(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 109727358 B
(45)授权公告日 2021.02.23

(21)申请号 201910129125.7

(22)申请日 2019.02.21

(65)同一申请的已公布的文献号
申请公布号 CN 109727358 A

(43)申请公布日 2019.05.07

(73)专利权人 深圳四海万联科技有限公司
地址 518052 广东省深圳市前海深港合作区前湾一路1号A栋201室

(72)发明人 张杨 向劲松 陈亚川 万海涛 朱志凌 殷凡 李迎春

(74)专利代理机构 北京酷爱智慧知识产权代理有限公司 11514
代理人 向霞

(51)Int.Cl.
G07C 9/00(2020.01)
H04W 4/80(2018.01)

(56)对比文件
CN 109285252 A,2019.01.29
CN 108569250 A,2018.09.25
张亚飞.基于可信执行环境的智能密码钥匙设计与实现.《中国优秀硕士学位论文全文数据库》.2016,
无.汽车共享和智能手机的新消费者 无线应用进入汽车领域.《办公自动化》.2017,

审查员 赵水

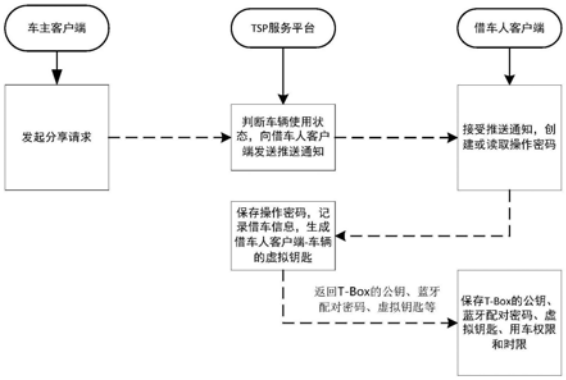
权利要求书2页 说明书12页 附图5页

(54)发明名称

基于蓝牙钥匙的车辆分享系统

(57)摘要

本发明提供的基于蓝牙钥匙的车辆分享系统,车主客户端生成分享请求发送给TSP服务平台;TSP服务平台对分享信息进行分析后,生成推送通知发送给借车客户端;在借车客户端接受推送通知后,生成确认信息发送给借车客户端;借车客户端实现与车载T-BOX模块之间的配对;还接收借车人的控制指令,发送给车载T-BOX模块;车载T-BOX模块建立与借车客户端的蓝牙通讯链路,接收控制指令,与其它车身电子控制单元配合以驱动车辆运行。该系统在借车过程中,不需要车主将车钥匙交给借车人,借车人通过借车客户端就能够驱动车辆,无需TSP服务平台参与,使用方便。该系统还在借车客户端授权后,才能驱动车辆,提高了私家车使用的安全性。



CN 109727358 B

1.一种基于蓝牙钥匙的车辆分享系统,其特征在于,包括:

车主客户端用于接收车主输入的分享信息,根据所述分享信息生成分享请求,发送给TSP服务平台;

TSP服务平台用于对所述分享信息进行分析后,生成推送通知发送给借车客户端;TSP服务平台还用于在借车客户端接受推送通知后,生成确认信息发送给所述借车客户端;所述确认信息包括蓝牙配对密码;

借车客户端用于接收借车人的接受指令,接受所述来自TSP服务平台的推送通知;借车客户端还用于接收确认信息,并利用蓝牙配对密码实现与车载T-BOX模块之间的配对;借车客户端还用于接收借车人的控制指令,发送给车载T-BOX模块;

车载T-BOX模块安装于车辆上,用于在与所述借车客户端配对成功后,建立与借车客户端的蓝牙通讯链路,接收借车客户端的控制指令,驱动车辆运行;

所述借车客户端还用于:在接受所述来自TSP服务平台的推送通知之后,创建操作密码或读取已保存的操作密码,根据所述操作密码和借车客户端的IMEI码生成接受确认反馈发送给TSP服务平台;

TSP服务平台还用于:接收所述接受确认反馈后,确定借车客户端接受所述推送通知;

所述确认信息还包括虚拟钥匙;

所述TSP服务平台具体用于:

获取以下加密数据:目标对象的用户名、目标对象的身份标志位、目标车辆的车辆VIN码、车主输入的用车权限掩码、车主输入的功能权限列表、分享时间、操作密码和借车客户端的IMEI;

获取借车客户端的证书文件,利用SHA256算法对所述证书文件进行加密,得到第一加密数据;

利用MD5算法对所述加密数据和第一加密数据进行加密,得到第二加密数据;

利用TSP服务平台预设的平台私钥文件对所述第二加密数据进行加密,得到平台签名;

获取目标车辆中车载T-BOX模块生成的车载公钥文件;

利用所述车载公钥文件对所述加密数据和平台签名进行加密,得到所述虚拟钥匙。

2.根据权利要求1所述基于蓝牙钥匙的车辆分享系统,其特征在于,

所述分享信息包括分享时间、目标车辆和目标对象;

所述TSP服务平台具体用于:

接收所述分享信息;当所述目标对象为家人时,生成推送通知发送给所述目标对象对应的借车客户端;当所述目标对象为陌生人时,读取所述目标车辆的使用状态,如果目标车辆在分享时间内的状态为空闲时,生成推送通知发送给所述目标对象对应的借车客户端。

3.根据权利要求1所述基于蓝牙钥匙的车辆分享系统,其特征在于,

所述确认信息还包括目标车辆中车载T-BOX模块生成的车载公钥文件、用车权限和分享时间;

所述用车权限由车主输入的用车权限掩码和功能权限列表获得。

4.根据权利要求3所述基于蓝牙钥匙的车辆分享系统,其特征在于,

所述TSP服务平台还用于将所述虚拟钥匙发送给车主客户端;

所述车主客户端还用于实现与车载T-BOX模块之间的配对;车主客户端还用于接收车

主的控制指令，发送给车载T-BOX模块；

所述车载T-BOX模块还用于在与所述车主客户端配对成功后，建立与车主客户端的蓝牙通讯链路，接收车主客户端的控制指令，驱动车辆运行。

5.根据权利要求4所述基于蓝牙钥匙的车辆分享系统，其特征在于，

所述车主客户端具体用于：当检测到车辆的蓝牙设备时，向所述车载T-BOX模块发起鉴权请求，所述鉴权请求包括车主的用户名，车主客户端的IMEI码和车主客户端的证明文件；车主客户端当接收到鉴权成功指令后，建立与车载T-BOX模块的蓝牙通讯链路；

所述车载T-BOX模块具体用于，判断鉴权请求中的证明文件是否是可信CA服务器签发的；如果不是，断开与车主客户端的蓝牙连接；如果是，存储所述证明文件，生成鉴权成功指令，发送给所述车主客户端。

6.根据权利要求4所述基于蓝牙钥匙的车辆分享系统，其特征在于，

所述车主客户端具体用于接收车主的控制指令后，获取控制指令、车主输入的操作密码和虚拟钥匙，生成控制请求，发送给车载T-BOX模块；

所述车载T-BOX模块具体用于在接收到控制请求后，当对所述控制请求中的虚拟钥匙成功解密并验证解密后的数据合法时，根据所述控制指令驱动车辆运行。

7.根据权利要求1所述基于蓝牙钥匙的车辆分享系统，其特征在于，

所述车载T-BOX模块还用于在有网络信号后，根据控制请求生成事件通知，发送给所述TSP服务平台；

所述TSP服务平台用于将所述事件通知发送给车主客户端。

8.根据权利要求1-7中任一项所述基于蓝牙钥匙的车辆分享系统，其特征在于，

所述借车客户端或车主客户端具体用于在与车载T-BOX模块进行数据传输时，利用所述车载公钥文件对待发送数据进行加密后，发送给车载T-BOX模块；

所述车载T-BOX模块具体用于在与借车客户端或车主客户端进行数据传输时，利用所述证书文件对待发送数据进行加密后，发送给所述借车客户端或车主客户端。

基于蓝牙钥匙的车辆分享系统

技术领域

[0001] 本发明属于物联网技术领域，具体涉及基于蓝牙钥匙的车辆分享系统。

背景技术

[0002] 随着科技的发展，汽车作为人们的重要出行交通工具已经开始走入普通家庭。但是由于汽车尾气对空气的污染以及汽车过多从而产生的道路拥堵等问题越来越突出，因此，为了缓解这些问题，共享汽车渐渐出现在人们视野中。

[0003] 但是现在的共享汽车的模式主要有以下几种：

[0004] 一种是采用公司经营的方式，公司购买大量汽车，并招聘大量司机，乘客通过公司开发的共享平台下单用车，司机驾驶汽车来到乘客指定的位置搭载乘客，到达目的地后，付款完成本次用车服务。

