目录(例如根目录(即,“/“)或某一其它目录)相关联的一组网络页面和/或文件。每一网络站点140可与网络页面服务器136中的不同配置设置相关联,而其它默认配置设置可在网络站点140间共享。

[0027] 执行认证服务137以促进账户创建和认证。认证服务137可通过网络站点140操作或者可由多个网络站点140使用。在认证服务137由多个网络站点140使用的情况下,认证服务137可被称作标识提供者。作为标识提供者,认证服务137可由通过许多不同实体操作的许多不同网络站点140使用。在一些情况中,网络站点140可支持多个认证服务137或标识提供者。在各种实施方案中,网络站点140和认证服务137可在同一计算装置106中或在不同计算装置106中执行。

[0028] 账户创建端点138可包括网络页面和/或软件,所述网络页面和/或软件被配置来方便使用账户创建协议在用于一个或多个网络站点140的客户端103处创建一个或多个账户和/或建立用于一个或多个用户的现有账户的安全凭证。在各种实施方案中,认证管理客户端124经由网络页面服务器136与账户创建端点138通信。为此,账户创建端点138可为网络页面服务器136的插件或其它模块,即,嵌入于网络页面内或否则嵌入于网络站点140内且借助解释程序或通用网关接口执行或以某其它方式经由网络页面服务器136来访问的脚本或其它软件。在其它实施方案中,账户创建端点138可以是在与网络页面服务器136相同或不同的计算装置106上执行的服务器应用程序。

[0029] 认证端点139可包括被配置来方便在用于一个或多个网络站点140的客户端103处进行用户认证的网络页面和/或软件。在各种实施方案中,认证管理客户端124经由网络页面服务器136与认证端点139通信。为此,认证端点139可为网络页面服务器136的插件或其它模块,即,嵌入于网络页面内或否则嵌入于网络站点140内且借助解释程序或通用网关接口执行或以某其它方式经由网络页面服务器136来访问的脚本或其它软件。在其它实施方

案中，认证端点139可以是在与网络页面服务器136相同或不同的计算装置106上执行的服务器应用程序。

[0030] 计算装置106包括数据存储装置142以及可能的其它数据存储装置，所述数据存储装置可包括数据以及被配置来能够访问所述数据的应用程序。可使用数据存储装置142来存储网络页面145、配置文件148、站点账户数据151、证书数据154和/或可能的其它数据。网络页面145可包括为网络页面服务器136所托管的网络站点140提供的网络页面和/或文件。配置文件148可包括一个或多个安全凭证规范和/或描述一个或多个账户创建端点138和/或认证端点139的界面。站点账户数据151包括安全凭证和/或与一个或多个网络站点140的用户相关联的其它数据。证书数据154包括可由网络页面服务器136、认证端点139和/或计算装置106上的其它应用程序用来识别网络站点和/或加密数据的数字证书。

[0031] 计算装置112可包括(例如)服务器计算机或提供计算能力的任何其它系统。替代地，可使用多个计算装置112，计算装置112被布置在(例如)一个或多个服务器组或计算机组或其它布置中。举例来说，多个计算装置112一起可包括云计算资源、网格计算资源和/或任何其它分布式计算布置。此类计算装置112可位于单个装置中或可分布在许多不同地理位置间。出于方便起见，计算装置112在本文中以单数来提及。尽管计算装置112以单数来提及，但应理解，如上所述，可在各种布置中使用多个计算装置112。

[0032] 根据各种实施方案，可在计算装置112中执行各种应用程序和/或其它功能性。此外，各种数据存储在计算装置112可访问的数据存储装置160中。如可了解到，数据存储装置160可表示多个数据存储装置160。存储在数据存储装置160中的数据(例如)与下文描述的各种应用程序和/或功能实体的操作相关联。

[0033] 在计算装置112上执行的组件(例如)包括认证管理服务163和本文中未详细论述的其它应用程序、服务、过程、系统、引擎或功能性。执行认证管理服务163以能够访问与用于网络站点140的用户账户相关联的由计算装置112存储的安全凭证。在各种实施方案中，认证管理服务163可被配置来在客户端103处代表用户针对网络站点140产生用户账户和/或建立安全凭证。在各种实施方案中，认证管理服务163可使用主控安全凭证和/或基于知识的问题对客户端103进行认证。

[0034] 在一个实施方案中，将认证管理服务163注册在此类服务的目录中。这样一个目录可由中立的第三方来维护。认证管理服务163相对于彼此可能是有区别的。一些认证管理服务163可(例如)提供隐私友好服务，所述隐私友好服务向用户保证认证管理服务163不会记录下他们的浏览习惯。其它认证管理服务163可选择追踪通过认证管理客户端124执行的登录。用户可以能够借助迁移协议将其账户数据从一个认证管理服务163迁移到另一认证管理服务163。

[0035] 存储在数据存储装置160中的数据包括(例如)服务器账户数据166、有效主控凭证169、有效辅助凭证170、静态的基于知识的问题172、用户数据175、配置文件176以及可能还有其它数据。存储在数据存储装置160中的数据可分割为用户特定数据和全局数据。服务器账户数据166包括安全凭证以便用户向网络站点140进行认证。此类安全凭证可以以加密形式或未加密形式来存储。服务器账户数据166还可包括关于账户创建端点138、认证端点139的信息和/或其它信息。认证管理客户端124可被配置来频繁地更新和同步服务器账户数据166与客户端账户数据130以在用户经由多个客户端103登录时确保新鲜度。

[0036] 使用有效主控凭证169来向认证管理服务163对用户进行认证。在一个实例中，有效主控凭证169可对应于用户建立的主控安全凭证的哈希版本。有效辅助凭证170对应于也可以用来向认证管理服务163对用户进行认证的辅助凭证。与主控安全凭证不同，对用户进行认证可能需要一个或多个有效辅助凭证170与对一个或多个基于知识的问题的正确回答的组合。可将相应权重应用于用以确定认证的得分的每一分量。

[0037] 静态的基于知识的问题172对应于用户已预先配置好答案的基于知识的问题。此类问题可由用户选择或可以是预先选择的。用户数据175对应于与用户相关联的各种数据。此类用户数据175可与用户与在线零售商的购买交易、浏览历史、订购历史、搜索历史、简档信息和/或其它数据有关。如将描述的，用户数据175可用以产生动态的基于知识的问题。在一些实施方案中，用户数据175可对应于描述用户与网络站点140的交互的数据。

[0038] 配置文件176可包括一个或多个安全凭证规范和/或描述一个或多个账户创建端点138和/或认证端点139的界面。虽然先前论述的在数据存储装置160中的数据具有用户特定的性质，但配置文件176可以是非用户特定的且因此可以被视为全局数据。

[0039] 便携式数据存储装置118可包括(例如)通用串行总线(USB)闪存存储装置、固态存储装置、便携式硬盘、软盘、光盘和/或其它便携式存储装置。在各种实施方案中，便携式数据存储装置118可包括包括处理器和存储器的处理器电路。在其它实施方案中，便携式数据存储装置118可仅由非暂时性计算机可读存储媒体组成。在一些实施方案中，便携式数据存储装置118可以是可卸除地附接到客户端103。

[0040] 便携式数据存储装置118可被配置来存储便携式账户数据178、认证管理客户端代码179和/或其它数据。便携式账户数据178可包括(例如)用以访问各种网络站点140或网络页面145的安全凭证、关于认证端点139的信息、用以对客户端账户数据130进行解密的主控安全凭证，和/或其它信息。在各种实施方案中，便携式账户数据178可为客户端账户数据130或服务器账户数据166的镜像。在其它实施方案中，便携式账户数据178可替代客户端账户数据130或服务器账户数据166。便携式账户数据178可以以加密格式来存储。

[0041] 为此，便携式数据存储装置118可包括用以对用户进行认证以便能够访问便携式数据存储装置118上的数据(例如便携式账户数据178)的装置(例如，指纹扫描仪或其它生物特征辨识装置、pin码小键板等)；或者它可包括准许用户键入密码和/或解密密钥以便能够访问便携式数据存储装置118上的数据的硬件和/或软件。另外，在一些实施方案中，认证管理客户端124可作为认证管理客户端代码179存储在便携式数据存储装置118上且例如在便携式数据存储装置118附接到客户端103时在客户端103中执行。

[0042] 接下来，提供对网络环境100中的各种组件的操作的大体描述。首先，用户可将认证管理客户端124安装到客户端103上且针对与网络站点140相关联的现有账户预先配置认证管理客户端124的操作。举例来说，用户可向认证管理客户端124和/或认证管理服务163提供现有安全凭证(例如，用户名、密码、安全密钥、证书和/或其它安全凭证)以及与所述安全凭证相关联的网络站点140和/或统一资源定位器(URL)的识别信息。认证管理客户端124可与多个认证管理服务163中的一个或多个相关联。认证管理客户端124可以或可以不借助标准的认证管理协议与认证管理服务163交互。在一些情况中，认证管理客户端124可以示出与对应的认证管理服务163相关联的某一标志或其它标牌。

[0043] 用户还可针对认证管理客户端124配置主控安全凭证，例如用户名、密码、生物特

征标识等，使得安全凭证可经加密或以其它方式进行保护以防在未经用户授权的情况下在客户端103上使用或观看。在一个实施方案中，在安装了认证管理客户端124之后，认证管理客户端124即刻使用随机产生的高熵主控密钥对客户端账户数据130进行加密。此主控密钥又可被加密成用户指定的主控密钥，其可与客户端账户数据130一起存储以便可以进行本地解密。在一些实施方案中，在客户端103中对操作系统用户会话的访问可以使得能够在没有单独用户登录的情况下访问客户端账户数据130。在客户端103执行Windows®操作系统的一个实施方案中，主控安全凭证可存储在“凭证管理器”中。

[0044] 在安全凭证存储在计算装置112的服务器账户数据166中的情况下，用户可针对认证管理服务163来建立有效主控凭证169。在一个实施方案中，用户的服务器账户数据166可以以加密形式来存储。在一个实施方案中，使用由于客户端103与计算装置112之间的SSL/TLS会话而产生的安全凭证，例如Rivest Cipher 4(RC4)对称密钥或某其它安全凭证，对用户的服务器账户数据166进行加密。所述加密可以在认证管理客户端124中执行，使得安全凭证细节不会不受阻碍地给予认证管理服务163。在一些情况中，用户可以针对认证管理服务163来配置静态的基于知识的问题172的答案。

[0045] 账户信息可由认证管理客户端124存储在客户端103上的客户端账户数据130中和/或存储在某其它位置处。举例来说，认证管理客户端124可以将账户信息备份到位于计算装置106上的账户数据160、位于便携式数据存储装置118中的便携式账户数据178和/或另一位置。与账户信息在客户端103上的存储有关的各种技术由2009年8月12日提交的发明名称为“认证管理器(AUTHENTICATION MANAGER)”的美国专利申请第12/539,886号描述，所述申请以全文引用的方式并入本文中。

[0046] 在一些实施方案中，账户信息可以集中托管在计算装置112的服务器账户数据166中。当使用计算装置112、便携式数据存储装置118或其它存储位置存储账户信息时，用户可以能够在另一客户端103上使用认证管理客户端124和账户信息。为此，可在另一客户端103上(例如)自动地下载、配置和载入认证管理客户端124。另外，被描述为由认证管理客户端124执行的各种功能可改为由认证管理服务163执行。举例来说，认证管理服务163可被配置来替代认证管理客户端124来创建账户、重新产生安全凭证等。在一些情况中，认证管理客户端124可表征为认证管理服务163的客户端应用程序。

[0047] 安全凭证可以在认证管理客户端124的多个用户间共享。作为非限制性实例，一组织中的若干用户可以共享在线银行账户。第一用户可以使用认证管理客户端124和/或认证管理服务163来为账户创建用户名和密码。第一用户可以将所述账户标记为共享的且提供被授权访问所述账户的用户的列表(包括第二用户在内)。当所述账户分布到客户端账户数据130、服务器账户数据166、便携式账户数据178时，它可以是受保护的，使得仅授权用户可以访问它。当第二用户接下来使用认证管理客户端124时，可向第二用户给予机会来同步新账户与位于属于第二用户的便携式数据存储装置118中或位于某其它位置中的便携式账户数据178。

[0048] 在安装过程期间，在一个实施方案中，用户可指定认证管理客户端124将作为浏览器121的插件还是作为独立的应用程序来操作。认证管理客户端124可经安装且针对多个浏览器121(例如Firefox®、Internet Explorer®、Safari®、Chrome®和/或其它浏览器121)来进行配置。还可在客户端103上针对多个用户来配置认证管理客户端124。

[0049] 当用户借助浏览器121或另一应用程序来访问网络站点140时，认证管理客户端124确定网络站点140是否与所存储的账户信息相关联，所述账户信息可(例如)集中存储在服务器账户数据166中或本地存储在客户端账户数据130中。认证管理客户端124可与网络站点140或单独的标识提供者的认证服务137通信。

[0050] 认证管理客户端124可用到网络站点140的域名以便将所存储的账户与网络站点140相关。在一些情况中，具有不同域名的多个网络站点140可使用相同的所存储账户。有时，此确定可基于域名的一部分，例如二级域名部分。作为非限制性实例，公司可能具有若干网络站点140，所述网络站点140具有针对各种地理位置的不同域名或一般的顶级域名，例如“e-retailer.com”、“e-retailer.net”、“e-retailer.co.uk”、“e-retailer.eu”、“e-retailer.co.jp”等等。认证管理客户端124可根据字符串“e-retailer”在域名中而非根据对域名的完全匹配来识别用户账户。然而，所述匹配可能不是决定性的，且网络站点140实际上可能是不相关的。因此，在与网络站点140交换来自所存储账户的任何受保护信息之前，可向用户呈现所述账户的标识以便进行显式确认。

[0051] 如果网络站点140不与所存储账户信息相关联，那么认证管理客户端124可通知用户且如果用户具有现有账户则可提示用户提供安全凭证。用户提供的安全凭证可接着由认证管理客户端124存储在客户端账户数据130、服务器账户数据166或便携式账户数据178中的一个或多个中。

[0052] 替代地或此外，认证管理客户端124和/或认证管理服务163可辅助用户创建网络站点140的账户。所述账户可以是一次性账户、用户的第一账户或用户的第二或后续账户。认证管理客户端124和/或认证管理服务163可(例如)基于嵌入于网络页面145内的表单的结构来确定如何创建网络站点140的账户。这样一个表单可用超文本标记语言(HTML)、可扩展标记语言(XML)或某一其它语言来定义。

[0053] 作为非限制性实例，在网络页面145上的提交输入元件与例如“创建账户”等文本相关联时，认证管理客户端124可识别账户创建表单。认证管理客户端124还可检查URL以查找相关关键字。作为另一非限制性实例，在质询响应测试(例如“Captcha”)存在时，认证管理客户端124可识别账户创建表单。认证管理客户端124可使用(例如)网络页面145上名为“用户名”、“密码”或其它可识别名称的输入元件来自动地识别安全凭证的必需字段。在各种实施方案中，认证管理客户端124可使用户识别账户创建表单和/或标记所述表单的输入元件，使得认证管理客户端124可准确地识别可如何通过表单填充来创建账户。这样一个标记列表可存储在配置文件176中，所述配置文件接着可上传到计算装置112。在此，配置文件176可由其它用户使用认证管理客户端124来访问且被他们用来简化由配置文件176所描述的在网络站点140上的账户创建。替代地或此外，配置文件176可由计算装置112存储以便认证管理客户端124、认证管理服务163和/或其它应用程序访问。

[0054] 在各种实施方案中，认证管理客户端124和/或认证管理服务163可通过表单填充以外的方法以自动方式来创建账户。举例来说，认证管理客户端124和/或认证管理服务163可从用于网络站点140的网络页面服务器136或可提供与网络站点140相关联的配置文件176的计算装置112获得与网络站点140相关联的配置文件148。配置文件148、176可定义用于网络站点140的一个或多个账户创建端点138，其中认证管理客户端124和/或认证管理服务163可通过填写表单之外的方法来认证和/或创建账户。举例来说，配置文件148、176可定

义通过账户创建端点138以自动方式创建账户所需的URL、参数、编码和/或其它信息。在一些实施方案中，一个账户创建端点138可由多个网络站点140和/或网络页面服务器136共享。为了防止对账户的未经授权自动创建，认证管理客户端124和/或认证端点139可包括“Captchas”，限制账户创建的速度和/或采取其它措施。

[0055] 配置文件148、176还可包括与网络站点140相关联的安全凭证规范。所述安全凭证规范可指定用于用户名和/或密码的字符集、最小长度、最大长度和/或其它参数。所述安全凭证规范还可指定可应用于公开密钥基础结构或其它类型的安全凭证的最小密钥长度、可接受算法和格式和/或其它参数。

[0056] 认证管理客户端124和/或认证管理服务163可基于安全凭证规范来产生一个或多个安全凭证。在一个实施方案中，认证管理服务163可被配置来根据基于订阅的推送模型来获得安全凭证规范。在另一实施方案中，认证管理服务163可被配置来按有规律的时间间隔从计算装置106拉取安全凭证规范。

[0057] 当认证管理客户端124和/或认证管理服务163正通过表单填充来创建账户时，认证管理客户端124可提示用户提供安全凭证规范，使得认证管理客户端124和/或认证管理服务163可产生一个或多个安全凭证以便填到表单中。用户可在账户创建表单附近看到关于显示于网络页面145上的安全凭证的必要属性的信息。认证管理客户端124可提供多个选项，包括但不限于安全凭证的长度、使用某一字符集的指示、使用至少一个数字的指示、使用至少一个非字母数字字符的指示以及其它选项。

[0058] 作为非限制性实例，认证管理客户端124可向用户呈现图形界面，所述图形界面列出了可用于产生安全凭证的各种属性。这样一个图形界面可包括(例如)复选框、单选按钮、下拉框、文本字段、文本区等。所述图形界面可用默认选择来预先配置。在安全凭证由认证管理服务163产生的情况下，认证管理服务163可执行表单填充，或可将安全凭证传送给认证管理客户端124以便认证管理客户端124执行表单填充。

[0059] 在各种实施方案中，当认证管理客户端124正在通过表单填充来创建账户时，认证管理客户端124可(例如)用精灵界面来替代填充表单过程中的正常用户交互。所述精灵界面可省略可以通过认证管理客户端124自动完成的任务或字段。然而，精灵界面可获得来自用户的输入以便填充例如“Captchas”和其它质询响应测试等字段。虽然认证管理客户端124和/或认证管理服务163可被配置来填充与其它个人信息(例如，姓名、出生日期、社会保险号码、电话号码、地址等)有关的字段，但认证管理客户端124可改为被配置来提示用户填写所述信息。在各种实施方案中，认证管理客户端124可空出未经辨识的表单字段以便用户完成。

