(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106575454 A
(43)申请公布日 2017.04.19

(21)申请号 201580042980.4

(22)申请日 2015.06.11

(30)优先权数据
62/010,880 2014.06.11 US

(85)PCT国际申请进入国家阶段日
2017.02.10

(86)PCT国际申请的申请数据
PCT/US2015/035415 2015.06.11

(87)PCT国际申请的公布数据
WO2015/191913 EN 2015.12.17

(71)申请人 威尔蒂姆IP公司
地址 英国伦敦

(72)发明人 H·奥约斯 J·布雷弗曼 G·晓 J·F·马瑟 S·斯特赖特

(74)专利代理机构 北京三友知识产权代理有限公司 11127
代理人 吕俊刚 师玮

(51)Int.Cl.
G07C 9/00(2006.01)

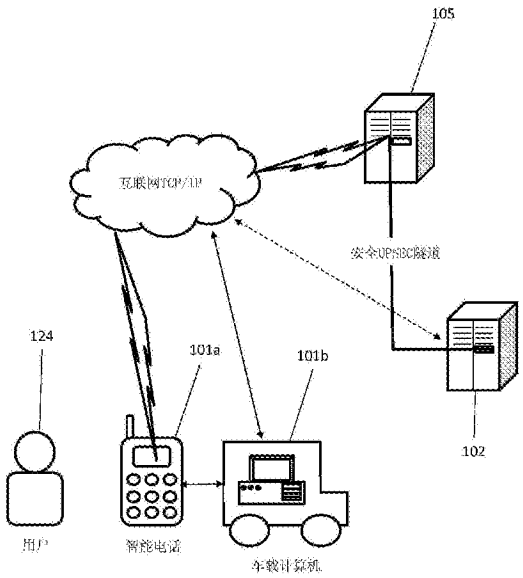
权利要求书4页 说明书26页 附图8页

(54)发明名称

基于生物特征信息帮助用户访问车辆的系统和方法

(57)摘要

提供用于授权用户对访问受控环境的访问的系统和方法。该系统包括与移动装置(例如,智能电话)通信的系统服务器平台和由用户访问的车载计算装置。这些实施方式使能一系列操作,其中,访问车辆的用户被提示使用用户的智能电话或车载计算机进行生物特征认证。此外,该系统还可以授权用户并且以电子方式帮助访问车辆以及执行与车辆的使用相关的其它授权的操作。此外,车辆访问系统与各种计算装置和用户可访问的基于计算机的服务集成。所述系统和方法还有助于使用光学传感器等主动监控车辆乘客和环境状况以提高安全性、便利性以及在车辆的使用期间的乘客的安全。



CN 106575454 A

1.一种用于授权用户访问车辆的方法,所述方法包括:

由计算装置访问计算机可读存储介质,所述计算机可读存储介质包括:

多个用户简档,其中,每个用户简档都与相应的用户和相应的移动装置相关联;

多个车辆简档,其中,每个车辆简档都与具有相应的车载计算机的相应的车辆相关联;以及

权限,所述权限与相应的用户简档和相应的车辆简档相关联,其中,所述权限控制由相应的用户对相应的车辆的访问;

由所述计算装置通过网络从移动装置接收授权请求,所述授权请求包括:与用户相关联的标识信息、标识所述车辆的访问信息;

由所述计算装置基于接收到的授权请求授权所述用户对所述车辆的访问,其中,所述授权步骤包括:

基于所述标识信息和所述访问信息,识别所述权限中的与所述用户和所述车辆相关联的一个或更多个权限;以及

基于所述一个或更多个权限,验证所述用户被授权访问所述车辆;

由存储设备中的计算装置创建关于授权访问的访问记录;以及

基于所述授权,由所述计算装置通过通信网络向与所述车辆相关联的远程计算装置发送授权通知,所述授权通知帮助所述用户访问所述车辆。

2.根据权利要求1所述的方法,所述方法还包括:

由所述计算装置从所述车载计算机接收关于所述用户对所述车辆的授权访问的使用信息;以及

基于所述使用信息更新所述访问记录。

3.根据所述权利要求2所述的方法,其中,所述使用信息包括以下中的一个或更多个:

所述授权访问期间的所述车辆的乘客的数量;

所述授权访问期间的所述车辆的位置;

所述用户的生命体征测量值;以及

所述用户的瞳孔放大。

4.根据所述权利要求4所述的方法,所述方法还包括:

由所述计算装置从所述车载计算机接收在所述授权访问期间发生的涉及所述车辆的事故的通知;

由所述计算装置向与急救响应机构相关联的远程计算装置发送包括所述车辆的乘客的数量的记录的至少一部分。

5.根据权利要求1所述的方法,其中,所述授权请求包括:与用户和移动装置相关联的标识信息、生物特征认证状态和标识所述车辆的访问信息,并且

其中,授权所述用户对所述车辆的访问包括:

由所述计算装置确定接收到的标识信息对应于在所述存储设备中存储的所述多个用户简档中的用户简档;

由所述计算装置确定所识别的车辆对应于在所述存储设备中存储的所述多个车辆简档中的车辆简档;

由所述计算装置基于接收到的生物特征认证状态,确定所述用户被所述移动装置生物

特征认证；

由所述计算装置在所述权限中识别与所述用户简档和所述车辆简档相关联的一个或更多个权限；以及

由所述计算装置基于所述一个或更多个权限，验证所述用户被授权访问所述车辆。

6.根据所述权利要求5所述的方法，所述方法还包括：

在所述授权访问期间，由所述计算装置从所述车载计算机接收后续授权请求，所述后续授权请求包括与所述用户和所述车载计算机相关联的标识信息、生物特征认证状态和标识所述车辆的信息；

基于所述后续授权请求和所述使用信息重复所述授权步骤，其中，所述验证步骤包括基于所述一个或更多个权限来分析所述使用信息；以及

基于重新授权向所述远程计算装置发送更新的授权通知。

7.根据权利要求5所述的方法，其中，所述移动装置和所述车载计算机是同一装置。

8.根据权利要求5所述的方法，其中，所述远程计算装置和所述车载计算机是同一装置。

9.根据权利要求1所述的方法，所述方法还包括：

其中，所述授权请求指定将使用所述车载计算机执行的操作，其中，所述操作是启动所述车辆和将所述车辆的车门解锁中的一种或更多种；以及

基于所述一个或更多个权限，验证所述用户被授权执行所述操作。

10.根据权利要求9所述的方法，其中，所述授权通知指示所述车载计算机通过执行所述操作来提供所述用户访问。

11.根据权利要求5所述的方法，其中，所述标识信息是所述用户和所述移动装置的唯一密钥，并且其中，确定接收到的标识信息对应于所述用户简档包括将接收到的密钥与和所述用户简档相关联的之前存储的密钥进行匹配。

12.根据权利要求1所述的方法，所述方法还包括：

在所述授权访问期间，由所述计算装置从所述车载计算机接收交易请求，所述交易请求包括与所述用户和所述车载计算机相关联的标识信息、生物特征认证状态以及关于将使用所述车载计算机进行的交易的交易细节；

由所述计算装置基于接收到的交易请求来授权所述用户进行所述交易，其中，所述授权步骤包括：

由所述计算装置确定接收到的标识信息对应于在所述存储设备中存储的用户简档；

由所述计算装置基于所述用户简档来识别与所述用户简档相关联的交易帐户；

由所述计算装置基于接收到的生物特征认证状态来确定所述用户被所述车载计算机生物特征认证；以及

由所述计算装置基于识别的交易账户和所述交易细节来验证所述用户被授权进行所述交易；以及

由所述计算装置基于所述授权向所述车载计算机发送第二授权通知，第二授权通知通过所述车载计算机推进所述交易。

13.根据权利要求1所述的方法，所述方法还包括：

其中，所述授权请求包括标识第二用户并限定控制所述第二用户对所述车辆的访问的

权限的设置；

由所述计算装置基于所述第二用户的标识，在所述用户简档中识别第二用户简档；以及

由所述计算装置基于接收到的设置来更新所述权限。

14.根据权利要求13所述的方法，所述方法还包括：

生成车辆访问密钥；

由存储器中的计算装置将所述车辆访问密钥的至少一部分与第二用户简档和与所述车辆相关联的车辆简档关联地存储在所述存储器中；

向所述第二用户移动装置发送所述车辆访问密钥。

15.根据权利要求14所述的方法，所述方法还包括：

由所述计算装置通过所述网络从所述第二用户移动装置接收第二授权请求，所述第二授权请求包括：与所述第二用户和所述第二用户移动装置相关联的标识信息、生物特征认证状态、所述第二用户密钥以及标识所述车辆的访问信息；

由所述计算装置基于所述第二授权请求来授权所述第二用户对所述车辆的访问，其中，所述授权步骤包括：

由所述计算装置确定包括在所述第二授权请求中的所述标识信息对应于所述第二用户简档；

由所述计算装置确定包括在所述第二授权请求中的所述第二用户密钥匹配与所述第二用户简档和所述车辆简档相关联的对应密钥；

由所述计算装置基于包括在所述第二授权请求中的所述生物特征认证状态来确定所述第二用户被所述移动装置生物特征认证；

由所述计算装置识别与所述第二用户简档和所述车辆简档相关联的一个或更多个权限；以及

由所述计算装置基于所述一个或更多个权限来验证所述第二用户被授权访问所述车辆；以及

由所述计算装置基于所述授权通过所述通信网络向所述车载计算机发送准予所述第二用户对所述车辆的访问的授权通知。

16.一种用于授权用户访问车辆的方法，所述方法包括：

由计算装置访问计算机可读存储介质，所述计算机可读存储介质包括：

多个用户简档，其中，每个用户简档都与相应的用户和相应的移动装置相关联；

多个车辆简档，其中，每个车辆简档都与具有相应的车载计算机的相应的车辆相关联；以及

权限，所述权限与相应的用户简档和相应的车辆简档相关联，其中，所述权限控制相应的用户对相应的车辆的访问；

由所述计算装置通过网络从移动装置接收授权请求，所述授权请求包括：与用户和移动装置相关联的标识信息、生物特征认证状态以及标识所述车辆的访问信息；

由所述计算装置基于接收到的授权请求来授权所述用户对所述车辆的访问，其中，所述授权步骤包括：

由所述计算装置确定接收到的标识信息对应于在所述存储设备中存储的所述多个用

户简档中的用户简档；

由所述计算装置确定识别的车辆对应于所述存储设备中存储的所述多个车辆简档中的车辆简档；

由所述计算装置基于接收到的生物特征认证状态，确定所述用户被所述移动装置生物特征认证；

由所述计算装置识别所述权限中的与所述用户简档和所述车辆简档相关联的一个或更多个权限；以及

由所述计算装置基于所述一个或更多个权限，验证所述用户被授权访问所述车辆；以及

由存储设备中的计算装置，创建关于所述授权访问的访问记录；以及

由所述计算装置基于所述授权通过通信网络向与所述车辆相关联的远程计算装置发送授权通知，所述授权通知帮助所述用户对所述车辆的访问。

基于生物特征信息帮助用户访问车辆的系统和方法

技术领域

[0001] 本发明涉及帮助用户访问车辆的系统和方法，具体地，涉及基于用户生物特征信息帮助用户访问车辆的系统和方法。

背景技术

[0002] 现有车辆，即使是具有每一个选项的最昂贵的车型也不知道其主人是谁。汽车仅在最基本意义上“知道”某人正在驾驶该汽车并且某人正坐在前座上。汽车还可能知道正在被用于访问该汽车的特定钥匙。一般来说，汽车在自我管理上很智能，但对谁在车内不知悉。目前的技术进步集中在有一些知悉外部世界的自动驾驶汽车。然而，没有汽车被配置为知晓驾驶员或乘客，或基于对汽车的乘客的识别和对乘客的主动监控而采取通知的行动。

[0003] 因此，需要能够知悉车主或用户的车辆。因此，需要能够使用传统的移动装置技术通过名字和脸来识别用户的基于车辆的系统。还需要将基于现有车辆的系统和其它用户装置和联网的系统以及与识别的用户相关联的服务安全地集成。此外，需要一种能够通过机器学习识别用户习惯和偏好的基于车辆的系统。此外，需要一种能够在车辆的使用期间监控车辆的使用和用户的基于车辆的系统。此外，需要一种利用上述以提供在用户日常生活中帮助用户的附加的与安全、安保和用户便利性相关的帮助和服务的基于车辆的系统。

[0004] 本发明解决这些问题和其它顾虑。

发明内容

[0005] 根据本申请的一个或更多个实施方式，本文公开了一种用于授权用户访问车辆的方法。该方法包括通过计算装置访问计算机可读存储介质，该计算机可读存储介质包括：多个用户简档，各个用户简档都与相应的用户和相应的移动装置相关联；多个车辆简档，各个车辆简档都与具有相应的车载计算机的相应车辆相关联；以及权限，所述权限与相应的用户简档和相应的车辆简档相关联。所述权限控制相应的用户访问相应的车辆。该方法还包括由所述计算装置通过网络从移动装置接收授权请求，所述授权请求包括与用户相关联的标识信息和标识车辆的访问信息。该方法还包括授权用户对车辆的访问。所述授权步骤包括识别与用户简档和车辆简档相关联的一个或更多个权限，并且基于一个或更多个权限验证用户被授权访问车辆。该方法还包括由存储装置中的计算装置创建关于授权访问的访问记录，并且通过通信网络向与车辆相关联的远程计算装置发送帮助用户访问车辆的授权通知。

[0006] 根据本发明的另一方面，提供一种用于授权用户访问车辆的方法。该方法包括通过计算装置访问计算机可读存储介质，所述计算机可读存储介质包括：多个用户简档，各个用户简档都与相应的用户和相应的移动装置相关联；多个车辆简档，各个车辆简档都与具有相应的车载计算机的相应车辆相关联；以及权限，所述权限与相应的用户简档和相应的车辆简档相关联。所述权限控制相应的用户访问相应的车辆。该方法还包括由所述计算装置通过网络从移动装置接收授权请求，所述授权请求包括与用户和移动装置相关联的标识

信息、生物特征认证状态和标识车辆的访问信息。该方法还包括授权用户对车辆的访问。所述授权步骤包括确定接收到的标识信息对应于存储在存储装置中的多个用户简档中的用户简档。所述授权步骤还包括确定所识别的车辆对应于存储在存储装置中的多个车辆简档中的车辆简档。所述授权步骤还包括基于接收到的生物特征认证状态，确定用户已被移动装置生物特征认证。所述授权步骤还包括识别所述权限中的与用户简档和车辆简档相关联的一个或更多个权限，并且基于所述一个或更多个权限，通过计算装置验证用户被授权访问车辆。该方法还包括通过存储装置中的计算装置创建关于授权访问的访问记录，并且通过通信网络向与车辆相关联的远程计算装置发送帮助用户访问车辆的授权通知，由计算装置通过网络从移动装置接收授权请求，所述授权请求包括：与用户和移动装置相关联的标识信息、生物特征认证状态和标识车辆的访问信息。

