(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 106375312 A
(43)申请公布日 2017.02.01

(21)申请号 201610793772.4

(22)申请日 2016.08.31

(71)申请人 长城汽车股份有限公司
地址 071000 河北省保定市朝阳南大街2266号

(72)发明人 应世明 牛域辉 郭岩松

(74)专利代理机构 北京清亦华知识产权代理事务所(普通合伙) 11201
代理人 张大威

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)
G07C 9/00(2006.01)
B60R 25/24(2013.01)

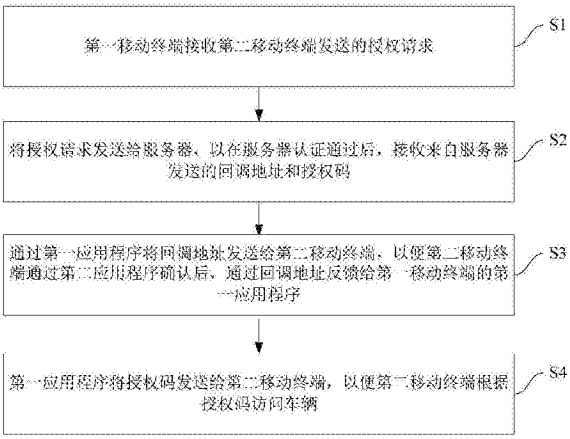
权利要求书1页 说明书6页 附图3页

(54)发明名称

虚拟钥匙的授权方法、系统、移动终端及服务器

(57)摘要

本发明提供了一种虚拟钥匙的授权方法、系统、移动终端及服务器，方法包括：第一移动终端接收第二移动终端发送的授权请求；将授权请求发送给服务器，以在服务器认证通过后，接收来自服务器发送的回调地址和授权码；通过第一应用程序将回调地址发送给第二移动终端，以便第二移动终端通过第二应用程序确认后，通过回调地址反馈给第一移动终端的第一应用程序；第一应用程序将授权码发送给第二移动终端，以便第二移动终端根据授权码访问车辆。本发明减少了获取授权码的交互流程，提高了效率，同时保证了传输过程的安全性，能够给钥匙授权的双方提供了更好的操作体验、便利性和安全保障。



CN 106375312 A

1.一种虚拟钥匙的授权方法，其特征在于，包括以下步骤：

第一移动终端接收第二移动终端发送的授权请求；

将所述授权请求发送给服务器，以在所述服务器认证通过后，接收来自所述服务器发送的回调地址和授权码；

通过第一应用程序将所述回调地址发送给所述第二移动终端，以便所述第二移动终端通过第二应用程序确认后，通过所述回调地址反馈给所述第一移动终端的第一应用程序；

所述第一应用程序将所述授权码发送给所述第二移动终端，以便所述第二移动终端根据所述授权码访问车辆。

2.根据权利要求1所述的虚拟钥匙的授权方法，其特征在于，所述第一移动终端与所述服务器之间的通信，以及所述第一移动终端与所述第二移动终端之间的通信采用隧道加密。

3.根据权利要求1所述的虚拟钥匙的授权方法，其特征在于，所述第一应用程序为APP、SMS或者IE，所述第二应用程序为脚本。

4.根据权利要求1所述的虚拟钥匙的授权方法，其特征在于，所述第一移动终端将所述授权请求发送给服务器时，还用于将第一移动终端身份信息发送给所述服务器，以便所述服务器对所述第一移动终端进行认证。

5.一种虚拟钥匙的授权系统，其特征在于，包括：第一移动终端、第二移动终端和服务器，其中，

所述第一移动终端接收第二移动终端发送的授权请求，并将所述授权请求发送给服务器，以在所述服务器认证通过后，接收来自所述服务器发送的回调地址和授权码，以及通过第一应用程序将所述回调地址发送给所述第二移动终端，以便所述第二移动终端通过第二应用程序确认后，通过所述回调地址反馈给所述第一移动终端的第一应用程序，所述第一应用程序将所述授权码发送给所述第二移动终端，以便所述第二移动终端根据所述授权码访问车辆。

6.根据权利要求5所述的虚拟钥匙的授权系统，其特征在于，所述第一移动终端与所述服务器之间的通信，以及所述第一移动终端与所述第二移动终端之间的通信采用隧道加密。

7.根据权利要求5所述的虚拟钥匙的授权系统，其特征在于，所述第一应用程序为APP、SMS或者IE，所述第二应用程序为脚本。

8.根据权利要求5所述的虚拟钥匙的授权系统，其特征在于，所述第一移动终端将所述授权请求发送给服务器时，还用于将第一移动终端身份信息发送给所述服务器，以便所述服务器对所述第一移动终端进行认证。

