(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 103828293 B
(45)授权公告日 2018.04.03

(21)申请号 201280045610.2
(22)申请日 2012.09.21
(65)同一申请的已公布的文献号
申请公布号 CN 103828293 A
(43)申请公布日 2014.05.28
(30)优先权数据
61/538,114 2011.09.22 US
13/623,641 2012.09.20 US
(85)PCT国际申请进入国家阶段日
2014.03.19
(86)PCT国际申请的申请数据
PCT/CA2012/050661 2012.09.21
(87)PCT国际申请的公布数据
WO2013/040713 EN 2013.03.28

(73)专利权人 动态身份安全系统公司
地址 加拿大,不列颠哥伦比亚省
(72)发明人 J·G·贝尔 K·W·詹宁斯
(74)专利代理机构 北京纪凯知识产权代理有限公司 11245
代理人 赵蓉民

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/08(2006.01)
H04W 12/06(2006.01)
(56)对比文件
CN 101427510 A,2009.05.06,
CN 1922845 A,2007.02.28,
US 7890761 B1,2011.02.15,
审查员 段燕辉

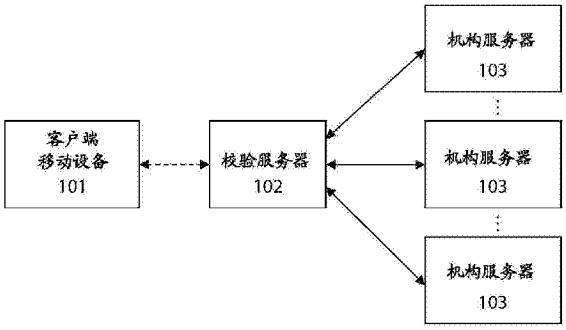
权利要求书2页 说明书6页 附图10页

(54)发明名称

用于用户认证的系统和方法

(57)摘要

本发明公开一种提供用户认证的系统和方法。非密和唯一用户识别号以及临时访问代码的使用将用户认证与任何用户密码或用户识别数据的传输分离,以及提供在不相关的机构对用户进行认证的普遍方法,而没有任何信息在这些机构之间传递。



CN 103828293 B

1.一种计算机执行的对用户进行认证的方法,所述方法包括:

在校验服务器生成唯一的用户ID号以及对应于所述用户的匹配加密密钥;

将所述唯一的用户ID号和匹配加密密钥传输至用户设备;

基于所述用户设备上的所述加密密钥生成临时访问代码;

向至少一个机构服务器提供所述唯一的用户ID号和临时访问代码,所述至少一个机构服务器适于在由独立的主机机构分别维护的至少一个计算机上运行;

将所述唯一的用户ID号和临时访问代码从所述至少一个机构服务器传输至所述校验服务器;

取回之前在所述校验服务器生成的匹配所述唯一的用户ID号的加密密钥以及通过与生成所述临时访问代码相同的方式在所述校验服务器上生成第二代码;

通过比较所述第二代码与所述临时访问代码在所述校验服务器上执行所述唯一的用户ID号和临时访问代码的验证,以获得校验结果;

将所述校验结果传输至所述至少一个机构服务器;以及

基于所述校验结果在所述至少一个机构对所述用户进行认证,

其中所述校验服务器适于在由第一机构维护的至少一个计算机上运行,所述至少一个计算机独立且分离于所述独立的主机机构及其各自的机构服务器,以及

其中所述唯一的用户ID是非密的,且与每个独立的主机机构共享。

2.根据权利要求1所述的方法,还包括修改所述至少一个机构服务器的客户端数据库,以提供用于用户记录的用于唯一的用户ID号的字段。

3.根据权利要求1所述的方法,还包括从所述至少一个机构服务器向用户提供下载在所述用户设备上可操作的基于客户端的安全软件的指令。

4.根据权利要求1所述的方法,还包括执行所述校验服务器和所述用户设备之间的时间同步。

5.一种对用户进行认证的计算机系统,所述系统包括:

在所述用户可操作的至少一个用户设备上可操作的基于客户端的安全软件组件;

在至少一个校验服务器上可操作的基于服务器的校验软件组件,所述至少一个校验服务器适于在由第一机构维护的至少一个计算机上运行;以及

至少一个主机机构服务器,所述至少一个主机机构服务器适于在由独立的主机机构分别维护的至少一个计算机上运行,

其中所述基于服务器的校验软件组件与所述基于客户端的安全软件组件通信,从而为所述至少一个用户设备上的用户提供唯一的用户ID号以及相应的加密密钥,

其中所述基于客户端的安全软件组件基于所述唯一的用户ID号和相应的加密密钥生成临时访问代码,

其中所述用户向所述至少一个主机机构服务器提供所述唯一的用户ID号和临时访问代码,

其中所述至少一个主机机构服务器通过向所述至少一个校验服务器传输包括所述用户ID号和临时访问代码的认证请求来对用户进行认证,

其中所述基于服务器的校验软件组件取回之前由所述校验软件组件提供的匹配所述唯一的用户ID号的所述加密密钥以及通过与生成所述临时访问代码相同的方式在所述校

验服务器上生成第二代码，

其中所述基于服务器的校验软件组件生成校验结果，

其中所述校验结果从所述校验服务器被传输至所述至少一个主机机构服务器，

其中由所述第一机构维护的所述至少一个计算机独立且分离于所述独立的主机机构及其各自的至少一个主机机构服务器，以及

其中所述唯一的用户ID是非密的，且与每个独立的主机机构及其各自的主机机构服务器共享。

6.根据权利要求5所述的系统，其中所述主机机构服务器运行与所述基于服务器的校验软件组件通信的通信软件组件。

7.根据权利要求5所述的系统，其中所述至少一个用户设备是具有足以操作所述基于客户端的安全软件组件的计算和通信能力的移动设备。

8.根据权利要求5所述的系统，其中所述设备选自包括以下各项的组：移动设备、平板电脑、笔记本电脑、个人媒体播放器、个人娱乐系统、信息服务亭和智能终端。

用于用户认证的系统和方法

[0001] 著作权声明

[0002] 本专利文献的一部分公开包含受到著作权保护的材料。著作权人不反对任何人传真复制专利文献或者专利公开，因为其出现在专利商标局的专利文件或记录中，但是在其它方面保留全部任何的著作权权利。