[0060] 因此，认证管理客户端124和/或浏览器121将与所产生的安全凭证相关联的账户创建请求发送给网络站点140。在提交了账户创建请求之后，将会或不会针对网络站点140创建账户。网络站点140通常提供指示账户创建是否成功的响应页面。这样一个网络页面145可由认证管理客户端124自动地剖析或可留给用户另外输入到认证管理客户端124。

[0061] 在一些情况中，响应页面将包括具有存在问题的指示的另一表单。作为非限制性实例，用户名字段可突出显示且具有指定用户名已被使用的解释。认证管理客户端124可被配置来自动地响应此类请求和/或寻求用户输入。经由认证端点139作出的账户创建响应可通过认证管理客户端124以类似方式处置。在一个实施方案中，认证管理客户端124可以只

是假定创建了账户。

[0062] 响应于账户创建，认证管理客户端124和/或认证管理服务163将账户信息(包括但不限于安全凭证、URL以及与账户和网络站点140相关联的域名)存储在客户端账户数据130、服务器账户数据166或便携式账户数据178中的一个或多个中。明确地说，网络站点140或认证端点139可在账户创建过程期间呈现来自证书数据154的受信任证书。与此受信任证书有关的信息(包括域名、证书授权中心和来自证书的其它信息)可与账户信息一起存储。

[0063] 所述账户信息因此可被标记为在与受信任证书中提供的域名对应的网络站点140上可用，或者在较高安全系数环境中仅在能够呈现所述特定证书的网络站点140上可用。存储在客户端账户数据130、服务器账户数据166或便携式账户数据178中的任一个中的账户信息可通过认证管理客户端124和/或认证管理服务163手动或自动地复制到任何其它客户端账户数据130、服务器账户数据166或便携式账户数据178，使得所述账户信息可在客户端账户数据130、服务器账户数据166或便携式账户数据178中的任两者或两者以上间镜像映射。

[0064] 为了进行备份，认证管理客户端124和/或认证管理服务163可以能够呈现客户端账户数据130、服务器账户数据166或便携式账户数据178中的所存储账户信息的列表以便查看或打印。为了方便查看或打印，认证管理客户端124和/或认证管理服务163可被配置来使用适当的字符集来产生人类可读或可打印的安全凭证。替代地，认证管理客户端124和/或认证管理服务163可使用编码方法(例如UUencoding、BinHex、多用途互联网邮件扩展(MIME)编码、Base64和其它编码方法)以可打印形式来对安全凭证进行编码。

[0065] 另外，为了进行恢复，可将主控安全凭证写入到可卸除式媒体，例如通用串行总线(USB)盘。为了在恢复情况中提高安全性，可将主控安全凭证加密成存储在客户端103中的密文。这样确保丢失的USB盘或其它可卸除式媒体不能用来访问服务器账户数据166。在一些实施方案中，恢复有时可至少部分由操作系统通过将主控安全凭证绑定到操作系统中的用户账户来实施。

[0066] 为了实现漫游和恢复，可由认证管理客户端124产生一组一次性密码。这些密码中的每一个都可用来产生主控安全凭证的额外经加密版本，所述经加密版本中每一个可附加到服务器账户数据166。在使用到一次性密码时，可以通过认证管理客户端124从服务器账户数据166移除每一条目来施行所述一次性密码。用户可负责将这些一次性密码保存在系统外的某些地方(例如，打印出、在钱包卡上等等)。

[0067] 在一些实施方案中，可以通过认证管理服务163依照机器来管理恢复和重置能力。在一个实施方案中，仅用于给定认证管理账户的第一客户端103可以能够进行恢复。认证管理服务163可提供用户界面来管理客户端103，包括允许在额外客户端103上进行恢复/重置的能力。另外，可支持不同类型的账户数据恢复机制(例如，一次性密码、操作系统恢复、存储在可卸除式媒体上的凭证等)，且可以依照客户端来启用或停用这些账户数据恢复机制的子集。举例来说，认证管理客户端124可被配置来请求准许使用所述账户数据恢复机制中的特定机制。这样一个请求可包括客户端识别令牌。

[0068] 认证管理服务163可根据是否已向特定客户端103授予授权来启用或停用所请求的账户数据恢复机制。作为非限制性实例，第一经注册客户端103(例如，家里的机器)可以能够使用所有恢复机制，但默认的是，没有恢复机制可以在其它客户端103(例如，朋友的机

器)上使用。这可以用来预先制止通过此类恢复机制进行安全攻击的可能性。可提供与认证管理服务163的接口以便用户针对特定客户端103选择性地启用或停用特定恢复机制。

[0069] 为了促进对丢失的主控安全凭证的恢复,可将主控安全凭证写入到便携式数据存储装置118或其它可卸除式媒体。为了在这样一种情形中提高安全性,可将主控安全凭证加密成存储在客户端103中的密钥,使得即便便携式数据存储装置118或可卸除式媒体被偷了,也只有在客户端103上才能对主控安全凭证解密。在一些实施方案中,主控安全凭证可对应于由操作系统管理的操作系统凭证。

[0070] 在一些实施方案中,可由认证管理客户端124产生一组一次性密码,且这些密码中的每一个都可用来产生主控安全凭证的额外经加密版本,所述经加密版本中的每一个可附加到客户端账户数据130和服务器账户数据166。为了施行所述一次性密码,在使用到一次性密码时,由认证管理客户端124从客户端账户数据130移除每一条目。用户可负责使这些一次性密码在系统外保持安全(例如,打印出、在钱包卡上等等)。

[0071] 当存在用于网络站点140的所存储账户时,认证管理客户端124和/或认证管理服务163确定是否向网络站点140提供安全凭证。作为初步事项,认证管理客户端124和/或认证管理服务163可要求用户借助主控安全凭证(例如密码、便携式数据存储装置118在客户端103处存在、生物特征标识、本机操作系统标识或某其它认证)来向认证管理客户端124和认证管理服务163进行认证。响应于认证,认证管理客户端124可对所存储的客户端账户数据130、服务器账户数据166或便携式账户数据178进行解密。在一些实施方案中,响应于提供主控安全凭证,认证管理客户端124将可以访问所存储的客户端账户数据130、服务器账户数据166或便携式账户数据178。认证管理客户端124接着验证网络站点140的标识。

[0072] 验证网络站点140的标识可(例如)通过将与在登录时由网络站点140提供的受信任证书相关联的域名与在所存储的账户信息中的与网络站点140相关联的域名进行比较来执行。认证管理客户端124可将与由网络站点140提供的受信任证书相关联的域名(例如)与由用户提供的域名、通过启发式分析推断出的域名或某其它域名进行比较,以便识别网络站点140看起来类似哪个所存储账户。通过使用受信任证书来验证网络站点140的标识可能比通过仅(例如)经由域名服务(DNS)名称解析或将所存储的域名与浏览器121的地址栏中显示的域名进行比较来验证标识较不易受到欺骗攻击。

[0073] 如果网络站点140不提供证书(例如,在HTTP下认证)或者如果证书不受信任(例如,自签名的或由证书信任数据133中不认为是受信任的证书授权中心发出的),那么认证管理客户端124可向用户显示警告。在一些情况中,用户可接受警告且继续操作。在一些实施方案中,认证管理客户端124可记住此类特性且使用它们来辅助将来对网络站点140的标识验证。在其它情况中,认证管理客户端124可识别欺骗攻击或其它网络钓鱼尝试的明确使用,且提供额外警告、停用特定网络站点140处的认证、要求用户向认证管理客户端124重新认证和/或采取其它预防措施。另外,通过将认证管理客户端124与提供网络站点140的信誉数据的站点集成,认证管理客户端124可警告用户网络站点140是恶意的。

[0074] 认证管理客户端124可另外通过其它方法来验证网络站点140的标识。一种验证方法可包括将浏览器121中的地址栏的内容与所存储的URL或域名进行比较。第二种验证方法可包括将所访问的网络站点140所发送的HTTP标头的内容与所存储的URL或域名进行比较。第三种验证方法可包括对与所访问的网络站点140相关联的互联网协议(IP)地址执行反向

DNS查找且将所述域名与所存储的URL或域名进行比较。还可使用其它验证方法。在降级到不那么安全的方法之前可使用较安全的方法，且用户可指定证明网络站点140的标识的可接受方法。

[0075] 一旦验证了网络站点140的标识，认证管理客户端124便可经由认证端点139自动地将安全凭证提供给网络站点140，或可获得用户确认。如果认证管理客户端124被配置来获得用户输入，那么认证管理客户端124可在浏览器121的顶部中或上呈现按钮或其它用户界面特征以获得确认。

[0076] 当没有为网络站点140定义认证端点139时，认证管理客户端124可被配置来检测是否呈现认证表单。认证管理客户端124可检查网络页面145以查找多个元件，例如与例如“登录”等文本相关联的提交输入元件、匹配“用户名”和/或“密码”的输入字段、使用密码类型的字段和其它识别元件。认证管理客户端124还可检查URL以查找相关关键字。在一些实施方案中，认证管理客户端124和/或认证管理服务163可将与网络站点140相关联的URL存储在客户端账户数据130、服务器账户数据166或便携式账户数据178中，所述URL可用于认证。认证管理客户端124可通过表单填充将安全凭证提供给网络站点140。这样一个表单的提交可以是自动的或可以通过用户输入(例如对“提交”或“登录”按钮或其它用户界面元件的选择)来进行。

[0077] 在一些情况中，用户可能会忘记主控安全凭证或者可能不可以在另一客户端103上访问主控安全凭证。用户接着可以能够通过由认证管理服务器163实施的程序来重置主控安全凭证或者可以至少暂时访问所存储的安全凭证。在用户选择了主控安全凭证或重置选项之后，认证管理服务163即刻可以产生提供一个或多个基于知识的问题的用户界面。举例来说，用户界面可对应于用于在浏览器121中呈现的网络页面。替代地，可向认证管理客户端124发送数据以便由认证管理客户端124呈现用户界面。

[0078] 用户界面可呈现由用户预先配置的静态的基于知识的问题172。举例来说，用户界面可呈现“你母亲婚前姓名是什么?”、“你出生在哪个城市?”、“你高中的吉祥物是什么?”等等问题。用户界面可呈现是非问题。“是”问题对应于可以由用户和认证管理服务163两者验证的对用户来说是独特的问题。“非”问题是经设计以抓住试图未经授权就访问安全凭证的攻击者的那些问题。举例来说，“非”问题可以是：“你上次出租卡车是多少钱?”，其中正确的答案应该是：“我没有卡车”。

[0079] 此外，用户界面可呈现由认证管理服务163动态地产生的基于知识的问题。就动态地产生的问题来说，用户可能预先不知道将会问哪一类型的问题。动态地产生的问题可使用用户数据175，包括独特的顾客问题，例如购买交易历史和/或其它数据。动态地产生的问题的一个实例可以是：“我看到你昨天从E-Retailer购买了物品，你能告诉我账单金额吗?”。

[0080] 在一用户界面中可呈现多个基于知识的问题。认证管理服务163可使用对基于知识的问题的回答来产生得分。当得分满足预定义阈值(例如，正确回答一个问题、正确回答三个问题、正确回答基于最近的数据的一个动态地产生的问题等等)时，可准许用户访问服务器账户数据166的所存储的安全凭证和/或可建立新的有效主控凭证169。注意，在产生得分过程中，可将不同权重应用于不同类型的问题。举例来说，可向基于最近的事件的动态问题给予比基于在账户创建期间获得的信息的静态问题大的权重。在对于动态地产生的问题

没有呈现出足够的用户数据175的新的或非常客用户的情况中，认证管理服务163可以转向使用静态的基于知识的问题172。

[0081] 一旦认证管理服务163经由使用基于知识的问题或经由有效主控安全凭证对用户进行了认证，便可将用户的来自服务账户数据166的安全凭证下载到客户端账户数据130以供认证管理客户端124使用。在一个实例中，客户端103对应于信息亭或另一公用客户端103。在这样一个实例中，安全凭证可以暂时留存在客户端103的存储器中，使得在用户注销、从浏览器121退出或以其它方式结束认证管理客户端124的会话时，将它们从存储器擦除。替代地，可将安全凭证保存到客户端账户数据130以便将来经由客户端103使用。

[0082] 此外，一旦认证管理服务163对用户进行了认证，便可向用户提出设置新安全凭证的机会。举例来说，用户可以将新安全凭证与先前的安全凭证一起或不与先前的安全凭证一起供应。通过认证管理服务163来更新有效主控凭证169以存储新的有效主控凭证169。注意，有效主控凭证169可以是经过哈希处理的或以其它方式进行编码。

[0083] 还可使用认证管理服务163来根据配置文件176中的安全凭证规范来产生或重新产生安全凭证。除了初始账户创建和配置之外，认证管理服务163还可被配置来周期性地或在由用户或管理员触发时重新产生安全凭证。举例来说，管理员可以响应于潜在的安全风险来触发为具有用于某一网络站点140的账户的许多用户自动地重新产生安全凭证。在重新产生安全凭证之后，认证管理服务163可即刻使用适当的账户创建端点138来借助各种网络站点140建立新产生的安全凭证。认证管理服务163可供应先前的安全凭证以方便建立新产生的安全凭证。安全凭证可经产生或经重新产生以具有安全凭证规范容许的最高安全强度。

[0084] 在多个认证管理服务163可用的情况下，认证管理客户端124可被配置来导入/导出客户端账户数据130以便与不同的认证管理服务163一起使用。认证管理客户端124可由认证管理服务163的不同提供者或由其它方部署。在一些实施方案中，特定的认证管理客户端124可仅与对应的认证管理服务163一起起作用。因此，认证管理客户端124可被配置来允许客户端账户数据130导入和导出到不同认证管理客户端124以便与不同的认证管理服务163一起使用。

[0085] 在一个实施方案中，认证管理服务163可提供撤销用户界面以便撤销与服务器账户数据166相关联的安全凭证。为了方便此集中撤销，服务器账户数据166中的安全凭证可以是基于令牌的而不是基于用户凭证的字面存储。在一些实施方案中，撤销和重置可由认证管理客户端124执行。举例来说，认证管理客户端124可包括将自动地将每一凭证重置为新产生的凭证的“重置所有凭证”功能。可以向用户提问基于知识的问题，以在执行自动凭证重置之前再一次检查用户的标识。

[0086] 除了凭证重置之外，认证管理客户端124还可支持凭证更换为用户指定密码等等。在用户正在度假而没法访问认证管理客户端124的情况中，此类支持可能是有用的。用户可能想要将自动产生的安全凭证更换为可以容易记住的单个临时密码。在度完假回来之后，用户可以将临时密码重置为新的自动产生的安全凭证。在一个实施方案中，单个临时密码可能具有终止期，这将由认证管理服务163施行。

[0087] 现在转到图2A，示出了根据本公开的各种实施方案的由在网络环境100(图1)中的客户端103(图1)中执行的浏览器121(图1)呈现的网络页面145(图1)的实例。在此实例中，

用户可能已经键入或可能已经自动重定向到URL“https://www.e-retailer.site/,”所述URL显示在浏览器121的地址栏203中。由网络站点140(图1)响应于URL而提供的网络页面145包括具有用户名字段206、密码字段209和提交按钮212的认证表单。

[0088] 浏览器121包括安全指示215,所述安全指示指示网络站点140已呈现受信任的证书且客户端103与计算装置106(图1)之间的通信经加密。在图2A中,认证管理客户端124(图1)已验证了网络站点140的标识且正呈现认证系统选择218。认证系统选择218指示用户已安装了认证管理客户端124且与网络站点140相关联的账户信息是可用的。明确地说,认证系统选择218允许从多个认证服务137(图1)中选择账户数据。在图2A中可假定用户先前已向认证管理客户端124进行认证或者假如选择了所支持的认证服务137则将提出认证机会。如果账户数据不存在,那么认证系统选择218可以允许借助所选的认证服务137来进行账户创建。

[0089] 一旦用户选择了认证服务137,认证管理客户端124便可填写用户名字段206和密码字段209。认证管理客户端124还可通过在程序上按下提交按钮212来自动地提交登录请求。在一些实施方案中,可以在验证了网络站点140的标识之后即刻借助安全凭证来自动预先填充用户名字段206和密码字段209。安全凭证可以示出为位置固定的字符或示出为纯文本。

[0090] 替代地,如果(例如)定义了认证端点139(图1),那么认证管理客户端124或认证管理服务163(图1)可以借助认证端点139在后台进行认证。认证管理客户端124可以给出成功或失败的指示且可以提供另一用户界面元件以便从网络站点140注销。

[0091] 移到图2B,示出了根据本公开的各种实施方案的由在网络环境100(图1)中的客户端103(图1)中执行的浏览器121(图1)呈现的网络页面145(图1)的另一实例。在图2B的实例中,在客户端103中配置了认证管理客户端124(图1),但没有找到用于当前网络站点140(图1)的账户。因此,向用户呈现用户名字段206和密码字段209以及没有找到账户的通知221。可以提供与通知221相关联的复选框或其它用户界面组件以便用户同意将所提供的旧账户信息添加到认证管理客户端124。另外,可提供链接、按钮或其它用户界面组件以便用户同意账户创建。

[0092] 参看图2C,示出了根据本公开的各种实施方案的由在网络环境100(图1)中的客户端103(图1)中执行的浏览器121(图1)呈现的网络页面145(图1)的又一实例。在图2C的实例中,网络站点140(图1)支持借助认证管理客户端124(图1)来进行认证,但没有检测到认证管理客户端124。在这种情况中,可以呈现大意如此的通知224。可以呈现与用户界面组件227(例如按钮、链接等)相关联的通知224,以允许用户查看关于认证管理客户端124的更多信息、借助认证管理服务163(图1)来创建账户、下载和/或安装认证管理客户端124和/或执行其它动作。替代地,用户可以使用用户名字段206和密码字段209用旧的用户名和密码来登录到网络站点140。

[0093] 接下来参看图3,示出了提供根据各种实施方案的认证管理客户端124的一部分的操作的一个实例的流程图。应理解,图3中的流程图仅提供了可用来如本文所述实施认证管理客户端124的所述部分的操作的许多不同类型的功能布置的实例。作为替代方案,图3中的流程图可被视为描绘了根据一个或多个实施方案的在客户端103(图1)中实施的方法的步骤的实例。