[0007] 通过以下参照附图对本发明的描述，本发明的其它特征和益处将变得显而易见。

附图说明

[0008] 图1是根据本文公开的至少一个实施方式的用于授权访问车辆的系统的高层图；

[0009] 图2A是根据本文公开的至少一个实施方式的计算装置的框图；

[0010] 图2B是根据本文公开的至少一个实施方式的计算机软件模块的框图；

[0011] 图2C是根据本文公开的至少一个实施方式的计算装置的框图；

[0012] 图3是示出根据本文公开的至少一个实施方式的用于使用车载计算机注册用户的例程的流程图；

[0013] 图4是示出根据本文公开的至少一个实施方式的用于基于用户的生物特征授权用户使用车辆的例程的流程图；

[0014] 图5A是示出根据本文公开的至少一个实施方式的车载计算装置的示例性构成的图；

[0015] 图5B是示出根据本文公开的至少一个实施方式的车载计算装置的示例性构成的图；

[0016] 图5C是示出根据本文公开的至少一个实施方式的包括车载计算装置的示例性车辆的图；并且

[0017] 图6A是根据本文公开的至少一个实施方式的示例性用户界面的屏幕截图。

具体实施方式

[0018] 仅作为示例并且为了概述和介绍的目的，本发明的实施方式如下所述，其涉及一种基于用户的生物特征认证，授权用户对特别是诸如机动车的车辆的访问受控环境(ACE)的访问。

[0019] 本文公开的系统和方法根据基于用户的生物特征信息的用户认证来帮助用户物理地访问车辆。类似地，公开的实施方式提供针对各种基于计算机的特征和与车辆和车辆的操作相关的功能的授权的用户访问。如本文中进一步描述的，术语“访问(access)”包含用户对车辆的一种或更多种的物理访问(例如，进入车辆的内部)、车辆的使用(例如，驾驶车辆)、与车辆的部件和功能交互、直接地或间接地使用用户计算装置(例如，调节各种部件和与车辆操作相关的设置、规范其他人对车辆的使用等)。用户访问还包括使用由集成至车

辆中的计算装置提供的特征、功能和服务，例如，通过通信网络使用车载计算机访问诸如基于订购服务(例如，音乐帐户、导航、支付帐户)的其它访问受控环境以在使用车辆的同时进行电子交易。

[0020] 本文公开的系统和方法提供基础设施以配置能够知悉车主的汽车。更具体地，车载计算机能够在车主访问之前和在使用车辆时通过名字和脸来识别车主。另外，该系统还被配置为使用遍布整个车辆布置的光学传感器和其它传感器，基于生物特征主动监控用户、在使用期间监控车辆和周围环境。因此，车载计算机可以通过机器学习学习用户属性、习惯和偏好。该系统还可以使用生物特征用户信息来检测异常的用户行为、紧急状况等。作为响应，该系统能够相应地调节车辆的操作或向合适的接收者提供通知和提醒。通过将车载计算机与其它用户装置和联网系统以及与用户关联的服务集成，机器学习可以进一步增强和了解情况。因此，通过基于生物特征的用户认证和监控、环境监控和机器学习，该系统能够提供与安全、安保和便利相关的帮助和服务以在日常生活中帮助用户。

[0021] 如图1所示，用于授权用户访问车辆100的系统可以包括与联网的服务器进行通信的联网的远程系统服务器平台100以及包括例如固定的计算机、车载计算装置(“车载计算机”101b)以及诸如膝上型计算机、平板计算机和智能电话的移动装置101a(不限于此)的面向用户的计算装置(“用户装置”)，以帮助用户的生物特征认证，并且基于与相应的车辆和/或相应的用户相关联的规则和权限授权用户所请求的访问。

[0022] 认证包括捕捉用户的生物特征信息，提取唯一的特征，并且将所述特征编码为标识符。可以由各种面向用户的装置单独地或与系统服务器协同地执行认证。在一些实现中，用户可以由用户的预先登记的智能手机装置被生物特征认证。附加地或另选地，用户可以被车载计算机认证。在通过车载计算机认证期间，例如，可以使用位于车辆中或周围并且在工作上连接至车载计算机的一个或更多个传感器来捕捉生物特征信息。使用捕捉的生物特征，车载计算装置可以执行用户的生物特征认证。除了生物特征认证，车载计算机能够与远程系统服务器共同授权用户访问车辆。

[0023] 如果用户被成功地认证并且被授权访问车辆，则用于授权用户访问车辆100的系统可以帮助用户的物理访问。例如，远程系统服务器105能够向车载计算机101b发送授权通知。此外，在用户被认证后，该系统还可以指示车载计算机执行其它操作，诸如启动车辆等。按照这种示意性方式，该系统可以帮助用户对车辆的物理访问，并且通过车载计算机提供对车辆的其它受计算机控制的功能和可用服务的物理或电子访问和控制。

[0024] 另外，本文公开的系统和方法还提供车载计算机101b与诸如用户的移动装置101a(又称为智能电话)或台式计算机的其它注册的用户计算装置的生物特征安全的集成，使得各种用户装置将能够用于与车载计算机交互，管理对车辆和车辆的其它计算机控制部件的访问。相似地，这样的集成还有助于跨包括系统100在内的各种装置来安全地分享车辆、基于车辆的功能和服务以及与用户和车辆的使用相关的信息。此外，用于基于安全生物特征的用户认证的系统和方法可以被配置为认证/授权用户对其它访问受控环境(例如，远程、联网的计算装置和它们通过车载计算机或用户的个人计算装置提供的服务)的访问。

[0025] 本申请的系统和方法根据基于生物特征访问管理为用户提供了很大的方便，并且通过补充或者消除物理钥匙、密码和/或专用于存储用户帐户信息的装置(例如卡或象征性的钥匙等)提供了增加的安全性。尽管在提供对车辆和计算机访问受控特征和与车辆的使

用相关的功能的上下文中描述了公开的实施方式，但是本文中公开的许多原理同样地适用于帮助虚拟地访问需要用户认证/授权的任何类型的系统，例如，诸如网站访问、物理访问控制、用户角色确定、组识别、自动化、密码管理、或其它访问受控的物理和虚拟环境。

[0026] 本文公开的系统和方法提供了包括计算装置的分布式基础设施，计算装置包括被配置为使用各种面向用户的装置协调基于生物特征的身份声明和访问管理的后端系统服务器。

[0027] 根据本申请的一个方面，可以使用市售的数字摄像头执行为了基于生物特征识别用户的目的的捕捉图像。例如，生物特征认证平台可以包括被配置成使用关联的摄像头装置捕捉用户的生物特征信息并基于生物特征认证用户的用户装置。在一个或更多个实现中，生物特征认证平台将脸部辨识技术与虹膜和眼周识别技术结合以帮助用户的生物特征认证。然而，应该理解，可以使用生物特征的任何组合，例如，脸部、虹膜、眼周、或甚至是声音、静脉图案等。另外，生物特征认证还可以包括“活性(liveness)”检测系统以验证“真人”正在尝试访问系统和/或完成交易。

[0028] 在一个或更多个实现中，示例性系统还可以实现生物特征开放协议标准(BOPS)。本文中使用的术语“BOPS”通常包含控制各种电子装置和/或系统服务器之间的安全通信的规则。特别地，BOPS协议能够通过用户装置与系统服务器之间的加密机制使能双向安全套接层(SSL)/传输层安全(TLS)连接，其还能够利用入侵检测系统。因此，双向SSL提供：各个正在通信的用户装置通过由服务器提供的证书来验证BOPS服务器的身份，并且服务器也通过安装在用户装置上的证书(对每个移动装置是唯一的并且在注册期间由BOPS生成)来验证用书装置的身份。附加地，在示例性实现中，使用571位椭圆曲线密码(Elliptic Curve Cipher)来提供TLS。因此，可以使用其中每一侧的长度是1024或2048位的双向SSL环境以及构成传输层的是571位的ECC加密的TLS层来保护通信。BOPS也可控制后端系统服务器与其它远程或基于云的服务器计算装置之间的通信。

[0029] 本文中使用的术语“客户端app”或应用一般是指一种用于有助于用户装置与后端生物特征认证平台的集成的面向用户的计算装置的应用。使用生物特征认证平台，客户端app能够配置用户装置以向用户提供对通常需要物理钥匙、密码和/或用户名等的系统和服务的安全访问。因此，执行客户端应用程序的用户装置与后端生物特征认证平台一起能够替换用户携带以标识自己和/或获得对访问受控环境的授权访问并执行安全交易的的所有物品(例如，信用卡、护照、驾驶执照、访问令牌、钥匙等)。

[0030] 用于授权访问车辆100的示例性系统被示出为图1中的框图。在一种布置中，该系统由系统服务器105、包括用户移动装置101a和车载计算装置(“车载计算机”)101b的面向用户的计算装置组成。系统100还可包括一个或更多个远程计算装置102。

[0031] 如本文中进一步描述的，实际上，系统服务器105可以是能够与用户装置和远程计算装置通信并且接收、发送和存储电子信息并处理请求的任何计算装置和/或数据处理装置。相似地，如本文中进一步描述的，实际上，远程计算装置102可以是能够与系统服务器和/或用户装置通信并且接收、发送和存储电子信息并处理请求的任何计算装置和/或数据处理装置。还应理解，系统服务器和/或远程计算装置可以是许多联网的或基于云的计算装置。

[0032] 在一些实现中，计算装置102可以代表通过车载计算装置向用户提供订阅服务的

联网的计算系统，诸如由密歇根底特律的通用汽车提供的On-Star®服务。如本领域的技术人员应理解的，这样的系统通过无线通信网络与车载计算装置通信，并且通过包括例如但不限制于通信系统、车载安全系统、免提通话系统、逐项(turn-by-turn)导航系统、和远程诊断系统的这样的装置向用户提供订阅服务。作为另一示例，计算装置102还可以表示与企业组织相关联的计算网络，所述企业组织保持用户帐户并在准予访问安全的联网环境(例如，安全网站、银行、VPN、支付供应商、订阅服务等)之前要求进行帐户持有人的验证或者为帐户持有人提供服务/进行交易。因此，由计算装置102代表的联网的系统可以被配置为保持用户帐户，并且在提供他们相应的服务之前一般需要用户的认证和授权。用于访问这样联网的系统或与这样联网的系统交互的各种类型用户帐户在本文中称为交易帐户。

[0033] 如文本中进一步描述的，包括移动装置101a和车载计算机101b的用户计算装置可以被配置为彼此通信、与系统服务器105和/或远程计算装置102通信，向它们发送电子信息并且从它们接收电子信息。用户装置还可以被配置为接收用户输入，并且通过捕捉和处理例如用户124的数字图像和录音的用户生物特征信息来帮助用户的生物特征认证。

[0034] 移动装置101a能够包括但不限制于平板计算机、个人数字助理、蜂窝电话、智能电话装置或类似的移动计算装置。应该理解，移动装置101a的特征和功能还可以使用诸如工作站、个人计算机、膝上型计算机、交易终端等的其它面向用户的计算装置来实现。车载计算机101b旨在代表被集成在车辆中的并且能够与用户交互的各种形式的移动计算装置，诸如车辆控制系统、导航系统、车载诊断(OBD)系统等。

[0035] 如本文中进一步描述的，用于授权对车辆100的访问的系统，根据用户的生物特征，针对与用户对车辆的访问和/或与用户对车辆的访问相关的服务，帮助用户124的认证。如前所述，使用用户的移动装置101a和/或车载计算机101b，可以至少部分地执行用户认证。

[0036] 在一些实现中，根据用户的生物特征的识别和/或认证在两阶段过程中利用用户的生物特征信息。第一阶段称为注册。在注册阶段，从个体收集合适的生物特征的样本(例如，图像)。分析和处理生物特征的这些样本以提取在每个样本中存在的特征(或特性)。可以将个体的生物特征中存在的特征的集合编码以提供个人的生物特征标识符。然后，存储这些标识符以完成注册阶段。在第二阶段中，测量个体的同一生物特征。与在注册阶段中一样，从生物提取特征以获得用户的当前生物特征信息。如果目的是识别，则将当前的生物特征标识符与在第一阶段中生成的存储的标识符仅进行比对(例如，一对多匹配)。如果出现匹配，则显示了个体的识别，否则识别失败。如果目的是认证，则将在第二阶段中生成的标识符与第一阶段中为特定个人生成的标识符进行比较(例如，一对一匹配)。如果出现匹配，则认证成功，否则认证失败。捕捉的生物特征信息还能够提供关于用户是否是有生命的主体的指示。如果目的是确定活性，可以分析特征或特性以确定它们是否表示有生命的主体。

[0037] 在一些实现中，系统服务器105可以被配置为安全地帮助用户的身份的识别/认证(统称为认证或身份认定(assertion))，而不授权用户对访问受控环境的访问或执行用户请求的潜在的交易/操作。以这样的方式，服务器不需要保留用于授权访问和/或潜在交易的用户的敏感交易帐户信息。取而代之，系统服务器被配置为通过在适当的安全级别识别一个用户来授权该用户。例如，系统服务器可以被配置为识别尝试访问车辆的用户并且向控制车辆访问和管理的独立系统(例如，由On-Star®服务操作的远程计算装置102)提供认

证的用户身份。作为另一示例，系统服务器可以被配置为识别根据支付处理器要求的标准使用车载计算机(或移动装置)进行金融交易的用户并且告知支付处理器的企业计算系统(例如，远程计算装置102)该用户已被认证。因此，一旦为了安全的目的确认了用户的身份，用于认证用户的示例性系统和方法可以通过与现有的基础设施和过程集成来补充和/或替换现有的企业认证过程，而不干扰已建立的用于授权访问/交易的过程。

[0038] 然而，除了身份认定，系统服务器105可以被配置为实现包括角色收集和访问控制在内的附加安全过程，从而帮助授权用户对访问受控环境进行访问。这样，用户授权过程可以包括身份认定，并且还可以包括通过确定用户的身份是否与对访问受控环境进行访问的必需权限相关联或与能够用于执行请求的交易的一个或更多个交易帐户相关联的授权。

[0039] 在一些实现中，系统服务器105还可以执行对用户可以与之交互的各种计算装置(例如，移动装置101a、车载计算机101b)与一个或更多个受信的后端服务器(例如，系统服务器105和远程计算装置102)之间的信息和/或信息的发送进行控制的规则。更具体地，系统服务器105可以实施对用户124对信息的访问进行控制的规则。如用户限定的，系统服务器还可以实施控制与经授权和认证的第三方共享用户信息的规则。例如，系统服务器可以根据用户限定的规则来调整对属于用户124的车辆的使用的信息的数据库的访问并限制其它用户和第三方(监控公司)对该信息的访问。作为另一示例，根据规则或之前给予用户的权限，保持信息的数据库并给予认证的用户对信息的访问。

[0040] 本文中还描述了系统服务器105的帮助身份认定、角色收集、访问控制以及包括审核和安全保证和问责的其它安全功能的示例性系统和方法。

[0041] 应该注意，尽管图1描述了关于移动装置101a和车载计算机101b和远程计算装置102用于授权对访问受控环境100的访问的系统，应该理解，任何数量的这样的装置可以按照本文中描述的方式与该系统进行交互。还应理解，在特定的实现中，引用的装置和机器以及它们相关的和/或伴随的操作、特征和/或功能可以诸如通过网络连接或有线连接或无线连接地跨任何数量的这样的装置和/或机器被结合或布置或采用。还应注意，尽管图1关于用户124描述了系统100，应该理解，任何数量的用户可以按照本文中描述的方式与系统交互。

