(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 118020070 A
(43)申请公布日 2024.05.10

(21)申请号 202280065467.7
(22)申请日 2022.09.27
(30)优先权数据
2021-159414 2021.09.29 JP
(85)PCT国际申请进入国家阶段日
2024.03.27
(86)PCT国际申请的申请数据
PCT/JP2022/035811 2022.09.27
(87)PCT国际申请的公布数据
WO2023/054297 JA 2023.04.06
(71)申请人 株式会社电装
地址 日本
申请人 艾德米亚法国公司
(72)发明人 松下杰 马雷克·科切茨基 米夏尔·瓦西莱夫斯基 菲利普·莱特 鲍特洛米耶·莱温斯基
(74)专利代理机构 北京集佳知识产权代理有限公司 11227
专利代理师 金雪梅
(51)Int.Cl.
G06F 21/44(2006.01)
B60R 25/24(2006.01)
H04L 9/08(2006.01)
H04L 9/32(2006.01)

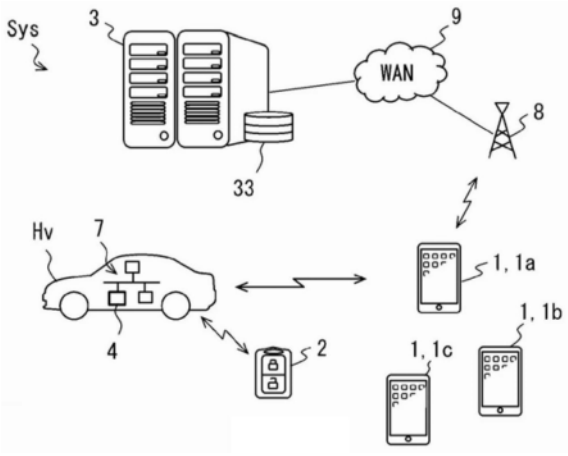
权利要求书4页 说明书34页 附图19页

(54)发明名称

车辆用数字钥匙系统、车辆用数字钥匙管理方法、车辆用装置、移动终端

(57)摘要

本申请的服务器基于来自移动终端的请求，发放用于使用指定的车辆的服务密钥、和多个一次性认证密钥，并分发至移动终端。一次性认证密钥是基于服务密钥生成的一次性的认证密钥，设定有有效期限。一次性认证密钥在车辆用装置认证作为通信对象的移动终端时被消耗。移动终端随时更换自身保持的一次性认证密钥。



CN 118020070 A

1.一种车辆用数字钥匙系统,包含:

车辆用装置(4),搭载于车辆使用;

移动终端(1),是由用户携带的信息处理终端;以及

服务器(3),生成每个上述移动终端固有的服务密钥作为用于使用上述车辆的密钥信息,并将上述密钥信息直接地或者间接地分发至上述移动终端以及上述车辆用装置,

上述车辆用装置构成为使用基于上述服务密钥生成的一次性的一次性认证密钥判断上述移动终端的合法性,

上述服务器基于来自上述移动终端的请求,生成多个上述一次性认证密钥,并带有效期限地分发至上述移动终端,

上述移动终端从上述服务器接收上述一次性认证密钥并保存于规定的终端侧存储装置(105),

上述移动终端构成为基于每个上述一次性认证密钥的有效期限,更换保存于上述终端侧存储装置的上述一次性认证密钥的一部分或者全部。

2.根据权利要求1所述的车辆用数字钥匙系统,其中,

上述车辆用装置和上述移动终端构成为能够通过作为符合规定的近距离无线通信标准的无线通信的近距离无线通信相互进行数据通信,

上述一次性认证密钥是通过将上述服务密钥与每次不同的变动代码组合而生成的代码,

上述移动终端执行:

从上述服务器接收上述一次性认证密钥、以及表示用于该一次性认证密钥的生成的上述变动代码的信息,

以在与上述车辆用装置之间已确立上述近距离无线通信的链路为条件,对上述车辆用装置发送上述变动代码,

上述车辆用装置具备车辆侧存储装置(45),上述车辆侧存储装置保持上述服务器发放的针对上述移动终端的上述服务密钥,

上述车辆用装置通过将保存于上述车辆侧存储装置的上述移动终端的上述服务密钥、与从上述移动终端接收的上述变动代码组合从而生成上述一次性认证密钥,

上述车辆用装置构成为使用生成的上述一次性认证密钥判断上述移动终端的合法性。

3.根据权利要求1所述的车辆用数字钥匙系统,其中,

上述车辆用装置和上述移动终端构成为能够通过作为符合规定的近距离无线通信标准的无线通信的近距离无线通信相互进行数据通信,

上述车辆用装置

从上述移动终端或者上述服务器取得对上述移动终端发放的多个上述一次性认证密钥并保存于车辆侧存储装置,

上述车辆用装置通过上述近距离无线通信与上述移动终端交换调整消息,上述调整消息用于使上述服务器发放的多个上述一次性认证密钥中用于认证处理的上述一次性认证密钥一致,

上述车辆用装置使用基于上述调整消息确定的上述一次性认证密钥判断上述移动终端的合法性。

4.根据权利要求1～3中任一项所述的车辆用数字钥匙系统,其中,

上述移动终端构成为定期地或者基于检测到规定的确认事件的产生来执行保存于上述终端侧存储装置的上述一次性认证密钥的剩余数量是否不足规定值的判定,

上述移动终端构成为在检测到上述一次性认证密钥的剩余数量不足规定值时能够访问互联网的情况下,执行用于从上述服务器取得上述一次性认证密钥的通信。

5.根据权利要求1～4中任一项所述的车辆用数字钥匙系统,其中,

上述服务器

具备数据库(33),针对上述车辆的所有者持有的上述移动终端亦即所有者终端的信息与具有作为上述所有者的权限的上述服务密钥亦即所有者密钥的信息建立对应地保存于上述数据库,

上述服务器构成为能够基于接收到从上述所有者终端发出的规定的客户密钥发放请求信号,发放用于上述所有者以外的上述用户亦即客户的上述服务密钥亦即客户密钥,

在上述客户密钥中,存在具有发放其它的上述客户密钥的权限的带发放权的客户密钥、和不具有其它的上述客户密钥的发放权限的无发放权的客户密钥这两种,

上述服务器构成为在基于来自上述所有者终端的请求发放上述客户密钥时,基于从上述所有者终端接收的信号,决定将该客户密钥设为带发放权的客户密钥还是设为上述无发放权的客户密钥。

6.根据权利要求5所述的车辆用数字钥匙系统,其中,

上述移动终端或者上述所有者终端基于用户操作,发送包含赋予新发放的上述客户密钥的权限的设定信息的数据集,作为上述客户密钥发放请求信号,上述移动终端具有上述带发放权的客户密钥,

上述服务器发放具有与从上述客户密钥的发放请求源取得的上述设定信息对应的限制的上述客户密钥。

7.根据权利要求6所述的车辆用数字钥匙系统,其中,

上述所有者终端构成为能够接收用于选择性地删除与上述车辆建立关联的上述客户密钥的操作,另一方面,无法接收不删除上述客户密钥而仅变更有效期限或者权限所涉及的设定的操作。

8.根据权利要求5～7中任一项所述的车辆用数字钥匙系统,其中,

上述服务器构成为:

将与一个上述车辆建立关联的多个上述客户密钥和与上述所有者密钥建立关联的识别编号亦即所有者密钥编号建立对应并保存于上述数据库,

基于该所有者密钥编号管理与一个上述车辆建立关联的上述服务密钥。

9.根据权利要求8所述的车辆用数字钥匙系统,其中,

上述服务器构成为在基于来自上述所有者终端的请求发放了上述客户密钥的情况下,对与上述客户密钥对应的上述移动终端亦即客户终端分发上述客户密钥以及上述所有者密钥编号。

10.根据权利要求8或9所述的车辆用数字钥匙系统,其中,

上述服务器构成为能够接受上述用户持有的上述移动终端的变更,

上述服务器构成为在变更了上述所有者持有的上述移动终端的情况下,也不删除分发

至与上述所有者建立关联的上述客户的上述服务密钥。

11.根据权利要求1～10中任一项所述的车辆用数字钥匙系统,其中,

在用于上述车辆的所有者以外的上述用户亦即客户的上述服务密钥亦即客户密钥中,设定有由该客户密钥的发放请求源指定的有效期限,

上述车辆用装置构成为自动地删除已过有效期限的上述客户密钥的信息。

12.根据权利要求1～11中任一项所述的车辆用数字钥匙系统,其中,

上述车辆用装置和上述移动终端构成为能够通过作为符合规定的近距离无线通信标准的无线通信的近距离无线通信相互进行数据通信,

上述服务器和上述移动终端构成为能够经由互联网进行通信,

上述车辆用装置构成为能够执行:

基于在与上述移动终端之间已确立上述近距离无线通信的链路,经由上述移动终端从上述服务器取得时刻信息;以及

使用取得的上述时刻信息,修正上述车辆用装置保持的时刻信息亦即内部时刻。

13.一种车辆用数字钥匙管理方法,是由以下单元执行的车辆用数字钥匙管理方法:

移动终端(1),是由用户携带的信息处理终端;

车辆用装置(4),搭载于车辆使用;以及

服务器(3),生成每个上述移动终端固有的服务密钥,作为用于使用上述车辆的密钥信息,

上述车辆用数字钥匙管理方法包含:

上述服务器基于来自上述移动终端的请求,根据上述移动终端的上述服务密钥生多个一次性的一次性认证密钥,带有效期限地分发至上述移动终端;

上述移动终端从上述服务器接收上述一次性认证密钥并保存于规定的终端侧存储装置(105);

上述移动终端基于每个上述一次性认证密钥的有效期限,定期地更换保存于上述终端侧存储装置的上述一次性认证密钥的一部分或者全部;

上述车辆用装置通过与上述服务器或者上述移动终端的通信,确定上述移动终端拥有的上述一次性认证密钥中的任意一个;以及

上述车辆用装置使用确定的上述一次性认证密钥判断上述移动终端的合法性。

14.一种车辆用装置,是构成为能够与由用户携带的信息处理终端亦即移动终端(1)、以及生成每个上述移动终端固有的服务密钥作为用于使用车辆的密钥信息的服务器(3)的每一个进行通信的搭载于上述车辆使用的车辆用装置,包含:

车辆侧存储装置(45),保存有每个上述用户的上述服务密钥;以及

车辆控制部(40),使用至少一个处理器而成,

上述车辆控制部构成为执行:

基于保存于上述车辆侧存储装置的上述服务密钥,生成作为一次性的认证密钥的一次性认证密钥;以及

使用上述一次性认证密钥判断上述移动终端的合法性。

15.一种移动终端,是构成为能够与搭载于车辆使用的车辆用装置(4)、以及生成作为用于使用上述车辆的密钥信息的服务密钥的服务器(3)的每一个进行通信的作为由用户携

带的信息处理终端的移动终端,具备:

终端侧存储装置(105),存储有上述服务密钥的数据;

近距离通信部(16),用于与上述车辆用装置实施作为符合规定的近距离无线通信标准的无线通信的近距离无线通信;

网络连接部(17、18),用于经由互联网与上述服务器进行通信;以及

终端控制部(10),使用至少一个处理器而成,

上述终端控制部构成为实施:

以已连接于上述互联网为条件,对上述服务器发送认证密钥请求信号,上述认证密钥请求信号请求集中分发多个基于上述服务密钥生成的带有效期限的一次性认证密钥;

从上述服务器接收上述一次性认证密钥并保存于上述终端侧存储装置;以及

基于每个上述一次性认证密钥的有效期限,更换保存于上述终端侧存储装置的上述一次性认证密钥的一部分或者全部。

车辆用数字钥匙系统、车辆用数字钥匙管理方法、车辆用装置、移动终端

[0001] 相关申请的交叉引用

[0002] 本申请以2021年9月29日在日本申请的日本专利申请第2021－159414号作为基础,将基础申请的内容整体上通过参照引用至本申请。

技术领域

[0003] 本公开涉及生成以及分发用于锁定/解锁车辆的密钥信息亦即数字钥匙的技术。

背景技术

[0004] 在专利文献1－2中,公开了以下系统,即,通过将从车辆的管理者发放的密钥信息分发至作为由用户携带的设备的移动终端以及车载器的每一个,从而能够将该移动终端作为车辆的电子钥匙使用。作为移动终端,例如假定智能手机等可连接互联网的通信终端。若能够像这样将智能手机等移动终端作为车辆钥匙使用,则用户在使用车辆时不需要持有专用的电子钥匙,便利性变好。此外,在专利文献1－2中,还提到了使车辆的使用权限在车辆的所有者与其他的人物(客户)间不同的结构。

[0005] 此外,作为验证连接于车辆的设备的合法性的方法,存在多种方法。例如在专利文献3中,公开了使用通过组合作为动态地变更的参数的变动符号和固定的密钥信息从而生成的认证代码,来认证连接于车辆的设备的方法。这些现有技术文献的记载内容能够作为本说明书中的技术要素的说明而通过参照引用至本说明书。

[0006] 专利文献1:日本专利第6635102号公报

[0007] 专利文献2:日本特表2019－536329号公报

[0008] 专利文献3:日本专利第6078686号公报

[0009] 在使用电密钥信息来允许车辆的使用的系统中,要求进一步加强安全性。作为与该需要对应的一个假定结构结构,假定以下结构:移动终端基于固有的服务密钥生成作为一次性的认证代码的一次性认证密钥,使用该一次性认证密钥对车辆用装置证明合法性。然而,在该假定结构中,使移动终端的处理负荷增大。作为移动终端,假定处理能力不同的多种设备。优选使移动终端具有的功能尽可能简单,以便即使在运算能力较低的设备上也进行动作。

[0010] 作为用于简化移动终端的功能的进一步的假定结构,还考虑将一次性认证密钥的生成功能设置于服务器,移动终端在与车辆进行通信时从服务器实时地取得一次性认证密钥并使用的结构。然而,移动终端并不一定一直处于可通信的状况。在移动终端在通信范围外的情况下,无法从服务器取得一次性认证密钥,无法使用车辆。即,用户的便利性可能降低。

发明内容

[0011] 本公开是基于上述的研究或着眼点而完成的,其目的之一在于能够兼具安全性和

用户的便利性的车辆用数字钥匙系统、车辆用数字钥匙管理方法、移动终端、车辆用装置。

[0012] 在此公开的车辆用数字钥匙系统是包含以下单元的车辆用数字钥匙系统:车辆用装置,搭载于车辆使用;移动终端,是由用户携带的信息处理终端;以及服务器,生成每个移动终端固有的服务密钥作为用于使用车辆的密钥信息,并将密钥信息直接地或者间接地分发至移动终端以及车辆用装置,车辆用装置构成为使用基于服务密钥生成的一次性的一次性认证密钥判断移动终端的合法性,服务器基于来自移动终端的请求,生成多个一次性认证密钥,并带有效期限地分发至移动终端,对移动终端而言,从服务器接收一次性认证密钥并保存于规定的终端侧存储装置,构成为基于每个一次性认证密钥的有效期限,更换保存于终端侧存储装置的一次性认证密钥的一部分或者全部。

[0013] 根据上述结构,使用基于每个移动终端固有的服务密钥生成的一次性认证密钥来进行移动终端(进而,用户)的认证,因此与使用固定的密钥信息来进行移动终端的认证的结构相比,能够提高安全性。另外,移动终端被控制为保持多个一次性认证密钥。因此,即使在移动终端无法与服务器进行通信的环境下,也能够减少用户无法使用车辆的担忧。此外,根据上述结构,移动终端保持的一次性认证密钥基于有效期限而被定期地更换。根据该结构,由于有效的一次性认证密钥随时间变更,因此能够进一步加强安全性。

[0014] 另外,本公开的车辆用数字钥匙管理方法是由以下单元执行的车辆用数字钥匙管理方法:移动终端,是由用户携带的信息处理终端;车辆用装置,搭载于车辆使用;以及服务器,生成每个移动终端固有的服务密钥,作为用于使用车辆的密钥信息,车辆用数字钥匙管理方法包含:服务器基于来自移动终端的请求,根据移动终端的服务密钥生多个一次性的一次性认证密钥,带有效期限地分发至移动终端;移动终端从服务器接收一次性认证密钥并保存于规定的终端侧存储装置;移动终端基于每个一次性认证密钥的有效期限,定期地更换保存于终端侧存储装置的一次性认证密钥的一部分或者全部;车辆用装置通过与服务器或者移动终端的通信,确定移动终端拥有的一次性认证密钥中的任意一个;以及车辆用装置使用确定的一次性认证密钥判断移动终端的合法性。

[0015] 根据上述方法,通过与车辆用数字钥匙系统相同的作用,能够进一步加强安全性。

[0016] 本公开的车辆用装置是构成为能够与由用户携带的信息处理终端亦即移动终端、以及生成每个移动终端固有的服务密钥作为用于使用车辆的密钥信息的服务器的每一个进行通信的搭载于车辆使用的车辆用装置,包含:车辆侧存储装置,保存有每个用户的服务密钥;以及车辆控制部,使用至少一个处理器而成,车辆控制部构成为执行以下内容:基于保存于车辆侧存储装置的服务密钥,生成作为一次性的认证密钥的一次性认证密钥;以及使用一次性认证密钥判断移动终端的合法性。

[0017] 根据上述车辆用装置,使用基于每个移动终端固有的服务密钥生成的一次性认证密钥来进行移动终端(进而,用户)的认证,因此与使用固定的密钥信息来进行移动终端的认证的结构相比,能够提高安全性。

[0018] 本公开的移动终端是构成为能够与搭载于车辆使用的车辆用装置、以及生成作为用于使用车辆的密钥信息的服务密钥的服务器的每一个进行通信的作为由用户携带的信息处理终端的移动终端,具备:终端侧存储装置,存储有服务密钥的数据;近距离通信部,用于与车辆用装置实施作为符合规定的近距离无线通信标准的无线通信的近距离无线通信;网络连接部,用于经由互联网与服务器进行通信;以及终端控制部,使用至少一个处理器而