[0005] 另一种是集合各种私家车到平台运营，乘客通过共享平台下单用车，私家车司机驾驶其自己的私家车到乘客指定的位置搭载乘客，到达目的地后，付款完成本次用车服务。

[0006] 不管是哪种方式的共享汽车，其还是停留在短时间、且出发地和目的地都确定的用车服务内容中，不能实现乘客长时间借车的需求。

发明内容

[0007] 针对现有技术中的缺陷，本发明提供基于蓝牙钥匙的车辆分享系统，为车主提供私家车共享服务，提高了私家车使用的安全性。

[0008] 一种基于蓝牙钥匙的车辆分享系统，包括：

[0009] 车主客户端用于接收车主输入的分享信息，根据所述分享信息生成分享请求，发送给TSP服务平台；

[0010] TSP服务平台用于对所述分享信息进行分析后，生成推送通知发送给借车客户端；TSP服务平台还用于在借车客户端接受推送通知后，生成确认信息发送给所述借车客户端；所述确认信息包括蓝牙配对密码；

[0011] 借车客户端用于接收借车人的接受指令，接受所述来自TSP服务平台的推送通知；借车客户端还用于接收确认信息，并利用蓝牙配对密码实现与车载T-BOX模块之间的配对；借车客户端还用于接收借车人的控制指令，发送给车载T-BOX模块；

[0012] 车载T-BOX模块安装于车辆上，用于在与所述借车客户端配对成功后，建立与借车客户端的蓝牙通讯链路，接收借车客户端的控制指令，驱动车辆运行。

[0013] 优选地，所述分享信息包括分享时间、目标车辆和目标对象；

[0014] 所述TSP服务平台具体用于：

[0015] 接收所述分享信息；当所述目标对象为家人时，生成推送通知发送给所述目标对象对应的借车客户端；当所述目标对象为陌生人时，读取所述目标车辆的使用状态，如果目标车辆在分享时间内的状态为空闲时，生成推送通知发送给所述目标对象对应的借车客户端。

[0016] 优选地，所述借车客户端还用于：在接受所述来自TSP服务平台的推送通知之后，创建操作密码或读取已保存的操作密码，根据所述操作密码和借车客户端的IMEI码生成接受确认反馈发送给TSP服务平台；

[0017] TSP服务平台还用于：接收所述接受确认反馈后，确定借车客户端接受所述推送通知。

[0018] 优选地，所述确认信息还包括虚拟钥匙；

[0019] 所述TSP服务平台具体用于：

[0020] 获取以下加密数据：目标对象的用户名、目标对象的身份标志位、目标车辆的车辆VIN码、车主输入的用车权限掩码、车主输入的功能权限列表、分享时间、操作密码和借车客户端的IMEI；

[0021] 获取借车客户端的证书文件，利用SHA256算法对所述证书文件进行加密，得到第一加密数据；

[0022] 利用MD5算法对所述加密数据和第一加密数据进行加密，得到第二加密数据；

[0023] 利用TSP服务平台预设的平台私钥文件对所述第二加密数据进行加密，得到平台签名；

[0024] 获取目标车辆中车载T-BOX模块生成的车载公钥文件；

[0025] 利用所述车载公钥文件对所述加密数据和平台签名进行加密，得到所述虚拟钥匙。

[0026] 优选地，所述确认信息还包括目标车辆中车载T-BOX模块生成的车载公钥文件、用车权限和分享时间；

[0027] 所述用车权限由车主输入的用车权限掩码和功能权限列表获得。

[0028] 优选地，所述TSP服务平台还用于将所述虚拟钥匙发送给车主客户端；

[0029] 所述车主客户端还用于实现与车载T-BOX模块之间的配对；车主客户端还用于接收车主的控制指令，发送给车载T-BOX模块；

[0030] 所述车载T-BOX模块还用于在与所述车主客户端配对成功后，建立与车主客户端的蓝牙通讯链路，接收车主客户端的控制指令，驱动车辆运行。

[0031] 优选地，所述车主客户端具体用于：当检测到车辆的蓝牙设备时，向所述车载T-BOX模块发起鉴权请求，所述鉴权请求包括车主的用户名，车主客户端的IMEI码和车主客户端的证明文件；车主客户端当接收到鉴权成功指令后，建立与车载T-BOX模块的蓝牙通讯链路；

[0032] 所述车载T-BOX模块具体用于，判断鉴权请求中的证明文件是否是可信CA服务器签发的；如果不是，断开与车主客户端的蓝牙连接；如果是，存储所述证明文件，生成鉴权成功指令，发送给所述车主客户端。

[0033] 优选地，所述车主客户端具体用于接收车主的控制指令后，获取控制指令、车主输入的操作密码和虚拟钥匙，生成控制请求，发送给车载T-BOX模块；

[0034] 所述车载T-BOX模块具体用于在接收到控制请求后，当对所述控制请求中的虚拟钥匙成功解密并验证解密后的数据合法时，根据所述控制指令驱动车辆运行。

[0035] 优选地，所述车载T-BOX模块还用于在有网络信号后，根据控制请求生成事件通知，发送给所述TSP服务平台；

[0036] 所述TSP服务平台用于将所述事件通知发送给车主客户端。

[0037] 优选地，所述借车客户端或车主客户端具体用于在与车载T-BOX模块进行数据传输时，利用所述车载公钥文件对待发送数据进行加密后，发送给车载T-BOX模块；

[0038] 所述车载T-BOX模块具体用于在与借车客户端或车主客户端进行数据传输时，利用所述证书文件对待发送数据进行加密后，发送给所述借车客户端或车主客户端。

[0039] 由上述技术方案可知，本发明提供的车辆分享系统，利用蓝牙技术实现借车人与车辆之间的控制，这样，即便是在网络较差的车库，也能够实现通过无线网络控制车辆的功能。同时该系统在借车过程中，不需要车主将车钥匙交给借车人，借车人才能使用。该系统车主通过TSP服务平台发出分享请求，借车人通过TSP服务平台接受分享请求，为车主提供私家车共享服务，在完成本次车辆分享后，借车人通过借车客户端就能够驱动车辆，无需TSP服务平台参与，使用方便。该系统还在借车客户端授权后，才能驱动车辆，提高了私家车使用的安全性。

附图说明

[0040] 为了更清楚地说明本发明具体实施方式或现有技术中的技术方案，下面将对具体实施方式或现有技术描述中所需要使用的附图作简单地介绍。在所有附图中，类似的元件或部分一般由类似的附图标记标识。附图中，各元件或部分并不一定按照实际的比例绘制。

[0041] 图1为本发明实施例一提供的车辆分享系统的分享方法流程图。

[0042] 图2为本发明实施例四提供的车主控制车辆的方法流程图。

[0043] 图3为本发明实施例五提供的借车人控制车辆的方法流程图。

[0044] 图4为本发明实施例七提供的车载T-BOX模块注册的方法流程图。

[0045] 图5为本发明实施例七提供的客户端注册的方法流程图。

[0046] 图6为本发明实施例八提供的客户端证书更新的方法流程图。

[0047] 图7为本发明实施例八提供的车载T-BOX模块的证书更新的方法流程图。

[0048] 图8为本发明实施例九提供的车主客户端绑定车辆的方法流程图。

具体实施方式

[0049] 下面将结合附图对本发明技术方案的实施例进行详细的描述。以下实施例仅用于更加清楚地说明本发明的技术方案，因此只作为示例，而不能以此来限制本发明的保护范围。需要注意的是，除非另有说明，本申请使用的技术术语或者科学术语应当为本发明所属领域技术人员所理解的通常意义。

[0050] 实施例一：

[0051] 一种基于蓝牙钥匙的车辆分享系统，参见图1，包括：

[0052] 车主客户端用于接收车主输入的分享信息，根据所述分享信息生成分享请求，发送给TSP服务平台；

[0053] 具体地，如果车主想要将自己的私家车租出去或分享出去时，可以在TSP服务平台上提交分享信息。

[0054] TSP服务平台用于对所述分享信息进行分析后，生成推送通知发送给借车客户端；TSP服务平台还用于在借车客户端接受推送通知后，生成确认信息发送给所述借车客户端；

所述确认信息包括蓝牙配对密码；

[0055] 具体地，TSP服务平台用于在接收到分享请求后，分析所述分享信息，分析的过程主要是判断分享信息是否填错或无效，如果分享请求正确或有效，此时可以向其他借车客户端推送该分享请求。推送时可以向指定一个或多个人推送，也可以推送给所有的借车客户端，也可以按照地区或时间进行推送。如果借车客户端接受推送通知后，TSP服务平台生成确认信息告诉借车人本次分享操作成功。