[0094] 以框303开始，认证管理客户端124使用户向认证管理服务163(图1)进行认证。举例来说，用户可以登录到绑定到认证管理客户端124的会话的操作系统会话。替代地，用户可以直接登录到认证管理客户端124。在框306中，认证管理客户端124从认证管理服务163获得经加密的账户数据。在一些情况中，此经加密的账户数据可能已经作为客户端账户数据130(图1)存储在客户端103中或者作为便携式账户数据178(图1)存储在便携式数据存储装置118(图1)中。在框309中，认证管理客户端124至少部分基于由用户供应的主控安全凭证来对经加密的账户数据进行解密。经解密的账户数据可以至少暂时作为客户端账户数据130来存储以便在认证管理客户端124的用户会话期间使用。

[0095] 在框312中，认证管理客户端124确定将要访问网络站点140(图1)的受保护资源。举例来说，用户可使用浏览器121(图1)来导航到受保护的网络页面145(图1)或其它受保护的网络资源。在框315中，认证管理客户端124确定客户端账户数据130是否包括用于网络站点140的账户(或由网络站点140使用的标识提供者)。为此，认证管理客户端124可以确定与网络站点140相关联的具有认证端点139(图1)和账户创建端点138(图1)的一个或多个认证服务137(图1)。在一些情况中，认证服务137可对应于第三方认证提供者。认证管理客户端124可向网络站点140发送查询以确定所支持的认证服务137和/或可以至少部分基于浏览器121已经获得的网络资源的内容来确定所支持的认证服务137。

[0096] 认证管理客户端124可根据网络站点140的域名或经由可从网络站点140获得的其它识别数据来确定客户端账户数据130中存在账户。在一个实施方案中，认证管理客户端124可向认证管理服务163查询以获得用以将网络站点140的域名映射到所存储账户的信息。在另一实施方案中，认证管理客户端124可对域名的至少一部分(例如二级域名，例如“e-retailer.com”和“e-retailer.co.uk”内的“e-retailer”)执行匹配。因此，在确定可使用哪个账户时，可忽略不同的一级域名。

[0097] 在跨不同域名执行匹配的情况下，在实际上利用经识别的现有账户之前，可以请求显式用户确认。在针对同一基础域名配置多个账户的情况下，可使用具有最长匹配的账户。作为非限制性实例，用于“us.e-retailer.com”的账户可以优先登录到“www.e-retailer.com”，而不是用于“e-retailer.com”的账户。

[0098] 如果识别出现有账户，那么在框318中，认证管理客户端124使用预先存在的账户的安全凭证来向网络站点140的认证服务137进行认证。随后，可访问网络站点140的受保护资源。在大多数情况中，此认证可以在没有用户介入的情况下自动地发生。然而，在一些情况中(例如，就高价值的交易来说)，认证服务137可在认证协议中设置旗标以要求显式同意，由此迫使用户同意使用认证管理客户端124来登录。此外，在识别出多个账户的情况下，认证管理客户端124可被配置来呈现用户界面以获得对所述账户中的一个的用户选择。其后，认证管理客户端124的部分结束。

[0099] 如果未识别出现有账户，那么认证管理客户端124从框315移动到框321且确定用户是否具有旧账户，即，客户端账户数据130中不可用的现有账户。为此，认证管理客户端124可呈现用户界面，所述用户界面被配置来提示用户键入旧账户信息和安全凭证(假如用户具有旧账户)。如果用户具有旧账户，那么在框324中，认证管理客户端124从用户获得旧账户信息。

[0100] 在框327中，认证管理客户端124将旧账户信息存储在客户端账户数据130中。在一

些情况中，认证管理客户端124可如安全凭证规范中定义般将所提供的安全凭证转变为较强的凭证。可提示用户同意这样一种凭证更换。在框330中，认证管理客户端124使用相应的认证服务137和旧账户信息来向网络站点140进行认证。其后，认证管理客户端124的部分结束。

[0101] 如果用户不提供旧账户信息，或者如果用户确认了用户没有现有账户能够访问受保护资源，那么认证管理客户端124从框321移动到框333。在框333中，认证管理客户端124确定是否将针对网络站点140创建新账户。举例来说，用户可能已指定可以与账户创建端点138共享以便创建账户的一组信息(例如姓名、电子邮件地址、年龄等)。用户可能已建立规则来自动地同意分享一些信息但不分享其它信息。如果没有要创建账户，例如，用户不没有给出同意或者所存储的偏好不允许分享信息，那么认证管理客户端124的部分结束。否则，如果将为用户创建新账户，那么认证管理客户端124从框333转移到框336。

[0102] 在框336中，认证管理客户端124从用户获得对分享创建能够访问受保护资源的账户所需的信息的同意。这样一个同意可对应于用户界面中的显式确认、所存储的同意偏好和/或其它形式的同意。认证管理客户端124可通过从账户创建端点138获得特定集合的指示来确定需要(信息超集中的)哪一个一组信息。在一些情况中，认证管理客户端124可从用户获得额外信息。所述额外信息可包括自由表单数据、多个选项选择、是或否回答和/或其它数据。

[0103] 在框339中，认证管理客户端124通过与账户创建端点138通信使用关于用户的一组信息来自动地创建账户。在一些情况中，所述账户可以借助网络站点140的操作者来完成。在其它情况中，所述账户可以借助第三方标识提供者来完成，所述第三标识提供者可以使得账户能够访问与多个操作者相关联的多个网络站点140上的多个受保护资源。

[0104] 在框342中，如果成功创建了账户，那么认证管理客户端124将所得账户信息，包括(例如)自动产生的安全凭证，存储在客户端账户数据130中。在框345中，认证管理客户端124使用新账户向网络站点140的认证端点139进行认证以方便访问受保护资源。其后，认证管理客户端124的部分结束。

[0105] 现在转向图4，示出了提供根据各种实施方案的认证管理客户端124的另一部分的操作的一个实例的流程图。具体来说，图4与可包括升级现有账户的账户创建工作流有关。可执行升级以访问现有账户原本不能访问的网络站点的受保护资源。举例来说，用户可在不提供送货地址的情况下用在线商家来创建账户以进行浏览，但送货地址可能是发出订单所必要的。用户可以能够通过提供送货地址来升级账户以发出订单。应理解，图4中的流程图仅提供了可用来如本文所述实施认证管理客户端124的所述部分的操作的许多不同类型的功能布置的实例。作为替代方案，图4中的流程图可被视为描绘了根据一个或多个实施方案的在客户端103(图1)中实施的方法的步骤的实例。

[0106] 以框403开始，认证管理客户端124确定将借助认证服务137(图1)创建账户以便访问网络站点140(图1)的一个或多个受保护资源。如果存在现有账户，那么可能会拒绝经由所述特定的现有账户访问特定受保护资源。在框406中，认证管理客户端124确定客户端账户数据130(图1)是否包括用于网络站点140的现有账户。如果客户端账户数据130不包括用于网络站点140的现有账户，那么认证管理客户端124移动到框409。

[0107] 如果客户端账户数据130不包括现有账户，那么认证管理客户端124从框406移动

到框412且确定现有账户是否可升级来访问所请求的受保护资源。如果现有账户不是可升级的，那么认证管理客户端124从框412移动到框409。注意，在一些实施方案中，所有或几乎所有的账户都是可以能够升级的以及在必要时用额外信息来扩充。也就是说，用户已经具有用于网络站点140的账户但必须创建另一账户可能是很少见的情形。

[0108] 在框409中，认证管理客户端124从用户获得对分享创建能够访问受保护资源的账户所需的信息的同意。这样一个同意可对应于用户界面中的显式确认、所存储的同意偏好和/或其它形式的同意。用户还可以提供额外信息。在框415中，认证管理客户端124通过与账户创建端点138(图1)通信使用关于用户的一组信息以及可能还有新提供的信息来自动地创建全新的账户。在框418中，如果成功创建了账户，那么认证管理客户端124将所得账户信息，包括(例如)自动产生的安全凭证，存储在客户端账户数据130中。其后，认证管理客户端124的部分结束。

[0109] 如果认证管理客户端124改为确定现有账户可升级以访问受保护资源，那么认证管理客户端124从框412前进到框421。在框421中，认证管理客户端124确定升级现有账户以访问受保护资源所需的用户一组信息的子集。在框424中，认证管理客户端124从用户获得对分享用户信息的子集的同意。认证管理客户端124还可以或者改为从用户获得在用户信息的集合中已经不可获得的其它信息。在框427中，认证管理客户端124通过向网络站点140的账户创建端点138提供额外用户信息(包括所述用户一组信息的子集和/或新提供的用户信息)来升级现有账户。其后，认证管理客户端124的部分结束。

[0110] 转向图5，示出了提供根据各种实施方案的认证管理客户端124的又一部分的操作的一个实例的流程图。明确地说，图5与认证管理客户端124的多用户使用以及从多个网络站点140(图1)注销有关。应理解，图5中的流程图仅提供了可用来如本文所述实施认证管理客户端124的所述部分的操作的许多不同类型的功能布置的实例。作为替代方案，图5中的流程图可被视为描绘了根据一个或多个实施方案的在客户端103(图1)中实施的方法的步骤的实例。

[0111] 以框503开始，认证管理客户端124响应于用户提供某一安全凭证而使用户向认证管理服务163(图1)进行认证。在框506中，认证管理客户端124从认证管理服务163获得经加密的账户数据。在框509中，认证管理客户端124至少部分基于由用户提供的主控安全凭证来对账户数据进行解密。在框512中，认证管理客户端124通过与认证服务137(图1)的认证端点139(图1)通信来登录到网络站点140。

[0112] 认证管理客户端124提供来自客户端账户数据130(图1)的所存储安全凭证。在多个认证服务137可用于给定网络站点140的情况下，用户可以显式地选择所述认证服务137中的一个，或者可以根据标识提供者偏好数据131(图1)中的所存储偏好来自动地选择一个认证服务。在账户不再存在的情况下，可以如先前结合图3和图4中的流程图所述般自动地创建或升级账户。

[0113] 在框515中，认证管理客户端124确定是否访问另一网络站点140。替代地，可以访问同一网络站点140的需要单独登录的另一受保护资源。如果访问另一网络站点140，那么认证管理客户端124返回到框512且使用所存储的安全凭证来登录到另一网络站点140。因此，认证管理客户端124可以向对应于多个网络站点140的多个认证服务137自动进行认证。可以为每一网络站点140建立相应会话，所述会话可包括会话数据，例如由浏览器121(图1)

存储的会话cookie、经高速缓存的网络资源等等。如果不访问另一网络站点140，那么认证管理客户端124改为从框515前进到框518。

[0114] 在框518中，认证管理客户端124从用户获得通用注销请求。这样一个注销请求可以是显式的，例如用户选择了认证管理客户端124的用户界面上的单个注销按钮，或者可以是隐式的，例如用户从认证管理客户端124退出。认证管理客户端124的用户会话可以在用户发出切换用户请求时或者在用户从操作系统账户注销时结束。在一些情况中，与认证管理客户端124的用户会话可以在预定义的不活动时段之后自动结束。在一些实施方案中，用户可以提供针对特定网络站点140或网络站点140的集合的注销请求。

[0115] 响应于所述注销请求，在框521中，认证管理客户端124从每一网络站点140注销。为此，认证管理客户端124可向认证服务137中的每一个自动发送相应注销指示。在框524中，认证管理客户端124可自动刷新任何会话数据和客户端账户数据130。具体来说，可将经解密的账户数据从客户端103移除。在注销请求是特定注销请求而非通用注销请求的情况下，可仅针对指定网络站点140执行注销。因此，在特定注销的情况中，用户可继续利用在特定注销请求中未指示的会话。

[0116] 在框527中，认证管理客户端124确定另一用户是否将要使用认证管理客户端124。举例来说，认证管理客户端124可被配置来在单个操作系统用户会话内容纳多个用户。如果将要对另一用户进行认证，那么认证管理客户端124返回到框503。否则，认证管理客户端124的部分结束。

[0117] 现在继续到图6A，示出了提供根据各种实施方案的认证管理客户端124的又一部分的操作的一个实例的流程图。明确地说，图6A与重置安全凭证有关。应理解，图6A中的流程图仅提供了可用来如本文所述实施认证管理客户端124的所述部分的操作的许多不同类型的功能布置的实例。作为替代方案，图6A中的流程图可被视为描绘了根据一个或多个实施方案的在客户端103(图1)中实施的方法的步骤的实例。

[0118] 以框603开始，认证管理客户端124响应于用户提供某一安全凭证而使用户向认证管理服务163(图1)进行认证。在框606中，认证管理客户端124从认证管理服务163获得经加密的账户数据。在框609中，认证管理客户端124至少部分基于由用户提供的主控安全凭证来对账户数据进行解密。在框612中，认证管理客户端124获得重置客户端账户数据130(图1)中的安全凭证的请求。这样一种请求可涵盖重置请求、更换请求和/或临时更换请求。

[0119] 在框615中，认证管理客户端124确定是否准许所述操作。举例来说，认证管理服务163可配置认证管理客户端124，使得仅准许针对特定认证管理账户向认证管理服务163注册的第一客户端103执行某些操作，例如重置凭证和/或其它操作。其它客户端103也可由用户预先授权。在一些情况中，用户可提供一次性密码来实现重置或更换，且认证管理服务163可施行所述一次性密码。此外，在一些情况中，认证管理客户端124可向用户呈现一个或多个静态的基于知识的问题172(图1)以验证用户的标识。关于是否准许所述操作的确定可以由认证管理服务163来进行。

[0120] 如果不准许所述操作，那么认证管理客户端124移动到框618且产生错误。其后，认证管理客户端124的部分结束。否则，认证管理客户端124前进到框621且重置或更换客户端账户数据130中的用于用户的账户的每一个安全凭证。

[0121] 在一些情况中，认证管理客户端124可建立单个临时密码来代替自动产生的凭证。

认证管理客户端124可针对临时密码来配置终止期，其中在终止期之后为用户的每一个账户重新产生和重置安全凭证。在框624中，认证管理客户端124使客户端账户数据130与服务器账户数据166(图1)同步。其后，认证管理客户端124的部分结束。

[0122] 转到图6B，示出了提供根据各种实施方案的认证管理客户端124的又一部分的操作的一个实例的流程图。明确地说，图6B与响应于服务器发出的请求而重置安全凭证有关。应理解，图6B中的流程图仅提供了可用来如本文所述实施认证管理客户端124的所述部分的操作的许多不同类型的功能布置的实例。作为替代方案，图6B中的流程图可被视为描绘了根据一个或多个实施方案的在客户端103(图1)中实施的方法的步骤的实例。

[0123] 以框633开始，认证管理客户端124响应于用户提供某一安全凭证而使用户向认证管理服务163(图1)进行认证。在框636中，认证管理客户端124从认证管理服务163获得经加密的账户数据。在框639中，认证管理客户端124至少部分基于由用户提供的主控安全凭证来对账户数据进行解密。在框642中，认证管理客户端124从认证管理服务163获得重置安全凭证的请求。这样一个请求在性质上可以是一次性或周期性的。

[0124] 认证管理客户端124前进到框651且重置或更换客户端账户数据130中的用于用户的账户的每一个安全凭证。在一些情况中，认证管理客户端124可建立单个临时密码来代替自动产生的凭证。认证管理客户端124可针对临时密码来配置终止期，其中在终止期之后为用户的每一个账户重新产生和重置安全凭证。在框654中，认证管理客户端124使客户端账户数据130与服务器账户数据166(图1)同步。其后，认证管理客户端124的部分结束。

[0125] 接下来参看图7，示出了提供根据各种实施方案的认证端点139的一部分的操作的一个实例的流程图。应理解，图7中的流程图仅提供了可用来如本文所述实施认证端点139的所述部分的操作的许多不同类型的功能布置的实例。作为替代方案，图7中的流程图可被视为描绘了根据一个或多个实施方案的在计算装置106(图1)中实施的方法的步骤的实例。

[0126] 以框703开始，认证端点139从认证管理客户端124(图1)获得认证请求。认证请求可借助受与认证管理服务163(图1)具有不同密切度的多个认证管理客户端124支持的认证协议来获得。举例来说，认证管理客户端124可由认证管理服务163的提供者分发，且认证管理客户端124可能与特定认证管理服务163具有密切度。作为另一实例，认证管理客户端124可由第三方分发但仍可与特定认证管理服务163或多个认证管理服务163的集合具有密切度。

[0127] 在框706中，认证端点139根据请求来确定认证管理客户端124的密切度。举例来说，认证端点139可根据用户代理字符串中的标识符来确定认证管理客户端124的密切度。情况可能是认证端点139支持一些认证管理客户端124但不支持另一些认证管理客户端。类似地，账户创建端点138(图1)可以支持一些认证管理客户端124但不支持另一些认证管理客户端。

[0128] 在框709中，认证端点139确定是否支持特定认证管理客户端124。如果不支持所述认证管理客户端124，那么认证端点139移动到框712且拒绝认证请求。其后，认证端点139的部分结束。如果支持所述认证管理客户端124，那么认证端点139从框709移动到框715。

[0129] 在框715中，认证端点139从认证管理客户端124获得安全凭证。在框718中，认证端点139确定凭证是否有效。如果凭证无效，那么认证端点139移动到框712且拒绝认证请求。其后，认证端点139的部分结束。

[0130] 在框721中，认证端点139响应于成功认证而为用户创建会话。为此，认证端点139可借助会话令牌来设置一个或多个会话cookie和/或执行其它动作。另外，认证端点139可向认证管理客户端124发送带标牌的经验数据(例如，标志、图形、文本等)。认证管理客户端124可被配置来至少部分基于带标牌的经验数据来在客户端103(图1)中为与认证端点139相关联的标识提供者定制用户界面。带标牌的经验数据可包括(例如)网络站点140或标识提供者的标志、到隐私策略的链接、用于使用条款的链接、和/或其它信息。

[0131] 在框724中，认证端点139确定是否将更换认证管理客户端124使用的安全凭证。可以在认证端点139中或在认证管理客户端124中通过来自用户的手动更换请求或通过预定义的更换时间间隔的终止来促进这样一种更换。如果将更换安全凭证，那么认证端点139从框724移动到框727且建立新的安全凭证。这样一个凭证可由认证端点139产生且发送给认证管理客户端124，或者它可由认证管理客户端124产生且接着发送给认证端点139。其后，认证端点139的部分结束。如果将不更换安全凭证，那么认证端点139的部分也结束。