成,终端控制部构成为实施以下内容:以已连接于互联网为条件,对服务器发送认证密钥请求信号,认证密钥请求信号请求集中分发多个基于服务密钥生成的带有效期限的一次性认证密钥;从服务器接收一次性认证密钥并保存于终端侧存储装置;以及基于每个一次性认证密钥的有效期限,更换保存于终端侧存储装置的一次性认证密钥的一部分或者全部。

[0019] 根据上述移动终端,通过与车辆用数字钥匙系统相同的作用,能够进一步加强安全性。

[0020] 此外,权利要求书所记载的括号内的附图标记示出与作为一个方式后述的实施方式所记载的具体单元的对应关系,并不对本公开的技术范围进行限定。

附图说明

[0021] 图1是表示车辆用数字钥匙系统的整体情况的图。

[0022] 图2是表示移动终端的结构的框图。

[0023] 图3是终端控制部的功能框图。

[0024] 图4是表示专用钥匙的结构的框图。

[0025] 图5是表示数字钥匙服务器的结构的框图。

[0026] 图6是表示储存于车辆数据库的数据的种类的一个例子的图。

[0027] 图7是表示储存于用户数据库的数据的种类的一个例子的图。

[0028] 图8是数据处理部的功能框图。

[0029] 图9是用于对车辆、所有者密钥、以及客户密钥的关系进行说明的图。

[0030] 图10是表示车载系统的结构的框图。

[0031] 图11是认证ECU的功能框图。

[0032] 图12是用于对服务密钥的发放以及登记所涉及的处理的整体情况进行说明的图。

[0033] 图13是用于对所有者密钥的发放处理进行说明的时序图。

[0034] 图14是用于对将所有者密钥登记至车辆的处理进行说明的时序图。

[0035] 图15是表示用于将所有者密钥向车辆登记的移动终端的显示画面的一个例子的图。

[0036] 图16是与车辆的通信连接所涉及的移动终端的显示画面的一个例子。

[0037] 图17是用于对客户密钥的发放处理进行说明的时序图。

[0038] 图18是表示客户密钥发放请求信号中应当包含的信息的一个例子的图。

[0039] 图19是表示向客户终端发送的终端登记用数据包中应当包含的信息的一个例子的图。

[0040] 图20是用于对将客户密钥登记至车辆的处理进行说明的时序图。

[0041] 图21是表示用于将客户密钥登记至车辆的移动终端的显示画面的一个例子的图。

[0042] 图22是用于对停车中的认证ECU的工作例进行说明的流程图。

[0043] 图23是表示认证ECU认证移动终端的处理的一个例子的时序图。

[0044] 图24是表示认证ECU认证移动终端的处理的另一例子的时序图。

[0045] 图25是移动终端补充一次性认证密钥的处理的时序图。

[0046] 图26是移动终端更换保存于密钥信息存储部的一次性认证密钥的处理的时序图。

[0047] 图27是用于对认证ECU实施的ECU时刻的修正以及基于有效期限的客户密钥的删

除进行说明的时序图。

[0048] 图28是用于对服务密钥的删除所涉及的时序的整体情况进行说明的图。

[0049] 图29是表示删除所有者密钥时的移动终端与DKS的交互的时序图。

[0050] 图30是表示删除所有者密钥时的所有者终端与认证ECU的交互的时序图。

[0051] 图31是表示删除客户密钥时的移动终端与DKS的交互的时序图。

[0052] 图32是表示删除客户密钥时的移动终端与认证ECU的交互的时序图。

[0053] 图33是表示经由车载HMI删除服务密钥的情况的一系列的处理的流程的时序图。

[0054] 图34是用于对删除了带发放权的客户密钥的情况的DKS的工作例进行说明的图。

[0055] 图35是用于对所有者持有的移动终端变更了机型的情况的DKS的工作进行说明的流程图。

具体实施方式

[0056] 以下,使用附图,对本公开的车辆用数字钥匙系统Sys进行说明。车辆用数字钥匙系统Sys是用于通过将用于使用车辆Hv的电子式的密钥亦即服务密钥分发至移动终端1,从而使得用户即使不持有专用钥匙2也能够进行对车辆Hv的访问的系统。如图1所示,车辆用数字钥匙系统Sys包含移动终端1、专用钥匙2、数字钥匙服务器(DKS:Digital Key Server)3、以及搭载于车辆Hv的车载系统7。车载系统7包含认证ECU4。ECU是电子控制单元(Electronic Control Unit)的缩写,是指电子控制装置。

[0057] ＜前言＞

[0058] 作为一个例子,以下的说明中的车辆Hv是由个人拥有的车辆。当然,车辆Hv也可以是公司组织拥有的公司用车、公共机构拥有的公用车。并且,车辆Hv也可以是用于出租服务的车辆(所谓的租赁汽车),也可以是用于汽车共享服务的车辆(所谓的共享汽车)。车辆Hv也可以是机器人出租车等用于客运服务的车辆。

[0059] 车辆Hv例如是发动机车辆。当然,车辆Hv也可以是混合动力车、电动汽车。这里的发动机车辆是指仅具备发动机作为动力源的车辆,混合动力车是指具备发动机和电动机作为动力源的车辆。电动汽车是指仅具备电动机作为驱动源的车辆。本公开中的行驶用电源是用于车辆Hv行驶的电源,在车辆为发动机车辆的情况下是指点火电源。在车辆Hv为电动汽车、混合动力车的情况下,系统主继电器相当于行驶用电源。本公开不限于四轮汽车,能够搭载于拖车、两轮汽车,三轮汽车等可行驶于道路上的多种车辆。带发动机的自行车也能够包含于两轮汽车。

[0060] 以下,主要以一个车辆Hv为对象来进行车辆用数字钥匙系统Sys的说明,但DKS3管理的车辆可以存在多个。另外,也可以一个所有者拥有的车辆Hv存在多个。

[0061] 本公开的用户是指车辆用数字钥匙系统Sys提供的服务的使用者。已创建用于使用车辆用数字钥匙系统Sys提供的服务的帐户的人物,换言之,已安装后述的数字钥匙应用104的移动终端1的拥有者相当于用户。

[0062] 本公开的各种时序图以及流程图均是一个例子。各时序图/流程图具备的步骤数、处理顺序、执行条件等能够适当地变更。

[0063] ＜整体情况的概要＞

[0064] 移动终端1是可由多个用户的每一个持有/携带的通用信息处理终端。图1所示的

移动终端1a表示车辆Hv的所有者持有的移动终端1。移动终端1b例如是所有者的家人拥有的移动终端1,移动终端1c是所有者的朋友持有的移动终端1。对移动终端1分配有每个终端固有的识别信息的设备ID。

[0065] 作为设备ID,例如能够采用设备地址、UUID(Universally Unique Identifier:全局唯一标识符)等。此外,Bluetooth(注册商标)中的设备地址能够以48位表示。另外,UUID能够以128位表示。设备地址也可以是固定的公共地址,也可以是随机地址。公共地址相当于Ethernet(注册商标,以太网)中的MAC(Media Access Control:媒体接入控制)地址。此外,设备ID也可以是在后述的数字钥匙应用104的安装时决定的随机数。

[0066] 移动终端1构成为能够经由无线基站8以及广域通信网络9与DKS3进行数据通信。图1所示的无线基站8例如也可以是蜂窝通信用的基站,也可以是Wi—Fi(注册商标)用的访问点。访问点是形成无线LAN(Local Area Network:局域网)的通信设备。在访问点的概念中除了路由器以外,还能够包含路侧机。广域通信网络9例如是互联网。对形成广域通信网络9的设备而言,移动终端1相当于用户装置(UE:User Equipment)。

[0067] 蜂窝通信例如是指符合4G、5G这样的标准的无线通信。作为Wi—Fi的标准,能够采用IEEE802.11n、IEEE802.11ac,IEEE802.11ax(所谓的Wi—Fi6)等多种标准。在本公开中,也将符合Wi—Fi标准的无线通信称为Wi—Fi通信。移动终端1与DKS3的通信通过蜂窝通信或者Wi—Fi通信实施。

[0068] DKS3是配置于车辆Hv的外部的服务器。DKS3构成为能够连接于广域通信网络9。DKS3可以经由广域通信网络9与移动终端1进行相互通信。DKS3基于来自来自移动终端1的请求,对规定的用户发放用于使用车辆Hv的服务密钥。

[0069] 另外,车载系统7和移动终端1构成为能够实施近距离无线通信。这里的近距离无线通信是指实质上的可通信距离例如为5m至30m,最大为100m左右的符合规定的近距离无线通信标准的通信。作为近距离无线通信的标准,例如能够采用BLE(Bluetooth Low Energy:蓝牙低能耗)、Bluetooth Classic(经典蓝牙)、Wi-Fi(注册商标)、ZigBee(注册商标)等。作为近距离无线通信的方式,还能够采用UWB—IR(Ultra Wide Band-Impulse Radio:超宽带-脉冲无线电)。在本实施方式中作为一个例子,以车载系统7和移动终端1构成为能够实施符合BLE标准的无线通信亦即BLE通信的情况为例对各部的工作进行说明。以下的BLE通信的记载能够替换为近距离无线通信来实施。通信连接以及加密通信等所涉及的通信方法的细节通过BLE标准中规定的时序来实施。

[0070] 此外,以下,对设定为车载系统7作为与移动终端1的通信中的主机进行动作的情况进行说明。移动终端1作为从机进行动作。BLE通信中的从机是间歇地发送广告信号,并且基于来自主机的请求来执行数据的收发的设备。从机也被称为外围设备。主机控制与从机的通信连接状态、通信定时。主机也被称为中央设备。作为其它的方式,也可以设定为移动终端1作为与车载系统7的通信中的主机进行动作。

[0071] 车载系统7包含用于进行BLE通信的BLE通信部57和认证ECU4。认证ECU4是构成车载系统7的ECU之一。认证ECU4相当于车辆用装置。认证ECU4与具有服务密钥的移动终端1进行基于无线通信的自动的认证处理。而且,以认证成功为条件,提供实施与用户相对于车辆Hv的位置对应的车辆控制的被动进入被动启动功能。这里的车辆控制是车门的锁定/解锁、电源接通/断开、发动机启动等。此外,移动终端1与用户对应,因此认证移动终端1相当于认

证用户。

[0072] ＜服务密钥的说明＞

[0073] 服务密钥按每个移动终端1而不同。例如服务密钥是根据设备ID确定的、按每个移动终端1而不同的代码。服务密钥能够设为具备规定的字符数的字母数字的罗列。例如DKS3采用将设备ID加上具有规定的长度的随机数后的值输入至规定的哈希函数而得到的输出值作为服务密钥。作为哈希函数,能够采用FNV132、FNV164、MD－5、SHA－1、SHA－256、SHA－512等多种函数。用于服务密钥的生成的函数可以根据作为服务密钥所需的位数(输出长度)来适当地选择。

[0074] 服务密钥可以通过具有8位以上的长度的位串来表示。服务密钥越长则其安全性越稳固而越合适。服务密钥例如能够以16字节、24字节、27字节等来表示。这里作为一个例子,服务密钥设为由24字节构成。根据将服务密钥设为27字节以下的结构,能够将服务密钥容纳在一个BLE加密通信包中。

[0075] 此外,优选服务密钥设为按车辆Hv与移动终端1的每个组合而不同的值。例如也可以将以结合车辆ID与设备ID后的值作为输入值的规定的哈希函数的输出值设为服务密钥。车辆ID是按每个车辆分配的固有的识别编号。作为车辆ID,例如能够采用车辆识别编码(VIN:Vehicle Identification Number)等。

[0076] 进一步地,服务密钥也可以是将对车辆ID和设备ID进一步连结与接受发放请求的纪元秒对应的值后的数据输入至规定的哈希函数而得到的输出值。另外,并不一定需要在服务密钥的生成中使用哈希函数。服务密钥也可以是对设备ID乘以、加上、或者连结车辆ID而得到的值。作为服务密钥的材料,还能够采用用户设定的密码等。例如服务密钥也可以是将用户登记的规定字符数的密码代入规定的哈希函数后的值。

[0077] 在服务密钥中存在多个种类。作为服务密钥的种类,主要存在所有者密钥(owner key)和客户密钥(guest key)。所有者密钥是对车辆Hv的所有者发放的服务密钥,大致具有与车辆Hv的使用相关的全部的权限。所有者密钥具有行驶用电源的接通断开、车门的锁定解锁、远程操作等车辆Hv的使用所涉及的全部的权限,并且具有发放用于其它的用户的服务密钥的权限。另外,所有者密钥基本上是未设定有效期限的无期限的服务密钥。

[0078] 客户密钥是用于客户的服务密钥,基本上由所有者发放。这里的客户是指所有者以外的用户。客户密钥是与所有者密钥相比权限被限制的服务密钥,还被设定有效期限。

[0079] 客户密钥更详细地划分为具有发放其它的客户密钥的权限的带发放权的客户密钥、和不具有其它的客户密钥的发放权限的无发放权的客户密钥。作为示例用例的一个例子,可以基于来自所有者的请求,对所有者的家人发放带发放权的客户密钥。另外,可以对所有者的朋友/熟人等发放无发放权的客户密钥。

[0080] 以下将所有者持有的移动终端1,换言之将保存有所有者密钥的移动终端1称为所有者终端。将客户持有的移动终端1,换言之保存有客户密钥的移动终端1称为客户终端。另外,将客户终端中的被赋予带发放权的客户密钥的移动终端1称为带发放权的客户终端,将被赋予无发放权的客户密钥的移动终端1称为无发放权的客户终端。在图1所示的例子中,移动终端1a相当于所有者终端,移动终端1b相当于带发放权的客户终端。另外,移动终端1c相当于无发放权的客户终端。

[0081] 若以所有者终端为父终端,则具有所有者终端发放的客户密钥的移动终端1相当

于对所有者终端而言的子终端。另外,具有带发放权的终端发放的客户密钥的移动终端1相当于对所有者终端而言的孙终端。各客户密钥的权限由发放源决定。客户密钥的权限设定得比发放源小(窄)。但是,作为其它的方式,车辆用数字钥匙系统Sys也可以构成为能够发放具有与发放源同等的权限的客户密钥。DKS3基于来自所有者终端或者带发放权的客户终端的请求,新发放客户密钥。新发放的服务密钥的类型、权限设定由发放源指定。例如DKS3在基于来自所有者终端的请求新发放客户密钥时,基于从所有者终端接收到的信号来决定将该客户密钥设为带发放权的客户密钥还是设为无发放权的客户密钥。此外,也可以带发放权的客户密钥被限制为仅能够发放无发放权的客户密钥。

[0082] ＜关于移动终端的结构以及功能＞

[0083] 这里,首先使用图2对移动终端1具备的结构/功能进行说明。作为移动终端1,例如能够采用智能手机、平板终端、可穿戴设备等。可穿戴设备是佩戴于用户的身体来使用的设备,能够采用腕带型、手表型、戒指型、眼镜型、耳机型等多种形状的设备。

[0084] 移动终端1具备终端控制部10、显示器11、触摸面板12、惯性传感器13、生物体认证装置14、近场通信部15、BLE通信部16、蜂窝通信部17、以及Wi－Fi通信部18。

[0085] 终端控制部10是控制移动终端1整体的动作的模块。终端控制部10例如构成为具备终端处理器101、RAM(Random Access Memory:随机存取存储器)102、储存器103等的计算机。终端处理器101是用于与RAM102结合的运算处理的硬件(换言之,运算核心)。终端处理器101例如是CPU(Central Processing Unit:中央处理器)。终端处理器101是在用户使用的设备中使用的处理器,因此能够称为用户处理器或者UE处理器。终端处理器101通过对RAM102的访问,来执行用于实现后述的各功能部的功能的各种处理。RAM102是易失性的存储介质。储存器103是包含闪存等非易失性的存储介质的结构。

[0086] 数字钥匙应用104是用于安全地进行用户的认证、服务密钥的取得/保存、与车载系统7的通信等的应用程序软件。数字钥匙应用104例如安装于储存器103等。

[0087] 终端控制部10构成为能够与显示器11、触摸面板12、惯性传感器13、生物体认证装置14、近场通信部15、BLE通信部16、蜂窝通信部17、以及Wi－Fi通信部18的每一个相互通信。关于终端控制部10具备的功能后述。

[0088] 显示器11例如是液晶显示器、有机EL显示器。显示器11显示与来本终端控制部10的输入信号对应的图像。触摸面板12是静电电容式的触摸面板,层叠于显示器11。触摸面板12以及显示器11相当于用于用户向移动终端1登记密钥信息,或将移动终端1与车载系统7配对的接口。触摸面板12是输入装置。触摸面板12输出的信号对应于用户针对移动终端1的操作。以下,也将触摸面板12的输出信号记载为操作信号。

[0089] 惯性传感器13是检测作用于移动终端1的惯性力的传感器。加速度传感器、陀螺仪传感器相当于惯性传感器13。惯性传感器13的输出(检测数据)输入至终端控制部10。

[0090] 生物体认证装置14例如是使用用户的指纹、脸部图像等来认证用户的装置。生物体认证装置14也可以是使用手、手指的静脉图案、虹彩图案来认证用户的装置。另外,生物体认证装置14例如也可以是使用声纹等发声语音的特征来进行认证的装置。用户的认证结果提供至终端控制部10。

[0091] 近场通信部15是用于实施作为符合NFC(Near Field Communication:近场通信)的标准的无线通信的近场通信的通信模块。这里的近场通信是指可通信的距离为几cm至几