[0056] 借车客户端用于接收借车人的接受指令，接受所述来自TSP服务平台的推送通知；借车客户端还用于接收确认信息，并利用蓝牙配对密码实现与车载T-BOX模块之间的配对；借车客户端还用于接收借车人的控制指令，发送给车载T-BOX模块；

[0057] 具体地，如果借车人觉得TSP服务平台符合自己的要求时，可以接受TSP服务平台的推送。借车客户端在接收到确认信息后，可以根据分享请求在规定的时间内使用某车辆。借车客户端与目标车辆采用蓝牙技术进行通信。借车人通过借车客户端的蓝牙设备与车载T-BOX模块进行配对，如果配对成功，借车人可以通过借车客户端下发控制指令。所述借车客户端可以加载在智能终端(例如手机、平板等)上，也可以加载在可穿戴智能设备(例如智能手表)上。同一个用户可以使用多个移动设备对车辆进行控制。

[0058] 车载T-BOX模块安装于车辆上，用于在与所述借车客户端配对成功后，建立与借车客户端的蓝牙通讯链路，接收借车客户端的控制指令，与其它车身电子控制单元配合以驱动车辆运行。

[0059] 具体地，车载T-BOX模块接收到控制指令后，驱动车辆运行，例如车门的开锁、闭锁以及车辆的启动等操作。

[0060] 本实施例提供的基于蓝牙钥匙的车辆分享系统，利用蓝牙技术实现借车人与车辆之间的控制，客户端和车载T-BOX模块均无需连接互联网，即便是在网络较差的车库，也能够实现通过无线网络控制车辆的功能。同时该系统在借车过程中，不需要车主将车钥匙交给借车人，借车人才能使用。该系统车主通过TSP服务平台发出分享请求，借车人通过TSP服务平台接受分享请求，为车主提供私家车共享服务，在完成本次车辆分享后，借车人通过借车客户端就能够驱动车辆，无需TSP服务平台参与，使用方便。该系统还在借车客户端授权后，才能驱动车辆，提高了私家车使用的安全性。

[0061] 实施例二：

[0062] 实施例二在实施例一的基础上增加了不同借车人的借车流程：

[0063] 所述分享信息包括分享时间、目标车辆和目标对象；

[0064] 具体地，分享时间是由车主确认的，可以是几个小时、几天或几个月等。目标车辆为车主本次想要租出去的车辆，目标对象可以是家人、朋友或陌生人。分享信息还包括车主的用户名、手机号等信息。

[0065] 所述TSP服务平台具体用于：

[0066] 接收所述分享信息；当所述目标对象为家人时，生成推送通知发送给所述目标对象对应的借车客户端；当所述目标对象为陌生人时，读取所述目标车辆的使用状态，如果目标车辆在分享时间内的状态为空闲时，生成推送通知发送给所述目标对象对应的借车客户端。

[0067] 具体地，车主可以将车辆分享给家人、朋友或陌生人。家人可以具有和车主相同的

用车权限，无时间上的限制，任意家庭成员可以在任何时候使用车辆，所以如果借车人是家人的话，不做判断，直接生成推送通知发送给家人的借车客户端。

[0068] 如果是陌生人，则需要判断目标车辆在分享时间内是否空闲，如果空闲，表示目标车辆在分享时间内没人使用，可以分享。如果不是空闲状态，则不能分享。例如：如果车主分享车辆给两个陌生人且分享时间有交叉时，TSP服务平台在接收到第二个分享请求，此时车辆的状态为使用，TSP服务平台将拒绝第二个分享请求。普通借车人(朋友或陌生人)需要按照车主约定的用车权限和用车时间使用，且同一时段只能有一个借车人使用车辆。

[0069] 本发明实施例所提供的系统，为简要描述，实施例部分未提及之处，可参考前述系统实施例中相应内容。

[0070] 实施例三：

[0071] 实施例三在其他实施例的基础上增加了蓝牙钥匙的使用功能：

[0072] 所述借车客户端还用于：在接受所述来自TSP服务平台的推送通知之后，创建操作密码或读取已保存的操作密码，根据所述操作密码和借车客户端的IMEI码生成接受确认反馈发送给TSP服务平台；

[0073] TSP服务平台还用于：接收所述接受确认反馈后，确定借车客户端接受所述推送通知。

[0074] 具体地，操作密码为借车人设定的密码，可以是数字串、手势信息、指纹信息或虹膜信息。如果借车客户端是首次使用，需要创建操作密码，如果借车客户端之前已存在操作密码，则在接受推送通知之后，需要读取操作密码。TSP服务平台用于保存操作密码和借车客户端的IMEI码。

[0075] 所述确认信息还包括虚拟钥匙；

[0076] 所述TSP服务平台具体用于：

[0077] 获取以下加密数据：目标对象的用户名、目标对象的身份标志位、目标车辆的车辆VIN码、车主输入的用车权限掩码、车主输入的功能权限列表、分享时间、操作密码和借车客户端的IMEI；

[0078] 获取借车客户端的证书文件，利用SHA256算法对所述证书文件进行加密，得到第一加密数据；

[0079] 利用MD5算法对所述加密数据和第一加密数据进行加密，得到第二加密数据；

[0080] 利用TSP服务平台预设的平台私钥文件对所述第二加密数据进行加密，得到平台签名；

[0081] 获取目标车辆中车载T-BOX模块生成的车载公钥文件；

[0082] 利用所述车载公钥文件对所述加密数据和平台签名进行加密，得到所述虚拟钥匙。

[0083] 具体地，TSP服务平台记录车辆分享信息，为借车客户端和目标车辆生成一个虚拟钥匙，虚拟钥匙由车载T-BOX模块的车载公钥文件加密，内容包含：目标对象的用户名、目标对象的身份标志位、目标车辆的车辆VIN码、车主输入的用车权限掩码、车主输入的功能权限列表、分享时间、操作密码和借车客户端的IMEI等，即：

[0084] 虚拟钥匙＝车载公钥加密(目标对象的用户名，目标车辆的车辆VIN码，目标对象的身份标志位，车主输入的用车权限掩码，车主输入的功能权限列表，分享时间，操作密码，

借车客户端的IMEI,MD5加密(借车客户端的证书文件),平台签名)；

[0085] 其中:目标对象的身份标志位为0,平台签名为：

[0086] 平台签名＝平台私钥加密(MD5(目标对象的用户名,目标车辆的车辆VIN码,目标对象的身份标志位,车主输入的用车权限掩码,车主输入的功能权限列表,分享时间,操作密码,借车客户端的IMEI,SHA256(借车客户端的证书文件)))。

[0087] 这样,该系统的各网元间通过非对称加密机制通信,证书秘钥加密存储并定期更换,防止被破解和盗用。

[0088] 确认信息除了包括蓝牙配对密码和虚拟钥匙以外,还包括目标车辆中车载T-BOX模块生成的车载公钥文件、用车权限和分享时间；

[0089] 所述用车权限由车主输入的用车权限掩码和功能权限列表获得。

[0090] 具体地,借车客户端在接收到确认信息后,具备了连接和控制目标车辆的能力。

[0091] 本发明实施例所提供的系统,为简要描述,实施例部分未提及之处,可参考前述系统实施例中相应内容。

[0092] 实施例四：

[0093] 实施例四在实施例三的基础上,增加了车主使用蓝牙钥匙连接和控制车辆的能力。

[0094] 本实施例的系统中,车主也可以通过车主客户端连接并控制车辆。车主使用的虚拟钥匙和借车人使用的虚拟钥匙生成方法相同,只是采集的数据不同,车主使用的虚拟钥匙通过以下方法获得：

[0095] TSP服务平台获取以下加密数据:车主的用户名、车主的身份标志位、车辆的车辆VIN码、车主输入的用车权限掩码、车主输入的功能权限列表、车主输入的使用时间、车主输入的操作密码和车主客户端的IMEI；

[0096] 获取车主客户端的证书文件,利用SHA256算法对所述证书文件进行加密,得到第三加密数据；

[0097] 利用MD5算法对所述加密数据和第三加密数据进行加密,得到第四加密数据；

[0098] 利用TSP服务平台预设的平台私钥文件对所述第四加密数据进行加密,得到平台签名；

[0099] 获取车辆中车载T-BOX模块生成的车载公钥文件；

[0100] 利用所述车载公钥文件对所述加密数据和平台签名进行加密,得到车主使用的虚拟钥匙。

[0101] 车主在连接车辆时,所述TSP服务平台还用于将虚拟钥匙发送给车主客户端；

[0102] 所述车主客户端还用于实现与车载T-BOX模块之间的配对;车主客户端还用于接收车主的控制指令,发送给车载T-BOX模块；

[0103] 所述车载T-BOX模块还用于在与所述车主客户端配对成功后,建立与车主客户端的蓝牙通讯链路,接收车主客户端的控制指令,驱动车辆运行。

[0104] 具体地,车主客户端在建立与车载T-BOX模块之间的连接后,同样,车主可以通过车主客户端发出控制指令,车载T-BOX模块在接收到车主客户端的控制指令后,同借车人一样,可以驱动车辆运行。