[0132] 转向图8，示出了提供根据各种实施方案的认证管理服务163的一部分的操作的一个实例的流程图。应理解，图8中的流程图仅提供了可用来如本文所述实施认证管理服务163的所述部分的操作的许多不同类型的功能布置的实例。作为替代方案，图8中的流程图可被视为描绘了根据一个或多个实施方案的在计算装置112(图1)中实施的方法的步骤的实例。

[0133] 以框803开始，认证管理服务163从客户端103(图1)处的认证管理客户端124(图1)获得对账户数据的请求。在框806中，认证管理服务163确定所述请求是否包括有效主控凭证169(图1)。如果所述请求不包括用于与账户数据相关联的用户的有效主控凭证169，那么认证管理服务163转移到框809且拒绝对账户数据的请求。其后，认证管理服务163的部分结束。

[0134] 如果所述请求指定了有效主控凭证169，那么认证管理服务163从框806继续进行到框812且确定客户端103是否对应于预先授权的客户端103。举例来说，认证管理服务163可评估所述请求的源网络地址、所述请求中存在的客户端识别令牌和/或其它数据。如果认证管理服务163确定客户端103不对应于预先授权的客户端103，那么认证管理服务163移动到框813且向客户端103提示需要有效的辅助凭证170(图1)，例如一次性密码、对基于知识的问题的回答等。如果不提供有效的辅助凭证170，那么认证管理服务163移动到框809且拒绝对账户数据的请求。其后，认证管理服务163的部分结束。

[0135] 如果提供有效的辅助凭证170，那么认证管理服务163从框813继续前进到框815。如果客户端103改为是经预先授权的，那么认证管理服务163从框812移动到框815。在框815中，认证管理服务163将一些或所有的经加密账户数据从服务器账户数据166(图1)发送给认证管理客户端124。在框818中，认证管理服务163可从认证管理客户端124获得对经加密账户数据的更新。如果认证管理服务163获得了此类更新，那么在框821中，认证管理服务163使服务器账户数据166同步。其后，认证管理服务163的部分结束。

[0136] 参看图9，示出了根据本公开的实施方案的客户端103的示意框图。客户端103包括(例如)具有处理器903和存储器906的至少一个处理器电路，处理器903和存储器906两者耦合到本地接口909。为此，客户端103可包括(例如)至少一个客户端计算机或类似装置。如可了解，本地接口909可包括(例如)具有随附地址/控制总线的数据总线或其它总线结构。可

类似于客户端103来对计算装置106和112进行说明，且以下论述也与计算装置106和112有关。

[0137] 可由处理器903执行的数据和若干组件两者存储在存储器906中。明确地说，浏览器121、认证管理客户端124以及可能还有其它应用程序存储在存储器906中且可由处理器903执行。数据存储装置127和其它数据也可存储在存储器906中。另外，操作系统可存储在存储器906中且可由处理器903执行。

[0138] 应理解，如可了解，可以有其它应用程序存储在存储器906中且可由处理器903执行。在本文中论述的任何组件实施为软件形式的情况下，可使用多种编程语言中的任一种，例如C、C++、C#、Objective C、Java®、JavaScript®、Perl、PHP、VisualBasic®、Python®、Ruby、Delphi®、Flash®或其它编程语言。

[0139] 多个软件组件存储在存储器906中且可由处理器903执行。就此来说，术语“可执行”表示呈最终可由处理器903运行的形式的程序文件。可执行程序的实例可以是(例如)可翻译为呈可下载到存储器906的随机存取部分中且由处理器903运行的格式的机器代码的经编译程序、可以用能够下载到存储器906的随机存取部分中且由处理器903执行的适当格式(例如目标代码)来表达的源代码或可以通过另一可执行程序解译以在存储器906的随机存取部分中产生指令以供处理器903执行的源代码等等。可执行程序可存储在存储器906的任何部分或组件中，包括(例如)随机存取存储器(RAM)、只读存储器(ROM)、硬盘、固态硬盘、USB闪存盘、存储卡、光盘(例如压缩光盘(CD)或数字通用光盘(DVD)、软盘、磁带或其它存储组件。

[0140] 存储器906在本文中被定义为包括易失性和非易失性存储器和数据存储组件两类。易失性组件是在失去电力之后不会留存数据值的那些组件。非易失性组件是在失去电力之后还留存数据的那些组件。因此，存储器906可包括(例如)随机存取存储器(RAM)、只读存储器(ROM)、硬盘、固态硬盘、USB闪存盘、经由存储卡读取器存取的存储卡、经由相关联的软盘驱动器存取的软盘、经由光盘驱动器存取的光盘、经由适当磁带驱动器存取的磁带和/或其它存储器组件或者这些存储器组件中的任两者或两者以上的组合。另外，RAM可包括(例如)静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)或磁性随机存取存储器(MRAM)以及其它此类装置。ROM可包括(例如)可编程只读存储器(PROM)、可擦除可编程只读存储器(EPROM)、电可擦除可编程只读存储器(EEPROM)或其它类似存储装置。

[0141] 此外，分别地，处理器903可表示多个处理器903，且存储器906可表示在并行处理电路中操作的多个存储器906。在这样一种情况中，本地接口909可以是方便多个处理器903中的任两者之间、任一处理器903与存储器906中的任一个之间或存储器906中的任两者之间等等的通信的适当网络。本地接口909可包括经设计以协调此通信(包括(例如)执行负载平衡)的额外系统。处理器903可以是电的或某一其它可用构造。

[0142] 虽然浏览器121、认证管理客户端124、网络页面服务器136(图1)、认证服务137(图1)、认证管理服务163(图1)以及本文中描述的其它各种系统可如上文所论述用由通用硬件执行的软件或代码来体现，但作为替代方案，它们也可由专用硬件或软件/通用硬件和专用硬件的组合来体现。如果以专用硬件来体现，那么上述每一个可实施为使用多种技术中的任一个或组合的电路或状态机。这些技术可包括但不限于具有用于在应用一个或多个数据信号之后即刻实施各种逻辑功能的逻辑门的离散逻辑电路、具有适当逻辑门的专用集成电

路或者其它组件等等。此类技术一般是本领域的技术人员众所周知的，因此本文中不进行详细描述。

[0143] 图3到图8中的流程图示出了认证管理客户端124、认证端点139(图1)和认证管理服务163的多个部分的实现方案的功能性和操作。如果以软件来体现，那么每一框可表示包括实施指定逻辑功能的程序指令的模块、区段或代码部分。所述程序指令可体现为以下形式：包括以编程语言编写的人类可读语句的源代码或包括可通过合适的执行系统(例如计算机系统中的处理器903或其它系统)辨识的数字指令的机器代码。机器代码可由源代码等转换而来。如果以硬件体现，那么每一框可表示用以实施指定逻辑功能的一个电路或多个互连电路。

[0144] 虽然图3到图8中的流程图示出了特定的执行次序，但应理解，执行次序可不同于所描绘的次序。举例来说，两个或两个以上框的执行次序可相对于所示的次序有所打乱。此外，图3到图8中连续示出的两个或两个以上框可以同时执行或者部分同时执行。另外，在一些实施方案中，可以跳过或省略图3到图8中所示的框中的一个或多个。另外，可向本文中描述的逻辑流增添任何数目的计数器、状态变量、警告信号灯或消息，以便实现增强的功用、计帐、性能测量或提供故障查找辅助等等。应理解，所有此类变化都属于本公开的范围内。

[0145] 此外，本文中描述的包括软件或代码的任何逻辑或应用程序(包括浏览器121、认证管理客户端124、网络页面服务器136、认证服务137和认证管理服务163)可体现在任何非暂时性计算机可读媒体中以供指令执行系统(例如计算机系统中的处理器903或其它系统)使用或与指令执行系统结合使用。在这个意义上，逻辑可包括(例如)包括可从计算机可读媒体提取且由指令执行系统执行的指令和声明的语句。在本公开的上下文中，“计算机可读媒体”可以是可容纳、存储或维护本文中所描述的逻辑或应用程序以供指令执行系统使用或与指令执行系统结合使用的任何媒体。

[0146] 计算机可读媒体可包括许多物理媒体中的任一个，例如磁性、光学或半导体媒体。合适计算机可读媒体的更多特定实例将包括但不限于磁带、软磁盘、硬磁盘、存储卡、固态硬盘、USB闪存盘或光盘。此外，计算机可读媒体可以是随机存取存储器(RAM)，包括(例如)静态随机存取存储器(SRAM)和动态随机存取存储器(DRAM)或者磁性随机存取存储器(MRAM)。另外，计算机可读媒体可以是只读存储器(ROM)、可编程只读存储器(PROM)、可擦除可编程只读存储器(EPROM)、电可擦除可编程只读存储器(EEPROM)或其它类型的存储装置。

[0147] 应强调，本公开的上述实施方案仅仅是为了清楚地理解本公开的原理而陈述的实现方案的可能实例。在不实质脱离本公开的精神和原理的情况下，可以对上述实施方案作出许多变动和修改。所有此类修改和变动在本文中意欲包括在本公开的范围内且受以下技术方案保护。

[0148] 可以鉴于以下条款来描述本公开的实施方案：

[0149] 条款1.一种体现可在计算装置中执行的程序的非暂时性计算机可读媒体，所述程序包括：

[0150] 维护多个用户中的每一个的用于多个网络站点的多个账户的代码；

[0151] 对所述用户中的一个进行认证的代码；

[0152] 使用主控安全凭证对与所述用户中的所述一个的所述账户有关的数据进行解密的代码，所述数据包括与所述账户有关的多个安全凭证和关于所述用户中的所述一个的一

组信息；

[0153] 确定所述计算装置将要访问所述网络站点中的一个的第一受保护资源的代码；

[0154] 使用与所述账户有关的所述数据中的第一安全凭证来访问所述第一受保护资源的代码；

[0155] 确定所述计算装置将要访问另一网络站点的第二受保护资源的代码；

[0156] 响应于确定所述账户不能够访问所述第二受保护资源且响应于从所述用户中的所述一个获得同意指示而借助所述另一网络站点来创建新账户的代码，其中将关于所述用户中的所述一个的所述一组信息的子集自动提供给所述另一网络站点以创建所述新账户；

[0157] 自动地产生用于所述新账户的第二安全凭证的代码；以及

[0158] 使用所述第二安全凭证来访问所述第二受保护资源的代码。

[0159] 条款2.如条款1所述的非暂时性计算机可读媒体，其中所述程序进一步包括在预定义的不活动时段之后结束所述用户中的所述一个的会话的代码，且在所述会话结束时将已解密的所述数据从所述计算装置移除。

[0160] 条款3.如条款1或2中任一项所述的非暂时性计算机可读媒体，其中所述程序进一步包括在所述用户中的所述一个的会话结束之后对所述用户中的另一个进行认证的代码。

[0161] 条款4.一种系统，其包括：

[0162] 计算装置；以及

[0163] 可在所述计算装置中执行的认证管理客户端应用程序，所述认证管理客户端应用程序包括：维护用户的用于多个网络站点的多个账户的逻辑；

[0164] 确定所述计算装置将要访问网络站点的受保护资源的逻辑；

[0165] 确定所述账户是否能够访问所述受保护资源的逻辑；以及

[0166] 响应于确定所述账户不能够访问所述受保护资源而借助所述网络站点来创建新账户的逻辑，其中将关于所述用户的一组信息自动提供给所述网络站点以创建所述新账户。

[0167] 条款5.如条款4所述的系统，其中所述认证管理客户端应用程序进一步包括：

[0168] 响应于确定所述账户不能够访问所述受保护资源而从所述用户获得所述用户没有现有账户能够访问所述受保护资源的确认的逻辑；且

[0169] 其中所述创建新账户的逻辑被配置来响应于所述确认而创建所述新账户。

[0170] 条款6.如条款4或5中任一项所述的系统，其中所述创建新账户的逻辑进一步包括确定所述用户先前是否授权使用所述一组信息进行自动账户创建的逻辑。

[0171] 条款7.如条款4到6中任一项所述的系统，其中所述创建新账户的逻辑进一步包括根据安全凭证规范自动地产生用于所述新账户的安全凭证的逻辑。

[0172] 条款8.如条款4到7中任一项所述的系统，其中所述创建新账户的逻辑进一步包括根据在所述计算装置与所述网络站点之间的传输层安全性(TLS)会话中产生的对称密钥来自动地建立用于所述新账户的安全凭证的逻辑。

[0173] 条款9.如条款4到8中任一项所述的系统，其中所述维护账户的逻辑被配置来维护处于经加密状态的与所述账户有关的数据且响应于从所述用户获得的主控安全凭证对与所述账户有关的所述数据进行解密。

[0174] 条款10.如条款9所述的系统，其中所述维护账户的逻辑被配置来：

[0175] 使用所述主控安全凭证对密钥进行解密;以及

[0176] 使用所述密钥对与所述账户有关的所述数据进行解密。

[0177] 条款11.如条款4到10中任一项所述的系统,其中所述创建新账户的逻辑进一步包括在创建所述新账户之前从所述用户获得额外信息的逻辑,所述额外信息包括在自动提供给所述网络站点以创建所述新账户的所述一组信息中。

[0178] 条款12.如条款4到11中任一项所述的系统,其中所述创建新账户的逻辑进一步包括在创建所述新账户之前从所述用户获得同意指示的逻辑。

[0179] 条款13.如条款12所述的系统,其中所述一组信息对应于关于所述用户的信息超集的多个子集中的一个,所述创建新账户的逻辑被配置来从所述网络站点获得所述子集中的所述一个的标识,且所述获得同意指示的逻辑被配置来向所述用户指示所述子集中的所述一个。

[0180] 条款14.如条款4到13中任一项所述的系统,其中所述一组信息包括所述用户的姓名。

[0181] 条款15.如条款4到14中任一项所述的系统,其中所述一组信息包括所述用户的实际地址。

[0182] 条款16.如条款4到15中任一项所述的系统,其中所述一组信息包括所述用户的出生日期。

[0183] 条款17.如条款4到16中任一项所述的系统,其中所述一组信息包括所述用户的联系信息。

[0184] 条款18.如条款4到17中任一项所述的系统,其中所述新账户是借助第三方标识提者来创建的,且所述新账户能够访问与多个网络站点操作者相关联的多个网络站点上的多个受保护资源。

[0185] 条款19.一种方法,其包括以下步骤:

[0186] 在计算装置中维护用户的用于多个网络站点的多个账户;

[0187] 在所述计算装置中确定所述计算装置将要访问网络站点的受保护资源;

[0188] 在所述计算装置中确定所述账户是否能够访问所述受保护资源;以及

[0189] 在所述计算装置中响应于确定所述账户不能够访问所述受保护资源而升级所述账户中的一个,其中将关于所述用户的一组信息提供给所述网络站点以升级所述账户中的一个。

[0190] 条款20.如条款19所述的方法,其中所述一组信息先前没有提供给所述网络站点用来创建所述账户中的一个。

[0191] 条款21.如条款19或20所述的方法,其进一步包括以下步骤:

[0192] 在所述计算装置中确定所述计算装置将要访问所述网络站点的另一受保护资源;

[0193] 在所述计算装置中确定所述账户是否能够访问所述另一受保护资源;

[0194] 在所述计算装置中响应于确定所述账户能够访问所述另一受保护资源而将与所述账户中的一个相关联的所存储安全凭证自动提供给所述网络站点;以及

[0195] 在所述计算装置中从所述网络站点访问所述另一受保护资源。

[0196] 条款22.如条款19到21中任一项所述的方法,其中所述升级步骤进一步包括在所述计算装置中从所述用户获得所述一组信息中的至少一个元素的步骤。

[0197] 条款23.如条款19到22中任一项所述的方法，其中所述升级步骤进一步包括在所述计算装置中从所存储的数据获得所述一组信息中的至少一个元素的步骤。

[0198] 条款24.如条款19到23中任一项所述的方法，其中所述升级步骤进一步包括在所述计算装置中从所述用户获得同意指示的步骤，且响应于获得所述同意指示而将所述一组信息自动提供给所述网络站点。

[0199] 条款25.如条款19到24中任一项所述的方法，其中所述维护步骤进一步包括在所述计算装置中维护处于经加密状态的用于所述账户的数据的步骤，且所述方法进一步包括以下步骤：

[0200] 在所述计算装置中从所述用户获得主控安全凭证；以及

[0201] 在所述计算装置中使用所述主控安全凭证对用于所述账户的所述数据进行解密。

[0202] 条款26.如条款25所述的方法，进一步包括在所述计算装置中从另一计算装置获得用于所述账户的所述数据的步骤。

[0203] 条款27.一种系统，其包括：

[0204] 计算装置；以及

[0205] 可在所述计算装置中执行的认证管理客户端应用程序，所述认证管理客户端应用程序包括：维护用户的用于多个网络站点的多个账户的逻辑，其中借助网络使用于所述账户的经加密安全凭证与认证管理服务同步；

[0206] 确定所述计算装置将要访问网络站点的受保护资源的逻辑；

[0207] 确定所述账户是否能够访问所述受保护资源的逻辑；以及

[0208] 响应于确定所述账户不能够访问所述受保护资源而使用旧账户向所述网络站点进行认证的逻辑，其中从所述用户获得用于所述旧账户的至少一个安全凭证。

[0209] 条款28.如条款27所述的系统，其中所述认证管理客户端应用程序进一步包括将所述旧账户增添到由所述维护逻辑维护的所述账户的逻辑。

[0210] 条款29.如条款28所述的系统，其中所述认证管理客户端应用程序进一步包括将所述至少一个安全凭证转变为根据与所述网络站点相关联的安全凭证规范自动产生的至少一个替换安全凭证的逻辑。

[0211] 条款30.如条款27到29中任一项所述的系统，其中所述认证管理客户端应用程序进一步包括从所述认证管理服务获得所述经加密安全凭证的逻辑。

[0212] 条款31.一种体现可在计算装置中执行的至少一个程序的非暂时性计算机可读媒体，所述至少一个程序包括：

[0213] 响应于从用户获得主控安全凭证对由第一认证管理客户端所存储的与用户账户相关联的安全凭证进行解密的代码；

[0214] 使用所述第一认证管理客户端借助认证协议将第一认证请求发送到与网络站点的受保护资源相关联的认证服务的代码，所述第一认证请求指定与所述用户账户相关联的所述安全凭证；在响应于所述第一认证请求而被所述认证服务认证之后访问所述受保护资源的代码；