十cm左右的通信。近场通信相当于与BLE通信相比可通信的距离足够小的通信方式。可通信的距离足够小的通信方式是指通信距离为10分之1以下的通信方式。作为用于实现近场通信的具体的通信标准,例如能够采用ISO/IEC 14443、ISO/IEC 18092等多种标准。近场通信也可以是适合于Type-F标准的通信,也可以是适合于Type-A或者Type-B标准的通信。Type-F标准相当于所谓的FeliCa(注册商标)。在移动终端1中,近场通信部15为任意的要素而也可以省略。

[0092] BLE通信部16是用于实施BLE通信的通信模块。BLE通信部16、57相当于近距离通信部。蜂窝通信部17是用于实施蜂窝通信的通信模块。蜂窝通信部17例如是负责LTE等无线通信协议中的数据链路层以及物理层的通信模块。蜂窝通信部17将表示与无线基站8的连接状况,例如表示是否在通信范围外等的信息提供至终端控制部10。

[0093] Wi—Fi通信部18是用于实施Wi—Fi通信的通信模块。Wi—Fi通信部18构成为能够经由访问点连接于广域通信网络9。Wi—Fi是规定的无线LAN标准的一种。因此,Wi—Fi通信部18相当于无线LAN模块的一个例子。

[0094] 各种通信模块具备能够收发设为收发的对象的频带的电波的天线、控制通信的微型计算机亦即通信微机、调制解调电路等。此外,移动终端1构成为能够实施蜂窝通信和Wi—Fi通信的至少任意一方作为与DKS3的通信方式即可。移动终端1不需要具备蜂窝通信部17和Wi—Fi通信部18双方。在移动终端1已通过蜂窝通信或者Wi—Fi通信连接于广域通信网络9的所谓的在线的状态的情况下,终端控制部10与DKS3进行各种数据通信。例如可以通过使用了TLS(Transport Layer Security:传输层安全)的加密通信来实施数据通信。蜂窝通信部17以及Wi—Fi通信部18相当于网络连接部。

[0095] 如图3所示,终端控制部10具备服务密钥管理部F1、一次性认证密钥管理部F2、以及车辆响应部F3,作为通过终端处理器101执行数字钥匙应用104从而表达的功能部。各种功能部可以在数字钥匙应用104认证用户的状态下有效。

[0096] 可以通过对数字钥匙应用104输入规定的用户ID和密码来进行用户的认证(登录)。用户的认证也可以使用生物体认证装置14来实施。数字钥匙应用104是车辆用数字钥匙系统Sys的一部分,因此用户已登录数字钥匙应用104的状态对应于用户已登录车辆用数字钥匙系统Sys的状态。此外,登录状态在从登录起经过规定的有效期限的情况下被解除,数字钥匙应用104迁移至需要用户的再认证的注销状态。

[0097] 另外,终端控制部10具备终端侧存储部105。终端侧存储部105是存储服务密钥等数字钥匙应用104使用的各种数据的存储区域。使用储存器103或者RAM102具备的存储区域来实现终端侧存储部105。终端侧存储部105具备密钥信息存储部M1和车辆用数据临时存储部M2。密钥信息存储部M1是用于储存服务密钥、后述的一次性认证密钥、用户ID等的存储区域。车辆用数据临时存储部M2是用于暂时地保存从DKS3接收到的用于向车辆Hv传送的数据的存储区域。终端侧存储部105相当于终端侧存储装置。

[0098] 服务密钥管理部F1管理DKS3已发放的本终端的用户用的服务密钥。本公开中的本终端是指从终端控制部10来看设置有自身的移动终端1。服务密钥管理部F1基于从触摸面板12输入的操作信号,请求面向本终端的服务密钥的发放,或者删除本终端用的服务密钥。面向本终端的服务密钥相当于用于本终端的用户的服务密钥。

[0099] 服务密钥管理部F1从DKS3取得面向本终端的服务密钥,并将面向本终端的服务密

钥保存于密钥信息存储部M1。服务密钥管理部F1在取得服务密钥时,取得服务密钥本身、以及作为附加的信息的密钥相关信息。密钥相关信息例如是指服务密钥ID、有效期限、权限设定、类型等。这些信息可以打包为一个数据集并分发。

[0100] 服务密钥ID是用于识别服务密钥的编号。服务密钥ID例如对每个用户设定唯一的值。服务密钥ID也可以是在帐户创建时生成的随机数。即使所有者进行移动终端1的机型变更而服务密钥的值被变更,与所有者建立关联的服务密钥ID也不变更。此外,服务密钥ID也可以设定为与车辆ID和用户ID的组合对应的唯一的值。

[0101] 有效期限数据是表示无期限的规定值,或者示出发放源指定的期间/日期。权限设定数据表示对本终端的用户允许的功能(即权限)。权限设定数据例如示出可否锁定解锁每个车门、可否接通/断开行驶用电源等。服务密钥类型表示是所有者密钥还是客户密钥。类型信息也可以与权限设定数据统合。

[0102] 服务密钥管理部F1除了面向本终端的服务密钥的取得以外,还执行显示与本终端用的服务密钥相关的状态确认画面的处理、用于删除面向本终端的服务密钥的处理。状态确认画面是表示本终端用的服务密钥的状态的画面。在服务密钥的状态中,包含有效期限、权限设定、有效/无效状态等。在状态确认画面中,可以包含与相当于发放源的用户的名称等相关的信息。

[0103] 此外,服务密钥管理部F1提供的功能根据对本终端分配的服务密钥的类型,换言之根据服务密钥的权限设定而不同。例如所有者终端的服务密钥管理部F1构成为能够执行用于发放用户指定的客户用的客户密钥的处理、将客户密钥删除/暂时无效化的处理。此外,仅限于所有者终端,构成为在客户密钥的发放时,作为权限设定的一种,能够指定有无发放客户密钥的权限。另外,所有者终端的服务密钥管理部F1显示用于车辆Hv所涉及的服务密钥的客户的列表、表示各客户密钥的状态的画面。所有者终端例如可从DKS3取得客户密钥的信息并显示。并且,所有者终端的服务密钥管理部F1构成为还能够使用从DKS3取得的规定的数据集,来实施将与所有者密钥相关的信息登记至车辆Hv的处理。

[0104] 另外,带发放权的终端具备的服务密钥管理部F1构成为能够执行对用户指定的客户新发放无发放权的客户密钥的处理。另外,带发放权的终端具备的服务密钥管理部F1构成为能够执行自身已发放的客户密钥的状态确认、该客户密钥的删除/无效化等。无发放权的终端的服务密钥管理部F1构成为能够实施状态确认、本终端用的服务密钥的删除/无效化。此外,客户终端的服务密钥管理部F1可以基于有效期限数据,实施本终端用的服务密钥的有效期限的确认。此外,也可以DKS3实施客户密钥的有效期限检查。

[0105] 一次性认证密钥管理部F2从DKS3取得用于与车辆Hv的认证处理的一次性认证密钥,并将一次性认证密钥保存于密钥信息存储部M1。一次性认证密钥管理部F2本身并不具备生成一次性认证密钥的功能。根据该结构,能够隐藏一次性认证密钥的生成方法的详细内容。进而能够提高车辆用数字钥匙系统Sys的安全性能。

[0106] 一次性认证密钥是通过将服务密钥与变动代码(变动因素)组合而得到的代码。变动代码是按每次发放而不同的值。变动代码例如能够设为纪元秒、发放次数的计数值、或者随机数。并且,变动代码也可以是规定的初始值减去认证密钥的发放次数后的值。假设一次性认证密钥为Ka,服务密钥为SK,变动代码为Cd,一次性认证密钥的生成函数为G,则一次性认证密钥可以通过Ka＝G(SK,Cd)表示。在该情况下,生成函数G是采用服务密钥和变动代码

这两个输入的函数。生成函数G也可以是采用一个输入值的函数,在该情况下,例如可以通过Ka＝G(SK+Cd)等生成一次性认证密钥。SK+Cd也可以是将服务密钥和变动代码相连后的(即连结后的)代码,也可以是将与它们对应的数列以2进制或者16进制的概念相加后的代码。

[0107] 此外,若将用于生成一次性认证密钥的第一因素设为服务密钥,则变动代码能够称为用于生成一次性认证密钥的第二因素。变动代码是认证密钥生成因素之一。并且,一次性认证密钥也可以除了服务密钥和变动代码以外,还使用规定的第三因素来生成。例如也可以通过将由表示发放次数的计数值、ECU编号、以及服务密钥按规定的顺序结合而成的位串输入至规定的函数从而生成一次性认证密钥。一次性认证密钥是使用一次后就被放弃的所谓的一次性的认证密钥。第三因素优选是预先登记于认证ECU4的信息。

[0108] 一次性认证密钥管理部F2随时发送对DKS3请求一次性认证密钥的分发的信号,以便维持在密钥信息存储部M1保持有规定量以上的一次性认证密钥的状态。例如一次性认证密钥管理部F2基于保存于密钥信息存储部M1的一次性认证密钥的剩余数量(Notk)不足规定的补充阈值(ThRp),将是否需要补充标志设定为接通(ON)。一次性认证密钥管理部F2基于是否需要补充标志设定为接通且为在线状态,通过与DKS3的通信取得多个一次性认证密钥。补充阈值例如能够设为150、300。是否需要补充标志是任意的要素,也可以省略。补充阈值ThRp也可以为200、400、500。

[0109] 此外,在一次性认证密钥中,设定以发放日为起算日的有效期限。有效期限例如可设定为1个月、3个月、6个月。一次性认证密钥的有效期限也由DKS3设定。DKS3也可以构成为能够基于所有者的指示操作变更针对一次性认证密钥的有效期限的长度。假设在车辆Hv为租赁汽车的情况下,一次性认证密钥的有效期限可设定为与租赁期间对应。另外,该技术思想也能够相同地应用于客户密钥的有效期限设定。

[0110] 一次性认证密钥管理部F2在规定的定时检查保存于密钥信息存储部M1的一次性认证密钥的有效期限,并删除已过有效期限的一次性认证密钥。也可以DKS3实施一次性认证密钥的有效期限检查。此外,作为删除了已过期限的一次性认证密钥的结果,在一次性认证密钥的剩余数量变得不足补充阈值的情况下,实施将是否需要补充标志设定为接通等用于从DKS3取得一次性认证密钥的处理。

[0111] 车辆响应部F3是基于已与认证ECU4确立BLE通信的链路(连接),来与认证ECU4执行基于BLE的数据通信的结构。例如车辆响应部F3基于已与认证ECU4确立BLE通信链路,来实施用于用户认证的无线通信。车载系统—用户间的认证处理例如可以通过质询—响应方式实施。在该情况下,车辆响应部F3针对从认证ECU4发送来的质询代码,使用一次性认证密钥生成响应代码,并将响应代码返回至认证ECU4。

[0112] 另外,车辆响应部F3基于来自认证ECU4的请求,进行中继认证ECU4与DKS3的通信的处理。例如车辆响应部F3将从认证ECU4通过BLE通信接收到的时刻请求信号转换为蜂窝通信的格式并发送至DKS3。另外,将从DKS3接收到的面向认证ECU4的数据,例如服务器时刻信息等转换为BLE通信的格式并传送至认证ECU4。

[0113] 此外,移动终端1也可以构成为能够通过近场通信执行与车载系统7的认证处理。移动终端1也可以构成为通过近场通信与车载系统7实施BLE通信所涉及的配对。另外,终端控制部10也可以构成为能够显示确认车辆Hv的状态的画面亦即车辆状态确认画面,作为数

字钥匙应用104的功能。车辆状态确认画面是表示汽油/电池的剩余量、各车窗以及各车门的开闭状态、锁定状态、车内温度等的画面。另外,终端控制部10也可以构成为能够远程操作车辆Hv具备的电气设备的一部分。例如也可以构成为能够远程操作空调装置的接通/断开、车窗的开闭、危险警告灯的点亮/熄灭等。此外,车辆状态确认、可远程操作的内容也可以根据服务密钥的权限而变更。

[0114] ＜关于专用钥匙的结构以及功能＞

[0115] 这里使用图4,对专用钥匙2的结构以及功能进行说明。专用钥匙2是用于操作车辆Hv的专用的电子钥匙。在购买车辆Hv时,专用钥匙2作为是车辆Hv的所有者的证明、或者作为具有实体的主钥匙,而与车辆Hv一起提供给所有者。专用钥匙2基本上由所有者持有。专用钥匙2能够理解为车辆Hv的附件之一。专用钥匙2能够采用扁平的长方体型、扁平的椭圆体型(所谓的fob类型)、卡型等多种形状。专用钥匙2可以被称为车辆用便携机、秘钥卡、钥匙卡、卡片钥匙、访问钥匙等。

[0116] 在专用钥匙2中,登记有证明是车辆Hv的密钥的规定的代码亦即专用钥匙代码。专用钥匙代码也登记于认证ECU4。专用钥匙2构成为能够通过与认证ECU4按照规定的过程进行通信,从而证明想要访问车辆Hv的人物是所有者。此外,专用钥匙2是任意的要素,也可以省略。

[0117] 如图4所示,专用钥匙2具备控制电路20、以及近场通信部21。控制电路20是控制专用钥匙2的动作的电路。使用MCU(Micro Controller Unit:微控制单元)201、RAM202、闪存203等实现控制电路20。也可以代替MCU而使用MPU(Micro-Processing Unit:微处理器)、FPGA(Field-Programmable Gate Array:现场可编程门阵列)实现控制电路20。在闪存203保存有上述的专用钥匙代码。

[0118] 近场通信部21是用于实施近场通信的通信模块。专用钥匙2例如构成为将来自车辆Hv具备的近场通信部56的电波转换为电力并发挥功能的无源型的无线标签。在近场通信部21与车辆Hv的近场通信部56通信连接的情况下,控制电路20基于来自认证ECU4的请求,返回专用钥匙代码本身或者根据专用钥匙代码而生成的响应代码。认证ECU4可以基于使用了专用钥匙代码的认证处理成功,而迁移至可登记所有者的状态。这样,专用钥匙2可作为用于将认证ECU4切换至能够进行所有者信息的登记的状态的设备发挥功能。

[0119] ＜关于DKS的结构以及功能＞

[0120] 这里,对DKS3的结构以及功能进行说明。如图5所示,DKS3具备数据处理部30、网络连接装置31、车辆DB32、以及用户DB33。部件名称中的DB是数据库(Database)的缩写。

[0121] 数据处理部30是基于从网络连接装置31输入的信号/数据执行多种处理的结构。数据处理部30与网络连接装置31、车辆DB32、以及用户DB33的每一个连接为能够相互通信。使用服务器处理器301、RAM302、储存器303构成数据处理部30。服务器处理器301是执行各种运算处理的运算核心,例如使用CPU、GPU等实现。在储存器303储存有规定的数字钥匙管理程序。通过服务器处理器301执行该数字钥匙管理程序,从而实现后述的各种功能部。此外,服务器处理器301执行该数字钥匙管理程序对应于执行与该程序对应的方法亦即车辆用数字钥匙管理方法。

[0122] 网络连接装置31是用于连接于广域通信网络9的通信模块。网络连接装置31例如构成为能够使用光纤等而与构成广域通信网络9的通信设备相互通信。由此,在移动终端1

为在线状态的情况下,DKS3能够与移动终端1进行数据通信。

[0123] 车辆DB32是登记关于车辆用数字钥匙系统Sys管理的车辆的信息的数据库。如图6所示,在车辆DB32中,每个车辆的车辆ID与车辆型号信息、所有者信息、客户信息建立对应关系并保存。车辆型号信息包含对象车型、年份、等级、OS(Operating System:操作系统)等所涉及的信息。

[0124] 车辆型号信息也可以包含在认证ECU4中使用的软件的版本、ECU编号等。这里的ECU编号是用于区分在多个车辆的每一个中使用的认证ECU4的编号,是按每个认证ECU4而不同的编号。作为ECU编号,能够采用认证ECU4的制造编号等。DKS3通过使用ECU编号,从而即使在多个车辆Hv中搭载有相同型号的认证ECU4的情况下,也能够执行将特定的认证ECU4设为对象的数据分发等。

[0125] 所有者信息是关于车辆Hv的所有者的信息,例如包含用户ID、作为联系方式的电话号码、电子邮件地址、设备ID等。客户信息是关于被分发与车辆Hv相关的服务密钥的用户(即客户)的信息。例如在车辆DB32中作为关于车辆Hv的客户信息,登记有每个客户的用户ID等。此外,车辆DB32也可以不具备客户信息。

[0126] 用户DB33是登记关于用户的信息的数据库。在用户DB33中,作为每个用户的用户数据,如图7所示,保存用户ID、密码、设备ID、密钥相关信息、备注信息等。用户ID和密码是用于认证用户的数据集。用户ID和密码例如在帐户创建时由用户登记。能够经由专用的网页或者数字钥匙应用104创建用于使用服务的帐户。例如可以通过DKS3与数字钥匙应用104通信从而登记用户持有的移动终端1的设备ID。

[0127] 密钥相关信息例如包含对象车辆信息、服务密钥ID、服务密钥、密钥属性、权限设定、所有者密钥ID。对象车辆信息表示用户可使用的车辆的ID。在由车辆DB32管理每个车辆的服务密钥信息的情况下,也可以用户DB33不具备对象车辆信息作为密钥相关信息。密钥类型例如表示是所有者密钥还是客户密钥等。密钥类型也能够解释为表示针对对象车辆的用户的属性(所有者/客户)的信息。权限设定如上述那样,表示能够锁定解锁的车门、是否允许行驶用电源的接通/断开等。所有者密钥ID表示对象车辆的所有者的服务密钥ID。所有者密钥ID相当于所有者密钥编号。所有者的用户数据中的所有者密钥ID这一栏也可以为空,也可以登记该所有者自身的服务密钥ID。