[0042] 还应理解，本文中在车载计算机101b的上下文中描述的示例性特征和功能不受限制并且可以使用诸如移动装置101a的其它使能的计算装置实现，反之亦然。

[0043] 图2A描述了用于与用于授权对车辆100的访问的系统一起使用的车载计算机101b的示例性框图。车载计算机能够包括位于相关联的车辆中或上的一个或更多个位置处并且用于使能系统100的操作的各种硬件和软件组件。车载计算机的组件包括一个或更多个处理器110、存储器120、麦克风125、显示器140、一个或更多个摄像头145、音频输出155、存储设备190和通信接口150。

[0044] 处理器110用于执行包括以可加载至存储器120中的可执行代码的形式的软件指令的客户端应用。取决于特定实现，处理器110可以是多个处理器、中央处理单元CPU、图形处理单元GPU、多处理器核或者任何其它类型的处理器。

[0045] 优选地，存储器120和/或存储设备190可被处理器110访问，从而使能处理器接收和执行在存储器和/或存储设备中编码的指令，从而使车载计算机及其各种硬件组件执行系统和方法的各方面的操作，如将在下面更详细地描述的。存储器可以是例如随机存取存

储器(RAM)或任何其它合适的易失性或非易失性计算机可读存储介质。另外，存储器可以是固定的或可去除的。取决于特定的实现，存储设备190可以采取各种形式。例如，存储设备可含有一个或更多个组件或装置，诸如硬盘驱动器、闪存、可重写光盘、可重写磁带或以上的一些组合。存储设备还可以是固定的或可去除的。

[0046] 一个或更多个软件模块130被编码在存储设备190和/或存储器120中。软件模块130可以包括具有代码形式的指令的一个或更多个软件程序/应用(称为“客户端应用”)。代码可以以一种或更多种编程语言的任意组合来编写并且可在处理器中执行，并且当在处理器110中执行时，代码将处理器配置为执行各种操作，如本文中进一步描述的。如图2B所述，优选地，软件模块130中包括用户界面模块170、生物特征捕捉模块172、分析模块174、注册模块176、数据库模块178、认证模块180和通信模块182。

[0047] 程序代码可以作为单独的软件包完全在车载计算机101b上执行、部分地在车载计算机和远程装置(诸如，系统服务器105)上执行。在后一种情况下，远程计算机可以通过包括局域网(LAN)或广域网(WAN)、移动通信网、蜂窝网、或使用互联网服务提供商的互联网的网络连接至车载计算机101b。

[0048] 如本领域的普通技术人员已知的，也可以说，软件模块130的程序代码和一个或更多个计算机可读存储装置(诸如存储器120和/或存储设备190)形成可以根据本发明制造和/或分发的计算机程序产品。

[0049] 还可以理解，不需要这些模块被车载计算机101b本地存储，并且可以以分布的方式存储。应该理解，在一些例示实施方式中，一个或更多个软件模块130可以通过网络经由通信接口150从另一装置或系统下载至存储设备190以在授权对车辆100的访问的系统内使用。此外，应注意，与本系统和方法的操作相关的其它信息和/或数据(诸如数据库185)还可以被存储在存储设备上。

[0050] 在一些实现中，敏感的用户信息可以被存储在加密数据存储部上，加密数据存储部被专门分配以安全地存储通过执行安全认证应用的处理器收集或产生的信息。加密措施可用于在存储设备上本地存储信息和向远程计算装置发送信息。例如，可以使用1024位多态密码或AES 256位加密方法(根据导出控制)来加密这样的数据。此外，可以使用远程密码键(种子)或本地密码键(种子)实施加密。可使用如本领域的技术人员所熟知的可替代的加密方法，例如，SHA256。此外，可使用用户的生物特征信息、活性信息或装置信息、或上述的任意组合将车载计算机101b和/或系统服务器105上存储的数据加密为加密密钥。例如，使用密钥推导函数，可以根据诸如生物特征信息的唯一的用户信息生成一个或更多个密钥，使得密钥由于从用户的生物特征信息导出而与用户唯一地关联。在一些实现中，上述的用户信息的组合可以用于创建可以使用椭圆曲线密码进行加密并存储在移动装置上的用户的复杂唯一密钥。此外，该密钥可以用于保护存储在移动装置上的和/或系统服务器上的用户数据。

[0051] 此外，优选地，数据库185存储在存储设备190上。如将在下面更详细地描述，数据库包含和/或保持在用于认证用户对车辆100的访问的系统和方法中的各种操作中始终使用的各种数据项和元素。如将在本文中更详细地描述，存储在数据库中的信息可以包括但不限于用户简档。应当指出，虽然数据库被描述为在车载计算机101b本地配置，但是在特定实现中，附加地或者另选地，数据库和/或存储于其中的各种数据元素能够远程地设置(如

在远程装置102或系统服务105，未示出)，并以本领域技术人员所熟知的方式通过网络连接至车载计算机。

[0052] 用户接口115也可在工作上连接至处理器。如在电子计算装置和车载计算装置领域中理解的，所述接口可以是一个或更多个输入输出装置，诸如开关、按钮、键、触摸屏、麦克风等。用户接口用于帮助捕捉来自用户的命令(诸如开关命令)或用户信息和与公开的实施方式的操作相关的设置。例如，在用户认证期间和在本文进一步描述的车辆的正常操作和使用期间，所述接口用于帮助捕捉来自用户的特定信息，诸如用于向系统注册的个人用户信息。

[0053] 显示器140也可以在工作上连接至处理器110。显示器包括屏幕或使系统能够指示或向用户提供关于车辆和车载计算机的操作的反馈的任何其它此类呈现装置。例如，显示器可以是数字显示器，诸如图5A中示出的安装在车辆的仪表组合(gauge cluster)中的点阵显示器或其它二维显示器或图5B中示出的仪表板上安装的显示器。

[0054] 作为另一示例，接口和显示器可以集成至触摸屏显示器。因此，显示器还被用于显示图形用户界面，图形用户界面能够显示各种数据并提供包括允许用户输入信息的区域的“窗体(form)”。在对应于图形用户界面的显示的位置处触摸触摸屏允许个人与该装置交互以输入数据、更改设置、控制功能等。因此，当触摸屏被触摸时，用户接口将变化发送至处理器，并且可改变设置或可捕捉到用户输入的信息并存储在存储器中。

[0055] 摄像头145也可以在工作上连接至处理器110。摄像头用于帮助捕捉用户的图像。在一些实现中，摄像头145可以包括一个或更多个可见光摄像头(例如，在消费型装置上常见的并具有足够分辨率的摄像头)、被配置为捕捉用户的NIR图像的近红外摄像头、红外摄像头和热红外摄像头或前述的组合。优选地，至少一个摄像头被设置在车辆中或车辆上，使得当用户在车辆外部时可以捕捉用户的影像。例如，在图5C中，示出外部安装的摄像头145a作为车辆的侧视镜组件的部分。如图5A中所示，一个或更多个附加的摄像头还可以布置在车辆内的不同位置处，例如，摄像头145b可以放置在仪表组合中以便在驾驶员坐在驾驶座中时捕捉驾驶员的影像。此外，一个或更多个摄像头可以设置在车辆内部的不同位置处以捕捉乘客的影像以用于监控或识别，如本文进一步描述的。

[0056] 在一些实现中，为了以生物特征方式从图像中识别/认证用户的目的而捕捉影像。此外，摄像头可以为了监控一个或更多个车辆乘客/用户的目的而捕捉影像，包括检测脸部表情、移动、身体语言、监控生命体征和各种情况的其它生物特征指标。例如，热IR摄像头可以用于捕捉车辆中的一个或更多个用户的影像，所述影响可被处理器使用以检测核心体温、心率等。可见光或NIR和IR摄像头可以用于检测瞳孔放大(例如，用于检测清醒状态/醉酒)、眼睛闭合(例如，入睡的生物特征标志)、监控如脉搏和呼吸频率的生命体征、检测脸部表情(例如，检测情绪/行为)等。

[0057] 返回到图2A，处理器110和/或摄像头145还可以通信地联接至例如可见光、红外或近红外光发射器等的一个或更多个光或信号发射器(未示出)，以在图像捕捉期间照亮对象。

[0058] 音频输出155也可在工作上连接至处理器110。如本领域技术人员理解的，音频输出可以是被配置成播放电子音频文件的任何类型的扬声器系统。音频输出可以被集成至移动装置101中或位于移动装置101的外部。此外，如本领域技术人员理解的，移动装置还可以

包括用于捕捉录音的一个或更多个麦克风104。

[0059] 各种附加硬件装置/传感器160也可以在工作上连接至处理器。如本领域技术人员理解的，传感器160可以包括：跟踪当日时间等的车载时钟；确定移动装置的位置的GPS使能装置；跟踪装置或关联车辆的方向和加速度的加速度计；重力磁力仪；接近传感器；RF辐射传感器、温度计以及在移动装置、车辆的车载计算机中常见的其它这样的传感器。

[0060] 通信接口150也可在工作上连接至处理器，并且可以是使能移动装置101a与包括系统服务器105在内的外部装置、机器和/或元件之间的通信的任何接口。优选地，通信接口包括但不限于调制解调器、网络接口卡(NIC)、集成网络接口、射频发射/接收器(例如，蓝牙、蜂窝、NFC)、卫星通信发射/接收器、红外端口、USB连接、和/或用于将移动装置连接至其它计算装置和/或诸如专用网和互联网的通信网络的任何其它这样的接口。这样的连接可以包括有线连接或无线连接(例如，使用802.11标准)，虽然应当理解的是，通信接口可以实际上是使能至移动装置的通信或来自移动装置的通信的任何接口。

[0061] 图2E是示出系统服务器105的示例性配置的框图。系统服务器105可以包括在工作上连接至各种硬件和软件组件的处理器210，各种硬件和软件组件用于使能系统的操作以帮助在终端100处对交易进行安全认证。如将在下面更详细地描述，处理器210用于执行指令以进行与用户认证和交易处理相关的各种操作。取决于特定实现，处理器210可以是多个处理器、多处理器核或者一些其它类型的处理器。

[0062] 在特定实现中，存储器220和/存储介质290可被处理器210访问，由此使得处理器210接收和执行在存储器220上和/或存储设备290上存储的指令。存储器220可以是例如随机存取存储器(RAM)或任何其它合适的易失性或非易失性计算机可读存储介质。另外，存储器220可以是固定的或可去除的。存储设备290可以采取各种形式，这取决于特定的实现。例如，存储设备290可含有一个或更多个组件或装置，诸如硬盘驱动器、闪存、可重写光盘、可重写磁带或以上的一些组合。存储设备290也可以是固定的或可去除的。

[0063] 包括可由处理器210执行的代码形式的指令的一个或更多个软件程序或应用(称为“安全认证服务器应用”)可以被编码在存储设备290中和/或存储器220中。例如，服务器应用程序可以包括软件模块130(图2B中示出)，并且模块130可作为一个独立的软件包在系统服务器105上完全地执行、在系统服务器105上部分地执行并在远程计算装置上部分地执行，诸如远程计算装置102、移动装置101a和/或用户计算装置101b、或在这样的远程计算装置上完全地执行。

[0064] 还优选地，数据库280存储在存储设备290上。如将在下面更详细地描述，数据库280包含和/或保持在系统100的各种操作中始终利用的各种数据项和元素，包括但不限制于将在本文进行详细描述的用户简档。应当指出，虽然数据库280被描述为计算装置205本地地配置，在特定实现中，数据库280和/或在其中存储的各种数据元素可以存储在远程地定位并通过网络(未示出)以本领域的普通技术人员已知的方式连接至系统服务器105的计算机可读存储器或存储介质上。

[0065] 通信接口255还在工作上连接至处理器210。通信接口255可以是使能系统服务器105与外部装置、机器和/或元件之间的通信的任何接口。在特定实现中，通信接口255包括但不限于调制解调器、网络接口卡(NIC)、集成网络接口、射频发射/接收器(例如，蓝牙、蜂窝、NFC)、卫星通信发射/接收器、红外端口、USB连接和/或用于将计算装置205连接至其他

计算装置和/或诸如专用网络和互联网的通信网络的任何其它这样的接口。这样的连接可以包括有线连接或无线连接(例如,使用802.11标准),虽然应当理解的是,通信接口255可以实际上是使能至处理器210的通信或来自处理器210的通信的任何接口。

[0066] 将参照如下面描述的用于认证用户的方法、结合图3至图4并接着参照图1和图2A至图2C、图5A至图5C进一步理解上述的用于授权访问车辆和各个元素和组件的系统的操作。

[0067] 图3和图4中示出的过程是从车载计算机101b和系统服务器105的角度描述的,但应理解,可使用移动装置101a或上述的任意组合整体或部分类似地执行这些过程。

[0068] 图3是示出用系统100注册用户124的例程400的流程图。注册过程验证用户的身份以确保用户的身份是真实的。注册还指定了在认证过程中用户124和/或用于认证用户的用户装置(例如,车载计算机101b和/或车载装置101b)被系统服务器105识别的方式。此外,注册可以创建将用户124与用户装置(例如,用户的移动装置101a和/或车载计算机101b)以及与用户的交易帐户(即,车辆的访问和车辆管理帐户,诸如On-Star®、或由远程计算装置102保持的车队车辆管理服务)中的一个或更多个相关联的用户简档。注册还包括捕捉(例如,读取)用户的生物特征、产生表征那些特征的一个或更多个生物特征标识符以及确定用户的活性。如本文进一步描述的,可执行这些步骤以用于验证并且为未来验证会话创建基线。因此,可以理解,关于图3讨论的许多步骤可以在关于图4讨论的随后的用户认证会话期间执行。

[0069] 该过程开始于步骤305,其中在车载计算机101b与系统服务器105之间创建初始通信会话。在一些实现中,可以使用在单向SSL通信上建立的双向安全套接层(SSL)来建立车载计算机与系统服务器之间的通信。更具体地,通过执行优选地包括通信模块182和注册模块176的一个或更多个软件而被配置的处理器110可向系统服务器105发送API调用并与系统服务器105建立单向SSL通信会话以便加密通信。API调用还可以包括专用双向SSL密钥以建立双向SSL安全通信环境。在一些实现中,车载计算机可以发送对车载计算机的客户端应用程序而言唯一的预加载双向SSL证书和API密钥。预加载证书和密钥可以是当客户端应用程序被存储至存储器中时存储的单次使用的实例。

[0070] 然后,在步骤310,车载计算机101b收集用户标识信息。更具体地,通过执行优选地包括注册模块176和用户界面模块170的一个或更多个软件模块130而被配置的处理器110可以提示用户输入用户标识信息,并通过用户接口115接收用户输入。用户标识信息可以包括关于用户身份(例如,姓名、地址、社会保险号等)的信息。例如,如图6A所示,车载装置显示器600可以提示用户输入关于用户身份610的这样的个人信息。在一些实现中,一些或全部的信息可以从车载计算机101b的存储器自动地收集或从另一计算装置自动地收集。例如,用户信息可以从如移动装置101a的另一登记的用户设备提供,或自动从与由系统服务器105或远程计算设备102维护的用户相关联的现有用户信息得到。

[0071] 此外,用户标识信息可以包括关于一个或更多个交易帐户的信息,用户可借此访问车辆或与车辆进行交互,如本文进一步描述的。例如,用户可以输入与用户的各种交易帐户相关联的预先存在的登录和密码615。在一些实现中,在根据用户提供的用户标识信息验证用户的身份之后,配置的处理器和/或系统服务器105可以直接从与交易帐户相关联的企业组织和/或ACE自动地获取这样的信息的一些或全部。