[0215] 将所述安全凭证从所述第一认证管理客户端导入到第二认证管理客户端的代码；

[0216] 使用所述第二认证管理客户端借助所述认证协议将第二认证请求发送到所述认证服务的代码，所述第二认证请求指定所述安全凭证；以及

[0217] 在响应于所述第二认证请求而被所述认证服务认证之后访问所述受保护资源的代码。

[0218] 条款32.如条款31所述的非暂时性计算机可读媒体，其中所述第一认证管理客户端和所述第二认证管理客户端是由认证管理服务的不同提供者部署。

[0219] 条款33.如条款31或32所述的非暂时性计算机可读媒体，其中所述程序进一步包括：

[0220] 响应于所述用户尝试访问所述网络站点的另一受保护资源而从所述用户获得升级确认的代码，所述用户账户被拒绝访问所述另一受保护资源；

[0221] 使用所述第二认证管理客户端将对所述用户账户的账户升级请求发送给所述认证服务的代码，所述账户升级请求指定关于所述用户的一组信息；以及

[0222] 在升级所述用户账户之后访问所述网络站点的所述另一受保护资源的代码。

[0223] 条款34.一种系统，其包括：

[0224] 至少一个计算装置；以及

[0225] 可在所述至少一个计算装置中执行的认证服务，所述认证服务包括：

[0226] 借助认证协议从在客户端计算装置中执行的认证管理客户端获得认证请求的逻辑，所述认证请求指定与用户账户相关联的安全凭证；

[0227] 至少部分基于所述认证管理客户端的密切度来确定是否支持所述认证管理客户端的逻辑；以及

[0228] 响应于所述认证请求且响应于支持所述认证管理客户端而在所述客户端计算装置处对所述用户账户进行认证以便访问网络站点的至少一个受保护资源的逻辑。

[0229] 条款35.如条款34所述的系统，其中具有不同密切度的多个认证管理客户端被配置来使用所述认证协议。

[0230] 条款36.如条款34或35所述的系统，其中支持所述认证管理客户端中的至少一个，且不支持所述认证管理客户端中的至少一个。

[0231] 条款37.如条款34到36中任一项所述的系统，其中所述认证服务被配置来借助用户代理字符串来识别所述认证管理客户端的所述密切度。

[0232] 条款38.如条款34到37中任一项所述的系统，其中所述认证服务进一步包括：

[0233] 从所述认证管理客户端获得账户创建请求的逻辑，所述账户创建请求指定关于用户的一组信息；以及

[0234] 响应于确定支持所述认证管理客户端而根据所述账户创建请求来创建所述用户账户的逻辑。

[0235] 条款39.如条款34到38中任一项所述的系统，其中所述用户账户与由多个实体操作的多个网络站点相关联。

[0236] 条款40.如条款34到39中任一项所述的系统，其中所述认证服务由标识提供者操作，所述认证服务进一步包括向所述认证管理客户端发送带标牌的经验数据的逻辑，且所述认证管理客户端被配置来至少部分基于所述带标牌的经验数据来在所述客户端计算装置中为所述标识提供者定制用户界面。

[0237] 条款41.如条款34到40中任一项所述的系统，其中所述认证服务进一步包括：

[0238] 在认证之后获得更换用于所述用户账户的所述安全凭证的请求的逻辑；以及

[0239] 响应于所述更换安全凭证的请求而建立用于所述用户账户的新安全凭证的逻辑。

[0240] 条款42.如条款41所述的系统，其中所述建立新安全凭证的逻辑进一步包括：

[0241] 自动地产生所述新安全凭证的逻辑；以及

[0242] 将所述新安全凭证提供给所述认证管理客户端的逻辑。

[0243] 条款43.如条款41或42所述的系统，其中所述更换安全凭证的请求是在所述认证管理客户端中自动发出。

[0244] 条款44.如条款41或42所述的系统，其中所述更换安全凭证的请求不是在所述认证管理客户端中发出。

[0245] 条款45.如条款41到44中任一项所述的系统，其中所述认证服务进一步包括：

[0246] 将安全凭证规范提供给所述认证管理客户端的逻辑；且

[0247] 其中所述更换安全凭证的请求指定所述新安全凭证，且所述新安全凭证是通过所述认证管理客户端根据所述安全凭证规范来自动产生。

[0248] 条款46.一种方法，其包括以下步骤：

[0249] 在至少一个计算装置中借助认证协议从在第一客户端计算装置中执行的第一认证管理客户端获得第一认证请求，所述第一认证请求指定与第一用户账户相关联的第一安全凭证；

[0250] 在所述至少一个计算装置中响应于所述第一认证请求而在所述第一客户端计算装置处对所述第一用户账户进行认证以便访问网络站点的至少一个受保护资源；

[0251] 在所述至少一个计算装置中借助所述认证协议从在第二客户端计算装置中执行的第二认证管理客户端获得第二认证请求，所述第二认证请求指定与第二用户账户相关联的第二安全凭证；

[0252] 在所述至少一个计算装置中响应于所述第二认证请求而在所述第二客户端计算装置处对所述第二用户账户进行认证以便访问所述网络站点的所述至少一个受保护资源；且

[0253] 其中所述第一认证管理客户端和所述第二认证管理客户端是由认证管理服务的不同提供者部署。

[0254] 条款47.如条款46所述的方法，其进一步包括以下步骤：

[0255] 在所述至少一个计算装置中向所述第一认证管理客户端和所述第二认证管理客户端发送带标牌的经验数据；且

[0256] 其中所述第一认证管理客户端被配置来至少部分基于所述带标牌的经验数据来在所述第一客户端计算装置中定制第一用户界面，且所述第二认证管理客户端被配置来至少部分基于所述带标牌的经验数据来在所述第二客户端计算装置中定制第二用户界面。

[0257] 条款48.如条款46或47所述的方法，进一步包括以下步骤：

[0258] 在所述至少一个计算装置中响应于所述第一认证请求而确定是否支持所述第一认证管理客户端；以及

[0259] 在所述至少一个计算装置中响应于所述第二认证请求而确定是否支持所述第二认证管理客户端。

[0260] 条款49.如条款46到48中任一项所述的方法，进一步包括以下步骤：

[0261] 在所述至少一个计算装置中在认证之后获得更换用于所述第一用户账户的所述

第一安全凭证的请求，所述更换第一安全凭证的请求是在所述第一认证管理客户端中自动发出；以及

[0262] 在所述至少一个计算装置中响应于所述更换第一安全凭证的请求而建立用于所述第一用户账户的新安全凭证。

[0263] 条款50.如条款49所述的方法，其中所述新安全凭证对应于所述第一客户端计算装置与所述至少一个计算装置之间的传输层安全性(TLS)会话使用的对称密钥。

[0264] 条款51.如条款46到50中任一项所述的方法，其进一步包括以下步骤：

[0265] 在所述至少一个计算装置中在认证之后从所述第一认证管理客户端获得账户升级请求，所述账户升级请求指定关于用户的一组信息；

[0266] 在所述至少一个计算装置中根据所述账户升级请求来升级所述第一用户账户；以及

[0267] 在所述至少一个计算装置中在升级之后在所述第一客户端计算装置处对所述第一用户账户进行认证以便访问所述网络站点的另一受保护资源。

[0268] 条款52.如条款51所述的方法，其中所述第一认证管理客户端被配置来响应于所述用户尝试在所述第一客户端计算装置中访问所述另一受保护资源且响应于从所述用户获得同意指示而向所述至少一个计算装置发送所述账户升级请求。

[0269] 条款53.一种体现可在计算装置中执行的至少一个程序的非暂时性计算机可读媒体，所述至少一个程序包括：

[0270] 维护用户的用于多个网络站点的多个账户的代码；

[0271] 确定所述计算装置将要访问网络站点的受保护资源的代码；

[0272] 至少部分基于所述网络站点的域名和从所述网络站点获得的所支持的第三方认证提供者的列表而识别被所述网络站点接受的多个账户以便向所述受保护资源进行认证的代码；

[0273] 使得显示被配置来获得对所述多个所述账户中的一个的用户选择的用户界面的代码；

[0274] 存储对与所述网络站点的所述域名相关联的所述多个所述账户中的所述一个的所述用户选择的代码；以及

[0275] 使用与所述多个所述账户中通过所述用户选择选择的所述一个账户相关联的安全凭证向所述网络站点进行自动认证的代码。

[0276] 条款54.如条款53所述的非暂时性计算机可读媒体，其中所述多个所述账户中的至少一个与多个所述网络站点相关联。

[0277] 条款55.如条款53或54所述的非暂时性计算机可读媒体，其中所述识别所述多个所述账户的代码进一步包括将所述域名的二级部分与不同的所存储域名的二级部分相比较的代码。

[0278] 条款56.一种系统，其包括：

[0279] 计算装置；以及

[0280] 可在所述计算装置中执行的认证管理客户端应用程序，所述认证管理客户端应用程序包括：维护用户的用于多个网络站点的多个账户的逻辑；

[0281] 确定所述计算装置将要访问网络站点的受保护资源的逻辑；

[0282] 根据所述网络站点的域名来识别所述账户中的一个的逻辑，所述账户中的所述一个与具有与所述域名不同的域名的不同网络站点相关联；以及

[0283] 使用与所述账户中的所述一个相关联的安全凭证向所述网络站点进行自动认证的逻辑。

[0284] 条款57.如条款56所述的系统，其中所述识别所述账户中的所述一个的逻辑进一步包括：

[0285] 向认证管理服务发送账户识别请求的逻辑，所述账户识别请求包括所述网络站点的所述域名；以及

[0286] 响应于所述账户识别请求而从所述认证管理服务获得账户标识的逻辑，所述账户标识指定所述账户中的所述一个。

[0287] 条款58.如条款56或57所述的系统，其中所述不同网络站点的所述不同域名包括与所述域名共同的部分，且所述共同部分不包括一级域名在内。

[0288] 条款59.如条款56到58中任一项所述的系统，其中所述网络站点是所述不同网络站点的附属网络站点。

[0289] 条款60.如条款56到59中任一项所述的系统，其中所述向所述网络进行自动认证的逻辑进一步被配置来在借助所述网络站点进行自动认证之前从所述用户获得同意指示。

[0290] 条款61.如条款60所述的系统，其中所述同意指示事先由所述用户存储。

[0291] 条款62.如条款56到61中任一项所述的系统，其中所述识别所述账户中的所述一个的逻辑进一步被配置来根据所述网络站点的二级域名而识别所述账户中的所述一个。

[0292] 条款63.如条款56到62中任一项所述的系统，其中所述认证管理客户端应用程序进一步包括：

[0293] 确定所述计算装置将要访问另一网络站点的另一受保护资源的逻辑；

[0294] 根据所述另一网络站点的另一域名来识别所述账户中的所述一个的逻辑；以及

[0295] 使用与所述账户中的所述一个相关联的所述安全凭证向所述另一网络站点进行自动认证的逻辑。

[0296] 条款64.如条款63所述的系统，其中所述域名和所述另一域名各自具有相同的二级域名和不同的一级域名。

[0297] 条款65.如条款56到64中任一项所述的系统，其中所述识别所述账户中的所述一个的逻辑进一步包括：

[0298] 根据所述网络站点的所述域名来识别多个所述账户的逻辑；

[0299] 产生被配置来获得对所述多个所述账户中的一个的用户选择的用户界面的逻辑；以及

[0300] 根据所述用户选择来识别所述账户中的所述一个的逻辑。

[0301] 条款66.如条款56到65中任一项所述的系统，其中所述识别所述账户中的所述一个的逻辑进一步包括：

[0302] 根据所述网络站点的所述域名来识别多个所述账户的逻辑；以及

[0303] 根据所存储的用户偏好来从所述多个所述账户中识别出所述账户中的所述一个的逻辑。

[0304] 条款67.一种方法，包括以下步骤：

[0305] 在计算装置中维护用户的用于多个网络站点的多个账户；

[0306] 在所述计算装置中确定所述计算装置将要访问网络站点的受保护资源；

[0307] 在所述计算装置中确定被所述网络站点接受的多个所述账户以便向所述受保护资源进行认证；

[0308] 在所述计算装置中选择所述多个所述账户中的一个以便向所述受保护资源进行认证；以及在所述计算装置中使用与所述多个所述账户中所选择的所述一个账户相关联的安全凭证来向所述网络站点进行自动认证。

[0309] 条款68.如条款67所述的方法，其中所述选择步骤进一步包括以下步骤：

[0310] 使得在所述计算装置中显示被配置来获得对所述多个所述账户中的所述一个的用户选择的用户界面；以及

[0311] 在所述计算装置中获得所述用户选择。

[0312] 条款69.如条款67或68所述的方法，其中所述选择步骤进一步包括在所述计算装置中根据所存储的偏好来选择所述多个账户中的所述一个的步骤。

[0313] 条款70.如条款67到69中任一项所述的方法，其中所述多个所述账户中的至少一个是借助第三方认证提供者来创建的。

[0314] 条款71.如条款67到70中任一项所述的方法，其中所述在所述计算装置中确定被所述网络站点接受的所述多个所述账户以便向所述受保护资源进行认证的步骤进一步包括在所述计算装置中至少部分基于所述网络站点的域名来识别所述多个所述账户的步骤。

[0315] 条款72.如条款67到71中任一项所述的方法，其中所述在所述计算装置中确定被所述网络站点接受的所述多个所述账户以便向所述受保护资源进行认证的步骤进一步包括在所述计算装置中从所述网络站点获得多个所支持认证提供者的列表的步骤。

[0316] 条款73.一种体现可在计算装置中执行的程序的非暂时性计算机可读媒体，所述程序包括：

[0317] 向认证管理服务发送对账户数据的请求的代码，所述请求指定用于访问所述账户数据的安全凭证和客户端识别令牌，所述账户数据包括用户的用于访问多个网络站点的多个安全凭证，其中所述认证管理服务被配置来维护处于加密形式的所述账户数据；

[0318] 响应于对所述账户数据的所述请求而从所述认证管理服务获得所述账户数据的代码；

[0319] 从所述用户获得主控安全凭证的代码；

[0320] 使用所述主控安全凭证对所述账户数据进行解密的代码；

[0321] 从所述用户获得将所述安全凭证重置为由所述用户指定的单个临时安全凭证的请求的代码；以及

[0322] 通过以下操作将所述安全凭证中的每一个自动重置为所述单个临时安全凭证的代码：

[0323] 使用所述相应安全凭证向相应认证服务进行认证；以及

[0324] 向所述相应认证服务发送指定所述单个临时安全凭证的对应重置请求。

[0325] 条款74.如条款73所述的非暂时性计算机可读媒体，其中所述程序进一步包括施行所述单个临时安全凭证的终止的代码。

[0326] 条款75.如条款73或74所述的非暂时性计算机可读媒体，其中所述程序进一步包

括：

[0327] 从所述用户获得将所述单个临时安全凭证重置为多个新的安全凭证的代码；以及

[0328] 通过以下步骤针对每一认证服务自动地重置所述单个临时安全凭证的代码：

[0329] 使用所述单个临时安全凭证向所述相应认证服务进行认证；以及

[0330] 针对所述相应认证服务将所述单个临时安全凭证重置为相应的新安全凭证。

[0331] 条款76.一种系统，其包括：

[0332] 至少一个计算装置；以及

[0333] 可在所述至少一个计算装置中执行的服务，所述服务包括：

[0334] 存储包括与用户的多个网络站点相关联的多个安全凭证的账户数据的逻辑，所述账户数据以加密形式来存储；

[0335] 从客户端获得对所述账户数据的请求的逻辑，所述请求指定用于访问所述账户数据的安全凭证；以及

[0336] 响应于确定所述客户端对应于预先授权的客户端且响应于确定用于访问所述账户数据的所述安全凭证是有效的而向所述客户端发送所述账户数据的逻辑。

[0337] 条款77.如条款76所述的系统，其中所述安全凭证由所述客户端的可卸除式计算机可读媒体存储。

[0338] 条款78.如条款76或77所述的系统，其中所述服务进一步包括至少部分基于所述请求的源网络地址来确定所述客户端是否对应于预先授权的客户端的逻辑。

[0339] 条款79.如条款76到78中任一项所述的系统，其中所述服务进一步包括至少部分基于所述请求中呈现的客户端识别令牌来确定所述客户端是否对应于预先授权的客户端的逻辑。

[0340] 条款80.如条款76到79中任一项所述的系统，其中所述账户数据是未从所述经加密形式解密发送到所述客户端。

[0341] 条款81.如条款76到80中任一项所述的系统，其中所述服务是由相对于所述网络站点的第三方实体操作。

[0342] 条款82.如条款76到81中任一项所述的系统，其中所述服务进一步包括：

[0343] 从所述客户端获得使用多个账户数据恢复机制中的一个的请求的逻辑；

[0344] 响应于确定所述客户端被授权使用所述多个账户数据恢复机制中的所述一个而启用对所述账户数据恢复机制中的所述一个的使用的逻辑；以及

[0345] 响应于确定所述客户端不被授权使用所述多个账户数据恢复机制中的所述一个而停用对所述账户数据恢复机制中的所述一个的使用的逻辑。

[0346] 条款83.如条款82所述的系统，其中对使用所述账户数据恢复机制的选定子集的授权是依照客户端来指定。

[0347] 条款84.一种方法，其包括以下步骤：

[0348] 在计算装置中向认证管理服务发送对账户数据的请求，所述请求指定用于访问所述账户数据的安全凭证，所述账户数据包括用户的用于访问多个网络站点的多个安全凭证；

[0349] 在所述计算装置中响应于对所述账户数据的所述请求而从所述认证管理服务获得所述账户数据；

[0350] 在所述计算装置中获得主控安全凭证；

[0351] 在所述计算装置中使用所述主控安全凭证对所述账户数据进行解密；以及

[0352] 在所述计算装置中将所述安全凭证中的每一个自动重置为相应的新安全凭证。

[0353] 条款85.如条款84所述的方法，其中所述在所述计算装置中获得所述主控安全凭证的步骤进一步包括以下步骤：

[0354] 在所述计算装置中从可卸除式计算机可读媒体获得所述主控安全凭证的经加密版本；以及在所述计算装置中至少部分基于存储在所述计算装置中的另一安全凭证而对所述主控安全凭证的所述经加密版本进行解密。