[0105] 参见图2,所述车主客户端具体用于:当检测到车辆的蓝牙设备时,向所述车载T-

BOX模块发起鉴权请求,所述鉴权请求包括车主的用户名,车主客户端的IMEI码和车主客户端的证明文件;车主客户端当接收到鉴权成功指令后,建立与车载T-BOX模块的蓝牙通讯链路;

[0106] 所述车载T-BOX模块具体用于,判断鉴权请求中的证明文件是否是可信CA服务器签发的;如果不是,断开与车主客户端的蓝牙连接;如果是,存储所述证明文件,生成鉴权成功指令,发送给所述车主客户端。

[0107] 具体地,车主开启车主客户端,当车主靠近车辆后,车主客户端将使用之前从TSP服务平台获取的蓝牙配对密码与车载T-BOX模块建立蓝牙安全连接。

[0108] 车主客户端发起鉴权请求,请求中包含车主的用户名、车主客户端的IMEI、车主客户端的证明文件user.crt,车载T-BOX模块检查user.crt是否由可信CA服务器签发,如果是暂存用户名和user.crt,向车主客户端回复鉴权成功消息。车主客户端收到鉴权成功消息后,在界面上允许车主对车辆进行操作。

[0109] 所述车主客户端具体用于接收车主的控制指令后,获取控制指令、车主输入的操作密码和虚拟钥匙,生成控制请求,发送给车载T-BOX模块;

[0110] 所述车载T-BOX模块具体用于在接收到控制请求后,当对所述控制请求中的虚拟钥匙成功解密并验证解密后的数据合法时,根据所述控制指令驱动车辆运行。

[0111] 具体地,例如:车主在车主客户端中点击“解锁车门”等指令按钮,输入操作密码后,车主客户端将指令ID、指令参数(指令ID和指令参数均由控制指令得到)、操作密码、虚拟钥匙、当前日期时间等信息加密后发送给车载T-BOX模块。其中,操作密码单独用车主客户端的私钥userPrivate.key进行加密。即:

[0112] 控制请求=车载公钥文件加密(指令ID,指令参数,车主客户端私钥文件加密(操作密码),虚拟钥匙,当前日期时间,其他干扰字符串);

[0113] 车载T-BOX模块收到控制请求后,进行如下操作:

[0114] 用车载私钥tboxPrivate.key解密整个控制请求;

[0115] 确认控制请求的日期时间和自身当前时间的差值是否在允许范围内(如5秒);

[0116] 如果是,用本地暂存的user.crt解密出操作密码;

[0117] 用车载私钥tboxPrivate.key解密并检查虚拟钥匙:

[0118] 验证虚拟钥匙中的签名信息是否来自可信平台,具体包括:

[0119] 比对虚拟钥匙中的用户名、VIN、操作密码、设备IMEI、user.crt的MD5值是否和控制请求的信息匹配;

[0120] 确认当前指令ID、请求参数是否满足虚拟钥匙中用户身份标识位、基础控制权限掩码、功能限制列表、用车时间范围的要求。

[0121] 如果上述校验均通过,则车载T-BOX模块认为该控制请求来自可信的车主客户端且满足控制权限,随后和车辆ECU交互完成车门解锁等操作。

[0122] 本发明实施例所提供的系统,为简要描述,实施例部分未提及之处,可参考前述系统实施例中相应内容。

[0123] 实施例五:

[0124] 实施例五在实施例三的基础上,增加了借车人使用蓝牙钥匙连接和控制目标车辆的能力。

[0125] 参见图3,所述借车客户端具体用于:当检测到目标车辆的蓝牙设备时,向所述车载T-BOX模块发起鉴权请求,所述鉴权请求包括借车人的用户名,借车客户端的IMEI码和借车客户端的证明文件;借车客户端当接收到鉴权成功指令后,建立与车载T-BOX模块的蓝牙通讯链路;

[0126] 所述车载T-BOX模块具体用于,判断鉴权请求中的证明文件是否是可信CA服务器签发的;如果不是,断开与借车客户端的蓝牙连接;如果是,存储所述证明文件,生成鉴权成功指令,发送给所述借车客户端。

[0127] 具体地,借车人开启借车客户端,当借车人靠近目标车辆后,借车客户端将使用之前从TSP服务平台获取的蓝牙配对密码与车载T-BOX模块建立蓝牙安全连接。

[0128] 借车客户端发起鉴权请求,请求中包含借车人的用户名、借车客户端的IMEI、借车客户端的证明文件user.crt,车载T-BOX模块检查user.crt是否由可信CA服务器签发,如果是则暂存用户名和user.crt,向借车客户端回复鉴权成功消息。借车客户端收到鉴权成功消息后,在界面上允许借车人对车辆进行操作。

[0129] 所述借车客户端具体用于接收借车人的控制指令后,获取控制指令、借车人输入的操作密码和虚拟钥匙,生成控制请求,发送给车载T-BOX模块;

[0130] 所述车载T-BOX模块具体用于在接收到控制请求后,当对所述控制请求中的虚拟钥匙成功解密并验证解密后的数据合法时,根据所述控制指令驱动车辆运行。

[0131] 具体地,例如:借车人在借车客户端中点击“解锁车门”等指令按钮,输入操作密码后,借车客户端将指令ID、指令参数(指令ID和指令参数均由控制指令得到)、操作密码、虚拟钥匙、当前日期时间等信息加密后发送给车载T-BOX模块。其中,操作密码单独用借车客户端的私钥userPrivate.key进行加密。即:

[0132] 控制请求=车载公钥文件加密(指令ID,指令参数,借车客户端私钥文件加密(操作密码),虚拟钥匙,当前日期时间,其他干扰字符串);

[0133] 车载T-BOX模块收到控制请求后,进行如下操作:

[0134] 用车载私钥tboxPrivate.key解密整个控制请求;

[0135] 确认控制请求的日期时间和自身当前时间的差值是否在允许范围内(如5秒);

[0136] 如果是,用本地暂存的user.crt解密出操作密码;

[0137] 用车载私钥tboxPrivate.key解密并检查虚拟钥匙:

[0138] 验证虚拟钥匙中的签名信息是否来自可信平台,具体包括:

[0139] 比对虚拟钥匙中的用户名、VIN、操作密码、设备IMEI、user.crt的MD5值是否和控制请求的信息匹配;

[0140] 确认当前指令ID、请求参数是否满足虚拟钥匙中用户身份标识位、基础控制权限掩码、功能限制列表、用车时间范围的要求。

[0141] 如果上述校验均通过,则车载T-BOX模块认为该控制请求来自可信的借车客户端且满足控制权限,随后和车辆ECU交互完成车门解锁等操作。

[0142] 该系统拥有便捷、安全、灵活的车辆租借流程,车主确认借车人的权限/时间范围,同时能够随时得到车辆的关键事件通知,例如车门解锁、启动等,及时处理异常用车情况。

[0143] 本发明实施例所提供的系统,为简要描述,实施例部分未提及之处,可参考前述系统实施例中相应内容。

[0144] 实施例六：

[0145] 实施例六在其他实施例的基础上，增加以下内容：

[0146] 所述车载T-BOX模块还用于在有网络信号后，根据控制请求生成事件通知，发送给所述TSP服务平台；

[0147] 所述TSP服务平台用于将所述事件通知发送给车主客户端。

[0148] 具体地，车载T-BOX模块可以在有网络信号的前提下，将控制请求发送给TSP服务平台，通过TSP服务平台发送给车主，方便车主实时监控到车辆的使用情况。

[0149] 优选地，所述借车客户端或车主客户端具体用于在与车载T-BOX模块进行数据传输时，利用所述车载公钥文件对待发送数据进行加密后，发送给车载T-BOX模块；

[0150] 所述车载T-BOX模块具体用于在与借车客户端或车主客户端进行数据传输时，利用所述证书文件对待发送数据进行加密后，发送给所述借车客户端或车主客户端。

[0151] 具体地，借车客户端或车主客户端和车载T-BOX模块进行数据传输时，均需要对传输数据进行加密后传输，客户端和车载T-BOX模块间进行双向认证，控制消息采用双重混合加密机制，防止黑客窃听、破解和重放，保障车辆安全。