背景技术

[0003] 在如今的现代社会，通过虚拟的、非个人的方法传输信息不断发生。被传输的大部分数据被发送或接收者认为是秘密的，而且在一些情况下，其是重要的因此引起频繁地尝试以欺诈手段获取该信息。对于政府、企业和个人而言，这已经变成日益严重的问题。

[0004] 目前，确保数据安全的普遍接受的方法是随处可见的“密码”、“口令”、“PIN”和许多其他同义词。密码经常与其欲保护的数据一起保存，或者由数据的个人所有者保存。这些以及其他用户习惯代表基于密码的安全措施中的主要缺陷。

[0005] 密码是被反复传输的静态数据片段，因此容易成为盗窃目标。或者，要求频繁改变密码的系统提升了用户可预测的模式，或者密码的遗忘和丢失，这导致低效以及用于密码恢复措施的增加的费用。

发明内容

[0006] 本发明提供用于用户识别的安全系统，以维护信息的保密性，以及解决传统的密码安全措施的上述缺陷。更具体而言，本发明用于防止身份盗窃，提供完全安全、难以被破解或侵入、以及普遍适用于几乎任何要求个人识别的环境中的系统。

[0007] 虽然本发明的系统可用在具有处理能力的各种硬件平台上(例如服务器计算机，个人计算机，笔记本电脑，移动电话，个人媒体播放器，信息服务亭(kiosk)，终端，飞机、火车、轮船上的个人娱乐系统，等等)，优选实施例在通常大多数时间或总是由用户保存的移动计算机设备(例如个人移动电话)上实施，以及在远离用户和远离至少一个主机机构的至少一个计算机服务器上实施。

[0008] 系统包括在至少一个校验服务器上安装和维护的基于服务器的校验软件(该校验服务器独立于任何用户或主机机构)，安装在用户的移动设备上的基于客户端的安全软件，以及可选的在至少一个主机机构的服务器(例如企业服务器、网站服务器等)上运行的通信软件组件。在以下描述中，术语“用户”、“客户端”和“顾客”可互换使用。用户通过客户端安全软件组件获得唯一的用户ID(识别)号，从而在系统中注册。该单一、非密的用户ID号可与使用本发明的系统以增强安全识别和维护其数据完整性的任何机构共享。在任何时候都不要求任何个人用户信息，用户注册和使用系统所需的时间和工作是最小的。

[0009] 部分地基于用户ID号，客户端安全软件向用户提供临时访问代码，该临时访问代码在用户的移动设备上每隔预定时间间隔产生。根据访问数据的方法(计算机、键盘等)，所有者将访问数字传输至机构进行校验。预定时间间隔过去之后，临时访问代码过期，生成新的临时访问代码。用户和机构都不能预测随后的临时访问代码。

[0010] 该新颖的校验方法在不能进行视觉识别的虚拟世界中是理想的，其可用于主校验或者辅助校验。

[0011] 在优选实施例中，本发明以如下形式提供：客户端安全应用软件，该客户端安全应用软件可下载到具有处理能力的移动设备(例如移动电话、个人媒体播放器)，在至少一个服务器上可操作的服务器校验软件，以及可选的在至少一个主机机构的服务器上可操作的通信软件组件。

[0012] 有利的，不需要用户输入任何个人用户信息，没有个人信息包含在运行客户端安全软件的设备中，也没有个人信息被传输至移动设备或者从移动设备被传输。

[0013] 本发明的另一个优点是一旦注册，客户端安全软件不需要设备保持与任何机构的服务器的网络连接。即用户可以向任何参与机构进行认证，可选的运行通信软件组件，与本发明的校验服务器通信，而校验服务器和客户端移动设备之间没有任何信息传送。另一个优点是可以使用客户端安全软件的单个实例在不相关机构的服务器进行认证，而在不相关机构的服务器之间没有任何信息传送。

[0014] 本发明的“通用”性能允许在不同和不相关的主机机构网站进行认证，不需要主机网站之间共享信息，从而为个人和机构等提供了非常廉价的安全系统。为了进一步降低成本，本发明使用现有的软件和硬件基础结构，只需很小修改或不需要修改。

[0015] 通过附图和以下详细描述，这些和其他优点将变得更清晰。

附图说明

[0016] 图1是显示根据本发明的一个实施例的安全系统的示例性框图。

[0017] 图2是显示根据本发明的一个实施例的用户注册过程的示例性流程图。

[0018] 图3是显示根据本发明的一个实施例的用户登录过程的示例性流程图。

[0019] 图4是显示根据本发明的一个实施例的移动设备上的客户端安全软件的示例图。

[0020] 图5是显示根据本发明的一个实施例的移动设备上的客户端安全软件的示例图。

[0021] 图6是显示根据本发明的一个实施例的移动设备上的客户端安全软件的示例图。

[0022] 图7是显示根据本发明的一个实施例的移动设备上的客户端安全软件的示例图。

[0023] 图8是显示根据本发明的一个实施例的移动设备上的客户端安全软件的示例图。

[0024] 图9是显示根据本发明的一个实施例的移动设备上的客户端安全软件的示例图。

[0025] 图10是显示根据本发明的一个实施例的移动设备上的客户端安全软件的示例图。

具体实施方式

[0026] 将参考附图详细描述本发明的不同实施例，其中在几幅附图中相同的附图标记代表相同的部件。对不同实施例的参考不限制本发明的范围，本发明的范围仅由所附权利要求书的范围限制。此外，本说明书中阐释的任何示例不旨在限制而仅仅是在阐释所要求保护的发明的许多可能实施例中的一些实施例。