9.一种移动终端，其特征在于，所述移动终端为根据权利要求5-8任一项所述的虚拟钥匙的授权系统中第一移动终端。

10.一种移动终端，其特征在于，所述移动终端为根据权利要求5-8任一项所述的虚拟钥匙的授权系统中第二移动终端。

11.一种服务器，其特征在于，所述服务器为根据权利要求5-8任一项所述的虚拟钥匙的授权系统中服务器。

虚拟钥匙的授权方法、系统、移动终端及服务器

技术领域

[0001] 本发明涉及信息安全技术领域，特别涉及一种虚拟钥匙的授权方法、系统、移动终端及服务器。

背景技术

[0002] 随着电子产品技术的快速发展，对生活中的便捷和安全要求越来越高。作为在生活中必不可少的安全锁系统，例如应用在汽车、家居等领域的电子锁系统，其设计已越来越贴近用户的期望需求。而普通钥匙的借用，需要将实物(包括机械钥匙、电子钥匙、非接触磁卡等)交给借用人，造成了时间和空间上的不方便。如今智能电子钥匙的出现为广大用户提供了新的钥匙分享平台，用户之间可以通过某些通讯方式，在电子设备上将钥匙授权给他人，解决了普通钥匙分享时间和空间上的局限性。

[0003] 根据用户的需求，各种智能电子钥匙被设计出来，移动设备例如手机，将手机和钥匙结合。由于手机作为便捷性移动设备的一种，在日常生活中应用广泛，以手机作为一种钥匙的使用和授权的平台已经成为一种趋势。

[0004] 目前，相关技术提出了一种车辆操作权限授予系统，具备：服务器，其从第1便携型电子设备接收对作为车辆的电子钥匙来使用的第1便携型电子设备进行识别的识别信息，且对识别信息的正当性进行确认，且将动作许可信号发送至车辆，该动作许可信号对与来自于第1便携型电子设备的要求相应的车辆操作进行许可；钥匙登录部，将服务器所提供的密钥登录在第1便携型电子设备中；以及访问权授予部，其通过使用登录在第1便携型电子设备中的密钥将访问服务器的访问权授予给第2便携型电子设备，并且使第2便携型电子设备作为具有车辆操作权限的电子钥匙来动作。该方法的缺点在于，存在一个钥匙密码同时存在的安全性，如果被授权者在开车的过程中，授权者仍有权限控制汽车，会给被授权者带来危险，被授权者往往作为临时使用者，在使用钥匙的过程中安全体验并不好。

[0005] 相关技术还公开了一种车辆的授权方法、系统和终端，方法包括：被授权移动终端通过蓝牙钥匙应用程序生成借车请求信息，并将借车请求信息发送至授权移动终端；授权移动终端接收借车请求信息；授权移动终端导入借车请求信息并设置车辆的借用时间，并且将标识信息、借用时间以及车辆蓝牙钥匙的账号和密码进行加密以生成授权信息；授权移动终端将授权信息发送至被授权移动终端；被授权移动终端接收授权信息，并导入授权信息，及获取自身的标识信息，且当自身的标识信息与授权信息中的标识信息一致时，在借用时间内控制车辆。该方法的缺点在于，虽然有提示在授权中控制使用的时间，但并没有对使用次数或其他权限做出说明，更没有对授权中如何实现类似限制做出方案。

发明内容

[0006] 有鉴于此，本发明旨在提出一种虚拟钥匙的授权方法，该方法减少了获取授权码的交互流程，提高了效率，同时保证了传输过程的安全性，能够给钥匙授权的双方提供了更好的操作体验、便利性和安全保障。

[0007] 为达到上述目的，本发明的技术方案是这样实现的：

[0008] 一种虚拟钥匙的授权方法，包括以下步骤：第一移动终端接收第二移动终端发送的授权请求；将所述授权请求发送给服务器，以在所述服务器认证通过后，接收来自所述服务器发送的回调地址和授权码；通过第一应用程序将所述回调地址发送给所述第二移动终端，以便所述第二移动终端通过第二应用程序确认后，通过所述回调地址反馈给所述第一移动终端的第一应用程序；所述第一应用程序将所述授权码发送给所述第二移动终端，以便所述第二移动终端根据所述授权码访问车辆。