[0152] 本发明实施例所提供的系统，为简要描述，实施例部分未提及之处，可参考前述系统实施例中相应内容。

[0153] 实施例七：

[0154] 实施例七在其他实施例的基础上，增加了车载T-BOX模块和客户端注册和注销的内容。

[0155] 1、车载T-BOX模块注册。

[0156] 参见图4，车载T-BOX模块在出厂时，预存车厂CA服务器的根证书、TSP服务平台的地址及证书信息，其中TSP服务平台的证书由车厂CA服务器签发。当车载T-BOX模块首次接入网络时，向TSP服务平台进行基本信息注册，基本信息包括设备编号、ICCID、SIM卡号、VIN等。车载T-BOX模块在注册成功后自行生成车载私钥文件并加密保存。车载私钥文件可以保存在车载T-BOX模块的硬件加密芯片中，或分散加密保存到车载T-BOX模块的存储器中。文件的加/解密密码每个车载T-BOX模块不同，如用ICCID+设备编号+SIM卡号+混淆字符串等。

[0157] 车载T-BOX模块用车载私钥文件生成车载公钥文件，然后生成6位随机数字的蓝牙配对密码，与TSP服务平台建立单向HTTPS/TLS安全连接，将车载公钥文件、蓝牙配对密码发到TSP服务平台。

[0158] 2、客户端注册。

[0159] 参见图5，客户端包括车主客户端和借车客户端。客户端中预存车厂CA服务器的根证书、TSP服务平台的地址及证书信息，其中TSP服务平台的证书由车厂CA服务器签发。客户端启动后与TSP服务平台建立单向HTTPS安全连接，用户(车主或借车人)进行如下操作：

[0160] 用户若为新用户，则创建用户信息，所述用户信息包括登录客户端的用户名和密码，通过实名制认证和手机号验证，完成账户注册。若用户已有客户端账户，直接输入用户名和密码进行登录。

[0161] 客户端为当前账户名生成客户端私钥文件userPrivate.key并加密保存，用客户端私钥文件生成证书请求文件user.csr，将user.csr文件发到TSP服务平台。客户端私钥文件需加密保存的移动设备的安全存储区中。

[0162] TSP服务平台通过CA服务器签发证书文件user.crt,TSP服务平台将user.crt返回给客户端,同时将用户当前设备的user.crt和有效期保存到用户数据库中。用户可以用同一个账户在多个移动设备上登录客户端,TSP服务平台将保存同一账户所有设备的user.crt和有效期。user.crt中包含了车厂CA服务器的签名信息,有效期为3年或车厂自定义。

[0163] 客户端保存证书文件user.crt,作为后续车载T-BOX模块和客户端通信时的身份认证信息和加密公钥。在同一个移动设备的客户端中,不同的账户将产生不同的私钥和证书文件。

[0164] 该系统,车厂独立管控TSP服务平台和CA服务器,通过数字证书管理和校验网元身份,把握安全核心。系统还可以与车厂深度合作,开发出各种提升用户体验的人性化功能,例如使用者靠近车辆时开启迎宾灯光等;同时,还能进一步细化的车辆使用的权限策略,例如车主能定义不同借车人的速度限制、地理范围、车内乘客人数限制、是否仅允许访问后备箱等,从而应对更多的使用场景和商业模式。

[0165] 3、客户端注销。

[0166] 当用户的某个移动设备丢失或弃用后,需完成设备注销流程以保证车辆安全。注销的流程如下:

[0167] 客户端接收用户的操作指令,操作指令为用户在客户端中删除属于自己用户名的某个设备(即待注销设备),客户端向TSP服务平台发送设备注销请求。

[0168] TSP服务平台删除该设备的IMEI、证书、虚拟钥匙信息,自动创建任务向车载T-BOX模块下发设备注销通知。

[0169] 车载T-BOX模块在有网络信号的情况下接收通知消息,把注销设备的用户名、IMEI列入黑名单,不再接受该设备的连接鉴权请求。

[0170] 本发明实施例所提供的系统,为简要描述,实施例部分未提及之处,可参考前述系统实施例中相应内容。

[0171] 实施例八:

[0172] 实施例八在其他实施例的基础上,增加了证书更新的内容。

[0173] 在需要时,TSP服务平台可以自动或由人工触发一次客户端和车载T-BOX模块的证书批量更新操作,具体流程为:

[0174] 1、客户端证书更新:

[0175] 参见图6,TSP服务平台向客户端下发推送消息,在客户端下一次打开时生成新的私钥userPrivate.key和证书请求文件user.csr,向平台发起证书签发请求;

[0176] TSP服务平台经CA服务器后向客户端下发新的user.crt证书文件;

[0177] 客户端根据当前绑定/借用的车辆情况,向平台发起更新虚拟钥匙的请求;

[0178] TSP服务平台根据新的user.crt生成新的虚拟钥匙,回复给客户端;

[0179] 客户端保存新的证书和虚拟钥匙到安全存储区,删除旧的私钥、证书和虚拟钥匙。客户端后续使用新的证书和虚拟钥匙和车载T-BOX模块通信。

[0180] 2、车载T-BOX模块的证书更新:

[0181] 参见图7,TSP服务平台通过OTA任务的形式向车载T-BOX模块下发证书更新消息,车载T-BOX模块接收后生成新的私钥和公钥文件,将公钥文件发给TSP服务平台;

[0182] TSP服务平台保存车载T-BOX模块的新公钥文件，为目前车辆绑定的所有车主/借车人生成新的虚拟钥匙，并向各设备的客户端下发推送消息；

[0183] 车主/借车客户端更新车载T-BOX模块的公钥、虚拟钥匙，删除旧的公钥、虚拟钥匙。

[0184] 车载T-BOX模块在一段时间内(如1个月)保留旧的私钥、公钥，以应对无网络时客户端用旧的T-BOX公钥、虚拟钥匙连接车辆的情况。

[0185] 本发明实施例所提供的系统，为简要描述，实施例部分未提及之处，可参考前述系统实施例中相应内容。

[0186] 实施例九：

[0187] 实施例九在其他实施例的基础上，增加了车主客户端绑定车辆的功能。

[0188] 参见图8，车厂为每辆车提供一个包含车辆身份信息的二维码，印在车辆保修卡或显示在中控大屏的特定界面中。

[0189] 车主用车主客户端扫描该二维码进行车辆绑定，创建该车的操作密码(6位数字)，车主客户端将车辆绑定请求消息发给TSP服务平台。一个车主可以绑定多辆车，每辆车需单独设置操作密码。当车主需要用车主客户端解锁车门、启动车辆时需要输入操作密码。一辆车只能被一个车主绑定。

[0190] TSP服务平台在数据库中存储车辆绑定请求，包括车主用户名、密码、绑定的车辆列表、各车辆的操作密码、同一车主不同移动设备的user.crt及有效期。

[0191] TSP服务平台向车主客户端回复车辆绑定成功消息，消息中包含车载T-BOX模块的公钥、蓝牙配对密码、虚拟钥匙，车主客户端将蓝牙配对密码、虚拟钥匙保存到安全存储区中。此时，车主客户端绑定车辆完成，具备连接和控制车辆的能力。

[0192] 本发明实施例所提供的系统，为简要描述，实施例部分未提及之处，可参考前述系统实施例中相应内容。

[0193] 实施例十：

[0194] 实施例十在其他实施例的基础上，增加了以下的扩展功能。

[0195] 1、车辆自动识别驾驶者。

[0196] 当车辆使用者(车主/借车人)进入车载T-BOX模块蓝牙信号通信范围时，客户端自动与车载T-BOX模块建立蓝牙连接、完成鉴权流程，此时车载T-BOX模块可以判断移动设备蓝牙信号的强弱，来确定使用者是否正在接近车辆，并与车辆ECU联动为使用者提供各种人性化服务。例如：

[0197] 当车载T-BOX模块识别到使用者距离车辆较近时(如10米)，车外照明系统自动亮起，帮助使用者在夜晚更容易确认汽车位置和进入车内；

[0198] 当识别到使用者里车辆很近时(如3米)，车辆迎宾灯光开启；

[0199] 车载T-BOX模块根据user.crt自动识别使用者身份，并按照使用者的习惯自动完成调节座椅位置、启动空调及娱乐系统等个性化设置；

[0200] 当车辆启动时，语音系统可以用用户在客户端中事先设置好的昵称和用户打招呼，以及继续后续的语音交互控制；

[0201] 车载T-BOX模块可以将每个使用者的驾驶习惯单独发送给TSP服务平台，实现基于用户的驾驶行为分析，而非基于车辆的驾驶行为分析。

[0202] 在车辆熄火的情况下，当车载T-BOX模块通过蓝牙信号强弱检测到使用者正在远离车辆，并且距离足够远时(如2米)，与车辆ECU联动完成自动升窗和车门锁止，使用者无需手动进行锁车操作。