[0072] 然后，在步骤315，收集装置标识信息。装置标识信息可以包括但不限于DeviceID、AndroidID、IMEI、CPU序列号、GPU序列号以及对车载计算机101b而言唯一的其它此类标识符中的至少一部分。更具体地，通过执行优选地包括注册模块176的一个或更多个软件模块130而被配置的处理器110可查询车载计算机101b的各种硬件和软件组件以获得相应的装置标识信息。

[0073] 然后，在步骤320，验证用户身份。身份验证提供了额外的安全性，并事实上确定用户124的真实性。应当理解，可以由系统服务器105、车载计算机101b或前述的组合来执行用户身份的验证。

[0074] 应当理解，根据安全认证系统100的特定实现所指定的安全级别，身份验证的严格性可以改变。例如，用户登录至在线论坛/讨论板可能仅要求用户身份的宽松验证，而其中所公开的系统和方法被用于验证金融交易的的应用可能需要严格的身份验证。

[0075] 然后，在步骤325，如果验证了用户身份，则可以生成和存储用户简档。用户简档可以包括一个或更多个用户标识信息和装置标识信息。此外，用户简档可包括关于用户的交易帐户中的一个或更多个以及可用于根据用户的偏好来指导系统100的操作设置的信息。

[0076] 在一些实现中，系统服务器105可以生成用户的唯一标识符(“用户Id”)和关联的装置标识符(“移动装置Id”)，并且将所述标识符存储在群集的持久环境(clustered persistent environment)中以便创建用户的简档。可使用一个或更多个用户标识信息和装置标识信息分别生成用户Id和移动装置Id。应当理解，附加的用户标识信息和装置标识信息也可以被存储以创建用户简档或与用户简档相关联地存储。

[0077] 此外，userId和关联的mobileId可以与关于在步骤315描述的一个或更多个交易帐户的信息相关联地存储。在一些实现中，特定的交易帐户信息可以存储在系统服务器105上，从而使系统服务器代表用户和企业组织授权所请求的交易的全部或部分。附加地或另选地，使用例如标识符(例如，站点ID或全球唯一标识符等)或至存储敏感的交易帐户信息的安全数据存储部(如由企业组织操作的远程计算装置102)的其它这样的指针，用户简档可以与交易帐户相关联。因此，不需要系统服务器105存储敏感的交易帐户信息，并且，如本文进一步描述的，系统服务器105可以生成和/或转发请求以授权用户至适合的企业组织以进一步处理。附加地或另选地，系统服务器可以查询安全数据存储部以收集用于处理任何这样的请求的必要的信息。

[0078] 此时，可以理解，userId可用于将用户简档映射至用户的传统交易帐户。此外，mobileId将装置与用户简档绑定。在一些实现中，userId是约定，而mobileId是强制性的，因为mobileId可独自将用户124和车载计算机101b对链接至由系统服务器105所保持的用户简档和/或用户交易帐户。此外，包含在用户简档中的任何附加信息可以在未来的授权请求中被系统服务器105用于不可抵赖或溯源的目的。

[0079] 可以理解，用户简档可以由系统服务器105和/或车载计算机101b创建。此外，用户简档的一个或更多个实例可存储在各种装置(例如，系统服务器105、移动装置101a、远程计算装置102或用户计算装置101b)上。此外，包括在用户简档的各种实例中的信息可以从装置到装置不同。例如，存储在车载计算机101b上的用户简档的一个实例可包括userID、mobileID、用户标识信息和关于用户的交易帐户的敏感信息(如帐号等)。作为另一实例，由系统服务器105存储的用户简档的实例可以包括userID、mobileID、指派给用户的其它唯一

标识符和标识用户的交易帐户的信息，但不包括敏感的帐户信息。

[0080] 在一些实现中，由系统服务器105生成用户简档还可以包括生成私钥(private key)。在一些实现中，私钥可以是唯一的双向SSL证书。该密钥可由系统服务器105生成，或附加地或可选地，由车载计算机101b生成。在一些实现中，可以使用用户标识信息(可以包括关于用户的交易帐户的信息)以及装置标识信息中的一个或更多个来产生密钥。在由系统服务器105产生私钥的情况下，所生成的私钥也可被发送回车载计算机101b以存储在装置中。因此，生成的密钥可用于结合身份认定会话的后续通信。

[0081] 例如，注册/成因(genesis)阶段可以通过将标识用户的信息(例如，userID、SSN、电子邮件或其他用户标识符)链接至通用名称(CN)在永久存储设备中建立注册用户的实例，这可以是特定的方式，其中，由系统服务器105和/或遗留交易帐户系统在双向安全套接字层密钥中的唯一地识别特定用户。因此，成因阶段也可以将与用户相关联的传统交易帐户(例如，用户的银行帐户)与由系统服务器105维护的用户身份链接。

[0082] 私钥(在系统服务器105和/或车载计算机101b或移动装置101a上生成)将特定的用户装置(例如，mobileID)和用户(例如，userID)对链接至将用于随后通信的用户身份(例如，用户标识符、通用名称等)。

[0083] 在一些实现中，如通过双向安全套接字层密钥认定的身份可被保持用于所有通信。这个密钥可以利用仅在注册期间使用的装置(在此示例中，车载计算机101b)知道的密码来编码。此外，该密钥被可编程地置于车载计算机101b上的密钥存储部中。它是允许身份和至成因阶段的链接的唯一机制。优选地，没有人或装置知道用于加密双向SSL密钥的密码。因此，车载计算机101b使用私钥在随后的通信中具有提供的身份。可以理解，与用户相关联的每个使能装置可以具有唯一的密钥，该密钥可被链接至同一用户简档，使能以相同的方式使用例如移动装置101a和车载计算机101b的多个装置。附加地或另选地，单独的用户简档可以针对每个用户装置对独立地或以链接的方式建立和保持。还可以理解，类似地，多个用户可以使用对应于单个用户简档或联合用户简档或以其它方式链接的用户简档的相同的(多个)装置。例如，特定的车辆可以被任何数目的被批准的用户共享，因此，在各自的成因阶段，与车辆关联的车载计算机101b可以被链接至每个被批准的用户。如在本文中进一步描述的，访问-控制和管理可以限定用户和相关的角色和关于相应用户对车辆的访问的规则的层次结构(例如，访问单独由车载计算机101b或结合诸如系统服务器105和远程计算装置102的一个或更多个远程装置监测/控制的特征/功能)。

[0084] 因此，作为成因/注册的结果，创建用户简档，用户简档将用户124与用户的注册装置相关联。此外，成因用于向机载计算机101b提供用于在与系统服务器105的后续通信(如用于认证和/或授权用户的身份认定会话)中标识用户124和/或车载计算机101b的信息(例如，唯一的用户标识符和装置标识符和/或唯一的密钥)。

[0085] 此外，注册可以将用户简档链接至车辆的一个或更多个存储记录和与车辆和/或用户相关联的交易帐户。因此，存储的车辆记录或车辆简档可以链接至相关联的车辆管理帐户/服务以及一个或更多个注册用户。例如，被授权配置与车辆使用相关的设置的车辆的所有者授权车辆的操作者等。

[0086] 可以理解，服务器可以以计算机可读存储介质中保持的服务器索引来管理这样的信息的存储。索引可以包括用于记录关于系统的用户的信息(例如，用户简档信息)的存货

条目。还可以创建包括关于车辆本身的信息(例如,与车载计算机关联的deviceID、车辆标识符、关联的管理帐户信息等)的存货条目。库存条目还可以包括关于涉及车辆的随后交易的信息,例如,用户访问的实例、关于车辆的使用的细节等。以这种方式,存货条目可以被更新或附加至之前的库存条目或者以其他方式在存储器中相关联/链接,从而创建索引,所述索引提供用于与系统和/或使用该系统访问车辆交互的各个用户的全面的审核跟踪引。此外,库存条目也可以反映由用户限定的、与汽车有关的访问规则和权限。例如,索引可以由系统服务器更新以反映授权用户简档与车辆之间的链接,并进一步反映与用户和/或车辆相关联的访问规则和权限。此外,当用户对车辆的访问被撤销或改变时,与该车辆和特定用户相关联的库存条目也可以从服务器索引擦除或以其他方式修改以反映访问的撤销/更新。

[0087] 然后,在步骤330,接收用户设置。设置包括由用户为引导系统100的操作而限定的的偏好和规则。在一些实现中,在注册过程期间或在其后的任何点处,车载计算机101b(或其它注册的用户计算装置)可提示用户输入设置和将那些设置与用户简档和/或车辆简档关联起来。这些设置可由机载计算机或系统服务器105或前述的组合存储。

[0088] 在一些实现中,用户输入设置可以指定使用系统授权用户的优选情况。例如,用户希望仅在早晨访问车辆之前被生物特征认证,而不是在一天当中访问车辆之后被重新验证。相似地,设置可以指定在授权用户访问车辆后自动执行的某些特征和功能。相似地,设置可以限定关于用户使用系统希望访问的各种访问受控的环境的偏好。例如,设置可以识别用户希望在被提供对车辆的访问之后使用系统100自动访问的特定订阅服务。在一些实现中,设置可以指定用户为了获得访问其它访问受控的环境中而期望进行认证的情况。

[0089] 在一些实现中,用户设置可包括用户限定的访问规则,所述指定控制一个或更多个其他用户对车辆的访问。例如,车主可以限定关于车主的孩子访问和使用的规则。作为另一示例,车队的经理可以限定哪个用户访问车队中的哪个车辆并提供使用限制和与车辆的使用相关的其它这样的规则。用户设置还可以包括隐私设置,隐私设置管理如何存储和/或共享与各种用户、用户的活动和车辆的使用相关联的信息。例如,设置可以识别有权访问由该系统收集的信息的其它装置、注册用户或企业组织以及访问信息的条款。

[0090] 在一些实现中,用户设置可指定在利用车辆时与其它访问受控环境进行交易的偏好。例如但没有限制,用户可以指定默认的支付方法/帐户,从而配置车载计算机101b和/或系统服务器105以在用户驾驶车辆时有效地处理交易。此外,用户可以将支付方法与指定的商家相关联。作为另一示例,用户可以指定控制车辆的使用的规则,比如,使系统服务器105防止在使用车辆的同时进行特定类型的交易,导致通知被提供至车主或执行附加的安全措施以确保被批准的帐户使用。

[0091] 应当理解,描述的设置都呈现为非限制性示例,并且如本文中进一步描述的,各种各样的设置可以用于控制系统的操作和用户如何与系统进行交互。

[0092] 还应理解,在注册期间和其后的任何时间以及当使用向系统注册的任何用户装置时(例如,移动装置101a和车载计算机101b),用户可以调整关于用于与系统100进行交互的用户的偏好的设置。例如,装置可接收来自用户的附加的用户标识信息、密码、交易帐户信息等以用于在移动装置101a上、系统服务器105上、车载计算机101b中或前述的组合上的本地存储。这样,系统100的任何计算装置可以被配置为充当用于通过使用这样的交易帐户自

动地帮助访问ACE并将用户的信息提供给各种使能的计算装置(例如,移动装置101a、用户计算装置101b、远程计算装置102)以提供访问的平台。

[0093] 然后,在步骤335,使用车载计算机101b捕捉用户的生物特征。在一些实现中,通过执行优选地包括注册模块176、分析模块174、用户界面模块170和捕捉模块172的一个或更多个软件模块130而配置的处理器110使用联接至处理器110的摄像头145提示用户捕捉用户的虹膜/多个虹膜、眼睛、眼周区域、脸部和手指等的影像中的一个或更多个,并将一个或更多个图像存储至存储设备190或存储器120。

[0094] 然后,在步骤340,从捕捉的生物特征信息生成一个或更多个生物特征标识符并存储以完成注册阶段。更具体地,通过执行优选地包括捕捉模块172、数据库模块178、分析模块174的一个或更多个软件模块130而配置的处理器110可以分析由摄像头捕捉的生物特征信息并产生生物特征标识符。

[0095] 在一些实现中,生物特征标识符可以与用户简档相关联地本地存储在车载计算机101b上,使得移动装置可以根据生物特征标识符进行生物特征认证。附加地或另选地,生物特征标识符可以与用户简档相关联地存储在远程计算装置上(例如,系统服务器105或远程计算装置102),使得那些设备能够进行用户的生物特征认证。

[0096] 在步骤345,通过执行优选地包括捕捉模块172的一个或更多个软件模块130而配置的处理器110还可接收基于非机器视觉的信息。基于非机器视觉的信息一般地涉及用户124在注册和后续认证会话以及与系统100的后续交互期间的、表明用户的偏好、身份以及用户的活性的行为特性。例如但没有限制,基于非机器视觉的信息可以包括从车载时钟接收到的时间、从GPS装置接收到的位置、根据影像和其它车载接近测量装置计算的在图像捕捉期间摄像头距用户脸部多远定位、从加速度计接收到的装置的方向和装置的加速度、由RF检测器检测到的RF辐射、重力磁力计检测地球磁场以确定装置被保持的三维取向、光传感器测量光强度等级等。

[0097] 在一些实现中,随时间变化接收基于非机器视觉的信息并存储,使得配置的处理器可通过应用如本领域的技术人员理解的行为算法来确定信息中的模式,所述模式对于用户124是唯一的。因此,在随后的认证阶段,可以分析所收集的当前的基于非计算机视觉的数据并且将其与用户的建立的行为特性比较来验证用户的身份,并且确定该信息是否表明活性。例如,基于时间和位置的行为模式可以随时间变化被识别并且当前位置与模式比较以确定是否呈现任何异常行为。作为另一示例,还可以相似地比较装置从用户的脸部的取向和离用户的脸部的距离。作为另一示例,在注册期间可以建立用户的RF辐射签名并且可以将RF辐射签名与未来测量结果进行比较以识别异常的RF辐射水平(例如,建议使用视频屏幕来欺骗系统)。如在用户与装置交互(例如,当使用注册装置或访问车辆时)的过程中从一个或更多个其它注册的用户装置收集或记录的用户信息那样,使用装置测量的基于非机器视觉的信息还可以用于确定关于用户使用系统的行为特性和偏好。

[0098] 在步骤350,通过执行优选地包括分析模块174的一个或更多个软件模块130而配置的处理器110可确定用户的活性。确定活性可包括产生表征所捕捉的用户的生物特征的一个或更多个活性标识符和/或表明用户的活性的基于非机器视觉的信息。如上所述,确定活性是可以在注册和后续认证会话期间执行的反欺骗措施,以确保由成像装置捕捉到的图像序列属于有生命的主体,而不是用户的视觉表示(例如,高分辨率视频)。在一些实现中,

通过检测生物特征的移动来确定活性，因为每次用户注册或确认，用户实际上将稍微移动，无论他/她试图多么稳定。

[0099] 然后，在步骤355，存储一个或更多个生物特征标识符和/或活性信息或行为信息。在一些实现中，通过执行优选地包括注册模块176和数据库模块178的一个或更多个软件模块130而配置的处理器110可以本地地存储生物特征标识符，以便在车载计算机101a上进行生物特征认证，从而避免将敏感的生物特征信息发送至系统服务器105以存储。

[0100] 在一些实现中，配置的处理器可以向系统服务器105发送生物特征标识符、活性标识符和在注册期间和其后产生/捕捉的其它信息作为一个或更多个数据包。应当理解，附加的用户特定信息和移动装置特定信息(例如，用户标识信息或身份认定密钥)也可以被发送至系统服务器以便将用户信息与特定用户相关联。