[0027] 呈现以下描述以使本领域技术人员利用和使用本发明，以下描述是在本发明的特定应用环境下给出的。对所公开的实施例的各种修改对于本领域技术员是显而易见的，在不背离本发明的范围的前提下，本文限定的基本原则可应用于其他实施例和应用中。对不同实施例和示例的参考不限制本发明的范围，本发明的范围仅由所附权利要求书的范围限

制。此外，本说明书中阐释的任何示例不旨在限制而仅仅是在阐释所要求保护的发明的许多可能实施例中的一些实施例。

[0028] 执行本发明的当前实施例的程序环境例如包括通用计算机或专用设备，例如手持式计算机。为清楚起见，可能省略这些设备(例如处理器、存储器、数据存储器、显示器)的细节。

[0029] 还应理解，可使用各种技巧来实施本发明的技术。例如，本文描述的方法可在计算机系统上执行的软件中实施，或者在采用微处理器的组合或者其他专门设计的专用集成电路、可编程逻辑器件、或其不同组合的硬件中实施。特别的，本文描述的方法可由存储在适当的计算机可读介质上的一系列计算机可执行指令实施。适当的计算机可读介质可包括可挥发(例如RAM)和/或不可挥发(例如ROM，磁盘)存储器，载波和传输介质(例如铜线、同轴电缆、光纤介质)。示例性的载波可采用电、电磁或光信号的形式，信号沿着局域网、可公开访问的网络(例如互联网或一些其他通信链路)传送数字数据流。

[0030] 相应地，根据一方面，本发明提供对用户进行认证的方法，该方法包括：在校验服务器生成唯一的用户ID号以及对应于用户的匹配加密密钥；将唯一的用户ID号和匹配加密密钥传输至用户设备；基于用户设备上的加密密钥生成临时访问代码；向至少一个机构服务器提供唯一的用户ID号和临时访问代码；将唯一的用户ID号和临时访问代码传输至校验服务器；在校验服务器上执行唯一的用户ID号和临时访问代码的验证，以获得校验结果；将校验结果传输至至少一个机构服务器；以及基于校验结果在至少一个机构对用户进行认证。所述方法还可包括取回匹配唯一的用户ID号的加密密钥，以及通过与生成临时访问代码相同的方式生成第二代码，以及比较第二代码和临时访问代码以获得肯定或否定的校验结果。所述方法还可包括修改至少一个机构服务器的客户端数据库，以提供用于用户记录的用于唯一的用户ID号的字段。所述方法还可包括从至少一个机构服务器向用户提供下载在用户设备上可操作的基于客户端的安全软件的指令。所述方法还包括执行校验服务器和用户设备之间的时间同步。

[0031] 根据另一方面，本发明提供对用户进行认证的系统，所述系统包括：在用户可操作的至少一个用户设备上可操作的基于客户端的安全软件组件；在至少一个校验服务器上可操作的基于服务器的校验软件组件；以及至少一个主机机构服务器，其中基于服务器的校验软件组件与基于客户端的安全软件组件通信，从而为至少一个用户设备上的用户提供唯一的用户ID号以及相应的加密密钥，以及其中主机机构服务器通过向至少一个校验服务器传输认证请求来对用户进行认证，以及其中基于服务器的校验软件组件生成校验结果。基于客户端的安全软件组件基于唯一的用户ID号和相应的加密密钥生成临时访问代码，以及其中用户向所述主机机构服务器提供唯一的用户ID号和临时访问代码。认证请求可包括用户ID号和临时访问代码。主机机构服务器可运行与基于服务器的校验软件组件通信的通信软件组件。至少一个设备可以是具有计算和通信能力足以操作基于客户端的安全软件组件的移动设备。此外，设备可选自包括以下各项的组：智能手机、平板电脑、笔记本电脑、个人媒体播放器、个人娱乐系统、信息服务亭和智能终端。

[0032] 用户ID号对于本发明的每个用户是唯一识别码。这是用户或者客户端需要与采用本发明保护用户或客户端身份的任何机构共享的唯一数字。用户ID号不需要由用户保密，其本身不以任何方式识别用户。最优选的，通过至互联网的无线连接在移动设备上取回用

户ID号，这是最方便的方法。有利的，需要传输的数据量小，小于1MB，优选的小于100KB，更优选的小于10KB，最优选的小于1KB。从独立于任何主机机构被维护的校验服务器取回用户ID号。

[0033] 一旦本发明的客户端安全软件组件被下载至移动设备而且用户已经被校验服务器分配了用户ID号，那么识别系统将作用于无限数量的机构或用户识别应用。有利的，在任何主机机构运行通信软件组件的服务器可以通过校验服务器向用户提供唯一的用户ID号，而不需要不同机构的不同服务器之间的任何通信。

[0034] 有利的，在几乎所有情况下，现有硬件和软件(对于用户和机构二者)足以使用本发明。重要的是应注意本发明不代替机构内部的用户信息或数据的数据库。相反，本发明的临时访问代码可用于代替传统密码或PIN数字。但是与其他传统的安全方法不同，超越已在使用的保护用户识别信息的现有安全措施，用户ID号不需要实施任何额外的安全措施(或者安全软件)。对于采用本发明的任何机构而言这是一个主要优势，因为实施成本远远低于替代的安全方法。

[0035] 本领域技术人员将理解，本发明允许用户而不是主机机构控制安全的关键环节。即通过传统安全方法，主机机构提供用于用户访问的所有参数，并将这些参数给予用户。通过本发明，恰恰相反，用户向主机机构提供所有参数。在安全方法中这提供了关键的优势，因为多数安全攻击以存储在主机机构的服务器(而不是个体用户)上的数据为目标。例如，用户能够出于任何理由、在用户期望的任何时间请求新的用户ID号。例如，用户可能感觉他/她的旧的用户ID号缺乏抵抗力(例如他们的移动设备被盗或者丢失并且被新的设备代替)，或者可能为了增加安全性的舒适性希望定期改变数字。请求新的用户ID是即时且可行的，给用户或者主机机构带来很小破坏或者没有破坏。有利的，本发明的系统和方法将认证过程和任何密码与主机机构存储用户数据和信息的服务器分离。