[0128] 备注栏可以登记年龄、驾驶技能的熟练度等。驾驶技能的熟练度也可以通过分数、级别等数值表示,也可以通过是否为初学者来表示。驾驶技能的熟练度也可以通过总行驶距离、总驾驶时间、是否为从取得驾驶执照起1年以内等来表示。此外,也可以在备注栏中登记事故的履历等。若在应用于汽车共享服务等的情况下,可以使用这些备注信息作为使用费、保险费等的计算材料。

[0129] 车辆DB32以及用户DB33均使用可改写的非易失性的存储介质实现。另外,车辆DB32以及用户DB33均构成为能够实施由服务器处理器301对数据的写入、读出、删除等。此外,车辆DB32和用户DB33也可以统合。上述的数据库的结构是一个例子。车辆DB32以及用户DB33不需要保持所有上述的项目。另外,也可以其它的服务器具备车辆DB32。本公开的DKS3也可以分为多个服务器来实施。每个服务器的任务分摊/功能配置能够适当地变更。

[0130] 如图8所示,数据处理部30具备用户管理部G1、用户认证部G2、服务密钥发放部G3、一次性认证密钥发放部G4、服务密钥删除部G5、以及机型变更接受部G6,作为功能部。

[0131] 用户管理部G1是管理用户信息的结构。例如用户管理部G1基于从网络连接装置31输入的数据,实施用户的新登记、删除、登记内容的变更。用户的新登记/删除对应于帐户的发放/删除。例如经由移动终端1以及网络连接装置31取得新登记、删除、登记内容的变更所涉及的用户操作/指示。

[0132] 以下,也将与帐户的创建、删除、登记内容的变更、服务密钥的发放/删除/无效化等这样的用户对车辆用数字钥匙系统Sys的操作/指示对应的信号简略地记载为操作信号。当然,直接接受用户的操作的接口不限定于移动终端1。DKS3可以经由设置于办公室、家庭的计算机取得上述操作信号。即DKS3构成为能够经由数字钥匙应用104、专用的网页取得用户的操作信号。

[0133] 用户认证部G2实施根据用户ID和密码的组合来认证用户的处理。基于用户认证部G2判定为认证成功,服务密钥发放部G3、一次性认证密钥发放部G4、服务密钥删除部G5、机型变更接受部G6等执行与用户的操作信号或者来自数字钥匙应用104的请求对应的处理。

[0134] 服务密钥发放部G3基于针对移动终端1等的用户操作来发放服务密钥。具体而言,基于从所有者终端、带发放权的客户终端发送来的服务密钥的发放请求信号,发放与请求内容对应的服务密钥。一次性认证密钥发放部G4基于从移动终端1发送来的一次性认证密钥发放请求信号,发放请求源用的一次性认证密钥。服务密钥删除部G5基于来自移动终端1的请求,删除指定的服务密钥。机型变更接受部G6是接受机型变更的申请,而发放与新的设备ID对应的服务密钥的结构。

[0135] 一次性认证密钥发放部G4、服务密钥删除部G5、以及机型变更接受部G6的详细内容另外后述。

[0136] 数据处理部30通过具备以上的功能部,从而保持系统管理的每个车辆的所有者与客户的对应关系。对于一个车辆,成为所有者的用户仅为一人,而客户可存在多个。数据处理部30综合地管理与一个车辆以及所有者建立关联的客户的信息。

[0137] 图9是概念性地表示针对一个车辆的所有者密钥与客户密钥的对应关系的图。数据处理部30基于所有者密钥的服务密钥ID,即所有者密钥ID,管理与一个车辆以及一个所有者密钥建立关联的多个客户密钥。此外,在图9中示出针对一个车辆发放了三个客户密钥的情况。各客户密钥如上述那样,权限设定、有效期限可能不同。

[0138] ＜关于车载系统7的结构以及功能＞

[0139] 这里,对车载系统7的结构以及功能进行说明。如图10所示,车载系统7具备认证ECU4、显示器51、输入装置52、车身ECU53、锁定电动机54、电源ECU55、近场通信部56、BLE通信部57、以及蜂窝通信部58。

[0140] 认证ECU4与显示器51、输入装置52、车身ECU53、电源ECU55、近场通信部56、BLE通信部57、以及蜂窝通信部58的每一个经由车辆内网络Nw或者通过专用的信号线连接为能够相互通信。车身ECU53与锁定电动机54连接为能够通信。车辆内网络Nw是在车辆Hv内构建的通信网络。作为车辆内网络Nw的标准,能够采用Controller Area Network(以下,CAN:注册商标,控制器局域网)、Ethernet(注册商标)、FlexRay(注册商标)等多种标准。此外,车身ECU53等的一部分也可以不经由车辆内网络Nw而与认证ECU4通过专用线连接。装置彼此的连接方式能够适当地变更。

[0141] 认证ECU4是通过与BLE通信部57等的合作来执行移动终端1的认证处理的ECU。另

外,认证ECU4以移动终端1的认证成功为条件,通过与其它的ECU的合作来实施车门的解锁、行驶用电源接通等这样的规定的车辆控制。认证ECU4具备车辆控制部40作为执行上述处理的核心模块。

[0142] 使用计算机实现该认证ECU4。即,认证ECU4具备认证处理器41、RAM42、储存器43、I/O44、以及将这些结构连接的总线等。认证处理器41例如是CPU。认证处理器41通过对RAM42的访问,来执行用于实现后述的各功能部的功能的各种处理。包含认证处理器41和RAM42的结构相当于车辆控制部40。认证处理器41与服务器处理器301相对比,也能够称为车辆处理器。在储存器43储存有访问车辆Hv的用户(实际上为移动终端)的认证处理所涉及的程序亦即车辆用认证程序。另外,也可以在储存器43保存有认证ECU4的ECU编号。I/O44是用于与其它装置进行通信的电路模块。认证ECU4的功能的详细内容后述。

[0143] 显示器51是显示图像的设备。例如显示器51可以基于来自认证ECU4的输入,显示所有者登记开始画面、服务密钥删除画面等。所有者登记开始画面是用于开始所有者密钥的登记的操作画面,例如可以包含输入所有者的密码的表单等。服务密钥删除画面是用于将由用户指定的服务密钥的数据从车辆侧存储部45删除的画面。认证ECU4保持的所有者密钥的数据也构成为能够经由该服务密钥删除画面删除。显示器51例如是设置于仪表板的车宽方向的中央区域的中央显示器。显示器51也可以是配置于驾驶座的正面区域的所谓的仪表显示器。

[0144] 输入装置52是用于接收用户针对车载系统7,更具体而言针对认证ECU4的指示操作的装置。作为输入装置52,例如能够采用层叠于显示器51的触摸面板。输入装置52也可以是设置于方向盘、仪表板等的机械式的开关。输入装置52将与用于对该装置进行的操作对应的电信号作为操作信号输出至认证ECU4。输入装置52输出的操作信号表示用户的操作内容。显示器51以及输入装置52相当于用于用户进行针对认证ECU4的服务密钥的登记/删除/动作设定的变更等的接口。也将显示器51以及输入装置52统称为车载HMI50。HMI是人机接口(Human Machine Interface)的缩写。

[0145] 车身ECU53是基于来自认证ECU4的请求以及用户的操作信号控制车身系统致动器的ECU。车身ECU53与各种车身系统致动器连接为能够通信。这里的车身系统致动器中包含构成各车门的锁定机构的锁定电动机54。

[0146] 电源ECU55是控制搭载于车辆Hv的行驶用电源的接通断开状态的ECU。例如电源ECU55例如基于来自认证ECU4的指示信号,将行驶用电源设定为接通。此外,在车辆Hv为发动机车辆的情况下,电源ECU55基于上述指示信号使发动机启动。

[0147] 近场通信部56是用于实施近场通信的通信模块。近场通信部56具有作为用于从专用钥匙2接收数据的读取器的功能。近场通信部56通过近场通信访问通信距离内的专用钥匙2,接收所有者验证所涉及的信息,例如接收基于专用钥匙代码或者专用钥匙代码的响应代码。近场通信部56不限于专用钥匙2,可以与移动终端1等位于通信范围内的多种设备也实施近场通信。

[0148] 作为近场通信部56,例如可以设置车外用的通信模块和车内用的模块。车外用的近场通信部56相当于用于进行面向锁定解锁控制的认证的结构。车内用的近场通信部56相当于用于进行面向行驶用电源的接通断开控制的认证的结构。车外用的近场通信部56例如设置于驾驶座用的外侧车门把手附近。外侧车门把手附近例如是指从外侧车门把手起0.2m

以内。在外侧车门把手附近中,也包含外侧车门把手的内部。另外,车内用的近场通信部56配置在车厢内的驾驶座周围。例如车厢内用的近场通信部56布置在配置于仪表板的开始按钮附近。车内用的近场通信部56也可以内置于开始按钮。并且,近场通信部56也可以设置于中央控制台、仪表板的车宽方向中央部。

[0149] BLE通信部57是用于实施BLE通信的通信模块。BLE通信部57例如配置于中央控制台、车内的车顶部、前/后玻璃的上端部、C柱等。蜂窝通信部58是实施蜂窝通信的通信模块。车载系统7也可以代替蜂窝通信部58、或者与蜂窝通信部58组合,而具备Wi—Fi通信用的模块。

[0150] 认证ECU4通过与DKS3以及移动终端1进行通信,来执行用户的认证所涉及的处理。此外,更具体而言,认证ECU4与移动终端1的通信可以通过移动终端1具备的BLE通信部16与车载系统7具备的BLE通信部57的合作来实现。

[0151] ,如图11所示,认证ECU4具备用户管理部H1、以及认证处理部H2,作为功能部。例如通过认证处理器41执行车辆用认证程序从而实现这些功能部。另外,认证ECU4具备用于存储所有者密钥等的车辆侧存储部45。使用储存器43或者RAM42具备的存储区域实现车辆侧存储部45。车辆侧存储部45具备所有者密钥存储部451和客户密钥存储部452。

[0152] 所有者密钥存储部451是用于储存与所有者密钥相关的信息的存储区域。客户密钥存储部452是用于储存与客户密钥相关的信息的存储区域。与所有者/客户密钥相关的信息除了服务密钥本身以外,还指服务密钥ID、用户ID、用户名等。在与客户密钥相关的信息中,还包含有效期限、权限设定等。客户密钥存储部452构成为能够保存多个客户密钥,另一方面,所有者密钥存储部451构成为仅能够保存一个所有者密钥。因此,新所有者密钥的登记相当于伴随着老所有者密钥的数据删除的所谓的重写处理。车辆侧存储部45相当于车辆侧存储装置。

[0153] DKS3已发放的服务密钥通过被登记至车辆侧存储部45而被有效化。即,用户以面向该用户的服务密钥保存于车辆侧存储部45为条件,而能够在分配给服务密钥的权限的范围内使用车辆Hv。

[0154] 用户管理部H1是管理能够使用车辆Hv的用户,即管理保存于车辆侧存储部45的服务密钥的结构。用户管理部H1如另外后述的那样,通过与移动终端1实施BLE通信,来经由移动终端1取得与DKS3已发放的服务密钥相关的数据,并将该数据保存于车辆侧存储部45。另外,用户管理部H1经由移动终端1取得用于删除保存于车辆侧存储部45的服务密钥的数据,并删除与成为对象的服务密钥相关的数据。

[0155] 认证ECU4具备能够接受所有者密钥的登记的可登记所有者模式、和不接受(拒绝)所有者登记的禁止登记所有者模式,作为动作模式。认证ECU4基本上以禁止登记所有者模式进行动作。因此,禁止登记所有者模式能够称为通常模式。认证ECU4基于输入有另外后述的安全解除代码,而暂时从禁止登记所有者模式移至可登记所有者模式。

[0156] 认证处理部H2与BLE通信部57协作,来实施确认(换言之,认证)通信对象是车辆Hv的用户持有的移动终端1的处理。用于认证的通信被加密并实施。认证方式本身可使用质询—响应方式等多种方式来实施。在本实施方式中作为一个例子,以使用了质询代码和一次性认证密钥的质询—响应方式进行认证。关于认证处理的详细的时序另外后述。认证处理部H2具备动态地生成认证处理中所需的一次性认证密钥的一次性认证密钥生成部H21作

为子功能部。此外,一次性认证密钥生成部H21是任意的要素,也可以省略。

[0157] 认证处理部H2实施认证处理的定时例如能够设为BLE通信部57与移动终端1的通信连接确立的定时。认证处理部H2也可以构成为在BLE通信部57与移动终端1通信连接期间,以规定的周期实施认证处理。认证处理部H2也可以以针对车辆Hv的规定的用户操作作为触发,实施用于认证处理的加密通信。

[0158] 作为成为认证处理的执行触发的用户操作,能够采用车门按钮的按下/对外侧车门把手的触摸、开始按钮的按下、车门的开闭等。车门按钮是指设置于外侧车门把手的用于解锁/锁定车门的按钮。可以由设置于外侧车门把手的触摸传感器检测对外侧车门把手的触摸。开始按钮是设置于仪表板等车厢内的用于切换行驶用电源的接通/断开的按钮。

[0159] ＜关于所有者密钥登记时序＞

[0160] 这里,使用图12、图13、以及图14,对所有者密钥的从发放至向车辆登记的时序的一个例子进行说明。如图12所示,所有者密钥的从发放至向车辆登记的时序大致能够分为发放阶段Ph1和车辆登记阶段Ph2。

[0161] 发放阶段Ph1是DKS3基于来自用户的请求,实际上基于从移动终端1发送的密钥发放请求信号,来发放服务密钥的阶段。发放的服务密钥仅分发至移动终端1。DKS3已发放的服务密钥并不直接分发至车辆Hv,而经由移动终端1登记至车辆。车辆登记阶段Ph2是通过BLE通信将移动终端1保持的服务密钥的信息登记至车辆Hv的阶段。DKS3已发放的服务密钥登记至车辆Hv而首次成为实质上可使用的状态,即被有效化。因此,车辆登记阶段Ph2也能够称为有效化阶段。此外,不限于所有者密钥,客户密钥的发放～有效化也包含发放阶段Ph1和车辆登记阶段Ph2。

[0162] 图13是表示与所有者密钥的发放阶段对应的各设备的交互的时序图。所有者密钥的发放时序由所有者终端和DKS3执行。如图13所示,所有者密钥的发放时序包含步骤S10～S17。

[0163] 步骤S10是DKS3认证用户/移动终端1,确认通信对象是所有者/所有者终端的步骤。是所有者的认证也可以使用用户ID以及密码实施,也可以使用生物体信息认证。使用了生物体信息的认证可以由生物体认证装置14执行。此外,步骤S10也可以是移动终端1的数字钥匙应用104认证用户的步骤。

[0164] 步骤S11是作为所有者终端的移动终端1基于用户的操作发送密钥发放请求信号的步骤。这里,发送的密钥发放请求信号是请求所有者密钥的发放的信号,因此能够称为所有者密钥发放请求信号。密钥发放请求信号例如包含设备ID或者用户ID等用于DKS3确定请求源的信息。另外,密钥发放请求信号包含设为发放对象的服务密钥的类型。此外,在设为发放对象的服务密钥为客户密钥的情况下,密钥发放请求信号可以追加地包含表示权限的设定、有效期限的设定等的信息。此外,密钥发放请求信号也可以包含设为对象的车辆的信息等。但是,对象车辆的信息能够通过以用户ID等为检索关键词参照车辆DB32来确定,因此也可以不包含于密钥发放请求信号。

[0165] 在步骤S12中,DKS3基于从所有者终端取得的所有者密钥发放请求信号,生成作为所有者密钥的服务密钥以及服务密钥ID。更具体而言,步骤S12的执行主体是服务密钥发放部G3。

[0166] 在步骤S13中,DKS3基于通过步骤S12生成的服务密钥,创建规定量的一次性认证

密钥。更具体而言,步骤S13的执行主体是一次性认证密钥发放部G4。在服务密钥发放时生成的一次性认证密钥的数量亦即初次发放数设定得比补充阈值多规定量,例如多300等。

[0167] 在步骤S14中,DKS3将包含通过步骤S12～S13生成的各种数据的数据集亦即终端登记用数据包朝向所有者终端发送。终端登记用数据包包含服务密钥、服务密钥ID、多个一次性认证密钥、以及用于各一次性认证密钥的生成的变动代码。各个一次性认证密钥与用于该一次性的生成的变动代码建立关联。包含多个一次性认证密钥以及变动代码的数据集也可以作为认证密钥数据包而与包含服务密钥的数据集分开发送。

[0168] 另外,终端登记用数据包可以包含终端校验码、搭载于对象车辆的认证ECU4的ECU编号。终端校验码是用于作为接收侧的移动终端1验证数据的完整性、接收数据的合法性、以及有无篡改的代码。终端校验码也可以是汉明码,也可以是将有效载荷输入至规定的哈希函数而得到的哈希值。也可以使用作为用于DKS3与移动终端1进行加密通信的密钥而预先发放的加密密钥来生成终端校验码。

[0169] 在步骤S15中,是作为所有者终端的移动终端1接收从DKS3分发的终端登记用数据包,并将其内容保存于密钥信息存储部M1的步骤。服务密钥管理部F1在使用上述的终端校验码验证接收数据的合法性的基础上,将接收到的服务密钥以及其相关信息保存于密钥信息存储部M1。

[0170] 步骤S16中,DKS3将用于将所有者信息登记至车辆Hv的数据集亦即车辆登记用数据包朝向所有者终端发送。车辆登记用数据包除了服务密钥、服务密钥ID以外,还可以包含车辆校验码。车辆校验码是用于作为最终的接收设备的认证ECU4验证数据的完整性、接收数据的合法性、以及有无篡改的代码。也可以车辆校验码与终端校验码相同地,是与有效载荷对应的汉明码、哈希值。也可以使用作为用于DKS3与认证ECU4进行加密通信的密钥而预先发放的加密密钥来生成车辆校验码。另外,也可以基于ECU编号生成车辆校验码。此外,也可以在车辆登记用数据包中附加有终端校验码。根据该结构,作为DKS3与认证ECU4的通信的中继角色的所有者终端也能够验证接收到的车辆登记用数据包的完整性、合法性等。