[0009] 进一步地，所述第一移动终端与所述服务器之间的通信，以及所述第一移动终端与所述第二移动终端之间的通信采用隧道加密。

[0010] 进一步地，所述第一应用程序为APP、SMS或者IE，所述第二应用程序为脚本。

[0011] 进一步地，所述第一移动终端将所述授权请求发送给服务器时，还用于将第一移动终端身份信息发送给所述服务器，以便所述服务器对所述第一移动终端进行认证。

[0012] 相对于现有技术，本发明所述的虚拟钥匙的授权方法具有以下优势：

[0013] 本发明的虚拟钥匙的授权方法，第一移动终端接收第二移动终端的授权请求，并发送给服务器，并在服务器人证通过后，接收回调地址和授权码，并通过第一应用程序将回调地址发送给第二移动终端，以便第二移动终端通过第二应用程序在确认后，通过回调地址反馈给第一移动终端，然后第一移动终端将授权码发送给第二移动终端，完成授权过程。因此，该方法减少了获取授权码的交互流程，提高了效率，同时在传输过程中采用隧道加密技术(TLS)保证传输过程的安全性，能够给钥匙授权的双方提供了更好的操作体验、便利性和安全保障。

[0014] 本发明的另一个目的在于提出一种虚拟钥匙的授权系统，该系统减少了获取授权码的交互流程，提高了效率，同时保证了传输过程的安全性，能够给钥匙授权的双方提供了更好的操作体验、便利性和安全保障。

[0015] 为达到上述目的，本发明的技术方案是这样实现的：

[0016] 一种虚拟钥匙的授权系统，包括：第一移动终端、第二移动终端和服务器，其中，所述第一移动终端接收第二移动终端发送的授权请求，并将所述授权请求发送给服务器，以在所述服务器认证通过后，接收来自所述服务器发送的回调地址和授权码，以及通过第一应用程序将所述回调地址发送给所述第二移动终端，以便所述第二移动终端通过第二应用程序确认后，通过所述回调地址反馈给所述第一移动终端的第一应用程序，所述第一应用程序将所述授权码发送给所述第二移动终端，以便所述第二移动终端根据所述授权码访问车辆。

[0017] 进一步地，所述第一移动终端与所述服务器之间的通信，以及所述第一移动终端与所述第二移动终端之间的通信采用隧道加密。

[0018] 进一步地，所述第一应用程序为APP、SMS或者IE，所述第二应用程序为脚本。

[0019] 进一步地，所述第一移动终端将所述授权请求发送给服务器时，还用于将第一移动终端身份信息发送给所述服务器，以便所述服务器对所述第一移动终端进行认证。

[0020] 所述的虚拟钥匙的授权系统与上述的虚拟钥匙的授权方法相对于现有技术所具有的优势相同，在此不再赘述。

[0021] 本发明的再一个目的在于提出一种移动终端，该移动终端减少了获取授权码的交

互流程，提高了效率，同时保证了传输过程的安全性，能够给钥匙授权的双方提供了更好的操作体验、便利性和安全保障。

[0022] 为达到上述目的，本发明的技术方案是这样实现的：

[0023] 一种移动终端，所述移动终端为本发明上述实施例所述的虚拟钥匙的授权系统中的第一移动终端。

[0024] 所述的移动终端与上述的虚拟钥匙的授权系统相对于现有技术所具有的优势相同，在此不再赘述。

[0025] 本发明的又一个目的在于提出一种移动终端，该移动终端减少了获取授权码的交互流程，提高了效率，同时保证了传输过程的安全性，能够给钥匙授权的双方提供了更好的操作体验、便利性和安全保障。

[0026] 为达到上述目的，本发明的技术方案是这样实现的：

[0027] 一种移动终端，所述移动终端为本发明上述实施例所述的虚拟钥匙的授权系统中的第二移动终端。

[0028] 所述的移动终端与上述的虚拟钥匙的授权系统相对于现有技术所具有的优势相同，在此不再赘述。

[0029] 本发明的又一个目的在于提出一种服务器，该服务器减少了获取授权码的交互流程，提高了效率，同时保证了传输过程的安全性，能够给钥匙授权的双方提供了更好的操作体验、便利性和安全保障。