[0036] 图1显示根据一个实施例的本发明的系统。特别的，客户端移动设备101被设置以及仅与校验服务器102通信，以获得新的用户ID号和加密密钥，如以虚线表示的双向箭头所示。一个或多个主机机构服务器103可与校验服务器102通信，但是不与客户端移动设备101通信，以校验和认证向主机机构服务器103(例如手动)提供输入的用户，如下详述。本领域技术人员可以理解，系统可包括图1中未显示的任意数量的校验服务器和客户端移动设备。

[0037] 在未显示的另一个实施例中，校验服务器和机构服务器可以相同。即基于服务器的校验软件组件(software component)可以直接在主机机构的服务器或者主机机构内的独立服务器上运行。很容易理解，在这种替代设置中，需要不同机构之间的通信或协作以保证唯一的用户ID号的互通性。

[0038] 图2和图3是显示分别根据本发明的一个实施例的用户注册过程和用户登录过程的示例性流程图，以下描述图2和图3中在互联网上在主机机构的网站进行的用户认证。

[0039] 参考图2，主机机构开始注册201，以实施本发明的系统。主机机构向其客户端数据库中增加202字段(例如长度为7字节)，从而为每个顾客或用户/客户端保留用户ID号。主机机构提供203工具，以在机构的数据库上记录唯一的用户ID号，并且向其用户发送通知和链接，涉及在哪以及如何在其移动设备上下载和安装客户端安全软件。优选地，该通知将通过电子邮件发送给用户。此外，主机机构修改204其网站登录页面，为用户认证提供使用传统密码或者使用本发明的用户ID号的选择。

[0040] 用户跟踪所提供的链接并在其移动设备上下载，安装206客户端安全软件。接下来，用户通过密码保护207其移动设备，以及通过密码保护208客户端安全软件，以完成用户安装和注册过程。移动设备的密码保护是可选的，但是优选的作为最佳实施方式，特别是在移动设备也从主机机构服务器接收通知（例如至智能手机的电子邮件）的情况下。最后，用户利用客户端安全软件获得209唯一的用户ID号，如下详述，并且将用户ID号提供210到主机机构的网站上的其个人资料中。

[0041] 基于服务器的校验软件使用当前日期和时间生成唯一的用户ID号。优选地，用户ID号生成为十六进制值，并通过一组数字被缩短，以生成仅有基于服务器的校验软件和客户端安全软件的供应商知晓的编号系统。然后，使用已知的加密技术对用户ID号进行加密，以生成有效的加密密钥，加密密钥优选是256位或更高位的。用户ID号和加密密钥都从校验服务器被直接传输至移动设备。优选地，只有用户ID号对用户是可见的。

[0042] 客户端安全软件使用提供至以上移动设备的加密密钥通过加密当前日期和时间生成临时访问代码。数值结果优选地被一系列算法操作（例如加法或减法）修改，以形成缩短的数字，优选的是4-8位数字，最优选的是6位数字，其是临时访问代码。

[0043] 参考图3，显示本发明的优选实施例中的用户识别。主机机构和用户都已经按照如上所述进行注册220，221。用户首先必须在客户端安全软件上输入222密码（优选的，额外的密码以解锁其移动设备）。客户端安全软件生成并显示223临时访问代码。用户通过在独立计算机设备上或者在其同一移动设备上使用网页浏览器导航224至主机机构的网站登录页面。

[0044] 主机机构的网站登录页面提供使用传统密码或使用本发明的用户ID号进行用户认证的选择225。用户选择226用户ID号认证，并查询用户移动设备上的客户端安全软件以获得由用户输入227主机机构的网站登录页面的临时访问代码。可选的，在使用移动设备导航至主机机构的网站的情况下，临时访问代码可自动插入登录页面中。

[0045] 主机机构的网站服务器通过通信软件组件将临时访问代码和用户ID号传输228至校验服务器进行验证和校验。返回的校验结果被提供229至主机机构的通信软件组件，基于该结果，允许用户访问230主机机构的网站，或者用户被拒绝访问231以及必须重新输入临时访问代码227。如果步骤231和步骤227中的重新输入之间已经过去足够的时间，所提供的临时访问代码将变为新的数字。

[0046] 拥有临时访问代码和用户ID号的基于服务器的校验软件执行与客户端安全软件相同的用于身份验证的步骤。即用户ID号用于查找之前由校验服务器生成的相应加密密钥。接下来，使用加密密钥通过当前时间和日期生成代码。数值结果被与以上公开相同的一系列算法操作修改，以形成缩短的数字，然后该数字与临时访问代码进行比较。如果产生的数字与临时访问代码匹配，那么校验服务器向主机机构的网站服务器上的通信软件组件传输校验确认。

[0047] 参考其余附图（图4至图10），描述在移动设备上可操作的客户端安全软件的本发明的优选实施例。

[0048] 主屏幕

[0049] 参考图4，显示移动设备101上的客户端安全应用软件。主屏幕显示以设定的时间间隔（优选为每分钟一次）更新的新的临时访问代码100。临时访问代码100可以提供为数字

或者包括字母与数字的代码。该时间间隔可以更长或更短，而且还可以变化。临时访问代码100在移动设备上生成，其不被传输，而是仅仅保留在移动设备101本地。时钟110以时间间隔递减计数，在图4中时间间隔显示为60秒。可以提供时钟110上的颜色变化，以通知用户何时接近临时访问代码100的到期时间。例如，可以采用绿色-琥珀色-红色的颜色方案。可以选择右侧软键130来显示选项菜单，而可以选择左侧软键120来退出应用。

[0050] 选项

[0051] 参考图5，选项131被呈现给用户，其是：(1)查看用户ID，(2)新的用户ID，(3)删除用户ID，以及(4)同步时间。通过滚动选项以及选择软键菜单140上的“下一项”执行在移动设备101上选择所需选项。