[0171] 步骤S17是作为所有者终端的移动终端1接收从DKS3分发的车辆登记用数据包,并将其内容保存于车辆用数据临时存储部M2的步骤。也可以在接收处理中包含使用了上述的终端校验码的验证处理。此外,在本实施方式中分别发送车辆登记用数据包和终端登记用数据包,但各种数据的发送方式不限于此。也可以车辆登记用数据包和终端登记用数据包作为一系列的数据发送。此时,也可以省略重复的数据。

[0172] 使用接下来的图14,对将所有者密钥登记至车辆Hv的时序进行说明。所有者密钥向车辆Hv的登记时序包含步骤S20～S29。

[0173] 首先,作为本时序开始时的初始状态(步骤S20),认证ECU4以禁止登记所有者模式(即通常模式)进行动作。步骤S21是规定的安全解除工具或者DKS3将规定的安全解除信号输入至认证ECU4的步骤。使用了安全解除工具或者DKS3的安全解除信号向认证ECU4的输入由所有者或者经销商工作人员执行。

[0174] 安全解除信号包含安全解除代码的信号。安全解除信号在一个方面相当于证明登记者是所有者自身的信号。安全解除信号相当于用于将认证ECU从禁止登记所有者模式(通常模式)暂时切换至可登记所有者模式的信号。基于输入安全解除信号,认证ECU4移至可登记所有者模式(步骤S22)。安全解除信号相当于所有者登记开始信号。

[0175] 安全解除工具例如是专用钥匙2。另外,作为安全解除代码,能够采用专用钥匙代码。例如也可以认证ECU4基于车内用的近场通信部56与专用钥匙2进行近场通信并接收到专用钥匙代码,而移至可登记所有者模式。此外,认证ECU4也可以构成为除了接收到专用钥匙代码以外,还以经由车载HMI50输入规定的密码为条件,移至可登记所有者模式。

[0176] 另外,安全解除工具也可以是由经销商商店等管理的专用工具。专用工具与认证ECU4的通信方式也可以是近场通信,例如也可以是使用了USB电缆等的有线通信。经由蜂窝通信部58接收来自DKS3的安全解除信号。此外,DKS3基于来自所有者终端的请求、或者来自设置于经销商商店的规定的终端的请求,发送以车辆Hv为目的地的安全解除信号。根据该结构,所有者或者经销商商店的工作人员能够通过操作所有者终端或者设置于经销商商店的规定的终端,来将认证ECU4切换至可登记所有者模式。

[0177] 若移至所有者登记模式,则作为步骤S24a,认证ECU4以规定的扫描间隔将BLE通信部57设定为等待状态,并实施移动终端1的搜索(所谓的扫描)。这里的待受状态是指能够接收广告信号的状态。在本实施方式中,通过被动扫描方式检测存在于车辆周边的移动终端1。作为其它的方式,也可以认证ECU4通过伴随着扫描请求的发送的主动扫描方式来搜索移动终端1。

[0178] 另一方面,所有者终端若经由触摸面板12接受所有者密钥的登记开始操作(步骤S23),则以规定的间隔实施用于所有者密钥的登记的广告的发送(步骤S24b)。通过经由BLE通信部57在认证ECU4接收该广告,从而认证ECU4和移动终端1开始用于通信连接的通信(步骤S25)。此外,例如如图15所示,所有者密钥的登记开始操作是显示于显示器11的所有者密钥登记开始按钮B1的按下。所有者密钥的登记开始操作也可以是指示所有者密钥的登记开始的语音指令的输入。

[0179] 若认证ECU4与BLE通信的连接确立,则所有者终端例如显示图16所示的配对确认画面。配对确认画面例如包含用于用户选择是否执行配对的按钮B2a、B2b。所有者终端若基于来自触摸面板12的信号检测到肯定按钮B2a被按下(步骤S26),则执行与认证ECU4的配对处理(步骤S27)。由此,能够在认证ECU4与所有者终端之间进行加密后的数据通信。这里的配对处理中不仅包含加密密钥的交换,还包含加密密钥的保存(所谓的绑定)。

[0180] 若配对处理完成,认证ECU4—所有者终端间的加密通信链路已确立,则所有者终端通过BLE通信将保管于车辆用数据临时存储部M2的车辆登记用数据包发送至认证ECU4(步骤S28)。步骤S24a～S28的一系列的通信对认证ECU4而言相当于用于从所有者终端取得所有者密钥的通信。

[0181] 若通过BLE通信从所有者终端接收车辆登记用数据包,则认证ECU4将该数据包中包含的密钥相关数据保存于车辆侧存储部45。更具体而言,将接收到的服务密钥、服务密钥ID保存于所有者密钥存储部451。由此,所有者密钥的车辆登记完成,所有者密钥被有效化。

[0182] 此外,禁止登记所有者模式也可以例如通过拒绝具有所有者权限的服务密钥的接收或者保存来实现,也可以通过拒绝通信连接本身来实现。另外,作为一个方式,认证ECU4也可以构成为将通过以包含规定的所有者登记用ID的广告为起点的通信链路接收到的服务密钥作为所有者密钥保存于所有者密钥存储部451。在该情况下,认证ECU4在禁止登记所有者模式时忽略包含所有者登记用ID的广告,另一方面,在所有者登记模式时进行基于包含所有者登记用ID的广告的通信连接。所有者登记用ID是表示是用于登记所有者信息的通

信的ID,可以通过UUID、Major、Minor这三个种类的标识符的组合来表示。

[0183] 根据上述的结构,仅在特定的所有者登记开始信号输入至认证ECU4的情况下,才将所有者密钥的数据登记至车辆Hv。因此,与始终能够登记所有者密钥的结构相比能够提高安全性。

[0184] ＜关于客户密钥登记时序＞

[0185] 接下来,使用图17、图18、图19、图20,对从客户密钥的发放至将该客户密钥登记至车辆Hv的时序的一个例子进行说明。客户密钥的从发放至车辆登记的时序也能够分为发放阶段Ph1和车辆登记阶段Ph2。

[0186] 图17是表示与客户密钥的发放阶段Ph1对应的各设备的交互的时序图。客户密钥的发放时序由所有者终端、对象客户终端、以及DKS3执行。对象客户终端是指与设为服务密钥的发放对象的客户建立关联的移动终端1。如图17所示,客户密钥的发放时序包含步骤S30～S37。

[0187] 客户密钥的发放以及向车辆的登记时序的说明中的客户终端是指对象客户终端。另外,以下对所有者发放客户密钥的情况进行说明,但客户密钥的发放者也可以是被赋予带发放权的客户密钥的客户。也将被赋予带发放权的客户密钥的客户记载为有发放权的客户。客户密钥的发放等的说明中的所有者终端/所有者的记载能够替换为带发放权的客户终端/有发放权的客户来实施。

[0188] 步骤S30是基于希望服务密钥的发放的客户的操作,客户终端朝向所有者终端发送客户密钥的发放委托的步骤。所有者终端若接收到来自客户终端的发放委托,则朝向DKS3发送客户密钥发放请求信号(步骤S31)。此外,虽然省略图示,但客户密钥的发放时序还可以包含DKS3认证作为所有者的用户的步骤。另外,步骤S30是任意的要素。即使没有来自客户终端的发放委托,所有者终端也可以基于所有者的操作发送将规定的客户设为对象的客户密钥发放请求信号。例如所有者构成为能够通过基于与客户的电话/邮件等的交涉来操作所有者终端,从而对任意的客户发放客户密钥。

[0189] 例如如图18所示,客户密钥发放请求信号包含容纳请求源信息、对象车辆信息、对象用户ID、有效期限信息、以及权限的设定信息的每一个的数据字段。请求源信息是表示客户密钥的发放请求源的信息,例如能够采用所有者的用户ID、服务密钥ID、设备ID等。对象车辆ID是用于确定能够通过新发放的客户密钥使用的车辆的信息,这里是指车辆Hv的车辆ID。对象用户ID是设为客户密钥的发放对象的客户的用户ID。也可以代替用户ID而采用设备ID等作为对象用户信息。在与有效期限对应的数据字段中,输入与所有者指定的期间/时间对应的值、或者规定值。权限设定信息表示有无客户密钥的发放权、有无行驶用电源的切换权限、能够锁定解锁的车门等。

[0190] 若接收到来自所有者终端的客户密钥发放请求信号,则作为步骤S32,DKS3基于接收到的客户密钥发放请求信号,生成面向对象客户的服务密钥以及服务密钥ID。另外,在步骤S33中,DKS3的一次性认证密钥发放部G4基于通过步骤S32生成的服务密钥,创建规定的初次发放数的一次性认证密钥。

[0191] 在步骤S34中,DKS3将包含通过步骤S32～S33生成的各种数据的数据集亦即终端登记用数据包向客户终端发送。例如如图19所示,客户密钥所涉及的终端登记用数据包除了基本信息以外,还可以包含客户用信息。基本信息具有与在所有者密钥发放时分发的数

据包大致相同的项目。即基本信息包含服务密钥、服务密钥ID、多个一次性认证密钥、以及每个一次性认证密钥的变动代码。客户用信息是客户密钥用的附加的信息。例如客户用信息包含发放源信息、所有者密钥ID、对象车辆信息、有效期限信息、权限设定信息。发放源信息基本上表示所有者。但是,在新发放的客户密钥是基于来自带发放权的客户终端的请求生成的密钥的情况下,也可以在发放源信息的数据字段(栏)储存表示作为发放源的客户的信息。终端登记用数据包也可以构成为仅具备发放源信息与所有者密钥ID的任意一方。朝向客户终端发出的终端登记用数据包还包含终端校验码等。

[0192] 在步骤S35中,作为客户终端的移动终端1接收从DKS3分发的终端登记用数据包,并将其内容保存于密钥信息存储部M1。在步骤S36中,DKS3将用于将客户密钥信息登记至车辆Hv的数据集亦即车辆登记用数据包向客户终端发送。客户密钥所涉及的车辆登记用数据包中包含的信息种类能够设为与通过步骤S36发送的车辆登记用数据包相同。在步骤S37中,是作为客户终端的移动终端1接收从DKS3分发的车辆登记用数据包,并将其内容保存于车辆用数据临时存储部M2的步骤。

[0193] 使用接下来的图20,对客户终端将从DKS3接收到的客户密钥登记至车辆Hv的时序进行说明。客户密钥向车辆Hv的登记时序包含步骤S40～S47。作为前提,假设客户终端存在于车辆Hv的周边,更具体而言存在于可BLE通信的位置。客户终端执行的步骤的实质上的执行主体是终端处理器101。另外,认证ECU4执行的步骤的实质上的执行主体是认证处理器41。

[0194] 首先,作为本时序开始时的初始状态(步骤S40),认证ECU4以通常模式进行动作。关于客户密钥,即使认证ECU4为通常模式也能够进行登记。因此,与所有者密钥的登记时序不同,所有者以及客户不需要使用安全解除工具等变更认证ECU4的动作模式。认证ECU4在通常模式时也以规定的扫描间隔实施扫描(步骤S42a)。

[0195] 另一方面,客户终端若经由触摸面板12接受客户密钥的登记开始操作(步骤S41),则以规定的间隔发送用于客户密钥的登记的广告的发送(步骤S42b)。通过经由BLE通信部57在认证ECU4接收该广告,从而认证ECU4和移动终端1开始用于通信连接的通信(步骤S43)。此外,例如如图21所示,客户密钥的登记开始操作是显示于显示器11的客户密钥登记开始按钮B3的按下。客户密钥的登记开始操作也可以是规定的语音短语的输入。

[0196] 若认证ECU4与BLE通信的连接确立,则客户终端例如显示图16所示的配对确认画面。若基于来自触摸面板12的信号检测到肯定按钮B2a被按下(步骤S44),则客户终端执行与认证ECU4的配对处理(步骤S45)。由此,能够在认证ECU4与客户终端之间进行加密后的数据通信。

[0197] 若配对处理完成,认证ECU4－客户终端间的加密通信链路已确立,则客户终端通过BLE通信将保管于车辆用数据临时存储部M2的车辆登记用数据包发送至认证ECU4(步骤S46)。

[0198] 若通过BLE通信从客户终端接收车辆登记用数据包,则认证ECU4将该数据包中包含的密钥相关数据保存于车辆侧存储部45(步骤S47)。更具体而言,将接收到的服务密钥、服务密钥ID、权限设定、有效期限等保存于客户密钥存储部452。由此,客户密钥向车辆Hv的登记完成,客户密钥被有效化。

[0199] 根据上述结构,不需要为了使客户密钥有效化而所有者终端与认证ECU4通过BLE

通信连接。即,所有者不需要每次发放客户密钥时都将所有者终端带至车辆Hv的附近。因此,根据上述的结构,能够减少客户密钥的有效化所涉及的所有者的负担。另外,在本实施方式中认证ECU4与所有者密钥、客户密钥这样的服务密钥的类型无关地,通过与移动终端1的BLE通信取得并保存车辆登记用数据包。根据该结构,能够抑制车辆Hv中的数据通信量。并且,在车辆Hv在地下停车场等通信范围外的情况下,能够伴随着用户的接近而将服务密钥登记至车辆Hv。当然,作为其它的方式,也可以认证ECU4通过蜂窝通信或者Wi－Fi通信从DKS3取得车辆登记用数据包。此外,经由移动终端1将服务密钥发送至车辆Hv的结构相当于将服务密钥间接地分发至认证ECU4的结构。

[0200] ＜用户使用车辆的情况的系统工作例＞

[0201] 这里,使用图22、图23,对用户使用车辆Hv时的认证ECU的工作进行说明。作为前提,这里所述的用户是携带保存有车辆Hv的服务密钥的移动终端1的人物。即,这里的用户相当于所有者或者客户,移动终端1相当于所有者终端或者客户终端。

[0202] 首先,在车辆Hv停车期间,认证ECU4定期地使BLE通信部57实施扫描,判定移动终端1是否存在于车辆周边(步骤S51)。基于是否接收到广告等从移动终端1发出的BLE信号,来实施移动终端1是否存在于车辆周边的判定。假设在接收到来自移动终端1的BLE信号的情况下(步骤S51“是”),与该移动终端1通信连接(步骤S52)。另一方面,在扫描的结果是未能发现移动终端1的情况下,结束本流程。此外,在结束了流程的情况下,在经过规定的扫描间隔的定时再次执行步骤S51。图22所示的流程图可以在车辆Hv停车的状态下以规定的扫描间隔反复实施。

[0203] 认证ECU4在已与移动终端1通信连接的情况下,执行认证处理作为步骤S53。关于认证处理另外后述。在作为认证处理的结果而移动终端1(进而用户)的认证成功的情况下(步骤S54“是”),移至待机模式(步骤S55)。

[0204] 待机模式相当于能够基于针对车门按钮等的用户操作,实施解锁/锁定、行驶用电源的接通/断开切换等的状态。待机模式在一个方面对应于认证处理器41识别出具有服务密钥的移动终端1/用户存在于车辆周边的状态。在车辆周边中,不仅包含车外还包含车厢内。在本实施方式中作为一个例子,对认证成功的判定结果设定有效期限。有效期限例如设定为13秒、5秒、10秒等。

[0205] 另一方面,在作为认证处理的结果而移动终端1的认证失败的情况下(步骤S54“否”),结束本流程。此外,在认证处理失败的情况下,也可以使车载设备动作,使得用户能够识别到认证未成功。例如,在认证处理未成功的情况下,也可以在显示器51显示规定的认证失败图像,也可以以规定模式使设置于侧方后视镜等的灯光装置点亮。也可以认证ECU4在认证处理失败的情况下,通过以BLE通信朝向移动终端1发送规定的控制信号,从而使显示器11显示认证失败画面。认证ECU4也可以通过将朝向车门周围的路面发出光的迎宾灯以规定模式点亮,从而表示认证失败。

[0206] 在步骤S56中,认证处理器41基于来自车门按钮、触摸传感器、开始按钮等的信号,判定是否进行了用于使用车辆Hv的用户操作。用于使用车辆Hv的用户操作例如是指触摸/握住车门把手等这样的想要打开车门的行为。开始按钮的按下也相当于用于使用车辆Hv的用户操作。

[0207] 在从车载传感器输入了与上述用户操作对应的信号的情况下(步骤S56“是”),认

证处理器41执行与用户进行了操作的部件以及车辆Hv的状态对应的车辆控制(步骤S57)。例如在车辆Hv锁定的状态下检测到车门按钮被按下/车门把手被握持的情况下,认证处理器41解锁车门。另外,在检测到开始按钮被按下的情况下,认证处理器41将行驶用电源从断开切换至接通,或者从接通切换至断开。

[0208] 此外,在实际上进行上述车门的解锁/锁定、行驶用电源的接通/断开这样的车辆控制时,不仅参照认证结果,还参照移动终端1的估计位置、服务密钥的权限、车辆Hv的状态。而且,在未满足规定的控制执行条件的情况下,可以取消与用户操作对应的车辆控制的执行。未满足控制执行条件的情况例如是服务密钥中设定的权限不足的情况、检测到的移动终端1的位置远离车辆2m以上的情况等。移动终端1的位置可以基于来自移动终端1的信号的接收状况来确定。作为移动终端1的位置估计材料,能够采用接收强度、信号的到达方向、ToF(Time of Flight;飞行时间),RTT(Round-Trip Time:往返时间)等多种指标。

[0209] 另一方面,在未进行用于使用车辆Hv的用户操作的情况下(步骤S56“否”),判定是否已过认证结果的有效期限,即从判定为认证成功起是否已经过规定时间。在为有效期限内期间(步骤S58“否”),维持待机模式。另一方面,在已过有效期限的情况下,认证处理器41再次执行用于认证处理的通信。