[0355] 条款86.如条款84或85所述的方法，其中所述主控安全凭证与所述计算装置的操作系统相关联。

[0356] 条款87.如条款84到86中任一项所述的方法，其进一步包括以下步骤：

[0357] 在所述计算装置中产生多个一次性安全凭证；以及

[0358] 在所述计算装置中将所述一次性安全凭证与所述账户数据一起存储。

[0359] 条款88.如条款87所述的方法，其进一步包括以下步骤：

[0360] 在所述计算装置中从所述用户获得所述一次性安全凭证中的一个；

[0361] 在所述计算装置中至少部分基于所述一次性安全凭证中的所述一个而产生所述主控安全凭证；以及

[0362] 在所述计算装置中将所述一次性安全凭证中的所述一个从所述账户数据移除。

[0363] 条款89.如条款84到88中任一项所述的方法，其中所述自动重置步骤是响应于所述用户起始的重置请求而执行。

[0364] 条款90.如条款89所述的方法，其进一步包括以下步骤：

[0365] 在所述计算装置中响应于所述重置请求而向所述用户呈现至少一个基于知识的问题；

[0366] 在所述计算装置中从所述用户获得对所述至少一个基于知识的问题的至少一个回答；

[0367] 在所述计算装置中向所述认证管理服务进行查询以确定所述至少一个回答是否有效；且

[0368] 其中所述自动重置步骤是响应于所述至少一个回答是有效的而执行。

[0369] 条款91.如条款84到90中任一项所述的方法，其中所述自动重置步骤是响应于预定义的重置时间间隔而执行。

[0370] 条款92.如条款84到91中任一项所述的方法，其中所述自动重置步骤进一步包括以下步骤：

[0371] 对于所述安全凭证中的每一个：

[0372] 在所述计算装置中使用所述相应安全凭证向与所述网络站点中的至少一个相关联的相应认证服务进行认证；以及

[0373] 在所述计算装置中向所述相应认证服务发送对应的重置请求。

[0374] 条款93.如条款84到92中任一项所述的方法，其中所述安全凭证中的一个与多个所述网络站点相关联。

[0375] 条款94.如条款84到93中任一项所述的方法，其中对所述账户数据的所述请求包

括由所述计算装置存储的客户端识别令牌。

[0376] 条款95.如条款84到94中任一项所述的方法，其中所述新安全凭证对应于从所述用户获得的单个新安全凭证。

[0377] 条款96.如条款84到95中任一项所述的方法，进一步包括在所述计算装置中根据与所述对应网络站点中的至少一个相关联的至少一个安全凭证规范来自动地产生所述新安全凭证中的至少一些的步骤。

[0378] 条款97.如条款84到96中任一项所述的方法，其进一步包括以下步骤：

[0379] 在所述计算装置中获得手动导出所述新安全凭证的请求；以及

[0380] 在所述计算装置中以明文来呈现所述安全凭证的列表。

[0381] 条款98.如条款84到97中任一项所述的方法，进一步包括在所述计算装置中更新由所述认证管理服务维护的所述账户数据以存储所述新安全凭证的步骤。

[0382] 条款99.如条款98所述的方法，其中所述更新步骤进一步包括在向所述认证管理服务发送所述账户数据之前在所述计算装置中使用所述主控安全凭证对包括所述新安全凭证的所述账户数据进行加密的步骤。

[0383] 条款100.一种体现可在计算装置中执行的程序的非暂时性计算机可读媒体，所述程序包括：

[0384] 经由网络从认证管理服务获得用于用户的用于多个网络站点的多个账户的账户数据的代码，所述账户数据包括用于所述账户中的每一个的相应安全凭证；

[0385] 响应于所述用户访问所述多个网络站点中的每一个而使用相应的多个所述账户来向与多个所述网络站点对应的多个认证服务进行自动认证的代码，其中为所述网络站点中的每一个建立相应会话；

[0386] 至少部分基于用户注销指示和预定的用户不活动时段的终止中的至少一个来确定将要执行注销的代码；以及

[0387] 通过结束所述会话中的每一个而执行所述注销的代码，所述执行注销的代码进一步被配置来：

[0388] 向所述认证服务中的每一个自动发送相应的注销指示；

[0389] 在所述计算装置中自动刷新与所述会话有关的数据；以及

[0390] 从所述计算装置自动刷新所述账户数据。

[0391] 条款101.如条款100所述的非暂时性计算机可读媒体，其中与所述会话有关的所述数据包括由在所述计算装置执行的浏览器应用程序存储的多个会话cookie。

[0392] 条款102.如条款100或101所述的非暂时性计算机可读媒体，其中所述账户数据是使用从所述用户获得的主控安全凭证来进行解密。

[0393] 条款103.一种系统，其包括：

[0394] 计算装置；以及

[0395] 可在所述计算装置中执行的认证客户端，所述认证客户端包括：

[0396] 维护用于用户的用于多个网络站点的多个账户的账户数据的逻辑，所述账户数据包括用于所述账户中的每一个的相应安全凭证；

[0397] 响应于所述用户访问所述多个所述网络站点中的每一个而使用相应的多个所述账户来向与多个所述网络站点对应的多个认证服务进行自动认证的逻辑，其中为所述网络

站点中的每一个建立相应会话；

[0398] 确定将要执行注销的逻辑；以及

[0399] 通过结束所述会话中的每一个而执行所述注销的逻辑。

[0400] 条款104.如条款103所述的系统，其中所述执行注销的逻辑被配置来向所述认证服务中的每一个自动发送相应的注销指示。

[0401] 条款105.如条款103或104所述的系统，其中所述执行注销的逻辑被配置来在所述计算装置中自动刷新与所述会话有关的数据。

[0402] 条款106.如条款105所述的系统，其中与所述会话有关的所述数据包括多个会话cookie。

[0403] 条款107.如条款103到106中任一项所述的系统，其中所述用户借助在所述计算装置中执行的浏览器应用程序来访问所述多个所述网络站点中的每一个。

[0404] 条款108.如条款103到107中任一项所述的系统，其中所述确定将要执行注销的逻辑被配置来从所述用户获得单个注销请求。

[0405] 条款109.如条款103到108中任一项所述的系统，其中所述确定将要执行注销的逻辑被配置来从所述用户获得切换用户请求。

[0406] 条款110.如条款103到109中任一项所述的系统，其中所述确定将要执行注销的逻辑被配置来确定预定的用户不活动时段是否已满。

[0407] 条款111.如条款103到110中任一项所述的系统，其中所述确定将要执行注销的逻辑被配置来确定所述用户是否已从操作系统账户注销。

[0408] 条款112.如条款103到111中任一项所述的系统，其中所述认证客户端被配置来从认证管理服务下载呈加密形式的所述账户数据。

[0409] 条款113.如条款112所述的系统，其中所述认证客户端被配置来使用从所述用户获得的主控安全凭证对所述账户数据进行解密。

[0410] 条款114.一种方法，其包括以下步骤：

[0411] 在计算装置中经由网络从认证管理服务获得用于用户的用于多个网络站点的多个账户的账户数据，所述账户数据包括用于所述账户中的每一个的相应安全凭证；

[0412] 在所述计算装置中响应于所述用户访问所述多个所述网络站点中的每一个而使用相应的多个所述账户来向与多个网络站点对应的多个认证服务进行自动认证，其中为所述网络站点中的每一个建立相应会话；

[0413] 在所述计算装置中确定将要执行注销；以及

[0414] 在所述计算装置中通过结束所述会话中的每一个而执行所述注销。

[0415] 条款115.如条款114所述的方法，其进一步包括在所述计算装置中使用从所述用户获得的主控安全凭证对所述账户数据进行解密的步骤。

[0416] 条款116.如条款114或115所述的方法，其进一步包括在所述计算装置中使用存储在所述计算机装置中的计算机可读媒体中的主控安全凭证来对所述账户数据进行解密的步骤。

[0417] 条款117.如条款114到116中任一项所述的方法，其中所述执行步骤进一步包括在所述计算装置中向所述认证服务中的每一个自动发送相应注销指示的步骤。

[0418] 条款118.如条款114到117中任一项所述的方法，其中所述执行步骤进一步包括在

所述计算装置中自动刷新与所述会话有关的数据的步骤。

[0419] 条款119.如条款114到118中任一项所述的方法，其中所述执行步骤进一步包括从所述计算装置自动刷新所述账户数据的步骤。

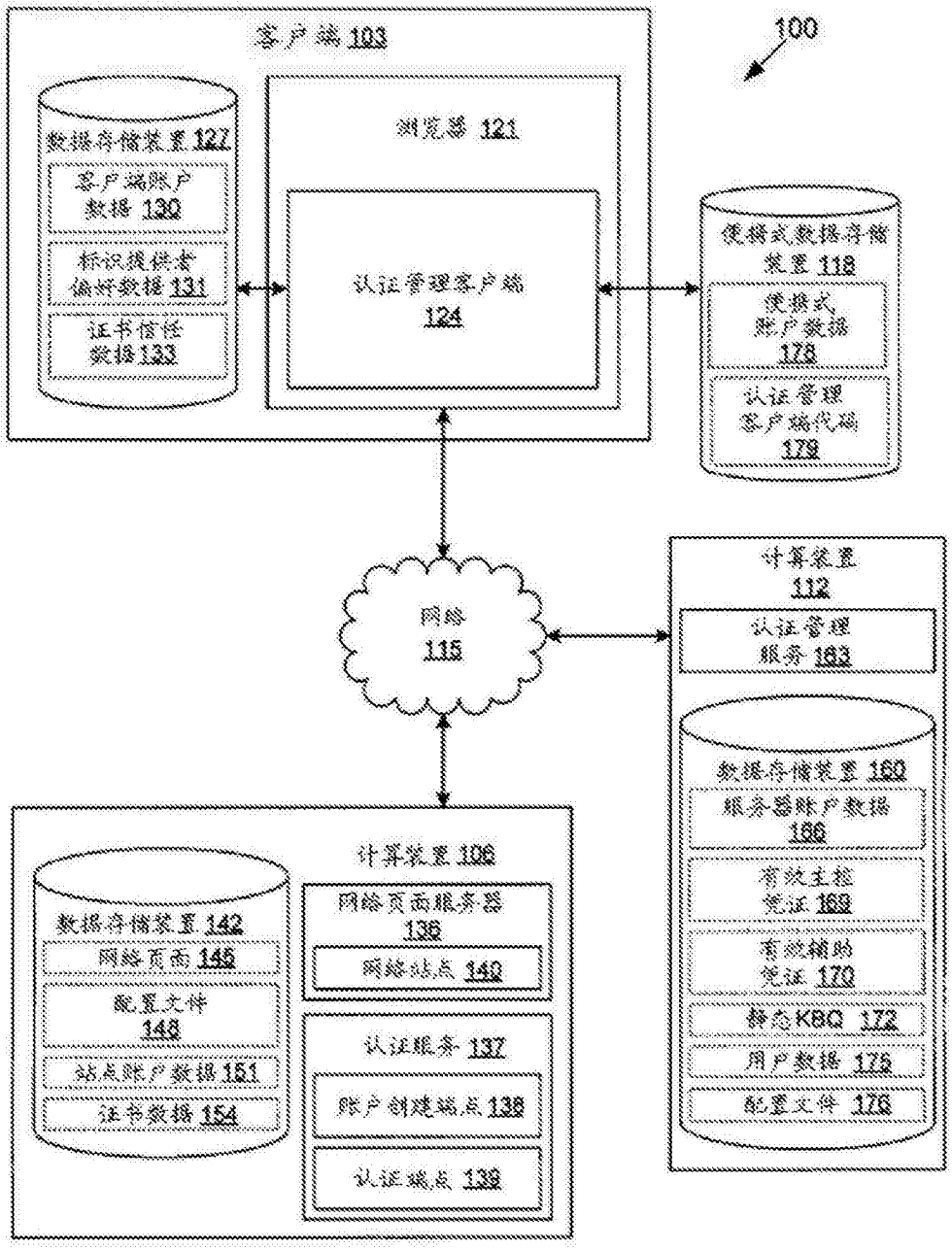

客户端 103
100
数据存储装置 127
客户端账户数据 130
标识提供者偏好数据 131
证书信任数据 133
浏览器 121
认证管理客户端 124
便携式数据存储装置 118
便携式账户数据 178
认证管理客户端代码 179
网络 115
计算装置 112
认证管理服务 163
数据存储装置 160
服务器账户数据 166
有效主张凭证 169
有效辅助凭证 170
静态KBQ 172
用户数据 175
配置文件 176
计算装置 106
数据存储装置 142
网络页面 145
配置文件 148
站点账户数据 151
证书数据 154
网络页面服务器 136
网络站点 140
认证服务 137
账户创建端点 138
认证端点 139

图1

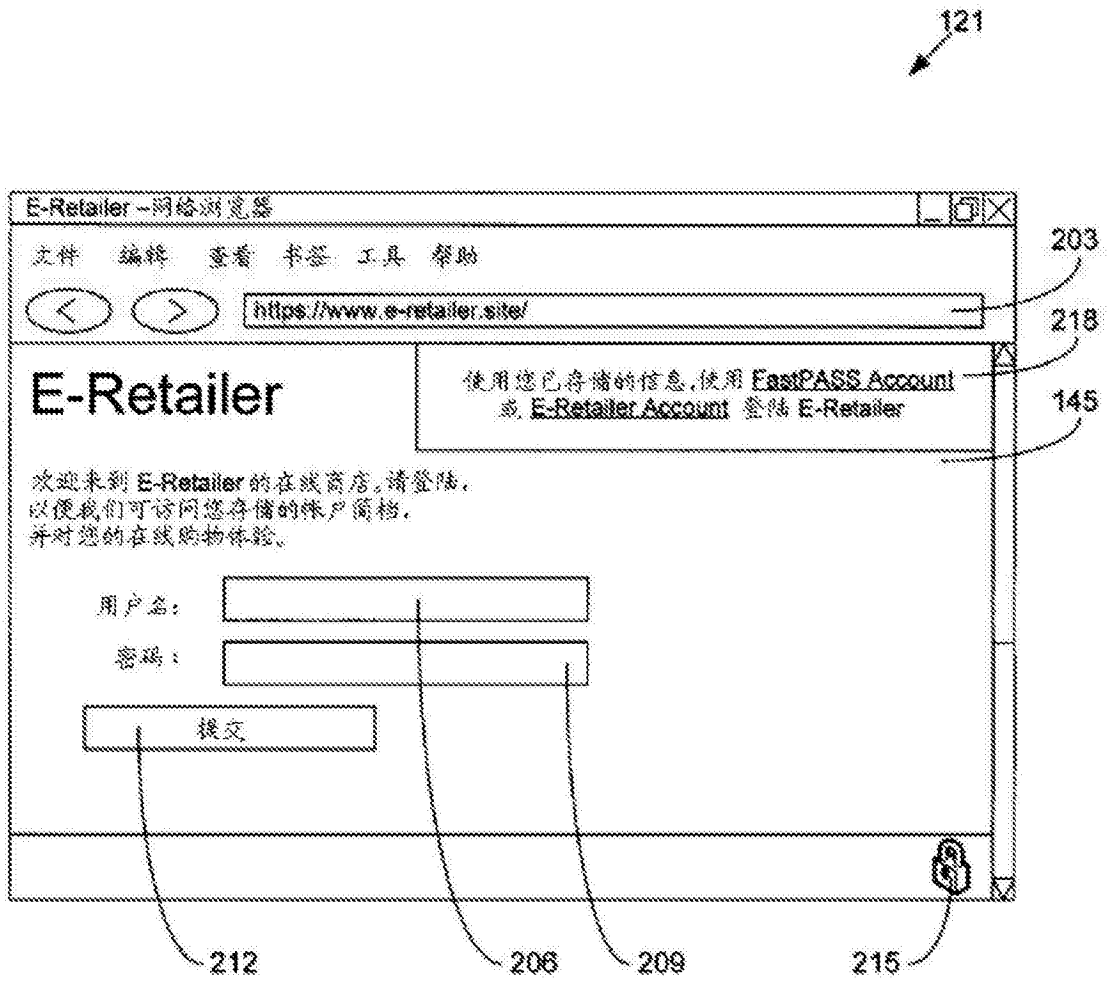

121
E-Retailer –网络浏览器
文件 编辑 查看 书签 工具 帮助
https://www.e-retailer.site/
203
218
E-Retailer
使用您已存储的信息，使用 FastPASS Account
或 E-Retailer Account 登陆 E-Retailer
145
欢迎来到 E-Retailer 的在线商店，请登陆，
以便我们可访问您存储的帐户简档，
并对您的在线购物体验。
用户名：
密码：
提交
212
206
209
215