[0052] 查看用户ID号

[0053] 参考图6，选择(1)查看用户ID显示用户ID号150。用户ID不需要保密，并且不涉及用户或用户的移动设备。按下写有“完成”的软键141将带用户返回选项131。

[0054] 获得新的用户ID号

[0055] 参考图7，当确认160时，移动设备101从校验服务器取回新的用户ID号150。如果用户ID号150目前存在于移动设备101上，其将被改写。当选择菜单142上的“是”时，通过至校验服务器的数据连接(例如至互联网的无线连接)用户ID号150将被复制到移动设备101上。选择菜单142上的“否”将返回选项131。将询问用户是否允许访问数据连接。这允许用户优化任何移动服务费以及确认数据的传输。有利的，需要传输的数据量很小，小于1MB，优选的小于100KB，更优选的小于10KB，最优选的小于1KB。

[0056] 参考图8，当新的用户ID号150被复制到移动设备101上时，显示结果的确认170。按下标签为“确认”的软键143带用户返回主屏幕，在主屏幕显示新的临时访问代码100(见图4)。用户可以通过导航至选项菜单130并选择选项131下的(1)查看用户ID来查看新的用户ID号150。

[0057] 接收到新的用户ID号150之后，用户必须将其提供给用户希望证明自己身份的任何机构。类似的，如果相同机构已经在文件中拥有相同用户的前一用户ID号，那么用户必须通知它已经获得了新的用户ID号。

[0058] 删除用户ID号

[0059] 参考图9，从选项131中选择(3)删除用户ID将删除存储在设备上的任何用户ID号150。操作的确认161被呈现给用户，在软键选项144中选择“是”将删除用户ID号。优选的，为了增加安全性，用户ID号150的删除是永久的，因此不能取回而只能获得新的用户ID号150。

[0060] 同步时间

[0061] 参考图10，从选项131中选择(4)同步时间保证临时访问代码100被正确校验。时间同步是通过数据连接在服务器和移动设备101之间执行的。操作的确认162被呈现给用户，在软键选项145下选择“是”将自动同步时间。可询问用户是否允许访问数据连接。在软键选项145下选择“否”将带用户返回前一屏幕。该时间同步与移动设备101上本身的时钟不相关，而是受到本发明的客户端应用软件的限制。这是有利的，因为定时机制对于用户和机构等是隐藏的，因此不容易被破解或侵入。