[0030] 为达到上述目的，本发明的技术方案是这样实现的：

[0031] 一种服务器，所述服务器为本发明上述实施例所述的虚拟钥匙的授权系统中的服务器。

[0032] 所述的服务器与上述的虚拟钥匙的授权系统相对于现有技术所具有的优势相同，在此不再赘述。

附图说明

[0033] 构成本发明的一部分的附图用来提供对本发明的进一步理解，本发明的示意性实施例及其说明用于解释本发明，并不构成对本发明的不当限定。在附图中：

[0034] 图1为本发明实施例的虚拟钥匙的授权方法的流程图；

[0035] 图2为本发明一个实施例的虚拟钥匙的授权方法的原理框图；

[0036] 图3为本发明一个实施例的虚拟钥匙分享授权示意图；

[0037] 图4为本发明一个实施例的钥匙分享授权过程中各模块关系示意图；

[0038] 图5为本发明一个实施例的虚拟钥匙的授权方法的授权机制示意图；以及

[0039] 图6为本发明实施例的虚拟钥匙的授权系统的结构框图。

[0040] 附图标记说明：

[0041] 100-虚拟钥匙的授权系统、110-第一移动终端、120-第二移动终端、130-服务器。

具体实施方式

[0042] 需要说明的是，在不冲突的情况下，本发明中的实施例及实施例中的特征可以相互组合。

[0043] 下面将参考附图并结合实施例来详细说明本发明。

[0044] 图1是根据本发明一个实施例的虚拟钥匙的授权方法的流程图。图2是根据本发明一个实施例的虚拟钥匙的授权方法的原理框图。

[0045] 如图1所示，并结合图2，本发明实施例的虚拟钥匙的授权方法包括以下步骤：

[0046] 步骤S1：第一移动终端接收第二移动终端发送的授权请求。具体地，第一移动终端即为图2中所示的智能手机1，第二移动终端即为图2中所示的智能手机2，服务器即为图2中的云端服务器。

[0047] 步骤S2：将授权请求发送给服务器，以在服务器认证通过后，接收来自服务器发送的回调地址和授权码。

[0048] 进一步地，在本发明的一个实施例中，第一移动终端将授权请求发送给服务器时，还用于将第一移动终端身份信息发送给服务器，以便服务器对第一移动终端进行认证。

[0049] 步骤S3：通过第一应用程序将回调地址发送给第二移动终端，以便第二移动终端通过第二应用程序确认后，通过回调地址反馈给第一移动终端的第一应用程序。

[0050] 其中，第一应用程序例如为APP、SMS或者IE，第二应用程序例如为脚本。

[0051] 步骤S4：第一应用程序将授权码发送给第二移动终端，以便第二移动终端根据授权码访问车辆。

[0052] 在本发明的一个实施例中，例如，第一移动终端与服务器之间的通信，以及第一移动终端与第二移动终端之间的通信采用隧道加密。

[0053] 为了便于更好地理解本发明，以下结合附图，以具体示例对本发明实施例的方法进行更为详细具体地说明。

[0054] 结合图2所示，本发明实施例的方法的原理主要概述为：租用者(智能手机2的所有者)向车主(智能手机1的所有者)发送授权请求，在接收到车主的授权凭证后，租车者将车主的智能手机1传输的授权凭证传输到云端服务器，从服务器接收到钥匙访问验证码，将该验证码保存到被授权者(租车者)的智能手机2，被授权者携带保存到被授权智能手机2上的受保护资源，与PEPS集成蓝牙模块汽车进行匹配，完成钥匙的认证通讯过程，具体的授权过程例如图3所示，具体如下：

[0055] 租用者向车主发起授权请求，从车主的移动设备1(即智能手机1或第一移动终端)获取授权凭证。这个授权凭证是用来表示车主同意对该租车者进行授权。租车者获得车主的授权凭证后，再将授权凭证及租车者移动设备凭证发送到云端服务器，进行请求授权码获得最终访问凭证。云端服务器对租用者移动设备2(即智能手机2或第二移动终端)进行认证，并验证授权凭证的有效性，如果通过验证后，云端服务器将返回访问凭证授权码给移动设备2。租车者使用访问凭证授权码代表车主向汽车PEPS进行数据请求。PEPS验证通过授权码后将受保护的资源返回给租用者移动设备2，图4列出了钥匙授权过程中各相关模块之间的关系，具体如下：