[0101] 应当理解，使用例如移动装置101a的其它用户装置，可以重复一些或全部注册过程步骤。例如，用户可以利用与系统100结合使用的其它用户装置来注册，从而使能使用多个注册用户装置来进行用户认证、授权和与系统100的交互。

[0102] 现在转至图4，图4是示出根据本文公开的至少一个实施方式的用于授权用户访问车辆的例程400的流程图。

[0103] 该过程开始于步骤405，其中，提示车载计算机101b认证用户124。在一些实现中，通过接收用户输入来提示车载计算机进行认证。例如，如图5C所示，车辆可以包括用户接口，所述用户接口通信地联接至处理器110并且用户可从车辆外部访问该用户接口(例如，在汽车外部上的按钮115a)。因此，经由按钮的用户输入可以使处理器110发起认证过程。在一些实现中，车载计算机101b可以自动地开始认证过程(例如，没有主动的用户输入)。例如，使用关联的接近传感器，处理器可以被配置为检测用户何时接近车辆的驾驶员侧或站在车辆附近并且响应于该检测而开始认证。

[0104] 在一些实现中，车载计算机101b可以接收来自另一计算装置(例如系统服务器105)的用户认证请求。例如，系统服务器可以响应于接收到来自远程计算装置的认证请求而发起认证过程。优选地，授权请求包括标识特定车辆的访问控制信息，从而使能系统服务器105使适当的车载计算机101b开始用户认证。作为另一示例并且没有限制，系统服务器可以直接从用于帮助用户对车辆的访问和与车辆的使用相关的其它服务(例如，控制电子车辆门锁的车辆访问管理系统、车辆操作特征或以其它方式经由车载计算机101b和其它注册的用户计算装置向用户提供订阅服务)的远程计算装置102接收认证请求。作为另一示例，注册的用户移动装置101a可以通过向系统服务器105或直接地向车载计算机发送请求而发起认证。更具体地，移动装置101a可被配置为提供用户被授权访问的装置/ACE(例如，车辆)的列表，使得用户可以选择特定的车辆。作为响应，移动装置可以通过向车载计算机101b直接发送请求或经由系统服务器105或远程计算装置102间接地发送请求来发起认证。

[0105] 然后，在步骤410，通过执行包括认证模块180、用户界面模块170、分析模块174和捕捉模块172的一个或更多个软件模块而配置的处理器110捕捉用户的当前生物特征信息。另外，配置的处理器还可以为了认证和活性检测的目的而捕捉基于当前非机器视觉的信息。如关于图3描述的，可以通过装置进行这样的信息的捕捉。

[0106] 例如，如关于图3描述的，然后在步骤415，通过执行包括认证模块180和分析模块174的一个或更多个软件模块而配置的处理器110生成一个或更多个当前生物特征标识符。

[0107] 然后，在步骤420，根据一个或更多个当前生物特征标识符，用户被生物特征认证。使用当前生物特征标识符，可以通过将生物特征标识符与之前在注册过程或后续认证会话期间生成的一个或更多个存储的生物特征标识符进行比较来认证用户的身份。

[0108] 此外，在步骤425，可以通过验证用户的活性进一步认证用户。在一些实现中，可以通过将至少当前的活性信息与之前生成的活性信息进行比较并且确定活性信息是否匹配到必要的程度来确定用户的活性。如上所述，验证用户的活性还可以包括分析所捕捉的生物特征和非机器视觉信息和/或活性标识符以确定它们是否在所指定的确定程度上呈现有生命的主体的特征。

[0109] 然后，在步骤440，系统服务器105授权用户。授权可以包括验证已经使用注册的车载计算机101b生物特征认证的注册用户正尝试访问车辆。

[0110] 在一些实现中，通过执行优选地包括认证模块180和通信模块182的一个或更多个软件模块130而被配置的处理器110可以生成至少一个认证请求并且向系统服务器105发送该认证请求。例如并且没有限制，交易请求可以包括：标识用户的信息(例如，用户标识信息或在认证或注册过程中生成的用户标识符)；标识车载计算机101b的信息(例如，deviceID或在装置注册期间生成的标识符)；表明用户是否被生物特征认证的信息。该请求还可以包括与用户正在尝试访问的车辆相关的访问信息。访问信息可以包括用于车辆的标识符，通过该标识符，系统服务器可以识别被访问的车辆。可以根据发送标识车载计算机101b的信息固有地提供标识符，然而，也可以单独地提供标识符，例如，在用户正在使用移动装置101a请求访问车辆的情况下。访问信息还可包括请求的访问的性质。换言之，涉及车辆并且用户期望执行的操作或功能(例如，将车门解锁、发动汽车、调节温度或其它车辆设置、访问卫星电台、联系On-star服务、在驾驶汽车时点餐并买单)修改控制车辆被如何使用和被谁使用的访问规则和权限。

[0111] 在一些实现中，交易请求可以包括在注册过程中生成的并且在车载计算机101b与系统服务器105之间建立双向SSL安全通信会话的专用双向SSL密钥。该密钥可以包括标识用户和装置的信息，例如，用户标识符和移动装置标识符。附加地或另选地，密钥可以包括可用于标识用户-移动装置对的信息。应当理解，交易请求和/或在交易请求中包括的信息可以被发送为一些单独的发送。同样地，可以通过移动装置101a、或系统服务器105、或远程计算装置102、或前述的组合以任何数目的步骤来执行如在步骤445处进一步描述请求的处理。

[0112] 响应于交易请求的接收，使用通过执行一个或更多个软件模块130而配置的处理器210，系统服务器105可以处理交易请求以确认用户认证有效，并且附加地或另选地，授权用户访问车辆。例如，系统服务器可以将在交易请求中标识的用户与用户简档的数据库交叉参照以确定用户是否与用户简档相关联并因此在系统100中注册。同样地，系统服务器可以确定正由用户使用以认证的装置是否与用户简档相关联。在一些实现中，可以这样来授权用户，即，通过将接收到的密钥和与相应的用户简档相关联存储的一个或更多个密钥进行比较来识别匹配，从而验证通过密钥识别的用户和/或车载计算机对应于在数据库中存储的用户简档。

[0113] 此外，授权用户的步骤还可以包括由系统服务器确定授权请求是否表明用户已使用用户装置被生物特征认证(例如，移动装置101a或车载计算机101b等)。在一些实现中，验

证生物特征认证可以包括确定交易请求是否符合预定配置。例如，车载计算机可被配置为一旦生物特征认证成功就访问在用户的注册期间使用特定车载计算机101b生成的身份认定密钥。因此，车载计算机可被配置为仅在用户的生物特征认证成功后生成包括密钥的交易请求。此外，向系统服务器105发送包括密钥的交易请求可以提供用户已使用车载计算机被生物特征认证的确认。作为另一示例，交易请求可以包括表明用户已被生物特征认证的附加的指针、标记、会话信息等并且还可以向发送的真实性提供附加的安全性。

[0114] 类似地，应当理解，在用户认证和后续通信期间的去往和来自各种计算装置(例如，移动装置101a、用户计算装置101b、系统服务器105和远程计算装置102)的所有发送可以被加时间戳并且是时间敏感的和/或包含会话信息。这样，根据在预定持续时间内发生的认证或从各个数据包被发送至系统服务器的时间戳开始的“生存时间”内发生的认证，授权过程还可以是视情况而定的。在畸形或MITM(中间人)型攻击的情况下(其中，数据包被重新设计)，生存时间提供了额外的安全性，这是由于在TTL被设置成的时间量内用正确数据重建新数据包是有困难的。

[0115] 授权还可以包括由系统服务器105确定用户是否有所请求的“访问”车辆的权限(即，执行与车辆相关的一个或更多个操作或“交易”)。优选地，在用户授权过程中，系统服务器105接收标识车辆的访问信息。例如，在车载计算机101b自动发起认证并在授权请求中提供标识车载计算机的信息的情景中，系统服务器105可以识别与所标识的车载计算机关联的特定车辆简档。作为另一示例，在移动装置101a被用于访问车辆的情景中，系统服务器可以接收车辆标识符并因此在存储装置中识别适当的车辆记录。

[0116] 此外，基于识别的车辆以及通过授权请求识别的用户，系统服务器105可以确定用户是否具有必要的权限来访问车辆。例如，系统服务器可以查询链接至用户简档和车辆简档的一个或更多个访问规则和权限，并基于访问规则来确定请求用户是否被授权访问车辆。

[0117] 如前面指出的，在一些实现中，由系统服务器105接收到的授权请求可以包括描述所请求的用户访问的性质的访问信息。因此，系统服务器105的用户授权可以包括进一步确定该用户是否具有必要的权限来执行特定操作。更具体地，系统服务器105可以查询一个或更多个限定的数据存储部以收集控制对特定车辆的访问的任何访问规则(例如，访问权限、角色、设置等)。系统服务器还可以确定访问规则/权限中的任一个是否涉及特定用户简档。基于这样收集的访问规则，系统服务器可以确定用户是否被授权执行请求交易中提供的特定交易/操作。

[0118] 然后，在步骤445，根据用户是否在步骤440处被授权而生成授权通知。在一些实现中，系统服务器105可以直接向与用户正在请求访问的车辆相关联的车载计算机101b发送授权通知。在一些实现中，可以经由一个或更多个其它计算装置间接发送授权通知。例如，认证通知可以被发送至被用户使用以访问车辆的移动装置101a。作为另一示例，授权通知可被发送至控制对车辆的访问并因此需要用户授权(例如，联网计算装置与车载计算机101b一起控制提供对车辆的访问的电子门锁，或者向车辆提供订阅服务，例如，经由车载装置提供音乐服务，因此在提供此类服务之前需要用户授权)的远程计算装置102。作为另一示例，授权通知可以被发送至正在由用户使用以尝试获得对车辆的访问的移动装置101a或用户计算装置101b。基于授权通知，接收到授权通知的远程计算装置可以帮助访问用户和/

或进一步授权用户访问车辆和/或处理请求的交易。

[0119] 授权通知的实质和形式可以取决于系统100的特定实现而变化。在一些实现中，发送至远程车辆管理系统的通知(例如，计算装置102)可以标识用户并表明用户已被生物特征认证和/或还被授权。远程装置可以授权用户并且向车载计算机101b发送指令以通过例如将车门解锁或以其它方式执行授权的操作来提供访问。类似地，系统服务器可以被配置为发送这样的指令以向车载计算机直接提供访问。

[0120] 附加地和另选地，通知可以包括关于一个或更多个交易帐户的信息，例如，用户的登录和密码信息或可用来获得对访问受控环境的访问的一次性密码。因此，车载计算机可利用接收到的信息来提供所请求的使用接收到的帐户信息的访问。在其它实例中，例如，当用户尝试在操作车辆的同时完成金融交易时，通知可被直接发送至第三方支付处理器(例如，计算装置102)以完成交易。

[0121] 在车辆的用户/车主请求更新访问规则以允许朋友驾驶该车辆的情况下，在授权车主并且识别与朋友相关联的用户简档后，系统服务器可以修改相应的索引项以反映该朋友被允许使用车辆。结果，系统服务器可以向车主的计算装置提供授权通知，确认对访问规则的更改。此外，系统服务器可以向朋友注册的计算装置发送通知，告知朋友更新的的权限并提供相关信息。在一些实现中，该朋友此后可以使用该朋友的移动装置请求访问车辆。在系统服务器对朋友授权之后，指令可发送至车载计算装置以提供访问。附加地或另选地，向朋友的移动装置提供的通知还可以包括可用于访问车辆的电子密钥。例如，通过向车载计算装置发送密钥。电子密钥可以是例如由系统服务器生成的并且链接至朋友的用户简档和车辆简档的一次性授权密钥。该密钥可以被同样在密钥生成期间由系统服务器生成和存储的唯一密码来保护/加密。因此，在系统服务器向朋友的移动装置提供密码之后(只有在朋友的生物特征认证和授权成功之后发生)，该密钥只能由朋友使用。

[0122] 如被本领域的计算人员所理解的，用于授权访问车辆的系统和方法不以任何方式限于示出的实施方式和/或布置，因为描述的示出的实施方式和/或布置仅仅是本文中公开的示例性系统和方法，其可以以各种形式呈现。一些另选的实施方式、布置和示例性的应用包括下面的示例性实施方式。

[0123] 如前指出的，本文公开的系统和方法提供基础设施以配置能够知道车主的汽车。更具体地，车载计算机101b可以通过名称和脸部来识别车主。此外，通过在使用车辆的同时监控对车辆的访问和用户活动，车载计算机可以学习用户的习惯，例如，车主希望做的事情、车主希望去的地方。机器学习可以通过将车载计算机与其它用户装置和联网的系统和与用户相关联的服务集成而被进一步了解情况。因此，通过机器学习，用于授权用户对车辆的访问的系统还可以提供附加的援助和服务以在用户的日常生活中帮助用户。此外，本文中公开的系统和方法以及示例性架构被进一步配置以在操作期间确保车载计算机101b与其它邻近和远程的计算装置之间的安全通信。

[0124] 此外，使用在汽车内和汽车外的各种策略性地放置的摄像头，示例性系统和方法可以将车主与车辆以及联接至车载计算机的其它计算装置链接起来。本文中进一步描述的是用于提供对车辆的认证访问的公开的系统和方法的一些示例性用途和配置。在这个示例中，通过机器学习，用户“乔”的车(即，车载计算机101b)知道他的习惯、他喜欢去哪、他喜欢吃什么以及他喜欢听什么，总之，知道是乔。这使用在他的智能电话上执行并监控的系统应

用“app”(该系统应用“app”将智能电话配置成进行生物特征认证),并通过将智能手机与他的汽车的车载计算机上的app的相似实现的集成来提供。

[0125] 例如,乔激活他的Android或iPhone并启动系统应用。该应用将发起并提示他进行认证以便访问。例如,可听地宣布“欢迎光临,请认证以便访问”,并且如前所述,响应乔在他的智能电话上的一瞥,生物特征认证乔。在认证后,该装置可以报告认证,例如,通过扬声器宣布“认证通过...欢迎乔回来。在认证后,该应用配置该装置以提供各种可行的选择,例如,诸如发动他的汽车的车辆相关活动,或诸如选择他的日常事务等的与他的一天相关的活动。响应于“发动汽车”和“设置温度至70F”的选择,智能电话将所选择的操作中继给系统服务器105,系统服务器105可以例如基于与乔和他的汽车相关联的访问规则进一步授权请求的操作。在授权访问后,从车载计算机和关联的传感器接收到的关于车辆状态的信息也可以通过乔的智能手机提供给乔。例如,在应用界面上闪烁的黄光可以表明油位并且基于一个或更多个规则提供警告“没油了”。在此类警告的情况下,该系统可以提示乔采取一个或更多个动作,例如,“添加加油站至你的路线”。通过选择此类动作,该系统可以被配置为使用一个或更多个地图服务,在到他的下一约会(从他的日历来确定)的路线上并根据他的当前位置自动选择最近的加油站。在乔物理地接近车门时,车载计算机可以使用关联的面向外的摄像头(例如图5C的摄像头145a)识别、认证和授权乔的物理访问,并且自动将车门解锁。此外,使用在方向盘后面的仪表盘中的另一摄像头捕捉的影像(例如,图5A的摄像头145b),车载计算机可以检测乔何时在驾驶员的座位中坐下。