[0210] 根据上述的结构,用户不操作专用钥匙2、移动终端1就能够访问车辆Hv。即,实现被动进入被动启动功能,能够提高用户的便利性。

[0211] ＜关于认证处理＞

[0212] 这里,对认证ECU4认证移动终端1的处理的时序进行说明。例如如图23所示,认证ECU4对移动终端1的认证处理具备步骤S61～S68。此外,以移动终端1与认证ECU4的加密后的通信链路已确立为前提来执行认证处理。

[0213] 步骤S61是从认证ECU4朝向移动终端1发送质询代码的步骤。作为质询代码,能够采用使用预先准备的随机数表生成的规定长度的随机数。质询代码也可以是使用认证ECU4具备的时刻信息(所谓的系统时刻)作为SEED而生成的随机数。质询代码可通过多种方法决定。

[0214] 步骤S62是移动终端1通过将保存于密钥信息存储部M1的任意的一次性认证密钥与接收到的质询代码以规定的方式组合,从而生成响应代码的步骤。步骤S63是移动终端1将通过步骤S62生成的响应代码、以及与用于该响应代码的生成的一次性认证密钥对应的变动代码集中/分别返回至认证ECU4的步骤。与某一次性认证密钥对应的变动代码是指在DKS3中用于该一次性认证密钥的生成的变动代码。

[0215] 步骤S64中,认证ECU4使用从移动终端1接收到的变动代码、与保存于车辆侧存储部45的与通信对象对应的服务密钥,通过与DKS3的一次性认证密钥发放部G4相同的方法生成一次性认证密钥。这里,认证ECU4用于一次性认证密钥的生成的服务密钥与变动代码的组合和移动终端1用于响应代码的生成的一次性认证密钥的生成材料相同。因此在步骤S64中认证ECU4生成的一次性认证密钥与移动终端1用于响应代码的生成的一次性认证密钥相同。这样的步骤S64相当于基于从移动终端1接收到的变动代码和自身保持的移动终端1的服务密钥,恢复移动终端1用于响应代码的生成的一次性认证密钥的处理。

[0216] 在步骤S65中,是认证ECU4基于通过步骤S64生成的一次性认证密钥和通过步骤S61发送的质询代码,生成验证用代码的步骤。验证用代码的生成方法本身与响应代码的生

成相同。在通信对象是保持登记于车辆侧存储部45的服务密钥的移动终端1的情况下,能够期待验证用代码与响应代码一致。另外,在通信对象是未登记的设备的情况下,不返回响应代码,或者响应代码与验证用代码不一致。因此,响应代码作为用于认证ECU4验证通信伙伴的合法性的信息发挥功能。

[0217] 在步骤S66中,认证ECU4通过比较通过步骤S65生成的验证用代码与从移动终端1接收到的响应代码,从而判断通信对象的合法性。即,在两个代码一致的情况下判定为认证成功(步骤S67)。另一方面,在两个代码不同的情况下判定为认证失败(步骤S68)。此外,在从质询代码的发送起经过规定的响应待机时间还未返回响应代码的情况下,认证ECU4也可以判定为认证失败。

[0218] 根据上述结构,使用基于每个移动终端1固有的服务密钥生成的一次性认证密钥来进行移动终端1以及用户的认证。因此,与使用固定的密钥信息进行移动终端的认证的结构相比,能够提高安全性。另外,根据上述的方法,在响应代码的生成时认证ECU4与移动终端1之间交换的信息是变动代码和质询代码。在认证时,不在认证ECU—移动终端间收发一次性认证密钥本身。在一次性认证密钥的生成中,需要另外在服务密钥的发放阶段分发的服务密钥,仅通过监听变动代码并不能进行一次性认证密钥的恢复。并且,用于认证的一次性认证密钥每次都变更。因此,根据上述的方法,能够防止无关的人物非法地使认证处理成功的担忧。这里的无关的人物是指未被赋予车辆Hv的服务密钥的人物。

[0219] 此外,上述的认证时序是一个例子,并不限于此。设计各设备的动作,使得在移动终端1与认证ECU4间,用于响应代码/验证用代码的生成的一次性认证密钥相同即可。例如认证处理也可以通过图24所示的步骤实施。即,作为另一个例子,认证处理可以具备步骤S61a～S69a。

[0220] 此外,在采用图24所示的认证处理模式的情况下,作为前提结构,假设认证ECU4和移动终端1保持共同的多个一次性认证密钥。例如认证ECU4通过接收包含多个一次性认证密钥的数据集作为车辆登记用数据包,从而取得与移动终端1保持的秘钥相同的一次性认证密钥。对各一次性认证密钥赋予用于识别它们的编号。此外,认证ECU4在保存于车辆侧存储部45的一次性认证密钥不足规定的补充阈值的情况下,以移动终端1的认证成功为条件,从移动终端1接收认证ECU4未取得的一次性认证密钥以及其密钥编号。由此,认证ECU4可以补充保存于车辆侧存储部45的一次性认证密钥。当然,认证ECU4也可以构成为从DKS3取得直接一次性认证密钥。移动终端1如另外后述的那样随时通过与DKS3的通信补充一次性认证密钥。

[0221] 步骤S61a是认证ECU4朝向移动终端1发送使用密钥确认信号的步骤。使用密钥确认信号是询问使用预定密钥的编号的信号。使用预定密钥是指用于之后的响应代码的生成的一次性认证密钥。使用密钥确认信号相当于调整消息。

[0222] 若接收到使用密钥确认信号,则作为步骤S62a,移动终端1将使用预定密钥的编号通知给认证ECU4。作为使用预定密钥的决定方法,能够采用任意的方法。例如将移动终端1保持的一次性认证密钥中编号最小的秘钥选定为使用预定密钥。

[0223] 此外,移动终端1通过后述的一次性认证密钥的有效期限管理依次删除已过有效期限的秘钥。认证ECU4也进行相同的有效期限管理,但认证ECU4与移动终端1的时刻信息并不一定完全一致。另外,进行基于有效期限的一次性认证密钥的废弃处理的定时也可以不

同。根据这些情况,认证ECU4并不一定保持移动终端1所保持的使用预定密钥。

[0224] 认证ECU4也可以在自身未保持从移动终端1通知的使用预定密钥的情况下,向移动终端1请求使用其它的密钥。步骤S61a～S62a也可以反复实施直到选择认证ECU4和移动终端1双方保持的一次性认证密钥。此外,为了更高效地进行使用预定密钥的磋商,使用密钥确认信号也可以包含从认证ECU4保持的一次性认证密钥中随机地/按规定规则选择出的多个候补的编号。移动终端1也可以构成为从这些多个候补中随机地/按照规定的规则选择使用预定密钥并回答。

[0225] 步骤S63a是认证ECU4与步骤S61相同地发送质询代码的步骤。步骤S64a是认证ECU4基于与从移动终端1作为使用预定密钥而通知的编号对应的一次性认证密钥、和通过步骤S63a发送的质询代码,生成验证用代码的步骤。一次性认证密钥本身使用保存于车辆侧存储部45的一次性认证密钥。

[0226] 步骤S65a是移动终端1使用与选定为使用预定密钥的编号对应的一次性认证密钥、和从认证ECU4接收到的质询代码,生成响应代码的步骤。用于响应代码的生成的一次性认证密钥本身是预先从DKS3取得并已保存于终端侧存储部105的秘钥。若响应代码的生成完成,则作为步骤S66a,移动终端1将该响应代码朝向认证ECU4发送。

[0227] 若从移动终端1接收响应代码,则作为步骤S67a,认证ECU4通过比较该响应代码与通过步骤S65a生成的验证用代码,来判断通信对象的合法性。即,在两个代码一致的情况下判定为认证成功(步骤S68a)。另一方面,在两个代码不同的情况下判定为认证失败(步骤S69a)。

[0228] 根据上述的方法,在响应代码的生成时认证ECU4与移动终端1之间交换的信息是使用预定密钥的编号和质询代码,一次性认证密钥本身并不通过通信收发。仅通过密钥编号无法恢复一次性认证密钥。因此,通过上述的方法,也与上述的认证方法相同地,能够减少无关的人物非法地使认证处理成功的担忧。此外,在上述的例子中,叙述了在响应代码的生成前,移动终端1将使用预定密钥的编号通知给认证ECU4的方式,但处理顺序不限于此。也可以移动终端1在生成响应代码后,对认证ECU4通知用于响应代码的生成的一次性认证密钥的编号。

[0229] ＜一次性认证密钥的补充时序＞

[0230] 这里,使用图25,对移动终端1执行的一次性认证密钥补充处理进行说明。一次性认证密钥补充处理是当一次性认证密钥低于规定的补充阈值ThRp时进行补充的处理。如图25所示,一次性认证密钥补充处理具备步骤S71～S77。例如以规定的剩余数量确认周期定期地执行一次性认证密钥补充处理。也可以以移动终端1是在线状态为条件执行一次性认证密钥补充处理。此外,也可以基于接收到从DKS3发送的剩余数量确认指示信号、用户实施了规定的剩余数量确认操作而开始一次性认证密钥补充处理。一次性认证密钥补充处理也可以作为后述的保存认证密钥更新处理的一部分来执行。剩余数量确认指示信号的接收、剩余数量确认操作的接受等相当于确认事件。

[0231] 作为一次性认证密钥补充处理的执行主体的移动终端1这一表达能够理解为终端处理器101/一次性认证密钥管理部F2。

[0232] 步骤S71是移动终端1确认保存于终端侧存储部105的一次性认证密钥的剩余数量(Notk)的步骤。步骤S72是移动终端1判定通过步骤S71取得的一次性认证密钥的剩余数量

(Notk)是否不足规定的补充阈值(ThRp)的步骤。在满足Notk＜ThRp的情况下,作为步骤S73,移动终端1朝向DKS3发送认证密钥请求信号。认证密钥请求信号是请求一次性认证密钥的分发的信号。认证密钥请求信号相当于补充请求信号。另一方面,在满足Notk≧ThRp的情况下,移动终端1结束一次性认证密钥的补充所涉及的时序。

[0233] 此外,如上述那样,可以通过是否需要补充标志来管理一次性认证密钥是否需要补充。在满足Notk＜ThRp的情况下,移动终端1将是否需要补充标志设定为接通。另外,在满足Notk≧ThRp的情况下,移动终端1将是否需要补充标志设定为断开。假设在移动终端1为离线状态的情况下可以维持将是否需要补充标志设定为接通的状态,之后基于变为在线而发送认证密钥请求信号。

[0234] 若接收到来自移动终端1的认证密钥请求信号,则作为步骤S74,DKS3从用户DB33读出请求源的服务密钥。然后,DKS3使用该服务密钥和随机地/按规定的规则生成的变动代码,生成多个一次性认证密钥(步骤S75)。通过步骤S75生成的一次性认证密钥的个数也可以为恒定数,也可以为补充阈值与剩余数量的差加上规定值(例如100)后的值。认证密钥请求信号也可以包含表示移动终端1中的一次性认证密钥的剩余数量的信息,以使DKS3能够确定需要的发放数。

[0235] 若一次性认证密钥的生成完成,则作为步骤S76,DKS3将认证密钥数据包朝向移动终端1发送。认证密钥数据包是各个一次性认证密钥与变动代码建立关联后的数据集。若从DKS3接收认证密钥数据包,则移动终端1将该认证密钥数据包中包含的数据保存于终端侧存储部105(步骤S77)。

[0236] 根据以上的结构,基于移动终端1保持的一次性认证密钥不足规定值而随时进行补充。因此,能够减少因一次性认证密钥耗尽而用户无法使用车辆Hv的担忧。另外,补充阈值例如设定为100以上的足够大的值。根据该设定,即使在用户暂时停留在山间部等通信范围外的情况下,也能够减少在通信范围外停留中一次性认证密钥不足的担忧。此外,数字钥匙应用104也可以构成为在比规定的最小值大的范围内,用户能够将任意的值登记为补充阈值。

[0237] ＜一次性认证密钥的定期更新时序＞

[0238] 这里,使用图26,对移动终端1执行的保存认证密钥更新处理进行说明。保存认证密钥更新处理是定期地更换保存于终端侧存储部105的一次性认证密钥的一部分或者全部的处理。如图26所示,保存认证密钥更新处理具备步骤S81～S83。例如以规定的更换周期定期地执行保存认证密钥更新处理。也可以以移动终端1是在线状态为条件执行保存认证密钥更新处理。作为构成保存认证密钥更新处理的处理步骤的执行主体的移动终端1这一表达能够理解为终端处理器101/一次性认证密钥管理部F2。

[0239] 步骤S81是移动终端1基于自身保持的时刻信息亦即终端时刻,确认保存于终端侧存储部105的每个一次性认证密钥的有效期限的步骤。移动终端1删除已过有效期限的一次性认证密钥(步骤S82)。此外,有效期限的确认相当于比较有效期限所示的时间与当前的时间。通过与DKS3等规定服务器的通信来随时修正终端时刻。

[0240] 步骤S83是移动终端1与DKS3协作,执行一次性认证密钥补充处理的步骤。关于一次性认证密钥补充处理如上所述。此外,在基于有效期限的补充处理中,也可以构成为与剩余数量(Notk)是否不足补充阈值(ThRp)无关地,仅补充通过步骤S82删除的数量。例如也可

以在通过步骤S82删除了20个一次性认证密钥的情况下,移动终端1发送请求20个一次性认证密钥的发放的信号,作为认证密钥请求信号。也可以认证密钥请求信号包含表示发放希望数的信息。

[0241] 根据上述的结构,基于有效期限,定期地更换保存于移动终端1的一次性认证密钥的一部分或者全部。根据该结构,可使用的一次性认证密钥随时间而变更。因此,能够进一步加强安全性。

[0242] <关于认证ECU中的时刻信息的更新>

[0243] 认证ECU4基于自身保持的时刻信息亦即ECU内部时刻来检查客户密钥的有效期限。因此,优选ECU内部时刻与DKS3的时刻信息同步。这里,使用图27,对在将ECU内部时刻修正为与DKS3的时刻信息同步的基础上,检查客户密钥的有效期限的处理进行说明。如图27所示,ECU时刻信息的更新以及客户密钥的有效期限检查所涉及的一系列的时序包含步骤S91～S97。此外,至少ECU内部时刻的更新所涉及的时序以在认证ECU4与移动终端1之间BLE的通信链路已确立为条件执行。这里的移动终端1可以是所有者终端或者客户终端的任一方。

[0244] 步骤S91中,认证ECU4朝向移动终端1发送时刻请求信号。时刻请求信号是请求DKS3保持的时刻信息亦即服务器时刻信息的信号。时刻请求信号例如也可以包含ECU编号或者车辆ID等表示请求源的信息。

[0245] 若通过BLE通信接收到来自认证ECU4的时刻请求信号,则作为步骤S92,移动终端1生成符合蜂窝通信或者Wi－Fi通信的格式的时刻请求信号并发送至DKS3。步骤S92相当于将来自认证ECU4的数据传送至DKS3的步骤。此外,优选在从移动终端1发送至DKS3的时刻请求信号中包含移动终端1的信息,以便DKS3能够确定服务器时刻信息的返回目的地。

[0246] 若接收到来自移动终端1的时刻请求信号,则DKS3将服务器时刻信息返回至请求源的移动终端1(步骤S93)。另外,移动终端1通过BLE通信将从DKS3接收到的服务器时刻信息传送至认证ECU4(步骤S94)。

[0247] 若从移动终端1接收服务器时刻信息,则认证ECU4使用该服务器时刻信息修正ECU内部时刻(步骤S95)。ECU内部时刻是指认证ECU4保持的时刻信息。此外,也可以在各设备中的数据的接收处理中包含有使用了校验码的合法性的验证处理。在使用了校验码的验证处理的结果是未发现合法性的情况下,可以拒绝请求。以上所述的步骤S91～S95相当于ECU时刻信息的更新所涉及的时序Sq1。

[0248] 认证ECU4例如基于进行了ECU内部时刻的修正,使用修正后的时刻信确认登记于车辆侧存储部45的每个客户密钥的有效期限(步骤S96)。然后,认证ECU4删除已过有效期限的客户密钥的数据(步骤S97)。此外,步骤S97也可以是保留密钥数据,而使用标志等使已过有效期限的客户密钥无效化的处理。

[0249] 步骤S96～S97相当于客户密钥的有效期限检查所涉及的时序Sq2。此外,ECU时刻信息的更新所涉及的时序Sq1和客户密钥的有效期限检查所涉及的时序Sq2也可以分别实施。客户密钥的有效期限的检查所涉及的时序Sq2不限于更新了ECU时刻信息的情况,也可以以规定的周期执行。另外,也可以基于行驶用电源从接通切换至断开的定时、从断开切换至接通,来执行客户密钥的有效期限的检查。

[0250] 根据认证ECU4具备的时钟振荡器的精度等,认证ECU4具备的时刻信息可能偏离实

际的时刻或者服务器时刻。根据以上的结构,每当与移动终端1连接,就修正ECU内部时刻。因此,能够减少认证ECU4基于错误的时刻信息将客户密钥删除/无效化的担忧。

[0251] ＜关于所有者密钥的删除处理＞

[0252] 车辆Hv的所有者可能因车辆Hv的买卖/转让而改变。在所有者改变的情况下,优选删除老所有者的服务密钥等。根据这样的情况,车辆用数字钥匙系统Sys需要构成为不仅能够删除客户密钥,还能够删除所有者密钥的信息。