[0056] (1)租用者移动设备2通过中间系统需向车主移动设备1请求访问授权码。

[0057] (2)车主移动设备1根据用户授权及对租用者信息认证通过后，向租用者移动设备2返回访问授权码。

[0058] (3)租用者移动设备2使用访问授权码调用开放平台数据接口访问受保护的用户资源，访问被云端服务器捕捉。

[0059] (4)云端服务器获取访问授权码，向车主请求授权码的相关用户类型、权限信息。

[0060] (5)车主移动设备1返回认证信息。

[0061] (6)云端服务器对请求中授权码所包含的权限信息与资源核准需要的权限信息进行校验。

[0062] (7)对于通过权限充分的请求通过云端服务器向汽车PEPS进行进一步的数据请求。

[0063] (8)汽车PEPS返回受保护的资源数据。

[0064] 基于上述提到的授权流程及各模块之间的关系，本发明的实施例采用了隐式的授权机制模式，即租车者通过移动设备2向车主移动设备1发送请求授权，车主通过设备上的APP、IE等应用进行账号密码的输入并对租用者的请求选择授权后，云端服务器并不是返回临时令牌给第三方应用，而是直接将授权码以URI片段的形式返回给移动设备2客户端，详细的授权机制例如图5所示，具体如下：

[0065] 1)租车者的移动设备2客户端通过车主的IE浏览器、APP等引导至云端服务器的授权数据交换节点开启授权流程。移动设备客户端2通过用户浏览器向云端服务器请求时，会带上客户端id、客户端设备id、请求权限范围、状态码以及用于云端服务器进行回调的回调地址。

[0066] 2)车主移动设备1在云端服务端输入用户凭证后，云端服务器对车主身份进行认证，然后由车主决定是否对移动设备2客户端的请求进行授权。

[0067] 3)假设车主通过了授权，云端服务器根据车主的授权模式启动相应的处理流程，之后以URI片段的形式将授权码附在利用步骤1传入的回调地址后面。

[0068] 4)移动设备1的浏览器需保留授权码在本地，同时向移动设备2客户端发送在web端回调地址的存储资源的请求。

[0069] 5)Web端通常返回一个HTML页面，其中带有能够获取步骤3中返回的带有授权码信息的完整回调地址的脚本。

[0070] 6)车主浏览器在本地运行脚本获取到授权码，将获取的授权码返回移动设备2。

[0071] 综上，根据本发明实施例的虚拟钥匙的授权方法，第一移动终端接收第二移动终端的授权请求，并发送给服务器，并在服务器人证通过后，接收回调地址和授权码，并通过第一应用程序将回调地址发送给第二移动终端，以便第二移动终端通过第二应用程序在确认后，通过回调地址反馈给第一移动终端，然后第一移动终端将授权码发送给第二移动终端，完成授权过程。因此，该方法减少了获取授权码的交互流程，提高了效率，同时在传输过程中采用隧道加密技术(TLS)保证传输过程的安全性，能够给钥匙授权的双方提供了更好的操作体验、便利性和安全保障。

[0072] 进一步地，如图6所示，本发明的实施例公开了一种虚拟钥匙的授权系统100，包括：第一移动终端110、第二移动终端120和服务器130。

[0073] 第一移动终端110接收第二移动终端120发送的授权请求，并将授权请求发送给服务器130，以在服务器130认证通过后，接收来自服务器130发送的回调地址和授权码，以及通过第一应用程序将回调地址发送给第二移动终端120，以便第二移动终端120通过第二应用程序确认后，通过回调地址反馈给第一移动终端110的第一应用程序，第一应用程序将授权码发送给第二移动终端120，以便第二移动终端120根据授权码访问车辆。其中，第一应用

程序例如为APP、SMS或者IE，第二应用程序例如为脚本。

[0074] 在本发明的一个实施例中，第一移动终端110与服务器130之间的通信，以及第一移动终端110与第二移动终端120之间的通信采用隧道加密。

[0075] 在本发明的一个实施例中，第一移动终端110将授权请求发送给服务器130时，还用于将第一移动终端110身份信息发送给服务器130，以便服务器130对第一移动终端110进行认证。

[0076] 综上，根据本发明实施例的虚拟钥匙的授权系统，第一移动终端接收第二移动终端的授权请求，并发送给服务器，并在服务器人证通过后，接收回调地址和授权码，并通过第一应用程序将回调地址发送给第二移动终端，以便第二移动终端通过第二应用程序在确认后，通过回调地址反馈给第一移动终端，然后第一移动终端将授权码发送给第二移动终端，完成授权过程。因此，该方法减少了获取授权码的交互流程，提高了效率，同时在传输过程中采用隧道加密技术(TLS)保证传输过程的安全性，能够给钥匙授权的双方提供了更好的操作体验、便利性和安全保障。