[0203] 2、细化的用车权限策略。

[0204] 车主通过车主客户端可以设置多种用车权限策略，并分配给不同的借车人。除了基本的车门解锁/锁止、启动车辆、使用时间段等权限外，可扩展如下使用限制：

[0205] 车辆速度限制：对于有不良驾驶习惯或驾驶经验不足的借车人，可以使用限速的方式在一定程度上确保车辆行驶的安全；

[0206] 地理范围限制：对特定的借车人设置不同的地理范围，例如泊车员只能将车开到100米范围内的停车场中，如果超过范围车主将收到短信、客户端推送通知提醒，同时车辆也将在合适的条件下自动熄火；

[0207] 车内乘客人数限制：结合车座上的压力传感器，可有效检测和防止用车人超载行驶；

[0208] 是否仅允许访问后备箱：赋予指定快递员该权限后，可以实现快递员将包裹放入车主车辆后备箱，车主稍后到车中取件的应用场景。

[0209] 3、远程动力锁止。

[0210] 当车主收到来自TSP服务平台的短信、客户端推送通知，确认当前车辆正被非法使用时，可以立即通过客户端和平台向车载T-BOX模块下发远程动力锁止指令，使车辆无法继续行驶，或无法再次启动。

[0211] 4、防止车载T-BOX模块被非法破坏。

[0212] 为防止非法用户拆卸、破坏、篡改车载T-BOX模块，车辆ECU在收到启动指令时，如果检测不到车载T-BOX模块的特定CAN报文，则拒绝启动车辆，防止车辆被盗用。

[0213] 本发明实施例所提供的系统，为简要描述，实施例部分未提及之处，可参考前述系统实施例中相应内容。

[0214] 最后应说明的是：以上各实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述各实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分或者全部技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的范围，其均应涵盖在本发明的权利要求和说明书的范围当中。

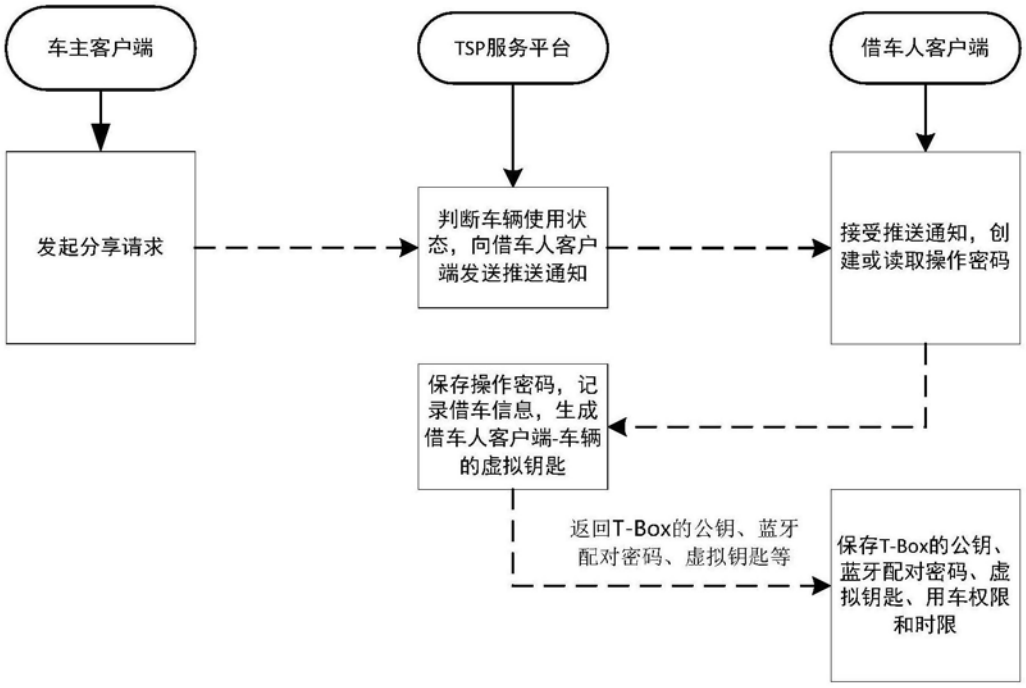

车主客户端
TSP服务平台
借车人客户端
发起分享请求
判断车辆使用状态，向借车人客户端发送推送通知
接受推送通知，创建或读取操作密码
保存操作密码，记录借车信息，生成借车人客户端-车辆的虚拟钥匙
返回T-Box的公钥、蓝牙配对密码、虚拟钥匙等
保存T-Box的公钥、蓝牙配对密码、虚拟钥匙、用车权限和时限

图1

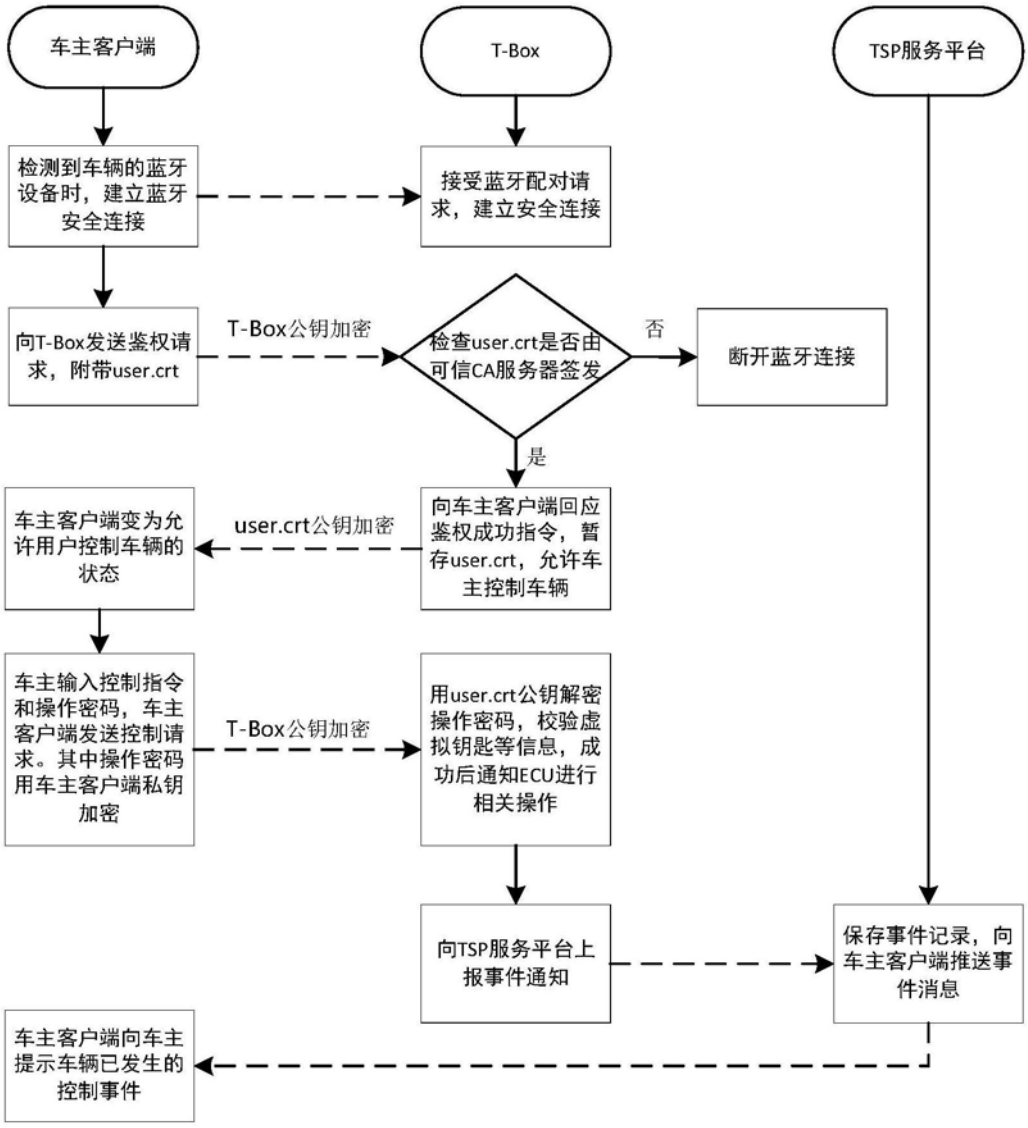

车主客户端
T-Box
TSP服务平台
检测到车辆的蓝牙设备时，建立蓝牙安全连接
接受蓝牙配对请求，建立安全连接
向T-Box发送鉴权请求，附带user.crt
T-Box公钥加密
检查user.crt是否由可信CA服务器签发
否
断开蓝牙连接
是
车主客户端变为允许用户控制车辆的状态
user.crt公钥加密
向车主客户端回应鉴权成功指令，暂存user.crt，允许车主控制车辆
车主输入控制指令和操作密码，车主客户端发送控制请求。其中操作密码用车主客户端私钥加密
T-Box公钥加密
用user.crt公钥解密操作密码，校验虚拟钥匙等信息，成功后通知ECU进行相关操作
向TSP服务平台上报事件通知
保存事件记录，向车主客户端推送事件消息
车主客户端向车主提示车辆已发生的控制事件