图2A

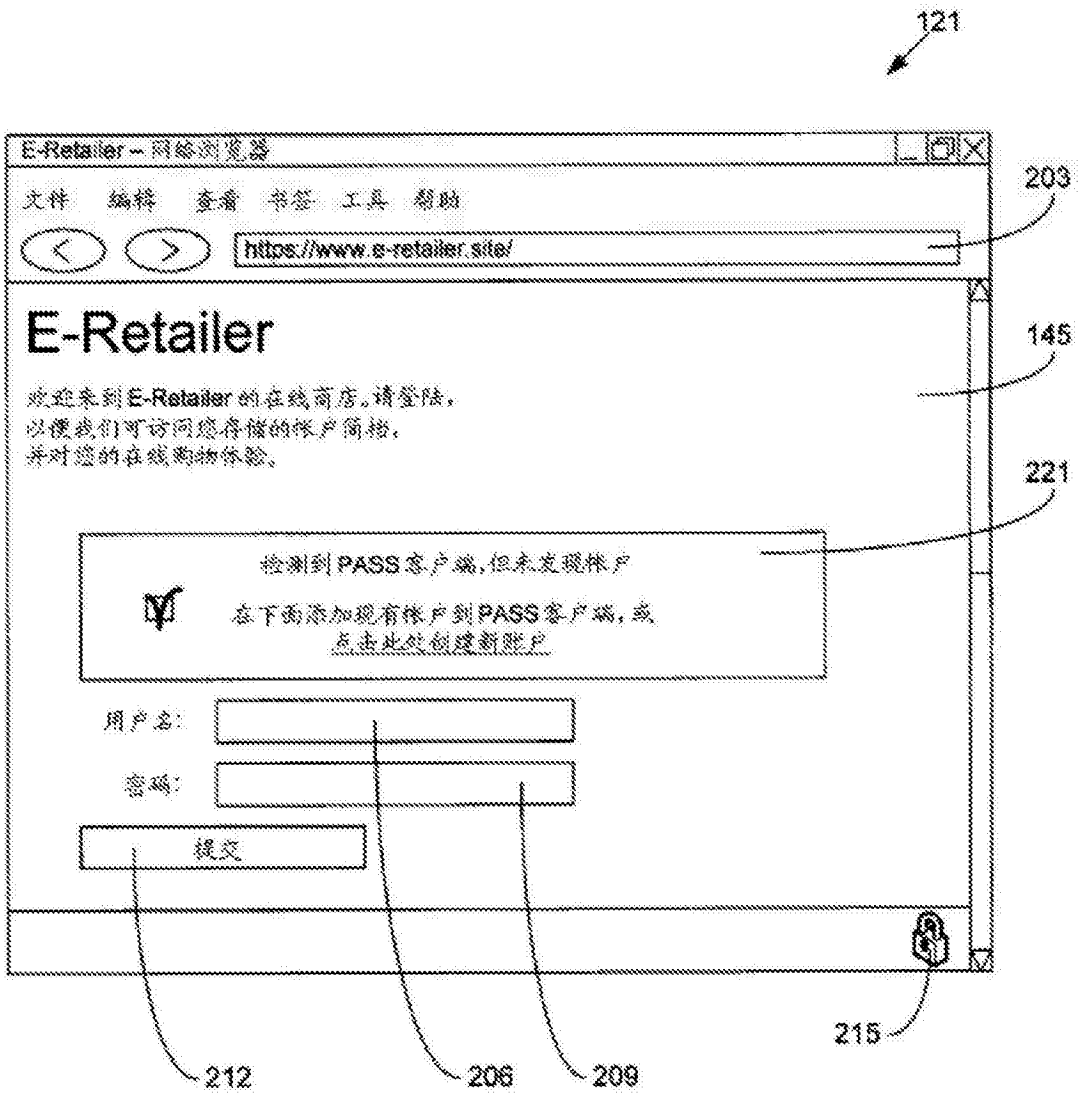

121
E-Retailer – 网络浏览器
文件 编辑 查看 书签 工具 帮助
https://www.e-retailer.site/
203
E-Retailer
欢迎来到E-Retailer的在线商店，请登陆，
以便我们可访问您存储的帐户简档，
并对您的在线购物体验。
145
221
检测到PASS客户端，但未发现帐户
在下面添加现有帐户到PASS客户端，或
点击此处创建新账户
用户名:
密码:
提交
212
206
209
215

图2B

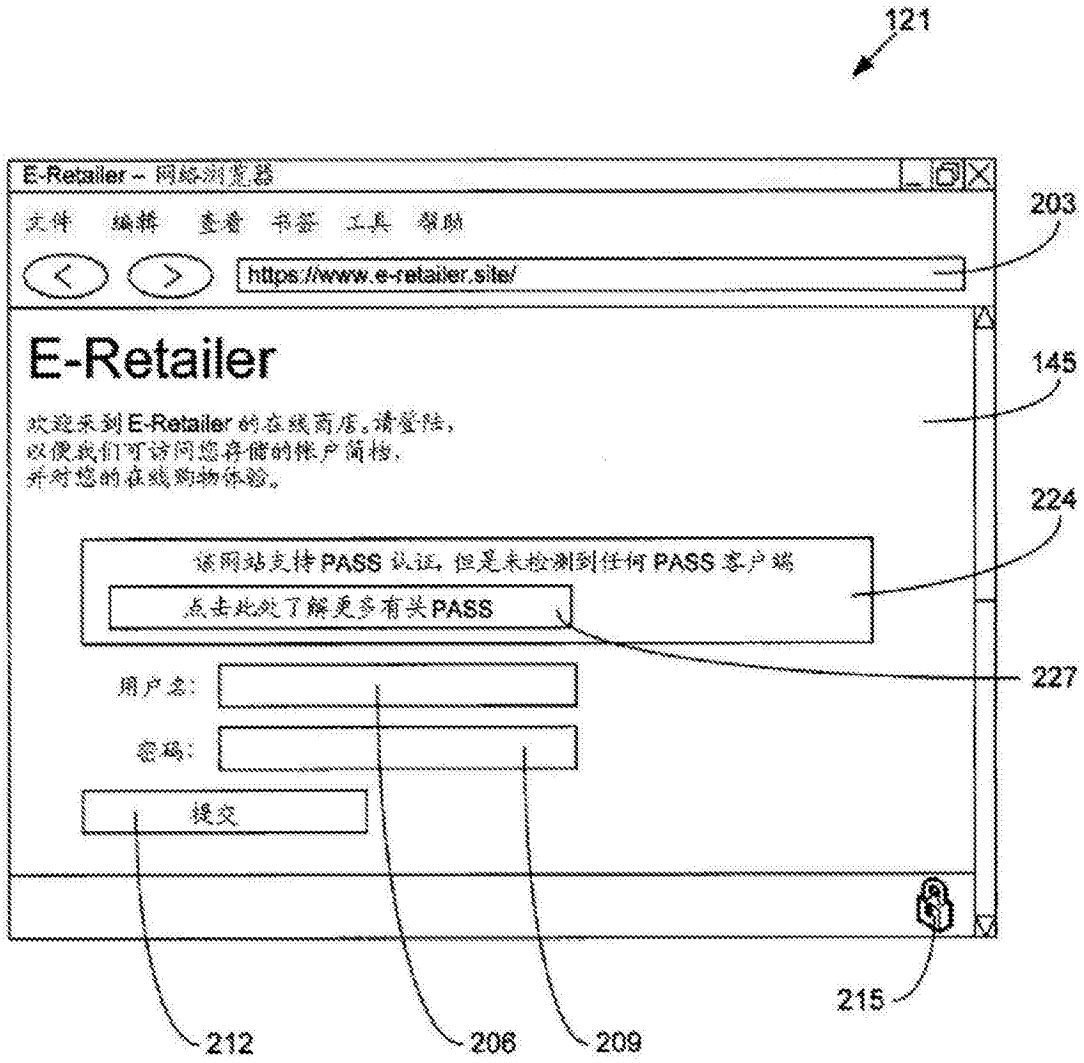

121
E-Retailer – 网络浏览器
文件 编辑 查看 书签 工具 帮助
https://www.e-retailer.site/
203
E-Retailer
145
224
227
用户名:
密码:
提交
212
206
209
215

图2C

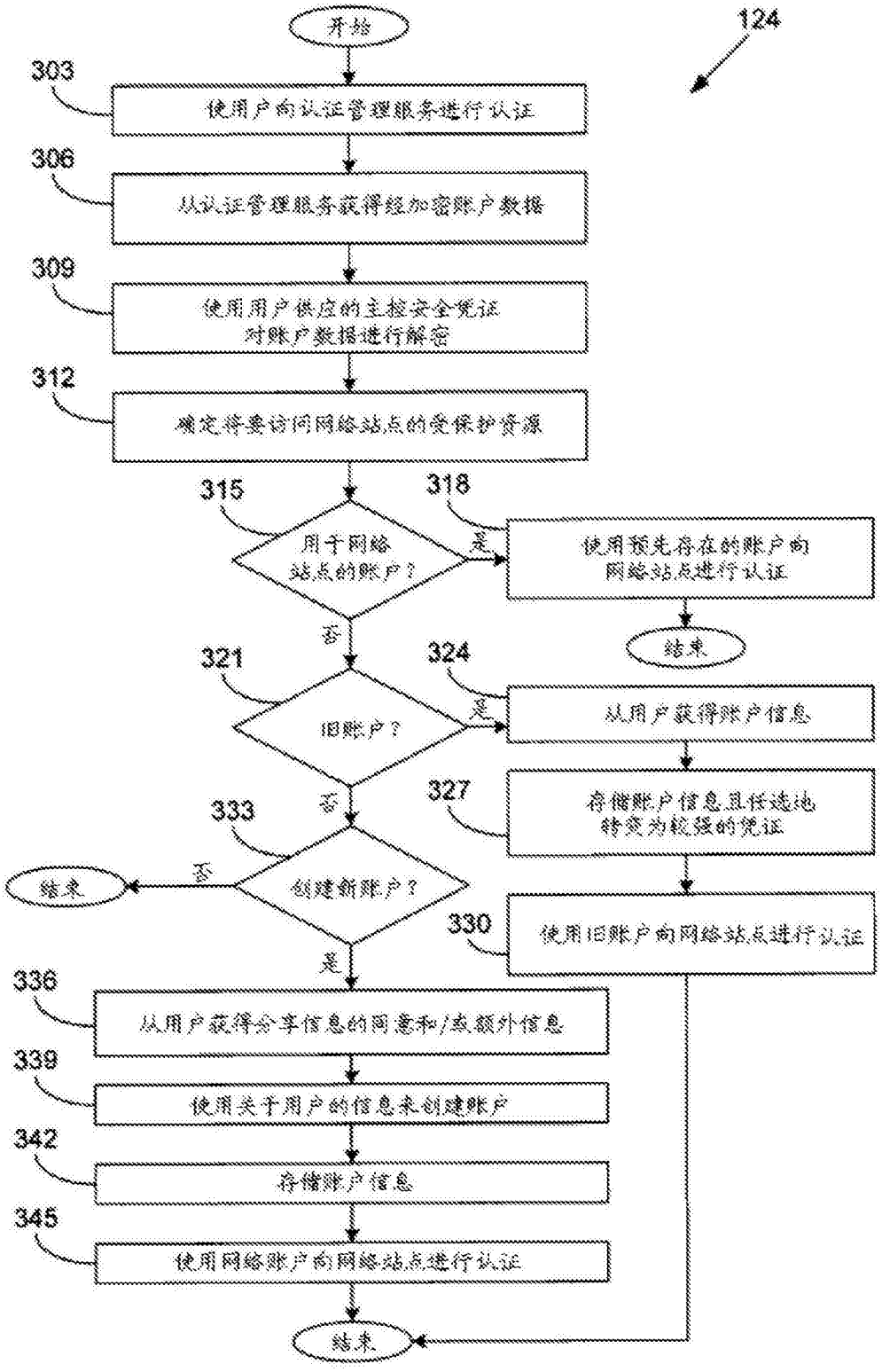

124
开始
303
使用户向认证管理服务进行认证
306
从认证管理服务获得经加密账户数据
309
使用用户供应的主控安全凭证
对账户数据进行解密
312
确定待要访问网络站点的受保护资源
315
用于网络
站点的账户？
是
318
使用预先存在的账户向
网络站点进行认证
结束
否
321
旧账户？
是
324
从用户获得账户信息
否
327
存储账户信息且任选地
转变为较强的凭证
333
创建新账户？
否
结束
330
使用旧账户向网络站点进行认证
是
336
从用户获得分享信息的同意和/或额外信息
339
使用关于用户的信息来创建账户
342
存储账户信息
345
使用网络账户向网络站点进行认证
结束

图3

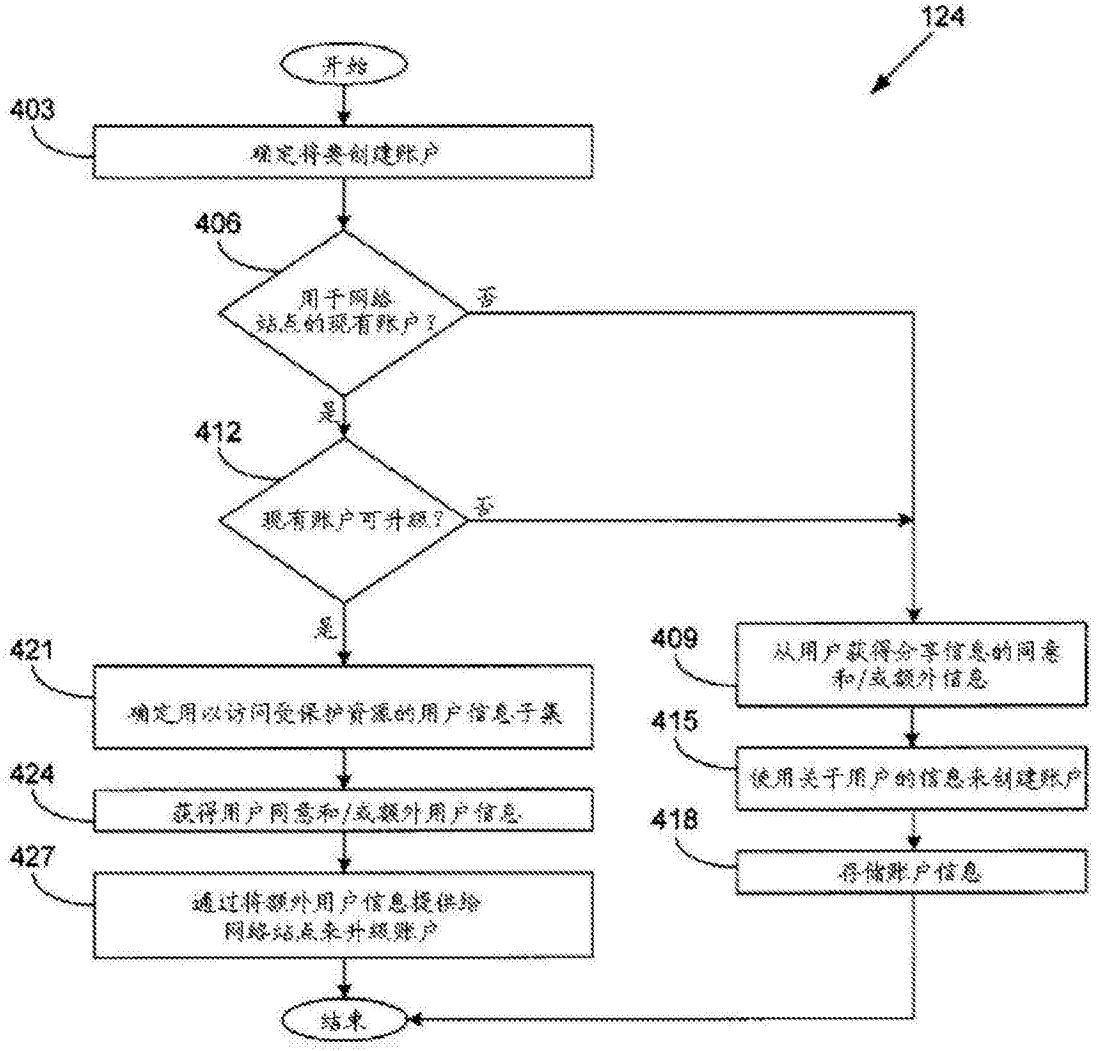

124
开始
403
确定将要创建账户
406
用于网站站点的现有账户？
否
是
412
现有账户可升级？
否
是
421
确定用以访问受保护资源的用户信息子集
424
获得用户同意和/或额外用户信息
427
通过将额外用户信息提供给网站站点来升级账户
409
从用户获得分享信息的同意和/或额外信息
415
使用关于用户的信息来创建账户
418
存储账户信息
结束

图4

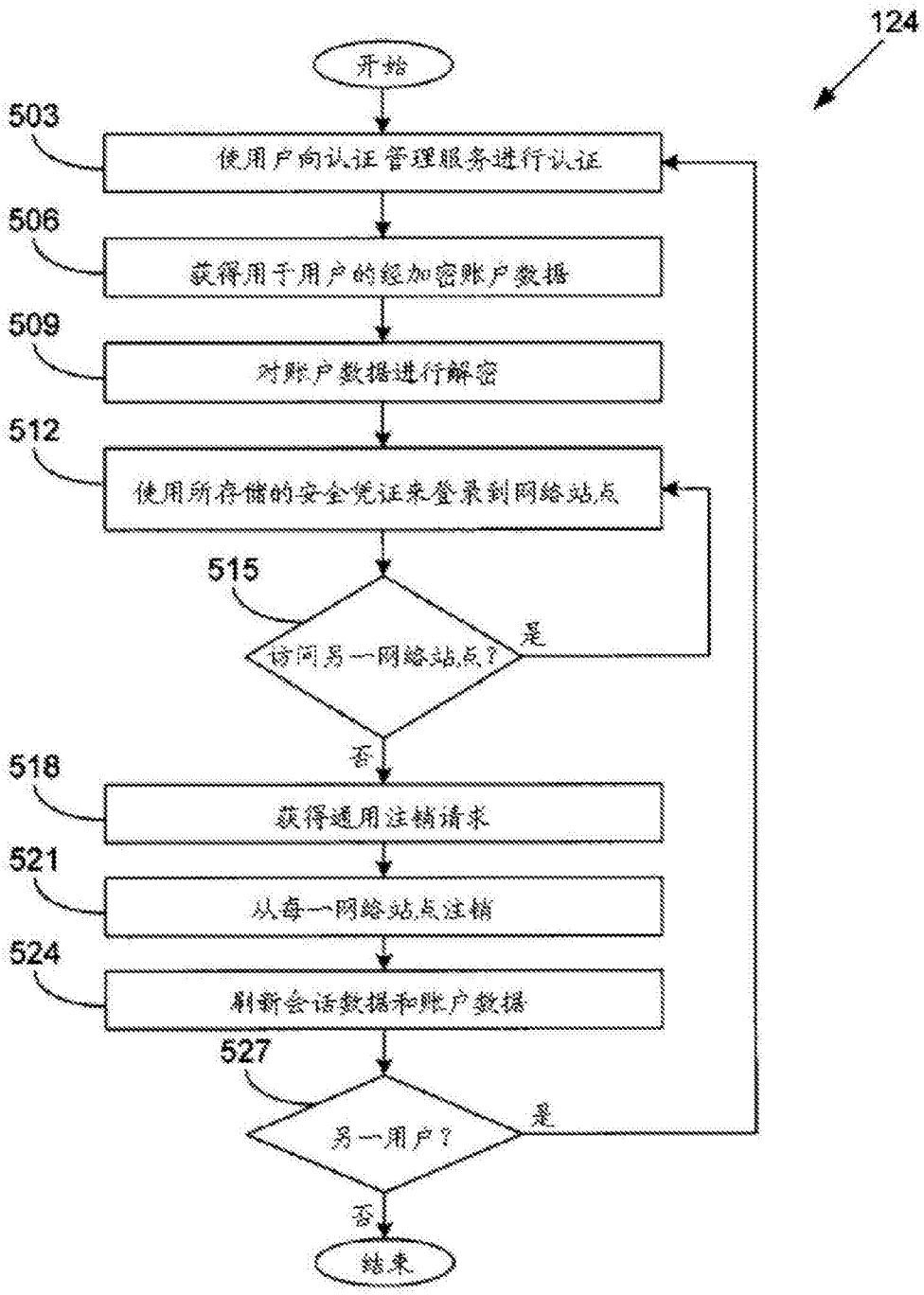

124
开始
503
使用户向认证管理服务进行认证
506
获得用于用户的经加密账户数据
509
对账户数据进行解密
512
使用所存储的安全凭证来登录到网络站点
515
访问另一网络站点?
是
否
518
获得通用注销请求
521
从每一网络站点注销
524
刷新会话数据和账户数据
527
另一用户?
是
否
结束