[0077] 需要说明的是，本发明实施例的虚拟钥匙的授权系统的具体实现方式与本发明实施例的虚拟钥匙的授权方法的具体实现方式类似，具体请参见方法部分的描述，为了减少冗余，此处不做赘述。

[0078] 进一步地，本发明的实施例公开了一种移动终端，该移动终端例如为本发明上述实施例所描述的虚拟钥匙的授权系统中的第一移动终端。因此，关于该移动终端的具体详细描述参见本发明上述对第一移动终端部分的描述。

[0079] 因此，根据本发明实施例的移动终端，减少了获取授权码的交互流程，提高了效率，同时保证了传输过程的安全性，能够给钥匙授权的双方提供了更好的操作体验、便利性和安全保障。

[0080] 进一步地，本发明的实施例公开了一种移动终端，该移动终端例如为本发明上述实施例所描述的虚拟钥匙的授权系统中的第二移动终端。因此，关于该移动终端的具体详细描述参见本发明上述对第二移动终端部分的描述。

[0081] 因此，根据本发明实施例的移动终端，减少了获取授权码的交互流程，提高了效率，同时保证了传输过程的安全性，能够给钥匙授权的双方提供了更好的操作体验、便利性和安全保障。

[0082] 进一步地，本发明的实施例公开了一种服务器，该服务器例如为本发明上述实施例所描述的虚拟钥匙的授权系统中的服务器。因此，关于该服务器的具体详细描述参见本发明上述对服务器部分的描述。

[0083] 因此，根据本发明实施例的服务器，减少了获取授权码的交互流程，提高了效率，同时保证了传输过程的安全性，能够给钥匙授权的双方提供了更好的操作体验、便利性和安全保障。

[0084] 以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

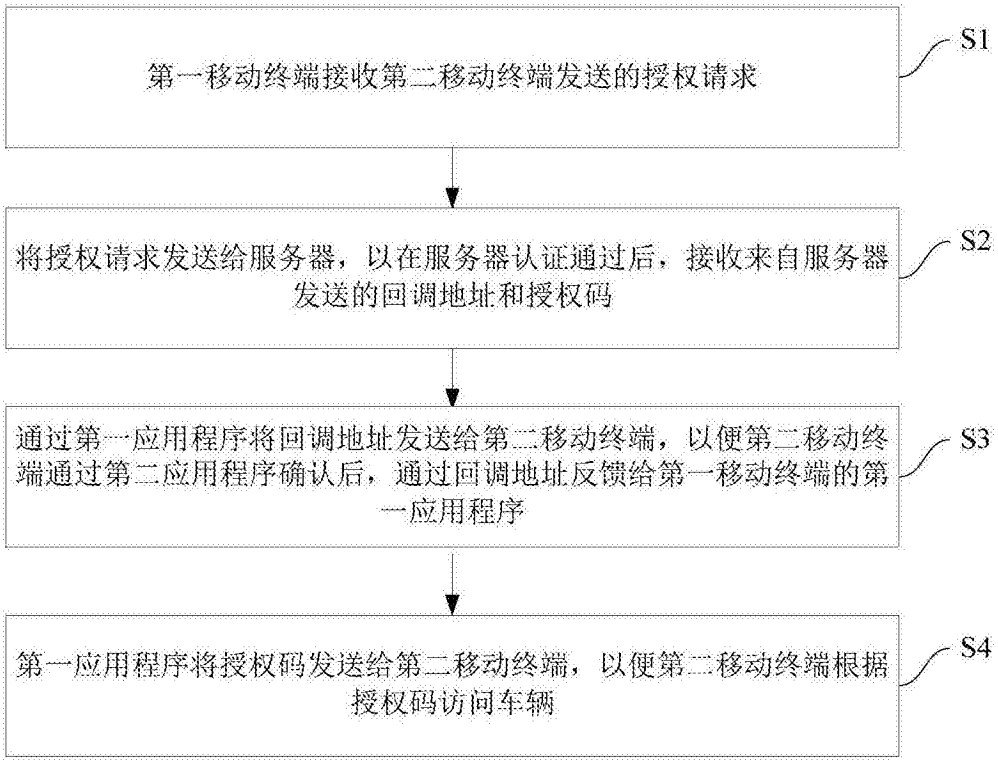

第一移动终端接收第二移动终端发送的授权请求
S1
将授权请求发送给服务器，以在服务器认证通过后，接收来自服务器发送的回调地址和授权码
S2
通过第一应用程序将回调地址发送给第二移动终端，以便第二移动终端通过第二应用程序确认后，通过回调地址反馈给第一移动终端的第一应用程序
S3
第一应用程序将授权码发送给第二移动终端，以便第二移动终端根据授权码访问车辆
S4