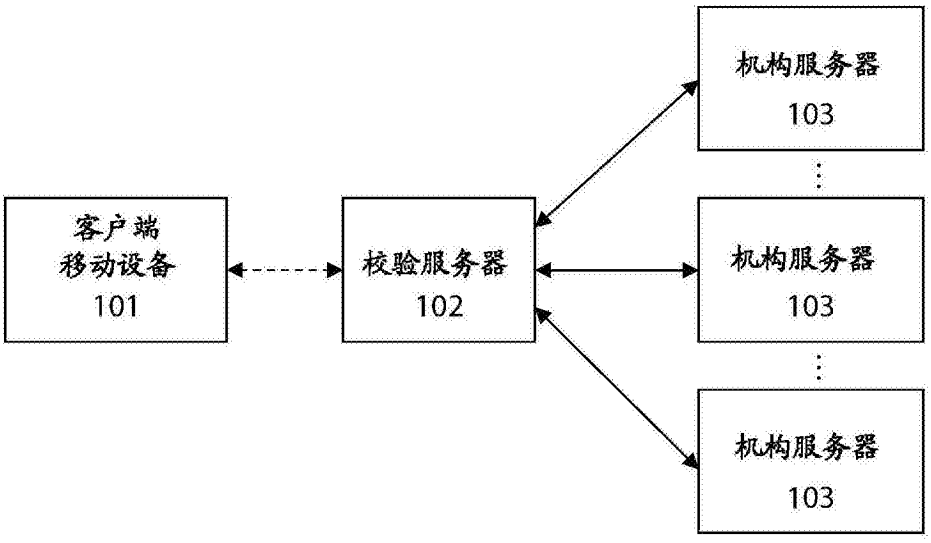


图1

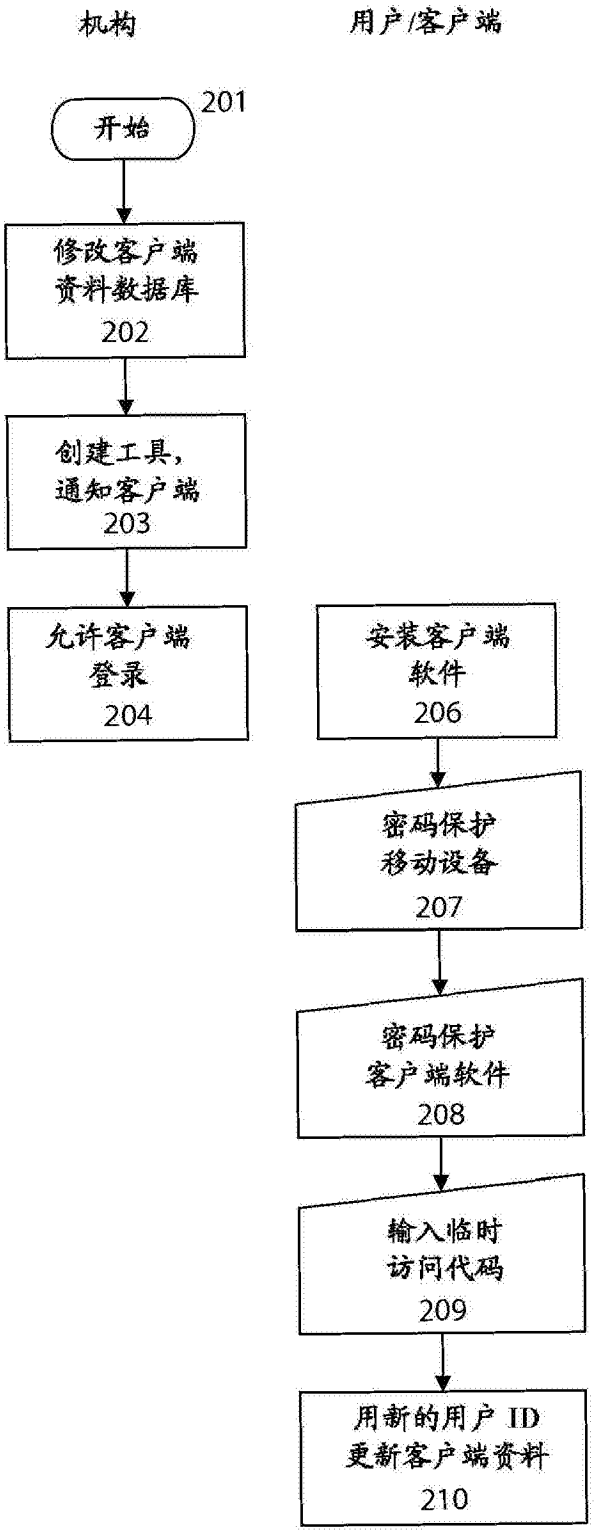

机构
用户/客户端
开始
201
修改客户端
资料数据库
202
创建工具，
通知客户端
203
允许客户端
登录
204
安装客户端
软件
206
密码保护
移动设备
207
密码保护
客户端软件
208
输入临时
访问代码
209
用新的用户 ID
更新客户端资料
210

图2

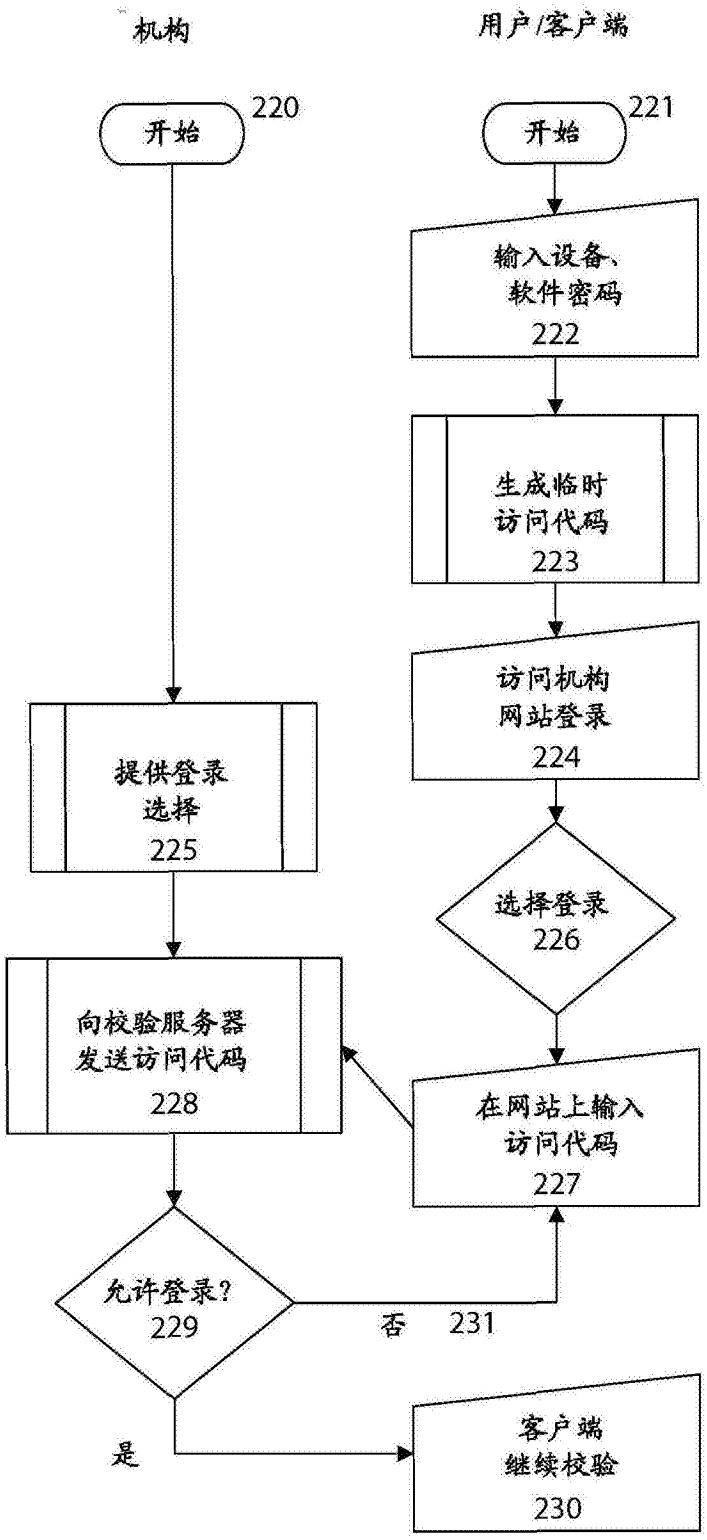

机构
用户/客户端
开始
220
开始
221
输入设备、
软件密码
222
生成临时
访问代码
223
访问机构
网站登录
224
提供登录
选择
225
选择登录
226
向校验服务器
发送访问代码
228
在网站上输入
访问代码
227
允许登录?
229
否
231
是
客户端
继续校验
230