[0126] 在生物特征检测到乔已坐下后,车载计算机也可以被配置为基于与乔的用户简档相关联的用户设置/偏好向乔提供信息和通知。例如,车载计算机可以从天气服务检索有关天气的信息并播报天气预报。作为另一示例,车载计算机可以与一个或更多个其他用户计算装置集成,例如,乔的智能电话检索语音消息并将消息下载至本地存储装置。相似地,车载计算机可以与一个或更多个企业帐户服务器(例如,电子邮件服务器)集成,并且基于用户简档设置预下载未读邮件。

[0127] 因此,在从乔接收到通过车载计算机使用关联的麦克风和语音识别软件检测到的播放语音邮件的口头指令后,不同于传统的语音邮件系统(用户必须按下号码来访问消息并处理繁琐的IVR),车载计算机基于存储的偏好已经将消息和其他这样的信息下载至内部的存储装置。因此,消息简单地开始播放。与其它装置和订阅服务集成还基于生物特征识别/授权的用户的偏好(诸如拨打电话呼叫、视频聊天会话、访问音乐库(基于本地和云二者)等)允许操作被无缝地进行。

[0128] 可以理解,用于生物特征识别和监控的系统和方法可以嵌入车辆的车载计算机中以及与其通信的使能的智能电话中(例如,经由无线通信)或前述的组合。因此,系统的分布的部件可以通过GSM/LTE无线数据网络连接起来。为了使汽车能够定位乔,优选地在汽车本身中内置有摄像头。摄像头可策略性地设置在驾驶员仪表盘中,不被看到。这些摄像头不贵,它们可以是较小的CMOS传感器,例如,分辨率为5至16兆像素的分辨率。其它摄像头可被放置在乘客位置,使得也可检测到乘客。

[0129] 此外,通过持续收集与用户相关的数据,可以进行机器学习算法、行为分析算法等以分析生物特征信息、使用汽车时的用户活动、关联的装置上的车辆数据和用户活动,以识别用户的独特特征。这些可以包括独特生物特征、用户的行为、习惯等的特征、以及周围环

境的特征。因此，提供生物特征访问的系统可以识别用户并且“学习”可被记录在存储器中(例如，与用户简档相关联)的并且可以自动指导系统的操作的特征，从而改善系统的操作并向用户提供独特定制的体验和服务。

[0130] 乔可以在他的系统应用中“注册”他的整个家庭，并且限定与他自己和汽车的其他注册用户/乘客相关的各种设置，例如，设置他们的年龄。还可以通过车辆的车主(即，管理员)限定和/或预限定与各个注册用户相关的访问规则/权限。因此，系统可以基于简档和规则/权限来确定当汽车行进时，只有6岁的莎莉不应该被允许坐在前座中，并且可以限制由用户中的一个或更多个对车辆的操作直到规则被遵守。可以使用系统监控和执行与其它类似的安全相关的注意事项。

[0131] 正如指出的，其它摄像头可位于汽车外侧、在门框本身中。当车载计算机使用这些摄像头检测到乔走近汽车时，车门可以自动解锁并且车载计算机可以根据用户简档中提供的设置自动调整各种车辆相关的设置，如温度、座椅设置等。

[0132] 公开的实施方式还提供车主可以用于共享对车辆的访问的基础设施。例如，如果车主想将车辆借给朋友。该朋友可以在他的移动装置上下载系统应用并登记。车主可以定义这样的设置，该设置识别朋友和车辆，提示系统服务器105产生加密的密钥并发送该加密的密钥至朋友的移动装置，该密钥只能通过使用他的移动装置进行生物特征认证来使用。此外，车主可以设置访客驾驶员为了访问和使用汽车被要求遵循的参数。

[0133] 针对其他用户的车主定义的访问规则可以包括地理围栏(geo-fencing)和安全增强。例如，乔可为他18岁的儿子比利的汽车使用定义约束，例如，汽车决不能超过55英里每小时，并且比利不被允许与朋友们一起开车，或者外出至距离乔的家以5英里为半径之外。这些和许多其它参数可以由车主限定并且由系统记录并执行。与参数相关的条件可以基于比利的生物特征认证和授权以及从提供比利被准予访问(例如，使用)汽车时的使用信息的车载传感器接收到的信息自动地执行。例如，车载传感器可以识别乘客的数量并且当在汽车内检测到乘客时防止比利驾驶车辆或向乔报告访问规则被违反。

[0134] 在用户尝试访问车辆并且授权的访问未被准予的情况下(例如，如果与特定用户和车辆相关联的访问规则不允许请求的访问时(例如，车辆超出了地理围栏，或太晚而不能驾驶车辆))，车主或管理员可以被通知授权尝试和关于用户和车辆的信息。例如，由车载计算机捕捉的用户的脸部图片、用户的名字(如果知道)、车辆的位置等可以被包括在通知中。此外，车主可以被提示对请求的访问表示同意。例如，车主的注册的智能电话可以提示车主接受/拒绝用户是否被授权访问并通过生物特征认证确认选择。经授权确认，系统服务器可以指示车载计算机提供访问。

[0135] 本文中公开的系统和方法还提供与驾驶员意识相关的附加特征。示例性生物特征监控使能的车载计算机系统还可以被配置为捕捉用户的生物特征信息、分析生物特征信息以检测用户的身体状况，例如，当驾驶员或乘客生病、困倦、或醉酒时。并入的生物特征认证系统和方法还可以检测一个或更多个驾驶员和乘客的呼吸率和心率。相似地，使用各种摄像头类型的视觉影像可以检测汽车中的乘客人数。生物特征监控信息还可用于根据预限定设置为用户、车主和和其它监控服务以及车辆的控制操作产生各种健康和安全相关的提醒。在使用车辆期间，由车载计算机收集的信息可以被本地存储和/或被存储在诸如系统服务器的远程装置上。

[0136] 更具体地，热红IR摄像头可用于捕捉车辆的一个或更多个乘客的热影像。使用热影像，车载装置处理器可以检测核心体温。因此，车载计算机可相应地调整车辆的内部温度以补偿升高的温度。此外，热影像可以用作用于检测诸如疾病的物理条件(例如，高体温)的基础。它还可以被用于检测车辆中的乘客人数。

[0137] 可见光或NIR和IR摄像头可以用于监控瞳孔放大，例如，以检测驾驶员的改变的状态/醉酒。相似地，从这样的影像检测脸部特征还可以检测驾驶员的眼睛闭合，其可以被计算装置解释为困倦的生物特征证据。例如，车载计算机可被配置为分析由内部摄像头捕捉的图像序列以识别在图像序列中捕捉到的脸部表情。例如，用于检测眼睛闭合的方法可包括识别特征(例如，图像中示出的一只或双只眼睛、眼睑、眉毛)并且然后可以检测和分析图像的序列之间的转换，因为它们涉及界标的位置/取向。使用任何检测到的转变，计算机可以通过将检测到的转变与和将被检测的用户的脸部表情相关联的独特的标志性转变进行比较来检测的脸部表情，诸如眨眼、延长的眨眼等。可以类似地检测和分析脸部表情和肢体移动。

[0138] 还可以使用可见光、NIR或IR成像装置检测用户脉搏和/或呼吸率。鉴于每个已知乘客的基线读数或其它预期的特征，可以捕捉和分析驾驶员或其它识别的乘客的这些和其它测量的生物特性和生命体征以检测身体状况、情绪和异常行为。车载计算机检测到异常状况可以提示系统自动生成提醒或执行增强车辆乘客的体验或实现安全防范措施的其他动作。

[0139] 作为另一示例，所公开的监控和访问控制系统可以被配置为确保没有孩子(或生物)被留在汽车中。更具体地，内置(如在后视镜上)的一个或更多个摄像头(常规或热成像)可以收集影像。影像可以由车载计算机进行分析以检测车辆中的乘客的存在。此外，车载计算机可以被配置为主动识别乘客(例如，基于存储的信息识别儿童并确定年龄，或者把儿童、成人或动物(例如，基于大小和/或形状)进行区分)。预定义的规则或安全设置可以进一步指定在车辆停靠后没有成人的情况下儿童不应该被允许留在车中。相应地，车载计算装置可以检测到留在车辆中的儿童并采取响应动作，诸如防止车门关闭或锁定或拉响汽车警报直到儿童离开或向用户、车主或官方传送通知。

[0140] 鉴于由计算装置检测到的环境状况，还可以进行基于生物特征信息的安全监控。例如，从外部摄像头、位置传感器、接近传感器、加速度计、车载诊断(OBD)传感器等接收到的信息可用于检测交通拥堵。伴随诸如加快的脉搏、表明压力的脸部表情的异常的生物特征读数，车载计算机可以自动进行操作以缓解压力，诸如播放舒缓的音乐、向用户提供通知提醒用户保持冷静、重新设置车辆路线、自动调整用户的日程、相应地通知其他人等。

[0141] 监控系统还可以被配置为检测紧急情况的发生并采取相应的动作。例如，在检测到事故的发生后，车载计算机可以向系统服务器发送通知，提供关于乘员的实时信息，包括车辆乘客的数量、一个或更多个乘客的生命体征。相似地，车载计算机和/或系统服务器可以进一步向应急响应系统中继事故和实施车辆/乘客信息、或之前存储的关于车辆的使用的信息。

[0142] 此外，在车辆开动的同时车载计算机检测到表明紧急情况的驾驶员的生命体征的情况下(例如，心脏病发作、或司机昏迷不醒、进入睡眠状态)，车载计算机可以将车辆减速至停止，打开危险警示灯以及利用包括车辆的当前位置和与事件相关的信息的预先记录的

语音消息自动拨打预设号码或911。

[0143] 如前指出的，本文中公开的系统和方法还使用车载计算机或其它配置的用户装置以帮助交易。例如，车载计算装置可以自动识别用户正在加油的加油站(基于位置、或通过车载计算机从汽油泵接收到的标识符或唯一代码)，并且用户完成加油之后可使用与授权用户的简档相关联的支付帐户自动地进行汽油的支付交易。作为另一示例，比如乔正在开车并且想要购买食品。无需停车，拿出他的手机，找到就餐的位置，或者尝试访问在当今的汽车中常见的老式导航HMI接口。取而代之，乔可以简单地询问车载计算机最近的餐馆的位置。在使用地图服务定位餐馆后，可由车载计算机将路径点添加至路线。随着车辆继续访问餐馆的菜单并且为乔呈现菜单，乔可以选择一项。在选择结束后，车载计算机可以被配置为自动地进行支付交易以完成购买。这可以包括光学扫描他的脸部、生物特征方式授权乔、识别与乔的用户简档相关联的交易帐户(例如，他的谷歌钱包，亚马逊或PayPal帐户)并且利用餐馆在线订单处理系统处理订单和交易。乔在服务员完成他的订单的地方停车。服务员也在她的销售点终端上看到乔的照片(这被中继为交易的一部分)。

[0144] 根据公开的实施方式，示例性系统和方法被配置为进行下面表1中列举的动作：

[0145]

安全	安保	便捷
NOD（打盹检测）-当系统检测到眼睛闭合时，警报响起	保护你的 GPS 位置，尤其是你的家	OnStar 集成，使用用于生物特征监控的示例性系统和方法、在线购买商品或服务而无需信用卡
IMED（紧急医疗应急检测）-车辆减速至停止，打开危险警示灯以及利用包括车辆的当前位置的预先记录的语音消息自动拨打预设号码或911	安全访问以打开车辆	路径预测
	与用户身份绑定的点火装置	兴趣点提供和预测
	授权其他驾驶员	日历事件
改变的状态/醉酒检测	预设其他驾驶员（即，青少年）可以解锁/闭锁/开动车辆的时间	基于关注，重新计算搜索结果
通过使用生物特征监控视觉模式匹配能力，在汽车中阻止手持电话的使用	远程启动发动机（热/冷车）	情绪检测-汽车将知道你处于何种情绪或是否有社交场合（即，约会等）并且可以设置内部灯光/音乐以适应
用于生物特征监控的示例性系统和方法以及医学扫描仪转移至电话的	总是确定汽车的位置	
	远程观察汽车中的其他乘客	总是确定汽车的位置

[0146]

方法-向紧急调度远程发送生命体征 防止未授权/未达法定年龄的驾驶员 防止“规定时间后”的使用（青少年驾驶员） 防止路怒-汽车将知道你正处于拥挤交通中，它将倾听汽车喇叭响并且关注你的情绪以及提供安慰声音/音乐/话语以使你冷静下来 坏天气检测-汽车可以告诉你天气是否差到无法上路		增强的 ZipCar 模型 汽车可以检测你是否单独在车中并且通过播放音乐列表或向你提出小问题等提供“与你相伴”

[0147] 可以理解，在一些实现中，系统服务器105还可以使用系统保持用户授权的历史，包括在示例性生物特征认证和授权过程中和其后收集到的和/或处理的任何和所有信息。例如，关于访问车辆的记录和细节以及进行的与用户访问相关的交易或操作可以被系统服务器存储在一个或更多个数据库中，从而为用户创建交易审计跟踪。应当理解，关于任何和所有访问请求、交易和活动的信息可以被系统服务器105存储。

[0148] 例如，与用户对车辆的授权使用相关的记录(可以包括GPS和其它此类的物理位置数据以及在使用过程中收集到的其他数据(例如，图片、传感器测量值、时间))可以被系统服务器105存储，从而创建用户的物理审计跟踪。此外，用户可以被定期认证或被提示进行认证，这简单地是为了以认证方式记录用户的个人位置的目的。例如，与商务驾驶员和及其货车相关联的设置可以要求驾驶员全天被车载计算机自动定期的认证以确保授权的驾驶员在驾驶并且监控驾驶员驾驶的时间和距离以遵循法律要求。基于该设置，可以由车载计算机和/或系统服务器关于驾驶员的合规性为驾驶员和管理员提供自动提醒。另外，如上所述，可以控制车辆的使用以确保遵守规则/设置。

[0149] 用户和其他授权的用户/管理员可以经由相应的计算装置访问存储的物理和交易审计跟踪。例如，使用执行安全认证应用的注册的移动装置101a或计算装置呈现的类似仪表盘的界面或通过基于网络的用户界面。使用仪表盘，用户可以调整设置、偏好并且指定审计跟踪的访问规则。例如，用户124可查看并指定被授权访问用户的审计跟踪数据或审计跟踪的特定部分的其他个人和组织。此外，用户可以根据用户的条件(包括但不限制于使用约束和费用)，准予有条件地访问指定的组织和个人。

[0150] 在一些实现中，根据公开的实施方式，可以通过用户的移动装置101a或与用户和/或被用户访问的车辆相关联的任何其它GPS使能的计算装置(例如，车载计算机101b)收集用户的GPS位置信息。用途和位置信息可以被系统服务器105存储在一个或更多个关联的数据库上。例如，GPS使能的计算装置101b可以位于用户车辆中并且收集关于汽车的位置的

GPS位置信息。该位置信息可被发送至系统服务器105或被直接发送至数据库，以便为汽车和计算装置101b保持GPS数据的物理审计追踪。

[0151] 作为另一示例，在一些实现中，根据公开的实施方式，系统服务器105还可控制对计算装置101b和/或相关联的ACE(例如，车辆)的访问/使用。例如，通过在提供对计算装置或车辆之前要求生物特征认证/用户授权，否则限制访问。