图1

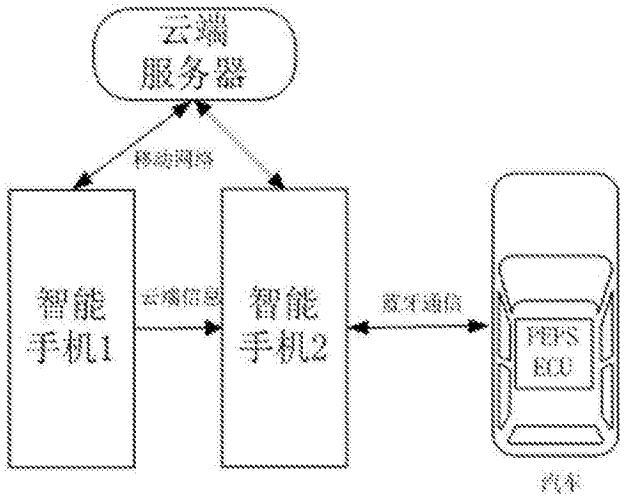

云端
服务器
智能
手机1
智能
手机2
POTS
ECU

图2

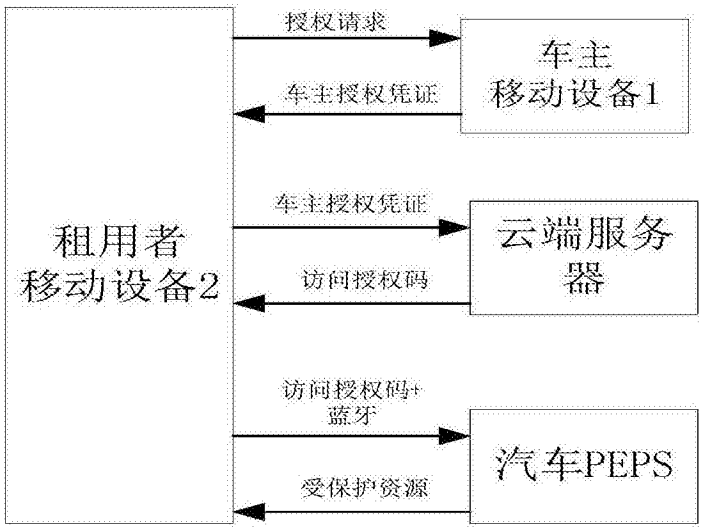

租用者
移动设备2
授权请求
车主
移动设备1
车主授权凭证
车主授权凭证
云端服务
器
访问授权码
访问授权码+
蓝牙
汽车PEPS
受保护资源

图3

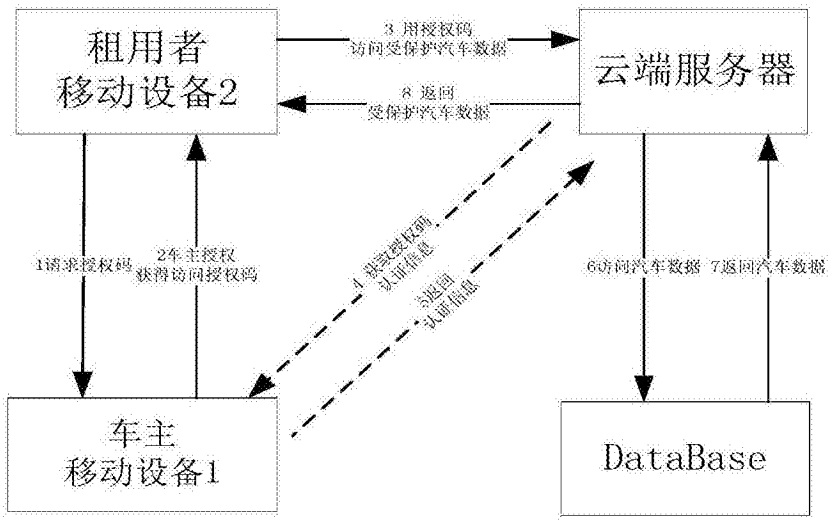

租用者
移动设备2
3 用授权码
访问受保护汽车数据
8 返回
受保护汽车数据
云端服务器
1请求授权码
2车主授权
获得访问授权码
4 验证授权码、
认证信息
5返回
认证信息
6访问汽车数据
7返回汽车数据
车主
移动设备1
DataBase