[0253] 本实施方式的DKS3构成为能够从所有者终端以及车载HMI中的任一设备接受所有者密钥的删除请求。DKS3在基于针对所有者终端的操作删除所有者密钥的情况下,如图28所示,作为处理整体而可以包含终端内数据删除阶段Ph3和车辆内数据删除阶段Ph4。终端内数据删除阶段Ph3是将指定的服务密钥(这里,所有者密钥)的数据从移动终端1删除的阶段。车辆内数据删除阶段Ph4是将指定的服务密钥从认证ECU4删除的阶段。这里,使用图29、图30,对基于针对所有者终端的操作删除所有者密钥的情况的时序进行说明。

[0254] 图29是表示与终端内数据删除阶段Ph3对应的各设备的交互的时序图。如图29所示,将所有者密钥数据从移动终端1删除的时序包含步骤T10～T18。

[0255] 步骤T10是与步骤S10相同地,DKS3认证用户/移动终端1的步骤。步骤T11是作为所有者终端的移动终端1基于用户的操作发送所有者密钥删除请求信号的步骤。所有者密钥删除请求信号例如是设备ID、用户ID、或者服务密钥ID等用于DKS3确定请求源的信息。另外,所有者密钥删除请求信号也可以包含服务密钥ID、ECU编号、或者车辆ID的信息等,作为用于确定设为删除对象的服务密钥的信息。若假定一个用户是多个车辆的所有者的情况,则优选所有者密钥删除请求信号包含用于确定设为删除对象的服务密钥的信息。

[0256] 若从所有者终端接收所有者密钥删除请求信号,则作为步骤T12,DKS3(服务密钥删除部G5)将车辆用所有者删除数据包朝向所有者终端发送。车辆用所有者删除数据包是用于从车辆Hv删除与全部的服务密钥相关的数据的数据集。车辆用所有者删除数据包可以包含终端校验码、车辆校验码。若接收到从DKS3分发的车辆用所有者删除数据包,则所有者终端在使用终端校验码验证了该车辆用所有者删除数据包的合法性的基础上,将车辆用所有者删除数据包保存于车辆用数据临时存储部M2(步骤T13)。

[0257] 另外,DKS3在针对车辆Hv发放了客户密钥的情况下,基于来自所有者终端的所有者密钥删除请求信号,朝向客户终端发送客户密钥删除指令(步骤T14)。针对车辆Hv发放了客户密钥的情况换言之相当于存在与设为删除对象的所有者密钥建立关联的客户密钥的情况。客户密钥删除指令是指示从客户终端删除车辆Hv用的服务密钥所涉及的数据的信号。客户密钥删除指令包含设为删除对象的服务密钥ID、终端校验码等信息。若接收到客户密钥删除指令,则客户终端在使用终端校验码验证了该客户密钥删除指令的合法性的基础上,从密钥信息存储部M1将与指定的服务密钥相关的数据全部删除(步骤T15)。作为更优选的方式,若客户密钥的删除处理完成则客户终端将以此为主旨的内容报告给DKS3。

[0258] DKS3基于来自所有者终端的所有者密钥删除请求信号,朝向所有者终端发送所有者密钥删除指令(步骤T16)。所有者密钥删除指令是指示从所有者终端删除车辆Hv用的服务密钥所涉及的数据的信号。所有者密钥删除指令包含设为删除对象的服务密钥ID、终端校验码等信息。所有者密钥删除指令以及客户密钥删除指令相当于用于删除服务密钥的指示指令,即服务密钥删除指令的一种。

[0259] 若接收到所有者密钥删除指令,所有者终端在使用终端校验码验证了该所有者密钥删除指令的合法性的基础上,从密钥信息存储部M1将与指定的服务密钥相关的数据全部删除(步骤T17)。此外,所有者密钥删除指令不作用至保存于车辆用数据临时存储部M2的数据。即,所有者终端即使接收所有者密钥删除指令,也不将保存于车辆用数据临时存储部M2的车辆用所有者删除数据包删除而保留规定期间。作为更优选的方式,若所有者密钥的删除处理完成则所有者终端将以此为主旨的内容报告给DKS3。

[0260] DKS3例如基于从所有者终端以及客户终端接收到服务密钥的删除完成,将与删除请求的所有者密钥相关的数据从用户DB33以及车辆DB32删除(步骤T18)。此外,服务器内数据的删除也可以在从车辆Hv接收到车辆内的数据删除也完成的报告后执行。在本实施方式中分别发送车辆用所有者删除数据包和所有者密钥删除指令,但各种数据的发送方式不限于此。车辆用所有者删除数据包和所有者密钥删除指令也可以作为一系列的数据集中发送。

[0261] 使用接下来的图30,对从车辆Hv删除与所有者密钥相关的数据的时序进行说明。在与所有者密钥相关的信息中,还包含客户密钥的数据。从车辆Hv删除与所有者密钥相关的数据的时序包含步骤T21～T24。此外,与所有者密钥的登记时序不同,认证ECU4在通常模式下也接受所有者密钥的删除指示。图30的说明中的移动终端1是保持车辆用所有者删除数据包的移动终端1,能够称为旧所有者终端。

[0262] 若保持车辆用所有者删除数据包的移动终端1进入车辆Hv的BLE通信范围内,则与保持服务密钥的状态相同地,认证ECU4与该移动终端1进行基于BLE的通信连接(步骤T21)。然后,开始加密通信(步骤T22)。移动终端1基于与认证ECU4的加密通信链路已确立,发送保存于车辆用数据临时存储部M2的面向车辆Hv的车辆用所有者删除数据包(步骤T23)。

[0263] 若从移动终端1接收车辆用所有者删除数据包,则认证ECU4基于该数据包中包含的命令/程序,删除保存于车辆侧存储部45的与全部的服务密钥相关的数据。这样,所有者终端构成为能够在与认证ECU4之间BLE通信的链路已确立的情况下从认证ECU4删除所有者密钥。

[0264] 此外,也可以在所有者终端与DKS3通信连接的状态下执行包含步骤T11～T13的时序。在该情况下,所有者终端从DKS3取得的车辆用所有者删除数据包可以通过步骤T23迅速地向认证ECU4传送,而从车辆侧存储部45也删除所有者密钥。此外,也可以在接收到车辆用所有者删除数据包的情况下,认证ECU4在基于接收数据中包含的车辆校验码验证了接收数据的合法性的基础上,执行全部的服务密钥数据的删除。

[0265] ＜关于基于所有者权限的客户密钥的删除处理＞

[0266] 优选构成为所有者基于来自客户的提议、违反使用条款等,而即使在有效期限内也能够删除客户密钥。这里,使用图31、图32,对DKS3基于来自所有者终端的请求,删除指定的客户密钥的处理的流程进行说明。

[0267] 与所有者密钥的删除相同地,客户密钥的删除处理也能够分为从移动终端1删除与客户密钥相关的数据的阶段Ph3、和从车辆Hv删除客户密钥的数据的阶段Ph4。图31是表示与从移动终端1删除客户密钥数据的阶段Ph3对应的各设备的交互的时序图。如图31所示,将客户密钥数据从移动终端1删除的时序包含步骤T30～T39b。

[0268] 此外,接受所有者的操作的设备不限于移动终端1,也可以是台式/笔记本PC(膝上

式计算机)。以下的所有者终端也可以是所有者操作的台式/笔记本PC。

[0269] 步骤T30是所有者终端中的数字钥匙应用104认证操作者是所有者的步骤。数字钥匙应用104中的认证方法也可以是使用密码的方法,也可以是使用生物体信息的方法。也可以在是否是所有者的验证中使用密码和生物体信息双方。用户认证能够采用两步认证等多种方法。

[0270] 步骤T31是所有者终端基于从触摸面板12输入的操作信号,在显示器11显示删除对象选择画面的步骤。删除对象选择画面是用于选择设为删除对象的客户密钥、或者与该秘钥对应的客户的画面。删除对象选择画面包含客户或者客户密钥的列表。此外,删除对象选择画面也能够称为表示客户的一览的客户列表画面或者客户删除画面。

[0271] 在步骤T32中,所有者终端基于触摸面板12的输出信号所示的针对删除对象选择画面的用户操作,确定设为删除对象的客户密钥。选择设为删除对象的客户密钥的用户操作相当于删除指示操作。若由所有者选择了作为删除对象的客户密钥,则所有者终端将以该客户密钥为对象的客户密钥删除请求信号发送至DKS3(步骤T33)。客户密钥删除请求信号包含删除对象的服务密钥ID或者用户ID,作为用于确定作为删除对象的服务密钥的信息。此外,客户密钥删除请求信号也可以是请求将多个客户密钥集中删除的信号。例如客户密钥删除请求信号也可以是请求将与所有者密钥建立关联的全部的客户密钥集中删除的信号。

[0272] 若接收到客户密钥删除请求信号,则DKS3朝向与由该接收信号指定的客户密钥建立关联的客户终端发送客户密钥删除指令(步骤T34)。若接收到客户密钥删除指令,则客户终端在使用终端校验码验证了该客户密钥删除指令的合法性的基础上,将与指定的服务密钥相关的数据从密钥信息存储部M1全部删除(步骤T35)。客户密钥删除指令相当于删除指示信号。作为更优选的方式,若客户密钥的删除处理完成则客户终端将以此为主旨的内容报告给DKS3。

[0273] 步骤T36是DKS3朝向所有者终端通知客户密钥的删除完成的步骤。DKS3也可以基于客户密钥删除指令的发送完成而发送客户密钥删除完成通知,也可以在从客户终端接收删除完成的报告后发送客户密钥删除。

[0274] 若从DKS3接收客户密钥删除完成通知,则所有者终端将删除完成通知画面显示于显示器11(步骤T37)。删除完成通知画面可包含与已删除的客户密钥建立关联的用户名等。

[0275] 另外,DKS3朝向所有者终端、以及与设定为删除对象的客户密钥对应的客户终端发送车辆用客户删除数据包(步骤T38a、T38b)。若接收到车辆用客户删除数据包,则各设备将该数据包保存于车辆用数据临时存储部M2(步骤T39a、T39b)。车辆用客户删除数据包相当于删除用数据集。

[0276] 接下来,使用图32,对从车辆Hv删除与客户密钥相关的数据的时序进行说明。从车辆Hv删除与客户密钥相关的数据的时序包含步骤T41～T44。在从车辆Hv删除与客户密钥相关的数据的时序中出现的客户终端相当于保持车辆用客户删除数据包的客户终端。

[0277] 若作为所有者终端或者客户终端的移动终端1进入车辆Hv的BLE通信范围内,则认证ECU4与该移动终端1进行基于BLE的通信连接(步骤T41)。然后,开始加密通信(步骤T42)。移动终端1基于与认证ECU4的加密通信链路已确立,发送保存于车辆用数据临时存储部M2的面向车辆Hv的车辆用客户删除数据包(步骤T43)。

[0278] 若从所有者终端/客户终端接收车辆用客户删除数据包,则认证ECU4基于该数据包中包含的命令/程序,将与被指定为删除对象的客户密钥相关的数据从车辆侧存储部45删除。

[0279] 此外,也可以在所有者终端/客户终端与DKS3通信连接的状态下执行包含步骤T41～T43的时序。另外,认证ECU4也可以在接收到车辆用客户删除数据包的情况下,在基于接收数据中包含的车辆校验码验证了接收数据的合法性的基础上,执行全部的服务密钥数据的删除。

[0280] 根据上述的结构,所有者能够在任意的定时删除任意的客户密钥。因此,能够根据客户对车辆Hv的使用状况、所有者的方便性,使客户对车辆Hv的使用停止。

[0281] 此外,若在客户使用车辆Hv时突然删除客户密钥,则可能对客户造成不便。特别是,在客户使用车辆Hv移动至远离本来的车辆Hv的保管位置的位置的情况下,若突然无法使用车辆Hv,则对客户和所有者都造成不便。根据这样的情况,可以在从客户密钥的删除的申请至实际执行删除处理为止设置一定时间的宽限期。也可以以车辆Hv停放至规定的保管位置为条件执行客户密钥等的删除。DKS3也可以使表示所有者进行了客户密钥的删除申请的画面显示于对应的客户终端。

[0282] 此外,如上述那样,所有者终端构成为能够接受用于选择性地删除与车辆建立关联的客户密钥的操作。另一方面,构成为无法接受不删除客户密钥而仅变更有效期限或者权限所涉及的设定的操作。DKS3也构成为关于已发放的服务密钥,无法在保留该服务密钥的同时变更权限设定以及有效期限。所有者在希望变更针对某客户的服务密钥的权限设定、有效期限的情况下,能够在暂时删除对应的客户密钥后,进行新发放进行了所希望的权限设定的客户密钥的手续。

[0283] 以上,叙述了所有者通过操作所有者终端等来删除客户密钥的情况,但客户密钥也可以通过客户自身的操作删除。DKS3在基于客户的操作删除了客户密钥的情况下,对与该客户密钥建立关联的所有者终端发送已删除客户密钥的通知。所有者终端基于该通知,例如显示包含已删除的客户密钥或者其用户名的客户删除画面。或者,基于来自DKS3的通知,更新每个客户的状态信息。

[0284] ＜使用车载HMI的服务密钥的删除处理＞

[0285] 这里,使用图33,对基于针对车载HMI的用户操作,删除由用户指定的服务密钥的处理的流程进行说明。如图33所示,基于针对车载HMI的用户操作,将由用户指定的服务密钥从认证ECU4以及相关的移动终端1删除的时序包含步骤T50～T57。此外,作为前提,DKS3构成为能够经由车载HMI接受与操作者的权限对应的服务密钥的删除请求。例如在车载HMI50的操作者是所有者的情况下,认证ECU4以及DKS3构成为经由车载HMI50不仅能够接受针对客户密钥的删除指示,还能够接收针对所有者密钥的删除指示。关于构成图33的步骤中的认证ECU4执行的步骤,其具体的执行主体能够解释为认证处理器41。

[0286] 步骤T50是认证ECU4认证操作车载HMI50的用户的步骤。作为认证方法,如上述那样,能够采用伴随着密码的输入的方法、使用生物体信息的方法等多种方法。该步骤T50能够解释为识别车载HMI50的操作者的步骤。另外,认证ECU4对用户的认证也可以挪用认证ECU4对移动终端1的认证结果。认证ECU4也可以将与作为通信对象的移动终端1对应的用户视作车载HMI50的操作者。

[0287] 步骤T51中,认证ECU4基于从输入装置52输入的操作信号在显示器51显示服务密钥删除画面。服务密钥删除画面是用于选择设为删除对象的服务密钥ID、或者用户的画面。在识别为操作者是所有者的情况下,服务密钥删除画面构成为也能够选择所有者密钥作为删除对象。服务密钥删除画面可以包含通过作为操作者的用户的权限可删除的服务密钥的列表、或者对应的用户的列表。

[0288] 在步骤T52中,认证ECU4基于输入装置52的输出信号表示的针对服务密钥删除画面的用户操作,确定作为删除对象的服务密钥。然后,作为步骤T53,认证ECU4从车辆侧存储部45删除与被指定为删除对象的服务密钥相关的数据。若来自车辆侧存储部45的数据删除完成,则认证ECU4显示删除完成画面(步骤T54)。删除完成画面可以包含与已删除的服务密钥建立关联的用户名等信息。此外,删除完成画面的显示是任意的要素,也可以省略。

[0289] 若与指定的服务密钥相关的数据的删除完成,则作为步骤T55,认证ECU4将表示服务密钥的删除时序完成的删除完成通知信号朝向DKS3发送。删除完成通知信号包含已删除的服务密钥的ID或者与其对应的用户ID等。此外,在指定所有者密钥作为删除对象的情况下,在步骤T53中,从车辆侧存储部45删除全部的服务密钥。

[0290] 若接收到来自认证ECU4的删除完成通知信号,则DKS3朝向与由该接收信号指定的服务密钥建立关联的移动终端1发送服务密钥删除指令(步骤T56)。假设在基于针对车载HMI50的操作从车辆侧存储部45删除了所有者密钥的情况下,DKS3朝向所有者终端以及与该所有者终端建立关联的全部的客户终端发送服务密钥删除指令。

[0291] 若接收到服务密钥删除指令,则移动终端1在使用终端校验码验证了该服务密钥删除指令的合法性的基础上,从密钥信息存储部M1将与指定的服务密钥相关的数据全部删除(步骤T57)。作为更优选的方式,若服务密钥的删除处理完成则各移动终端1将以此为主旨的内容报告给DKS3。

[0292] 如上述那样,所有者也能够使用车载HMI50删除任意的客户的服务密钥。另外,所有者也能够使用车载HMI50删除所有者密钥。此外,能够代替所有者,由经销商商店的工作人员使用车载HMI50执行相同的删除处理。

[0293] 此外,认证ECU4也可以构成为以从安全解除工具或者DKS3输入安全解除信号为条件,执行使用了车载HMI50的所有者密钥的删除处理。根据这样的结构,能够减少因操作失误、非法的操作而删除所有者密钥以及与该所有者密钥建立关联的全部的客户密钥的担忧。所有者密钥的删除的影响范围比客户密钥的删除大。因此,也可以面向所有者密钥的删除的用户认证与面向客户密钥的删除的用户认证相比更高级/复杂地构成。例如用于删除所有者密钥的用户认证的步骤数也可以设定得比删除客户密钥时的用户认证步骤数多。

[0294] 另外,DKS3根据是否如以上所述那样经由车载HMI50实施了所有者密钥的删除操作,对所有者终端发送不同的数据。例如在通过所有者终端进行了所有者密钥的删除操作的情况下,DKS3朝向所有者终端发送车辆用所有者密钥删除数据包,另一方面,在通过车载HMI50进行了所有者密钥的删除操作的情况下,DKS3不发送车辆用所有者密钥删除数据包。根据该结构,能够抑制所有者终端的数据通信量。另外,在通过车载HMI50进行了所有者密钥的删除操作的情况下,本来认证ECU4就不从DKS3接收删除用数据集,而删除全部的服务密钥。即,DKS3的通信量本身也能够减少。