图2

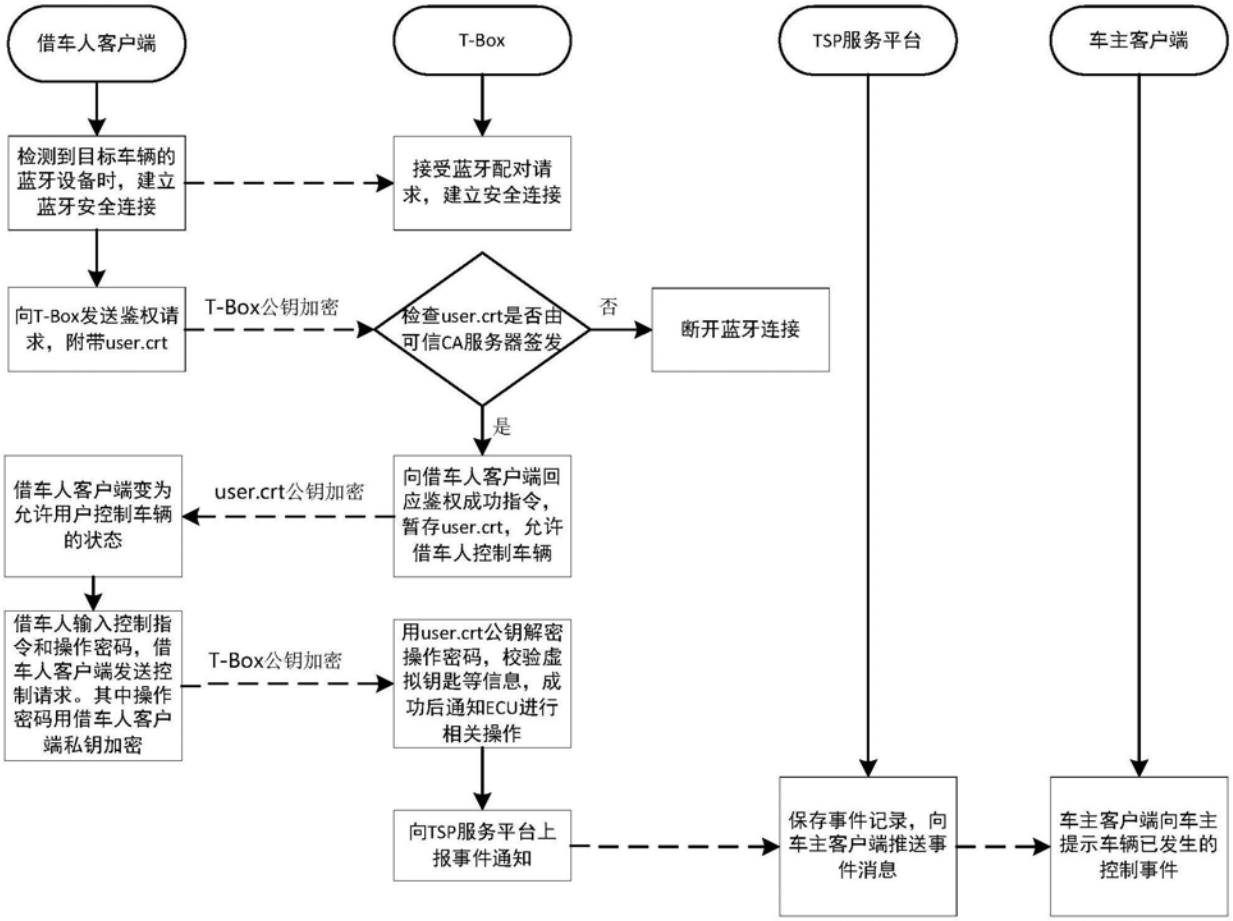

借车人客户端
T-Box
TSP服务平台
车主客户端
检测到目标车辆的蓝牙设备时，建立蓝牙安全连接
接受蓝牙配对请求，建立安全连接
向T-Box发送鉴权请求，附带user.crt
T-Box公钥加密
检查user.crt是否由可信CA服务器签发
否
断开蓝牙连接
是
借车人客户端变为允许用户控制车辆的状态
user.crt公钥加密
向借车人客户端回应鉴权成功指令，暂存user.crt，允许借车人控制车辆
借车人输入控制指令和操作密码，借车人客户端发送控制请求。其中操作密码用借车人客户端私钥加密
T-Box公钥加密
用user.crt公钥解密操作密码，校验虚拟钥匙等信息，成功后通知ECU进行相关操作
向TSP服务平台上报事件通知
保存事件记录，向车主客户端推送事件消息
车主客户端向车主提示车辆已发生的控制事件

图3

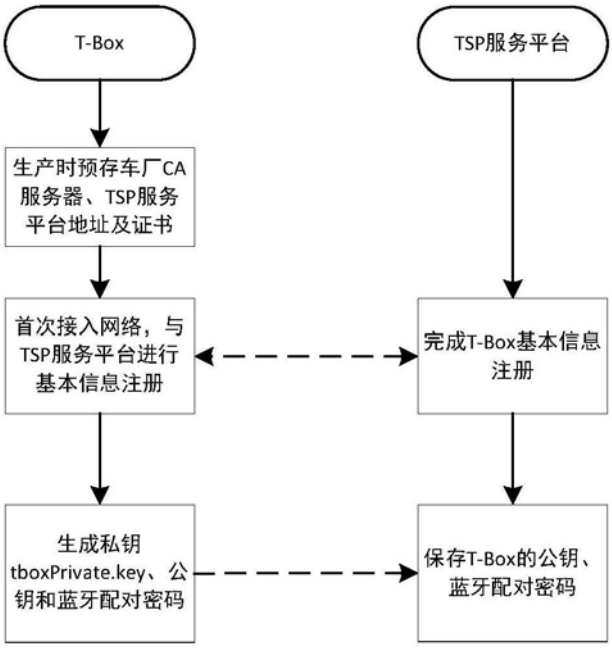

T-Box
TSP服务平台
生产时预存车厂CA服务器、TSP服务平台地址及证书
首次接入网络，与TSP服务平台进行基本信息注册
完成T-Box基本信息注册
生成私钥tboxPrivate.key、公钥和蓝牙配对密码
保存T-Box的公钥、蓝牙配对密码

图4

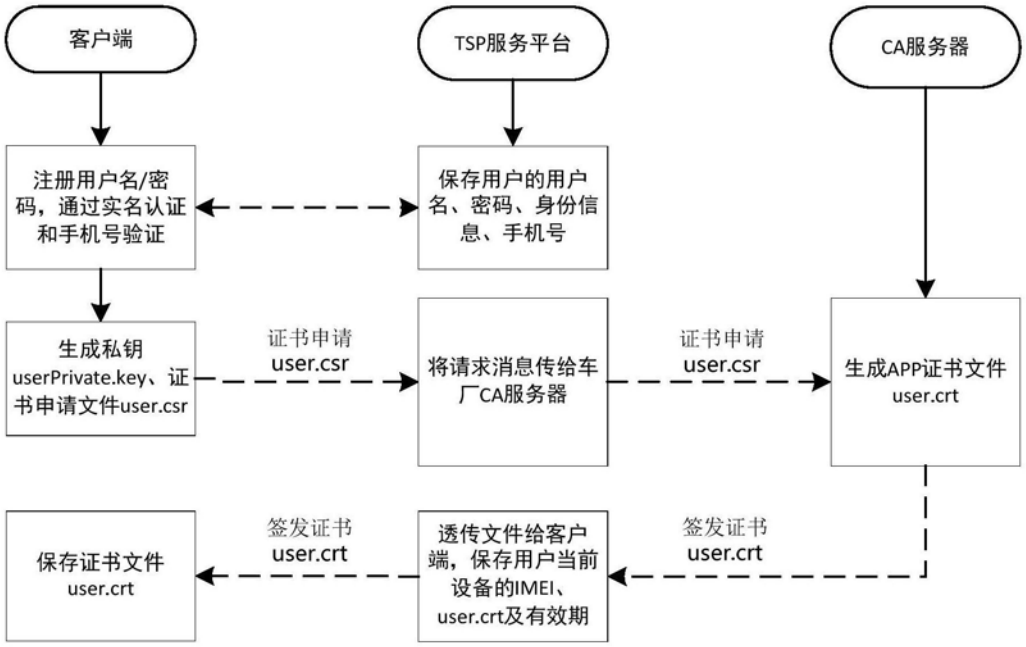

客户端
TSP服务平台
CA服务器
注册用户名/密码，通过实名认证和手机号验证
保存用户的用户名、密码、身份信息、手机号
生成私钥userPrivate.key、证书申请文件user.csr
证书申请user.csr
将请求消息传给车厂CA服务器
证书申请user.csr
生成APP证书文件user.crt
保存证书文件user.crt
签发证书user.crt
透传文件给客户端，保存用户当前设备的IMEI、user.crt及有效期
签发证书user.crt