图3

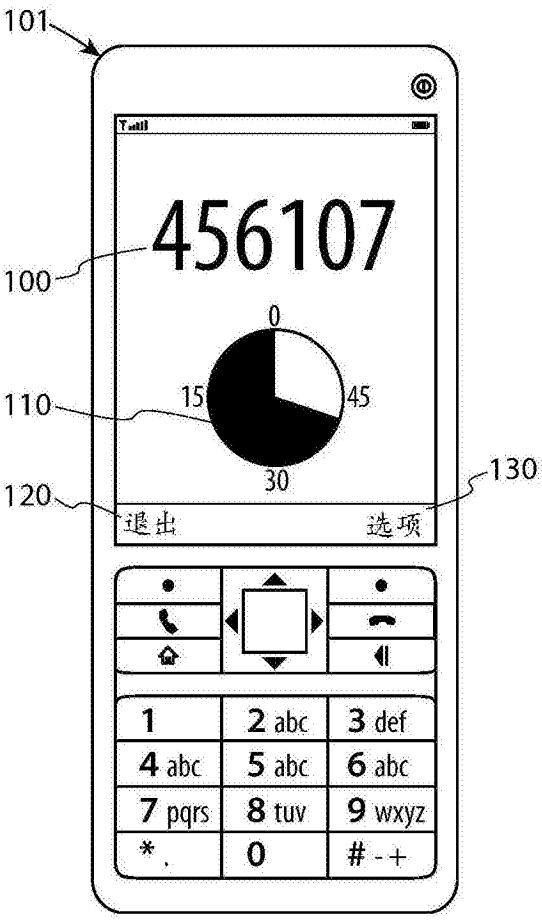

101
100
110
120
130
456107
0
15
45
30
退出
选项
1
2 abc
3 def
4 abc
5 abc
6 abc
7 pqrs
8 tuv
9 wxyz
* .
0
- +

图4

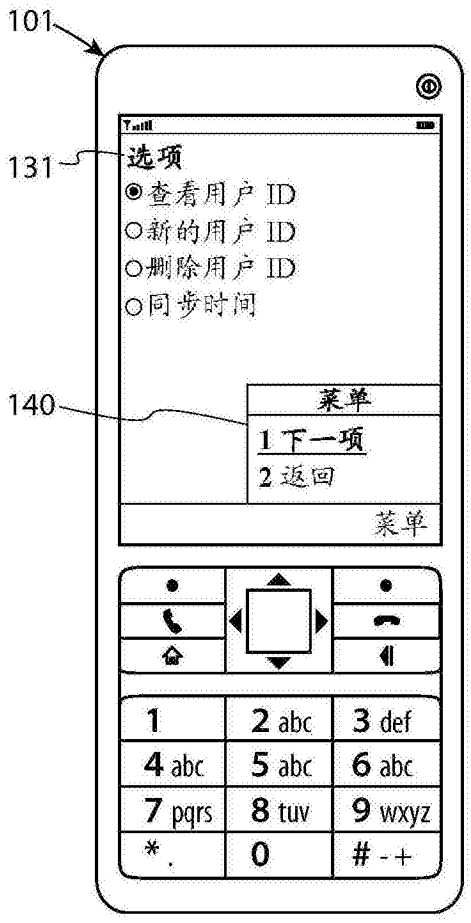

101
131
140
选项
查看用户 ID
新的用户 ID
删除用户 ID
同步时间
菜单
1 下一项
2 返回
菜单
1
2 abc
3 def
4 abc
5 abc
6 abc
7 pqrs
8 tuv
9 wxyz
*.
0
-+

图5

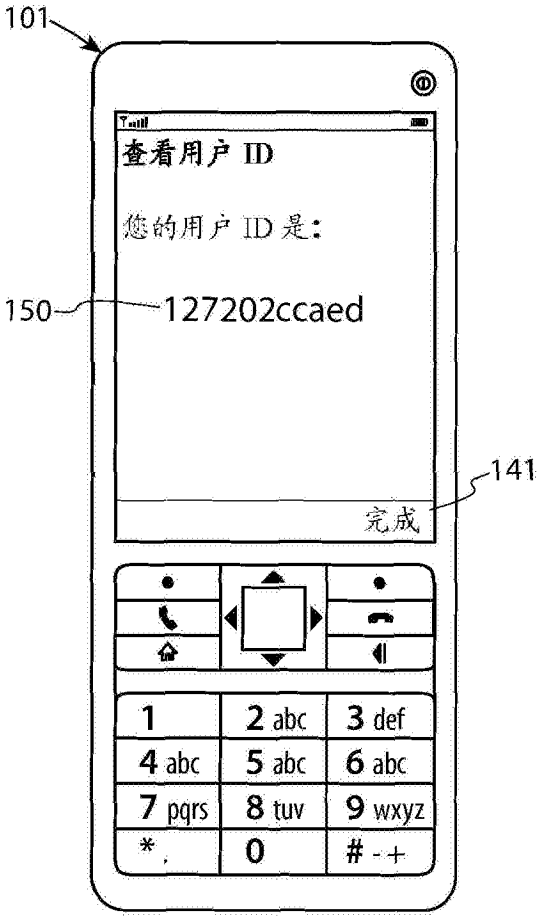

101
查看用户 ID
您的用户 ID 是:
150
127202ccaed
141
完成
1
2 abc
3 def
4 abc
5 abc
6 abc
7 pqrs
8 tuv
9 wxyz
*
0
- +

图6

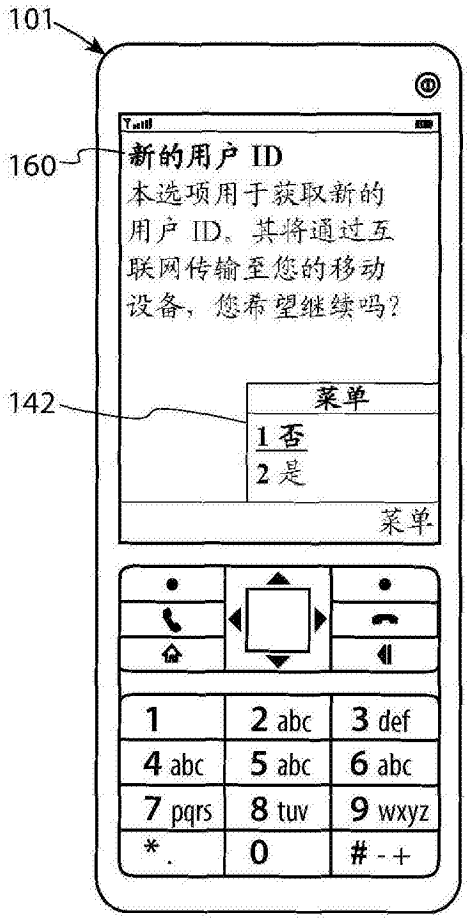

101
160
142
新的用户 ID
本选项用于获取新的用户 ID。其将通过互联网传输至您的移动设备。您希望继续吗?
菜单
1 否
2 是
菜单
1
2 abc
3 def
4 abc
5 abc
6 abc
7 pqrs
8 tuv
9 wxyz
*.
0
- +