[0152] 位置数据可以用于一些用途，举例并且没有限制，跟踪车队车辆的移动、监控用途、跟踪被盗车辆等。因此，可以理解，在一些实例中，期望监控和共享由计算装置101b和相关联的车辆收集的位置信息。然而，鉴于隐私问题，除非必要，用户可能不希望位置被跟踪。鉴于这样的隐私顾虑，在一些实现中，用户124可以指定规则，所述规则限定例如计算装置101b、或移动装置101a或其它计算装置(例如，专用车辆位置跟踪装置)的位置信息应被收集的程度的或所述信息应被个人/企业系统监控的程度。例如，用户124可以指定他们不希望共享当用户在车辆中时收集的用户的位置信息，但希望在用户不在汽车中时位置被监控(例如，为了车辆防盗追踪的目的)。作为另一示例，如果管理车队和雇员，用户124可以指定他们希望当雇员在车中时跟踪包括计算装置101b的车辆的位置。

[0153] 根据公开的实施方式，在一些实现中，当计算装置101b被交互(例如，被用户激活、有人发动汽车使得计算装置101b开始收集位置信息等)，计算装置可以扫描用户的生物特征并且生物特征认证用户。附加地或另选地，计算装置101b可向系统服务器105发送授权请求。授权请求可标识计算装置101b并且还可以包括附加信息，比如，计算装置的GPS位置、用户的身份等。响应于该请求，系统服务器可以根据接收到的信息和存储的用户简档来确定计算装置101b与用户124关联，并且提示关联的移动装置101a对用户进行认证。作为另一示例，如果多个用户可以访问具有跟踪装置(例如，计算装置101b)的车辆，在访问车辆之前或之后，用户可被要求向计算装置101b表明自己的身份以便授权。因此，认证请求可以标识特定用户，使得系统服务器可以提示适当的用户的移动装置101a将要生物特征认证用户。附加地或另选地，系统服务器105可以告知所有被批准的用户，使得适当的用户可以继续认证。附加地或另选地，基于计算装置101b的位置，系统服务器可以识别具有相应位置的注册移动装置并提示关联的用户进行认证。

[0154] 在一些实现中，用户可以使用计算装置101b和/或用户的移动装置101a发起认证过程。例如，当用户进入具有计算装置101b的汽车时，用户能够发起认证过程，使得用户的位置不被移动装置101a或计算装置101b跟踪。附加地或另选地，在被允许访问/激活与计算装置101b相关联的汽车(例如，启动汽车)之前，用户可被要求进行认证。

[0155] 假设用户的身份被认证，则系统服务器105可以准予访问ACE(例如，计算装置、汽车等)或根据与用户124、移动装置101a、计算装置101b、ACE等相关联的访问规则收集/提供对由那些装置记录的信息的访问。例如，如果用户的偏好指定用户的位置信息可以由配偶访问，但不应该与防盗监控公司共享，则系统服务器105可以准予配偶访问但拒绝防盗追踪公司访问。作为另一示例，如果车主在与计算装置101b相关联的设置中指定特定用户可在上午8点至下午11之间访问车辆并且当由该特定的用户使用时位置应被持续监控，则在成功的认证/授权后，系统服务器可以允许特定的用户在指定时间窗口期间访问汽车，在使用中可对位置进行连续监控，并且还可以向车主提供对位置信息的访问。

[0156] 在此刻，应该指出的是，虽然许多前面的描述涉及用于授权用户根据用户的生物

特征来访问的车辆的系统和方法，本文公开的系统和方法可以在所参照的场景以外的场景、情形和环境中类似地部署和实现。

[0157] 尽管本说明书包括多种具体细节，这些不应被解释为是对任何实现的范围或要求保护的范围的限制，相反，是作为针对特定实现的特定实施方式的特征的描述。在本文中的说明书中或不同实施方式中描述的特定特征也可以通过与单个实施方式结合来实施。反之，在单个实施方式的背景中描述的各种特征也可以在多个实施方式中单独地或以任何合适的子组合实现。此外，尽管可以根据特定组合中的动作对特征进行描述，并且即使初始地这样要求，但是，来自要求的组合的一个或一些特征可以在一些情况中从组合中实现，并且要求的组合可以涉及子组合或子组合的变化。

[0158] 类似地，在附图中按照特定顺序来描述操作，这不应该理解为需要按照示出的特定顺序或连续的顺序实施这些操作，或实施示出的全部操作来获得所期望的结果。在特定的情况中，多任务处理和并行处理可以是有利的。此外，上文中在实施方式中所描述的各个系统部件的分离不应理解为在所有实施方式中均需要这些分离，并且应该理解为所描述的编程组件和系统通常可以一起集成到单个软件产品中或封装在多个软件产品内。相似地，在特定组件中的诸如软件模块的系统组件的组合不应被理解为在所有实施方式中需要这样的组合，而是应当理解，组件和相应的特征/功能可跨一个或更多个单独的组件实现。

[0159] 本文中所使用的术语是仅用于描述特定实施方式的目的，而不是为了限制本发明。如本文中所使用的，除非上下文清楚地表明，否则单数也旨在包括复数形式。将进一步理解，当在该说明书中使用时，术语“包括”和/或“包含”指定阐述的特征、要件、步骤、操作、元件和/或组件的存在，但不排除附加的一个或更多个其他特征、要件、步骤、操作、元件、组件和/或它们的组的存在。应该指出，在权利要求中使用以修饰要求保护的元素的诸如“第一”、“第二”、“第三”的序数词本身不意味着任何优先权、优先级、或一个要求保护的元素与另一个的顺序或实施方法的步骤的时间数据，但是仅作为标记以从具有相同名称的另一元素区分具有特定名称的一个要求保护的元素(但是为序数词的使用)以区分要求保护的元素。此外，本文中使用的措辞和术语是为了描述的目的，不应该被视为限制。使用“包括”、“包含”或“具有”、“含有”、“涉及”及本文中它们的变体的使用旨在包括其后列出的项目及其等同物以及附加项目。应该理解，附图中的相同标记贯穿若干附图表示相同的元件，并且为了所有的实施方式或布置不要求参照附图描述的和示出的所有组件和/或步骤。

[0160] 因此，本系统和方法的说明性的实施方式和布置提供一种授权用户访问车辆的计算机实现的方法、计算机系统以及计算机程序产品。附图中的流程图和框图根据各个实施方式和布置示出了系统、方法和计算机程序产品的可能实现的架构、功能和操作。在这方面，流程图或框图中的每个框可以表示包括用于实现指定的逻辑功能的一个或更多个可执行指令的代码的模块、段或部分。还应指出，在一些另选的实现中，在框中指出的功能可能以不同于附图中指出的顺序发生。例如，取决于涉及的功能，连续示出的两个框可能实际上基本上同时执行，或有时框可能以相反的顺序执行。还应指出，框图和/或流程图中的每个框以及框图和/或流程图中的框的组合可以由执行指定功能或动作的专用硬件系统或专用硬件与计算机指令的组合来实现。

[0161] 上述主题仅作为例证方式提供，并且不应被解释为限制。可以对本文中描述的主题进行各种修改和改变而不遵循示出的和描述的示例性实施方式和应用，并且不背离在下

面的权利要求中列出的本发明的真正精神和范围。

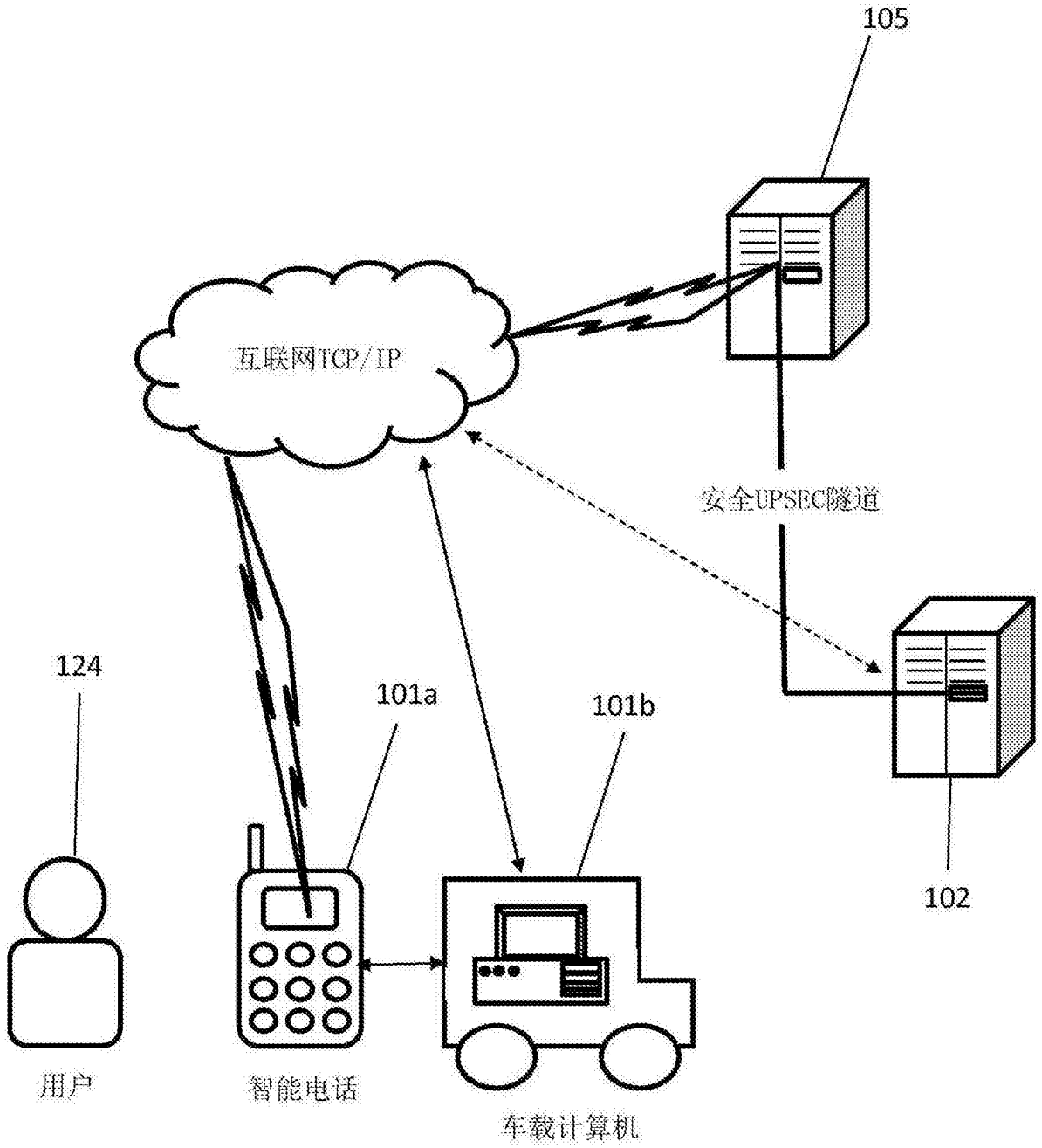


图1

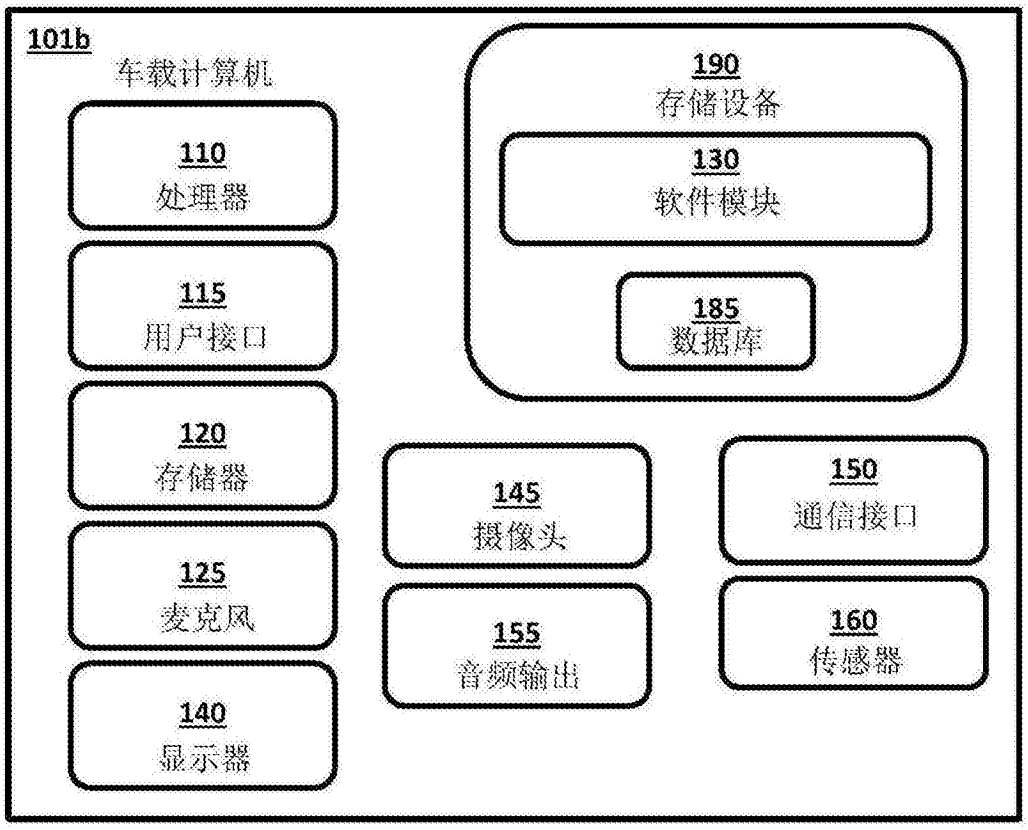

101b
车载计算机
110
处理器
115
用户接口
120
存储器
125
麦克风
140
显示器
190
存储设备
130
软件模块
185
数据库
145
摄像头
155
音频输出
150
通信接口
160
传感器