图5

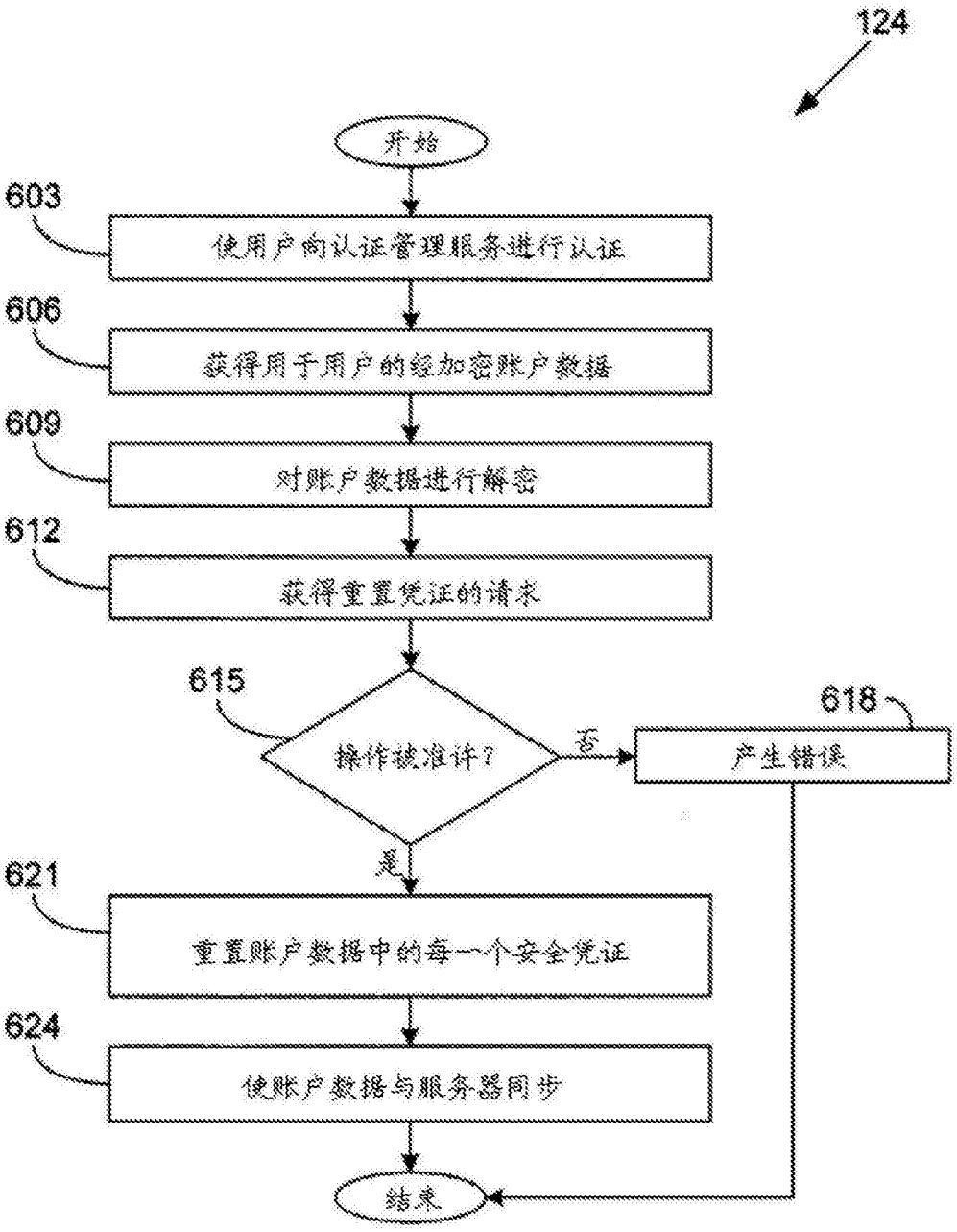

124
开始
603
使用户向认证管理服务进行认证
606
获得用于用户的经加密账户数据
609
对账户数据进行解密
612
获得重置凭证的请求
615
操作被准许?
否
618
产生错误
是
621
重置账户数据中的每一个安全凭证
624
使账户数据与服务器同步
结束

图6A

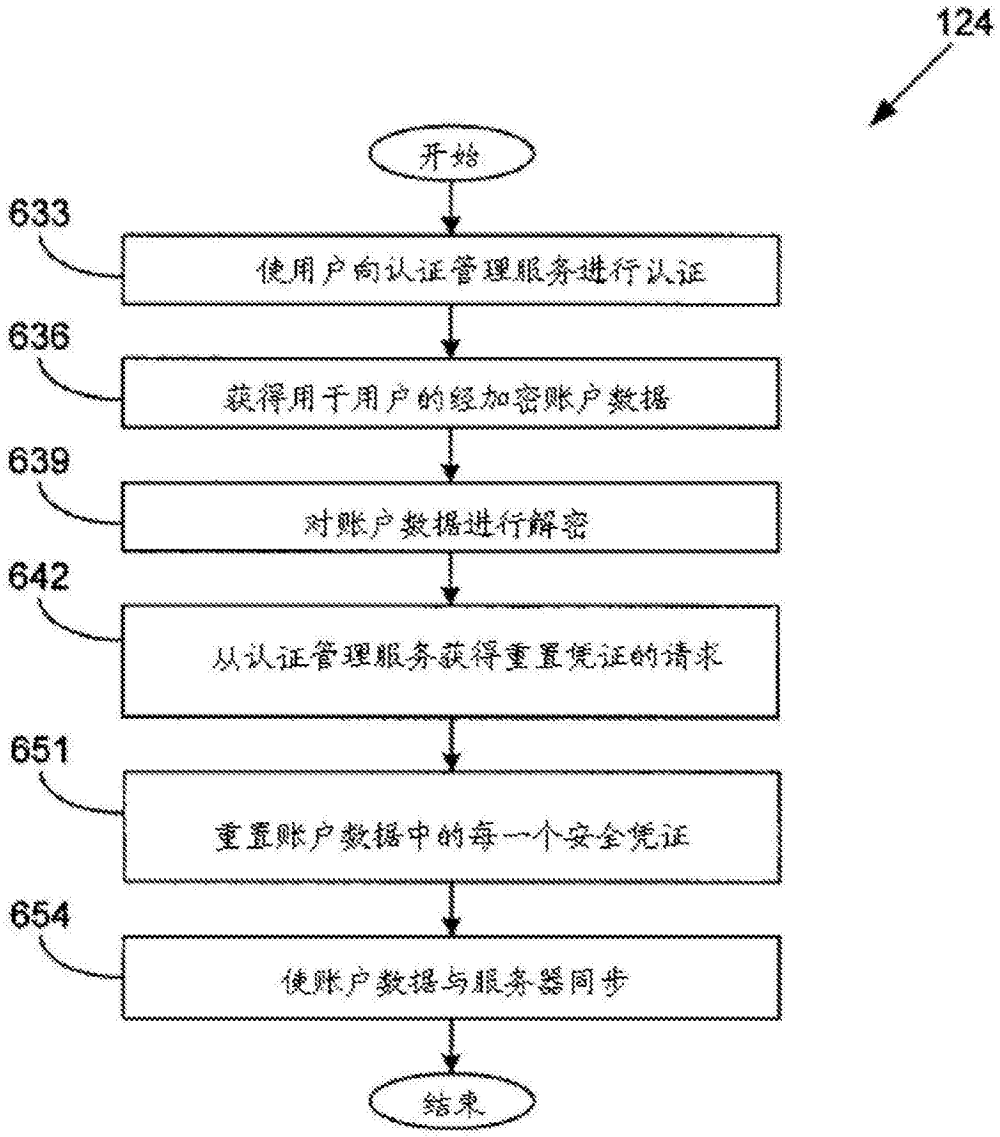

124
开始
633
使用户向认证管理服务进行认证
636
获得用于用户的经加密账户数据
639
对账户数据进行解密
642
从认证管理服务获得重置凭证的请求
651
重置账户数据中的每一个安全凭证
654
使账户数据与服务器同步
结束

图6B

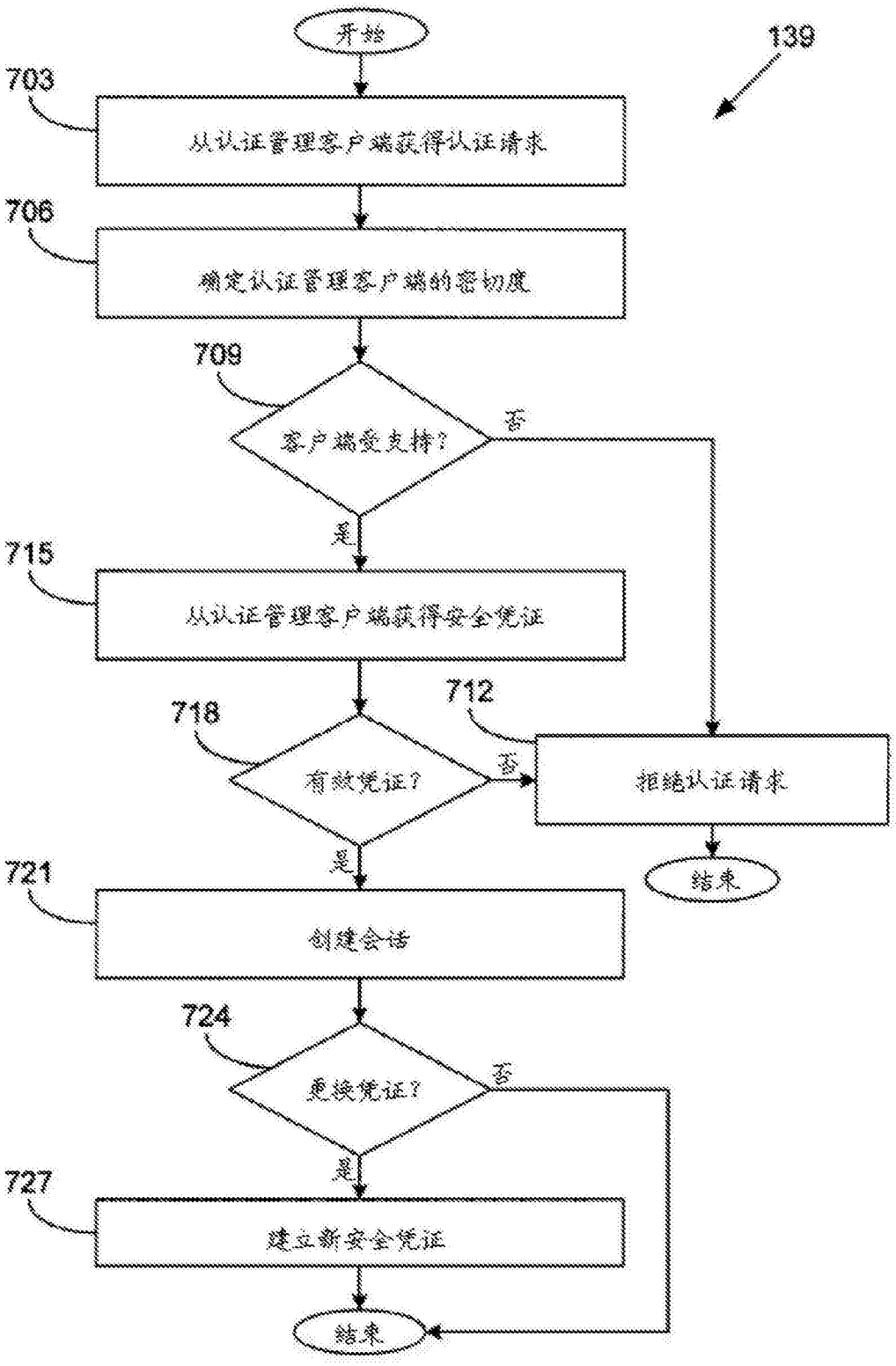

开始
139
703
从认证管理客户端获得认证请求
706
确定认证管理客户端的密切度
709
客户端受支持?
否
是
715
从认证管理客户端获得安全凭证
712
718
有效凭证?
否
拒绝认证请求
结束
是
721
创建会话
724
更换凭证?
否
是
727
建立新安全凭证
结束

图7

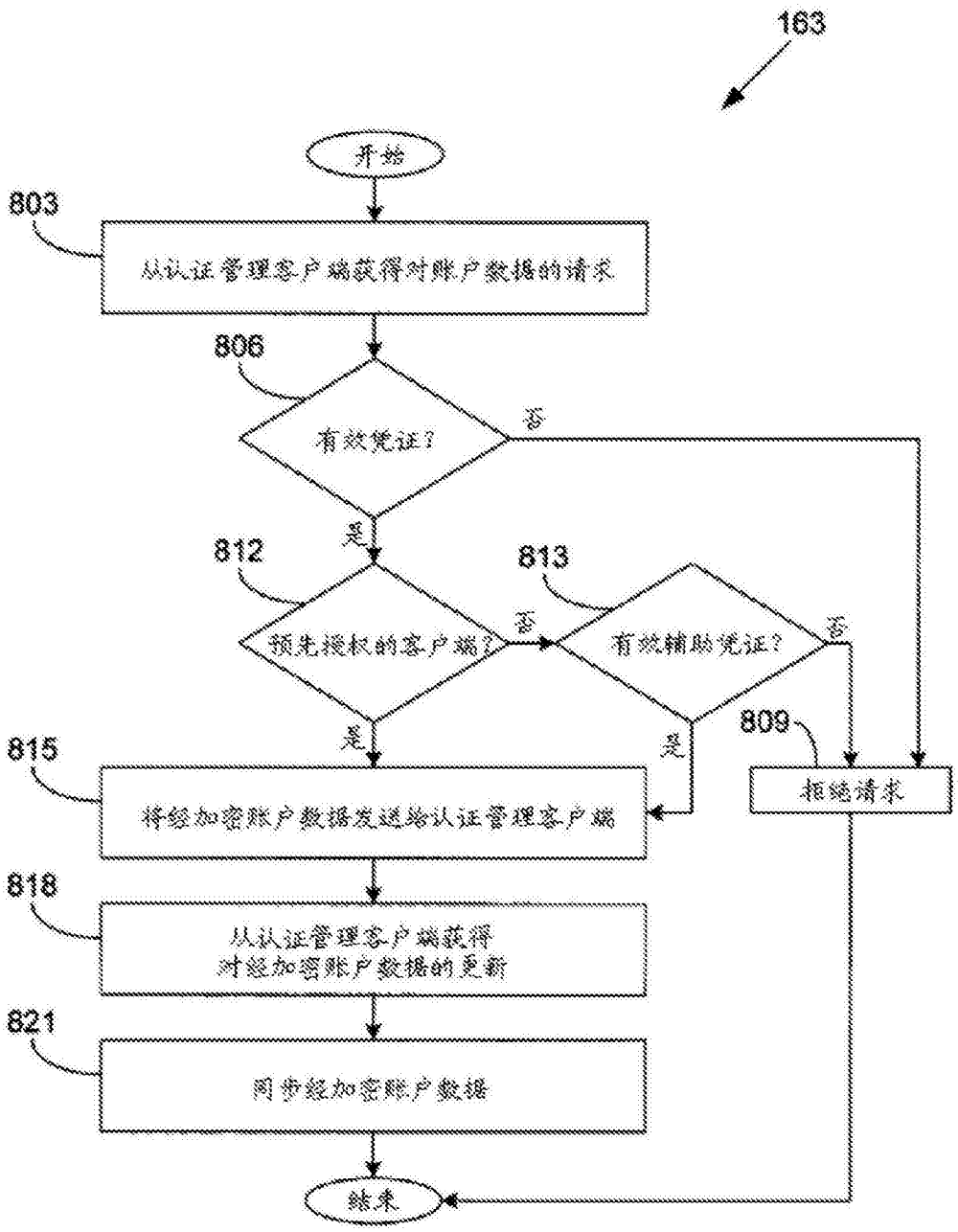

163
开始
803
从认证管理客户端获得对账户数据的请求
806
有效凭证？
否
是
812
预先授权的客户端？
否
813
有效辅助凭证？
否
是
是
809
拒绝请求
815
将经加密账户数据发送给认证管理客户端
818
从认证管理客户端获得
对经加密账户数据的更新
821
同步经加密账户数据
结束

图8

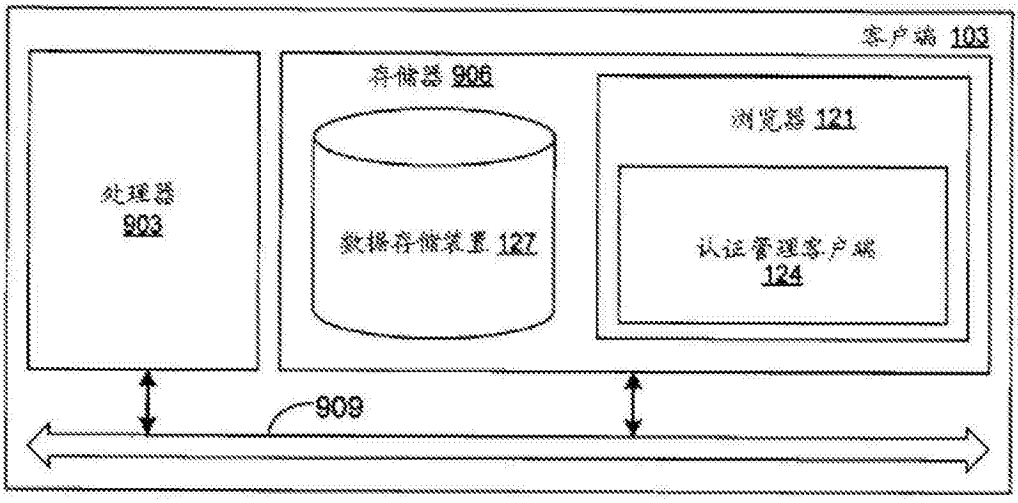


图9