图7

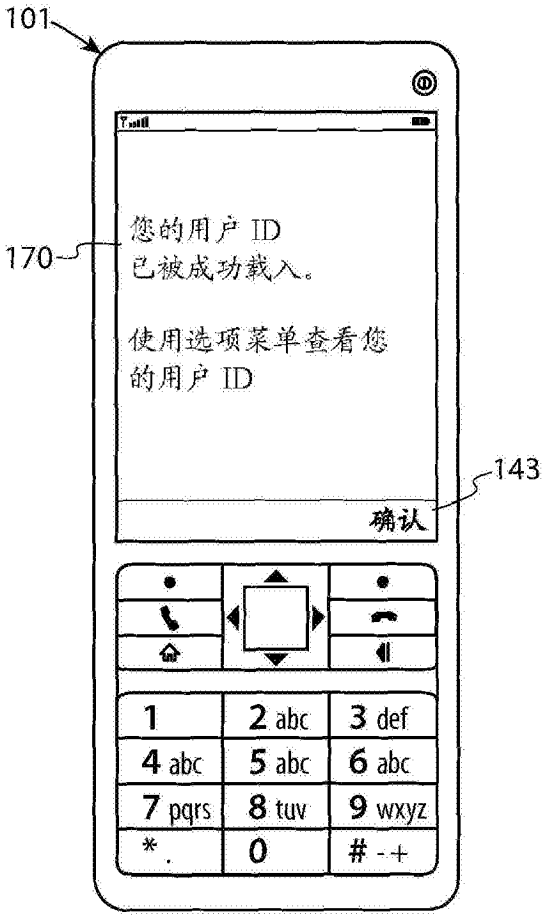

101
170
您的用户 ID
已被成功载入。
使用选项菜单查看您
的用户 ID
143
确认
1
2 abc
3 def
4 abc
5 abc
6 abc
7 pqrs
8 tuv
9 wxyz
*.
0
-+

图8

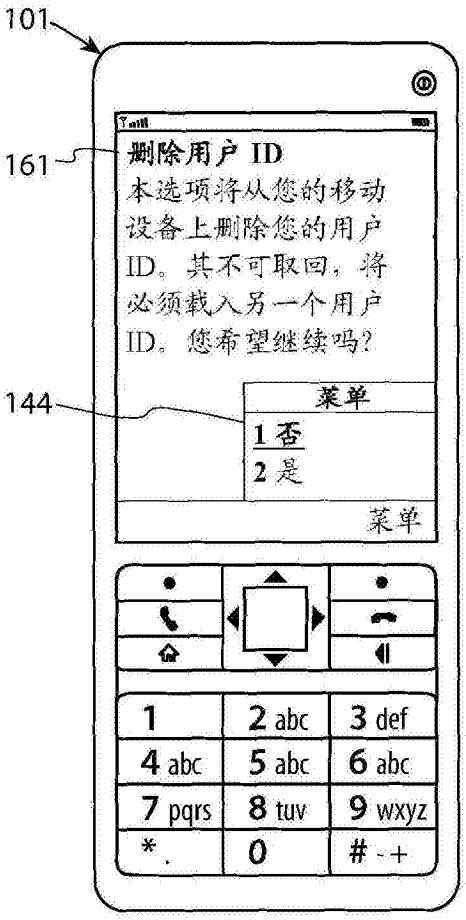

101
161
144
删除用户 ID
本选项将从您的移动设备上删除您的用户 ID。其不可取回，将必须载入另一个用户 ID。您希望继续吗?
菜单
1 否
2 是
菜单
1
2 abc
3 def
4 abc
5 abc
6 abc
7 pqrs
8 tuv
9 wxyz
*.
0
#-+

图9

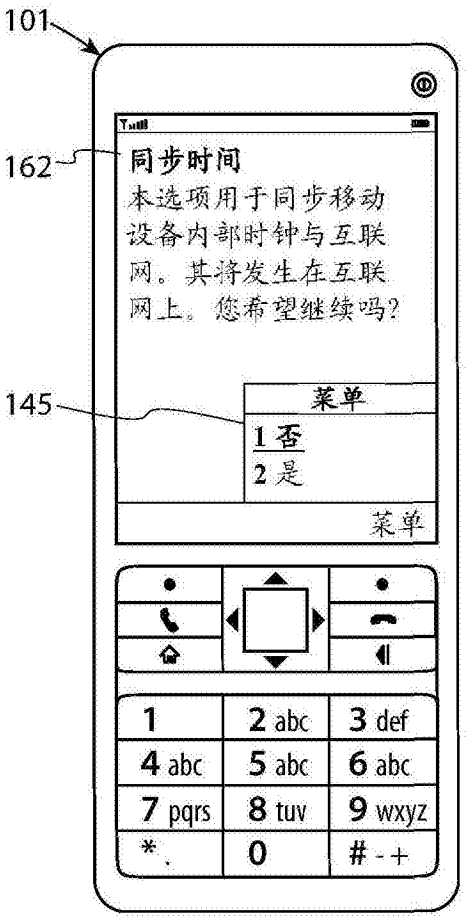

101
162
145
同步时间
本选项用于同步移动设备内部时钟与互联网。其将发生在互联网上。您希望继续吗?
菜单
1 否
2 是
菜单
1
2 abc
3 def
4 abc
5 abc
6 abc
7 pqrs
8 tuv
9 wxyz
*
0
- +

图10