图2A

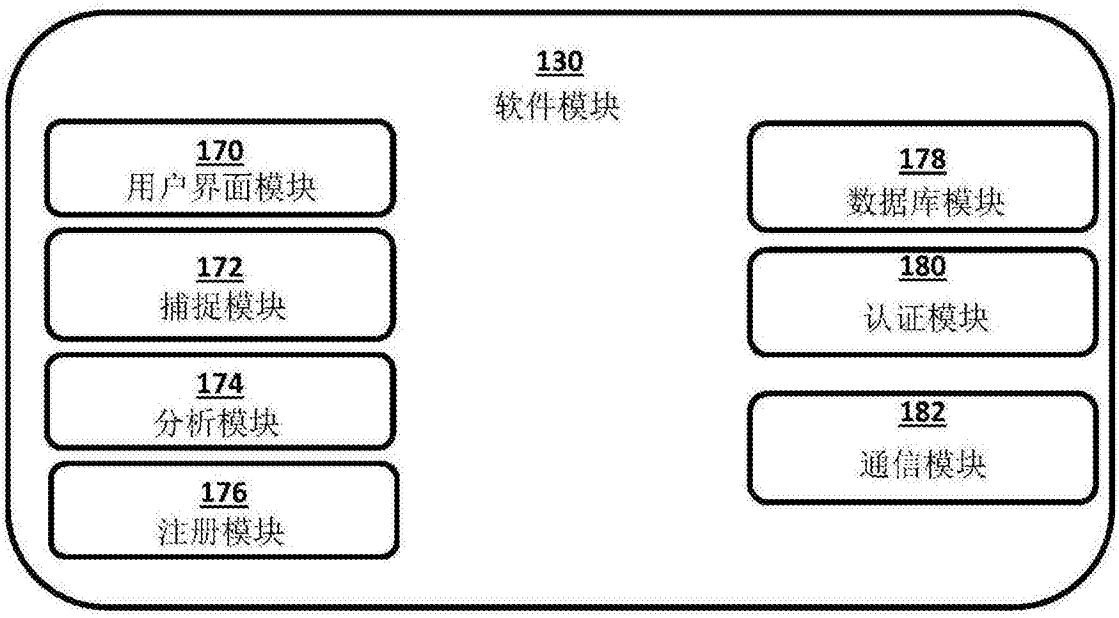

130
软件模块
170
用户界面模块
172
捕捉模块
174
分析模块
176
注册模块
178
数据库模块
180
认证模块
182
通信模块

图2B

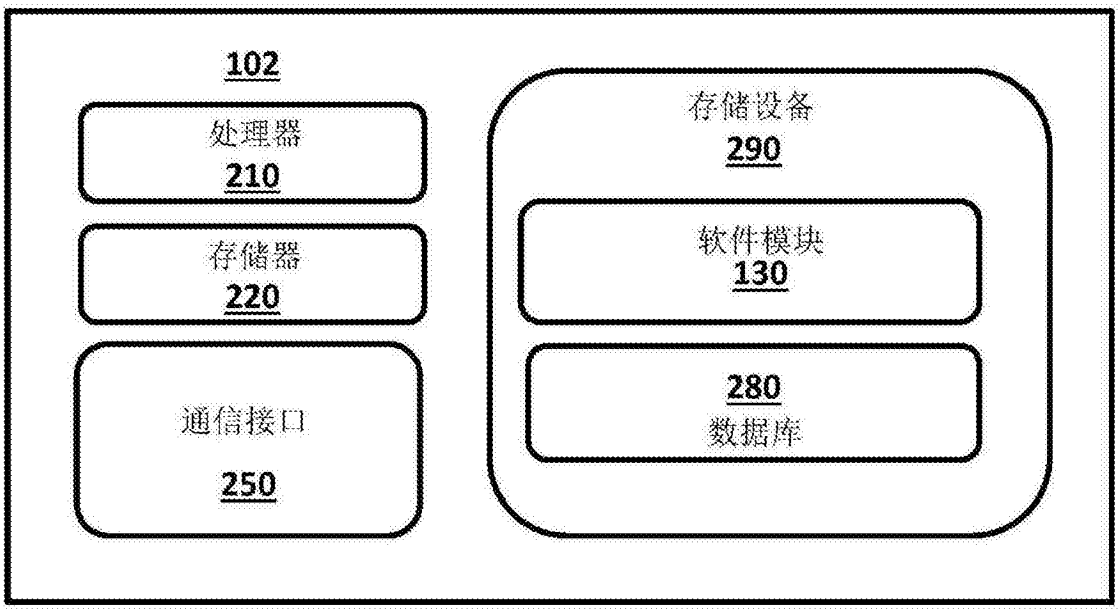


图2C


300
建立通信会话并初始化移动装置
305
收集用户标识信息
310
收集移动装置标识信息
315
验证用户身份
320
生成用户简档
325
接收用户设置
330
捕捉用户生物特征
335
生成生物特征标识符
340
接收基于非机器视觉的信息
345
确定活性
350
存储生物特征/活性信息
355

图3


400
开始认证
405
捕捉用户生物特征
410
生成生物特征标识符
415
认证用户生物特征
420
确定用户活性
425
通过系统服务器进一步认证用户
430

图4

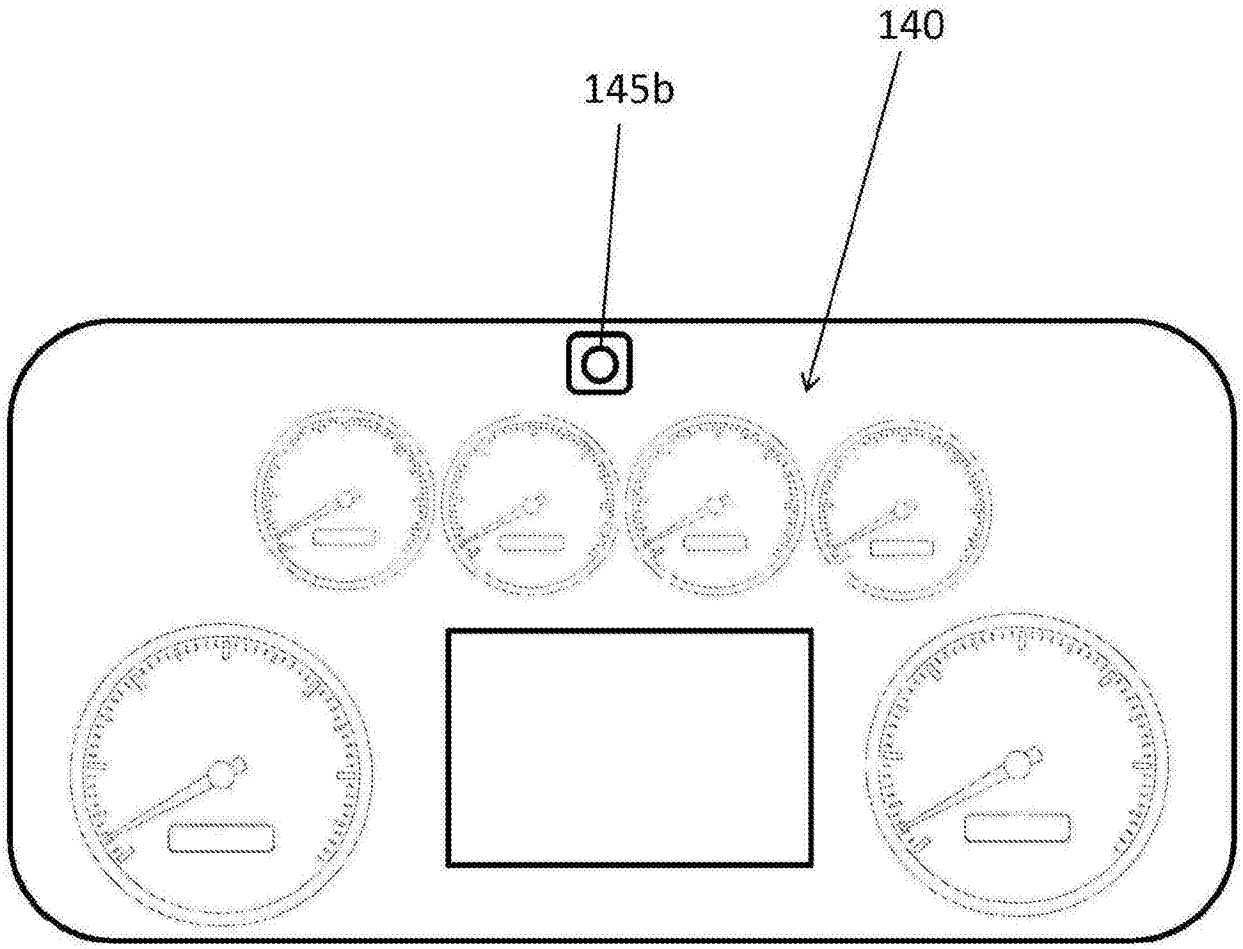


图5A

图5B

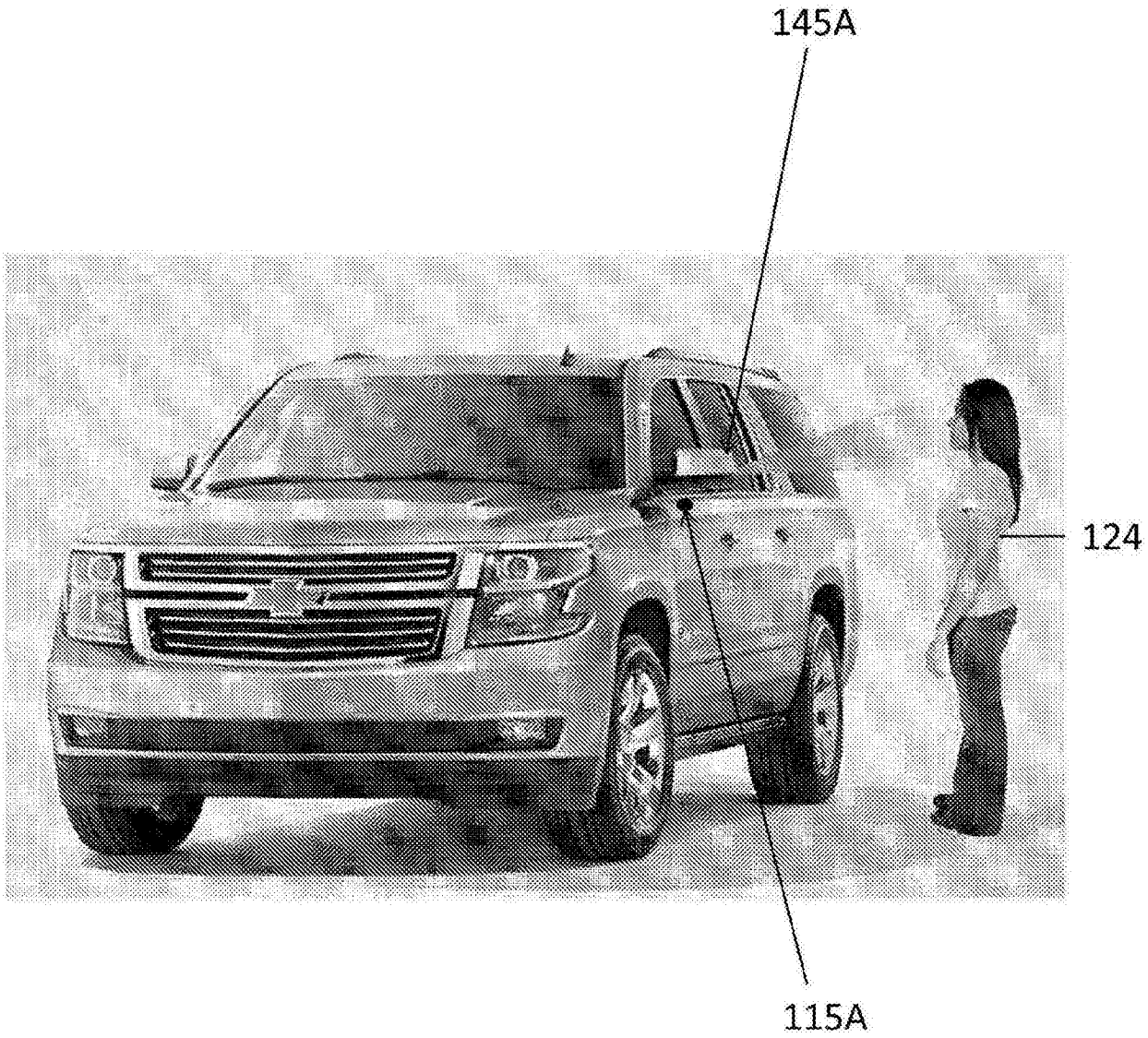


图5C

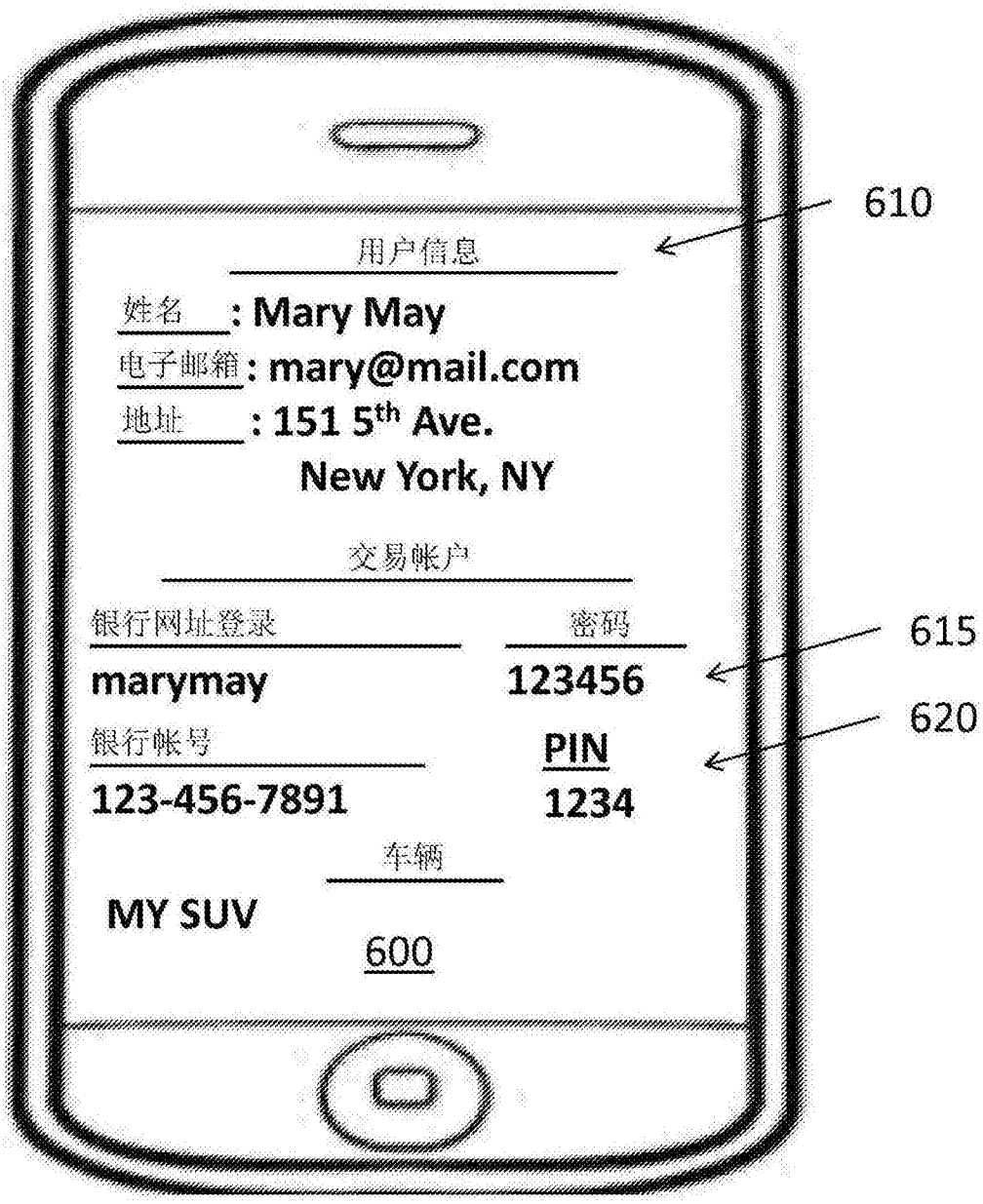

610
用户信息
姓名 : Mary May
电子邮箱 : mary@mail.com
地址 : 151 5th Ave.
New York, NY
交易帐户
银行网址登录
密码
615
marymay
123456
620
银行帐号
PIN
123-456-7891
1234
车辆
MY SUV
600

图6A