图5

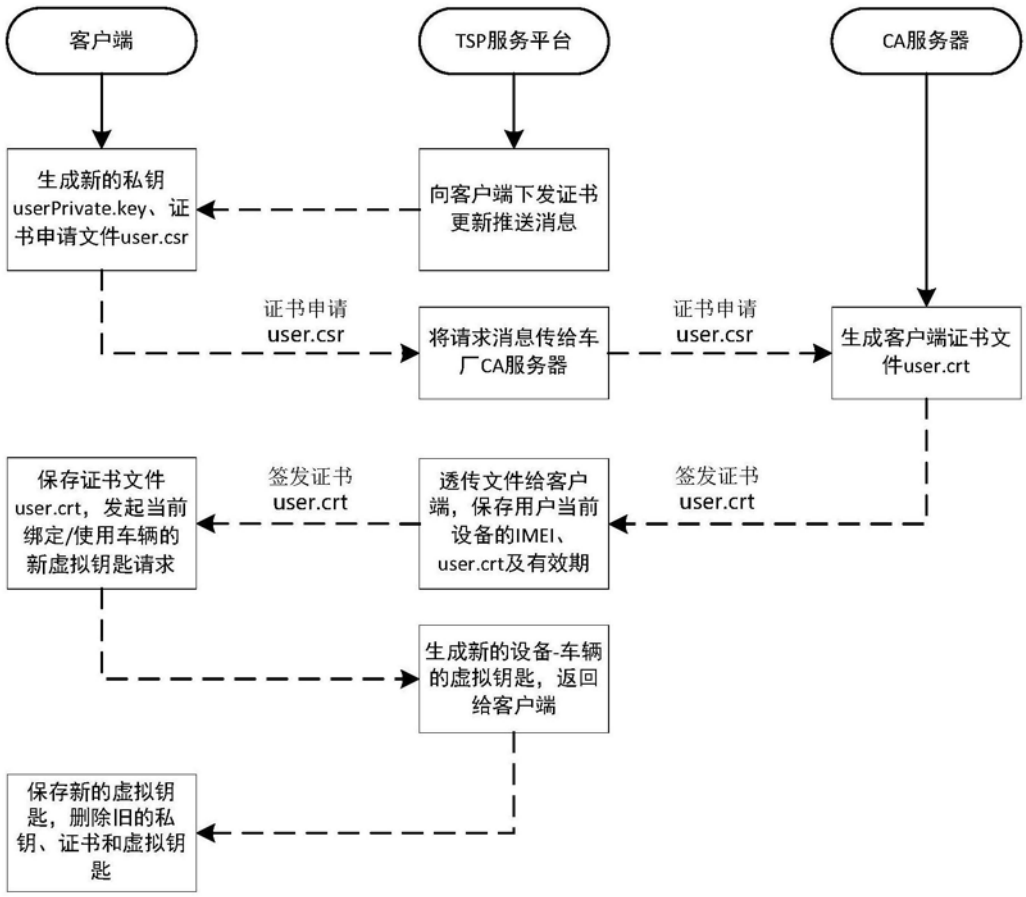

客户端
TSP服务平台
CA服务器
生成新的私钥userPrivate.key、证书申请文件user.csr
向客户端下发证书更新推送消息
证书申请user.csr
将请求消息传给车厂CA服务器
证书申请user.csr
生成客户端证书文件user.crt
保存证书文件user.crt，发起当前绑定/使用车辆的新虚拟钥匙请求
签发证书user.crt
透传文件给客户端，保存用户当前设备的IMEI、user.crt及有效期
签发证书user.crt
生成新的设备-车辆的虚拟钥匙，返回给客户端
保存新的虚拟钥匙，删除旧的私钥、证书和虚拟钥匙

图6

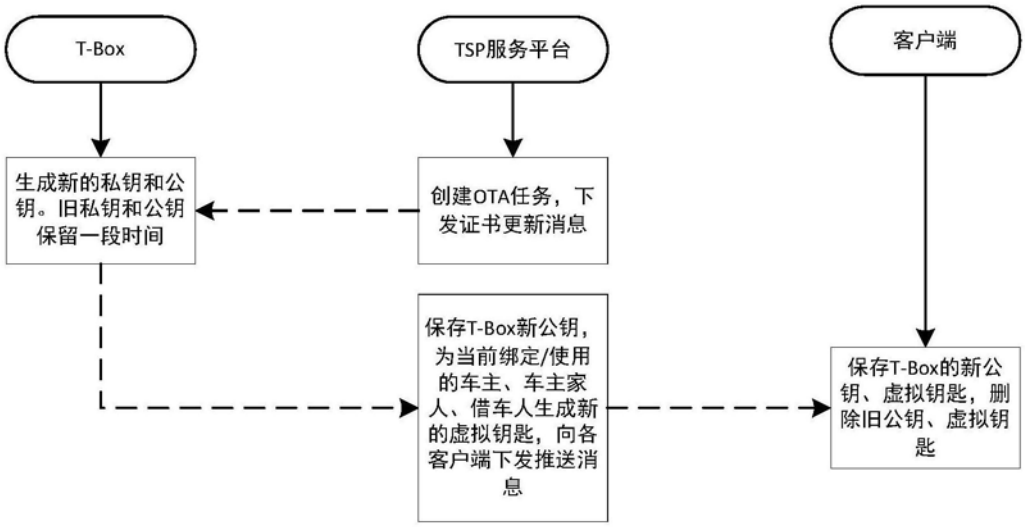

T-Box
TSP服务平台
客户端
生成新的私钥和公钥。旧私钥和公钥保留一段时间
创建OTA任务，下发证书更新消息
保存T-Box新公钥，为当前绑定/使用的车主、车主家人、借车人生成新的虚拟钥匙，向各客户端下发推送消息
保存T-Box的新公钥、虚拟钥匙，删除旧公钥、虚拟钥匙

图7

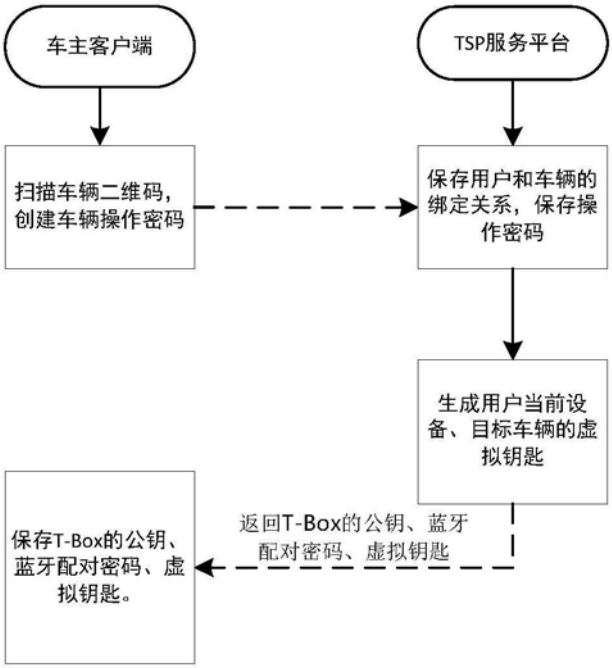

车主客户端
TSP服务平台
扫描车辆二维码，创建车辆操作密码
保存用户和车辆的绑定关系，保存操作密码
生成用户当前设备、目标车辆的虚拟钥匙
返回T-Box的公钥、蓝牙配对密码、虚拟钥匙
保存T-Box的公钥、蓝牙配对密码、虚拟钥匙。

图8