图4

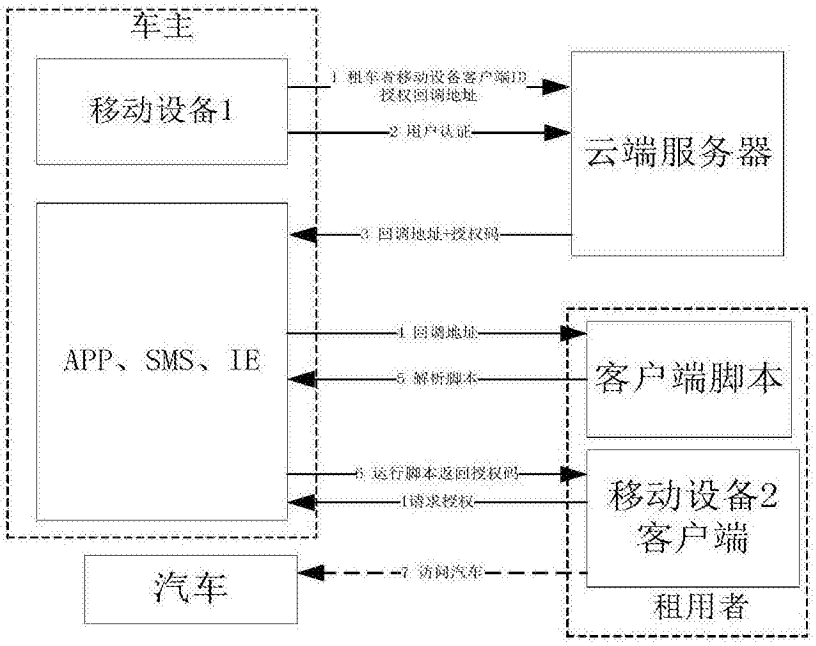

车主
移动设备1
1 租车者移动设备客户端ID
授权回调地址
2 用户认证
云端服务器
3 回调地址+授权码
APP、SMS、IE
4 回调地址
5 解析脚本
客户端脚本
6 运行脚本返回授权码
4请求授权
移动设备2
客户端
7 访问汽车
汽车
租用者

图5

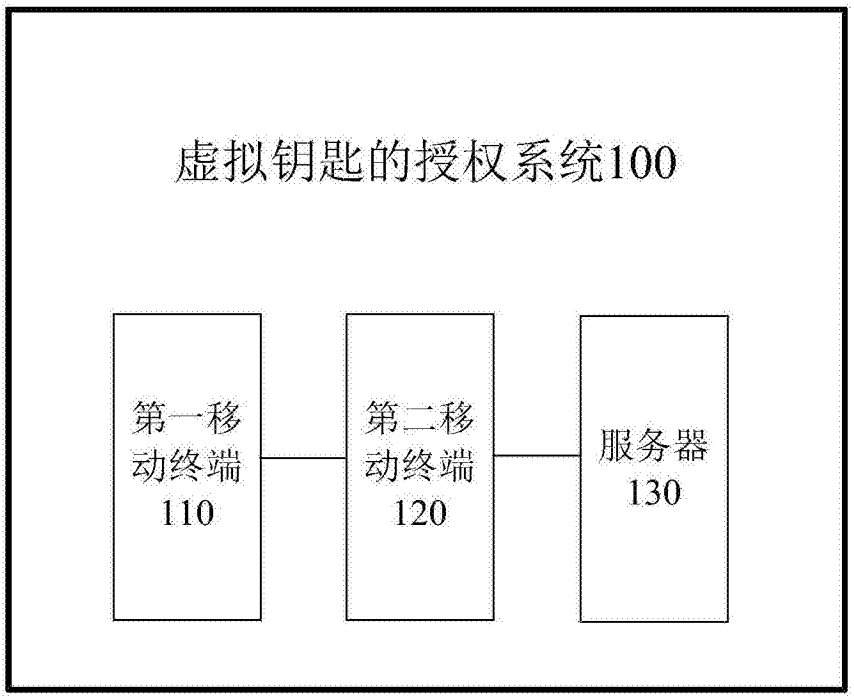

虚拟钥匙的授权系统100
第一移动终端110
第二移动终端120
服务器130

图6