[0295] ＜DKS对服务密钥的管理方法的补充＞

[0296] DKS3将与一个所有者密钥建立关联的客户密钥全部与所有者密钥的服务密钥ID建立关联并管理。如图34所示,DKS3在删除了带发放权的客户密钥的情况下,也不删除通过该带发放权的客户密钥的权限发放的孙世代/第三世代的客户密钥。孙世代/第三世代的客户密钥作为与所有者密钥建立关联的客户密钥而继续存在。此外,图34中的1x表示所有者密钥,1y表示带发放权的客户密钥,1z表示孙世代/第三世代的客户密钥。1v是所有者密钥已发放的客户密钥,有无发放权是任意的。为方便起见,也将与一个所有者密钥建立关联的客户密钥的组称为族。通过所有者密钥ID管理构成族的服务密钥。

[0297] 并且,DKS3构成为能够接受用户对移动终端1的机型变更的申请。在由用户进行了机型变更的情况下,设备ID可能变化。然而,关于服务密钥ID,即使在进行了机型变更情况下也不变更。族由所有者密钥的服务密钥ID形成,因此假设在所有者变更了移动终端1的机型的情况下,对客户密钥也没有影响,族本身继续存在。例如即使在所有者变更了移动终端1的机型的情况下,也仅变更所有者终端的设备ID以及服务密钥。变更了具有带发放权限的客户密钥的客户的移动终端1的情况也相同。即,车辆用数字钥匙系统Sys构成为即使在成为客户密钥的发放源的移动终端1变更为其它的设备的情况下,也不会对其它的客户密钥造成影响。

[0298] DKS3例如通过图35所示的步骤实施所有者终端变更处理。所有者终端变更处理是所有者终端的机型变更所涉及的处理。如图35所示,所有者终端认证处理可以包含步骤T61～T68。基于从移动终端1或者PC等输入相当于机型变更的提议的信号而开始所有者终端变更处理。所有者操作的终端也可以是机型变更前的移动终端1亦即旧终端,也可以是机型变更后的移动终端1亦即新终端。另外,所有者申请机型变更的设备可以是台式/膝上式PC等任何可访问互联网的终端。通过由所有者进行的规定的数据交接操作,在新终端也安装数字钥匙应用104,且登记用户ID等信息。

[0299] 步骤T61是认证操作者/申请者是所有者的步骤。是所有者的认证方法如上述那样。若认证操作者是所有者,则DKS3基于用户ID等参照用户DB33,取得所有者的旧设备ID以及服务密钥ID(步骤T62)。旧设备ID是指旧终端的设备ID。另外,DKS3通过与新终端实施数据通信,从而取得新终端的设备ID亦即新设备ID(步骤T63)。步骤T64是DKS3使用新设备ID新发放作为所有者密钥的服务密钥的步骤。具体的服务密钥的生成方法如上述那样。

[0300] 若生成新所有者密钥,则DKS3更新用户DB33的登记内容(步骤T65)。例如,在所有者的用户数据中,删除旧所有者密钥并登记新所有者密钥。旧所有者密钥是在机型变更前使用的服务密钥,是基于旧设备ID的服务密钥。此外,在本实施方式中,即使在变更了所有者的设备的情况下也不变更所有者的服务密钥ID而维持此前的ID,因此关于客户的用户数据不需要采取特别的措施。作为其它的方式,在也变更服务密钥ID的情况下,DKS3可将与客户密钥建立关联的所有者的服务密钥ID替换为新所有者密钥ID。此外,若生成新所有者密钥,则DKS3创建规定量的与新所有者密钥对应的一次性认证密钥。

[0301] 然后,DKS3朝向新终端发送终端用密钥交换数据包(步骤T66)。终端用密钥交换数据包至少包含新所有者密钥。终端用密钥交换数据包也可以是使保存于密钥信息存储部M1的所有者密钥替换为新所有者密钥的指令/程序。终端用密钥交换数据包可以包含与新所有者密钥对应的多个一次性认证密钥、和变动代码。此外,终端用密钥交换数据包也可以包含终端校验码。一次性认证密钥所涉及的数据集也可以作为认证密钥数据包而与终端用密

钥交换数据包分开发送。

[0302] 作为新终端的移动终端1若从DKS3接收终端用密钥交换数据包,则在基于终端校验码验证了数据的合法性之后,将新所有者密钥所涉及的接收数据保存于密钥信息存储部M1。具体而言,终端处理器101保存接收到的作为新所有者密钥的服务密钥、和与变动代码建立关联的多个一次性认证密钥。

[0303] 另外,DKS3将用于将与新所有者密钥相关的数据登记至认证ECU4的数据集亦即车辆用密钥交换数据包发送至新终端。车辆用密钥交换数据包包含作为新所有者密钥的服务密钥、和车辆校验码。车辆用密钥交换数据包也可以是使保存于车辆侧存储部45的所有者密钥替换为新所有者密钥的指令/程序。

[0304] 若接收到车辆用密钥交换数据包,则作为新终端的移动终端1将该数据包保存于车辆用数据临时存储部M2。然后,基于已与认证ECU4确立BLE加密通信链路,将车辆用密钥交换数据包传送至认证ECU4。即,车辆用密钥交换数据包还与车辆用登记数据包相同地经由移动终端1分发至认证ECU4。

[0305] 认证ECU4若接收到车辆用密钥交换数据包,则在基于车辆校验码验证了数据的合法性之后,将新所有者密钥所涉及的接收数据保存于车辆侧存储部45。具体而言,认证处理器41将接收到的作为新所有者密钥的服务密钥保存于所有者密钥存储部451。此外,伴随于此,认证ECU4删除保存于所有者密钥存储部451的旧所有者密钥。关于服务密钥ID,由于在机型变更后也维持,因此也可以不删除而挪用。当然,服务密钥ID也可以在暂时删除后新登记。

[0306] 此外,认证ECU4也可以在所有者密钥存储部451保存有所有者密钥的状态下接受所有者密钥的登记操作的情况下,使规定的警告消息显示于显示器11、51。警告消息例如是表示所有者已经登记的消息。此外,认证ECU4也可以在所有者密钥存储部451保存有所有者密钥的状态下接受所有者密钥的登记操作的情况下,使催促规定的密码的输入的画面显示于显示器11、51。这里,作为请求输入的密码,例如能够采用与所有者的用户ID建立关联的密码,或者用于删除所有者密钥的规定代码。

[0307] 此外,作为步骤T68,DKS3朝向旧终端发送服务密钥删除指令。由此,在旧终端维持在线状态的情况下,从旧终端删除服务密钥。此外,步骤T68是任意的要素,也可以省略。

[0308] ＜系统整体所涉及的其他的补充＞

[0309] 以上,作为一个例子假定了车辆Hv是由个人拥有的车辆,所有者也是个人的情况,但上述的车辆用数字钥匙系统Sys也能够用于MaaS(Mobility as a Service:出行即服务)。所有者例如也可以是提供车辆租赁服务、共享服务的企业/组织。在该情况下,属于该企业/组织的作为操作人员的工作人员可以进行所有者终端的操作。另外,所有者拥有的车辆Hv也可以为50台、100台等多台。作为所有者的服务密钥ID也可以对多个车辆而言共用,也可以按每个车辆不同。DKS3的结构也可以根据业务的形式而分为管理车辆信息的服务器、和管理服务密钥的服务器。

[0310] 在上述的实施方式中,对认证ECU4从移动终端1取得服务密钥的登记/删除所涉及的数据的结构进行了叙述,但不限于此。认证ECU4也可以构成为不经由移动终端1通过蜂窝通信或者Wi－Fi通信从DKS3接收各种数据包。

[0311] ＜附记(1)＞

[0312] 以上所述的移动终端1能够解释为便携式的通用信息处理终端,该便携式的通用信息处理终端构成为执行以下步骤:

[0313] 朝向基于用户的操作生成用于使用车辆的服务密钥的服务器(3)发送所有者密钥发放请求信号,上述所有者密钥发放请求信号请求发放作为针对该用户拥有的车辆的服务密钥的具有作为所有者的权限的所有者密钥;

[0314] 作为服务器针对所有者密钥发放请求信号的响应,从服务器接收所有者密钥;

[0315] 将接收到的所有者密钥保存于规定的终端侧存储装置(105);以及

[0316] 以与搭载于车辆的车辆用装置(4)已确立近距离无线通信的通信链路为条件,开始用于将所有者密钥登记至车辆用装置的通信。

[0317] 另外,数字钥匙应用104能够解释为使通用的计算机作为移动终端1执行的计算机程序。此外,保存有数字钥匙应用104的存储介质相当于储存有使计算机作为上述的移动终端1动作的指令集的存储介质。

[0318] <附记(2)>

[0319] 本公开所记载的装置、系统以及它们的方法也可以通过专用计算机来实现,该专用计算机构成被编程为执行由计算机程序具体化的一个或多个功能的处理器。另外,本公开所记载的装置及其方法也可以使用专用硬件逻辑电路来实现。并且,本公开所记载的装置及其方法也可以由一个以上的专用计算机来实现,该一个以上的专用计算机由执行计算机程序的处理器和一个以上的硬件逻辑电路的组合构成。

[0320] 例如认证处理器具备的功能的一部分或者全部所具备的功能的一部分或者全部也可以作为硬件来实现。在将某个功能作为硬件来实现的方式中,包含使用一个或者多个IC等来实现的方式。作为处理器(运算核心),能够采用CPU、MPU、GPU、DFP(Data Flow Processor:数据流处理器)等。另外,认证处理器具备的功能的一部分或者全部也可以将多种运算处理装置组合来实现。认证处理器具备的功能的一部分或者全部也可以使用片上系统(SoC:System-on-Chip)、FPGA、ASIC等来实现。FPGA是Field-Programmable Gate Array的缩写。ASIC是专用集成电路(Application Specific Integrated Circuit)的缩写。上述补充说明对于终端处理器以及服务器处理器也能够相同地应用。另外,计算机程序也可以作为由计算机执行的指令,存储于计算机可读取的非迁移有形记录介质(non-transitory tangible storage medium)。作为程序的保存介质,能够采用HDD(Hard-disk Drive:硬盘驱动器)、SSD(Solid State Drive:固态硬盘),闪存等。

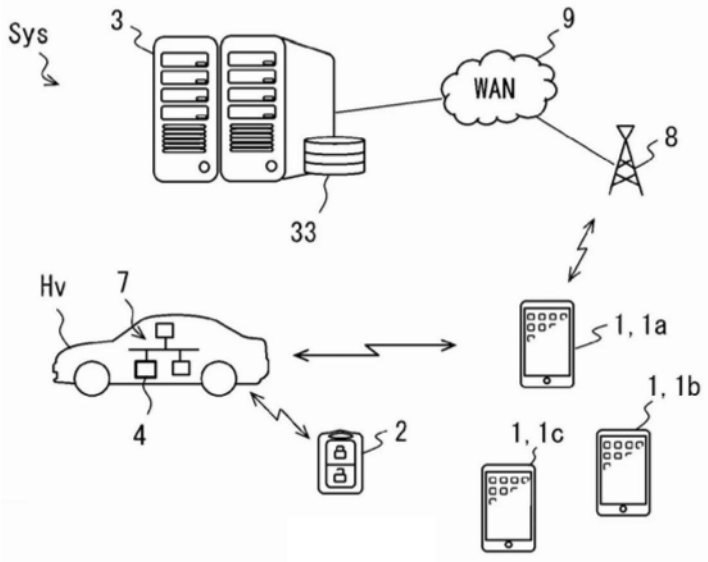

Sys
3
9
WAN
8
33
Hv
7
4
2
1, 1a
1, 1b
1, 1c

图1

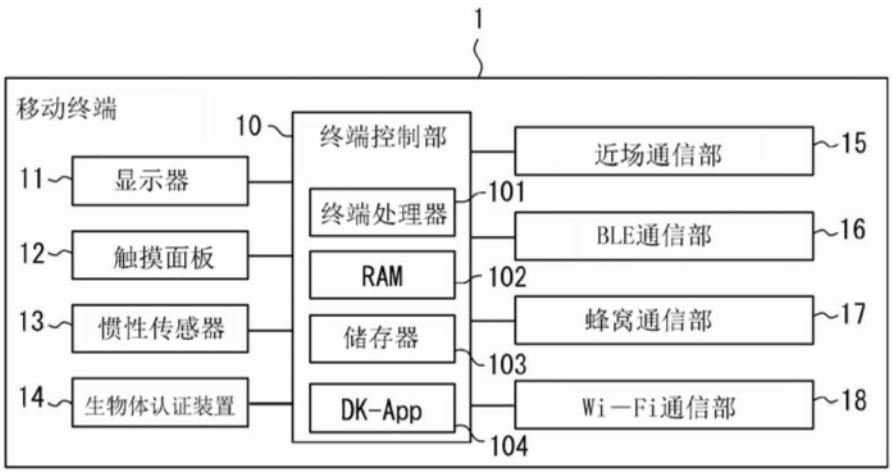

1
移动终端
10
终端控制部
11
显示器
12
触摸面板
13
惯性传感器
14
生物体认证装置
终端处理器
101
RAM
102
储存器
103
DK-App
104
近场通信部
15
BLE通信部
16
蜂窝通信部
17
Wi－Fi通信部
18

图2

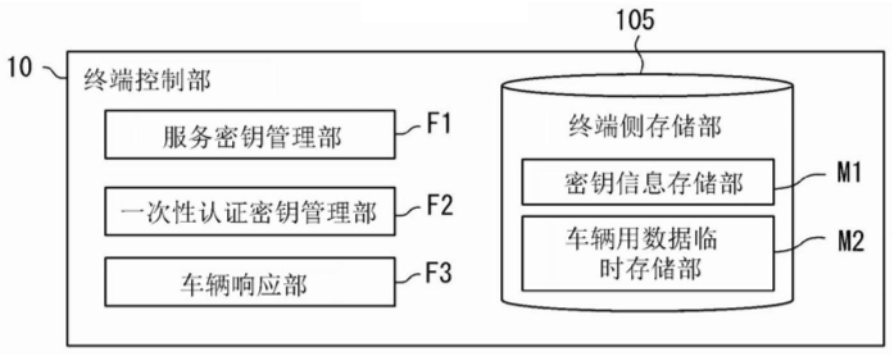

105
10
终端控制部
服务密钥管理部
F1
一次性认证密钥管理部
F2
车辆响应部
F3
终端侧存储部
密钥信息存储部
M1
车辆用数据临时存储部
M2

图3

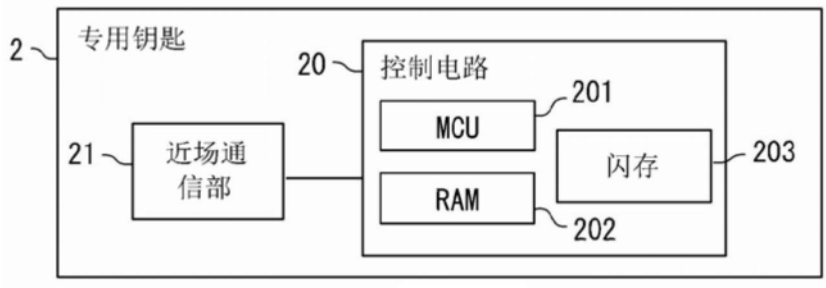

2
专用钥匙
20
控制电路
201
MCU
21
近场通信部
闪存
203
RAM
202

图4

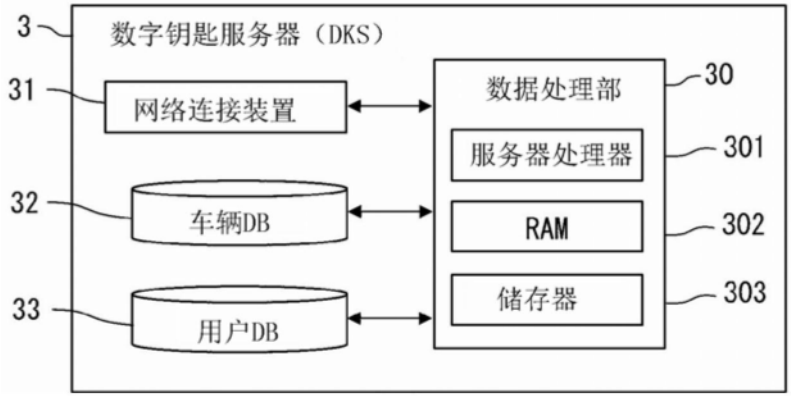

3
数字钥匙服务器（DKS）
31
网络连接装置
数据处理部
30
服务器处理器
301
32
车辆DB
RAM
302
33
用户DB
储存器
303

图5


车辆信息
车辆ID
车辆型号信息
所有者信息
客户信息

图6

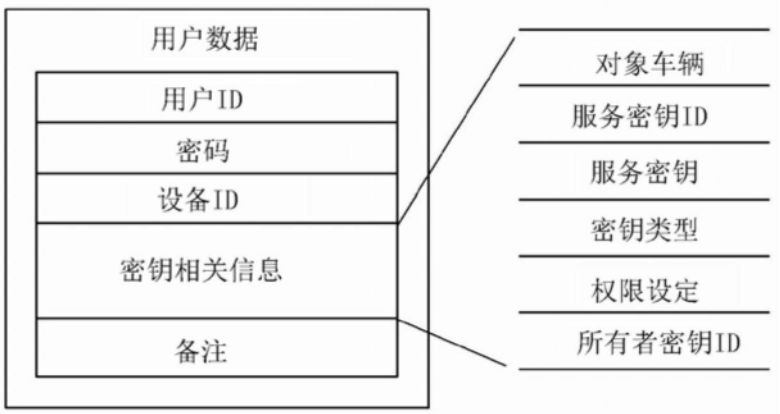

用户数据
用户ID
密码
设备ID
密钥相关信息
备注
对象车辆
服务密钥ID
服务密钥
密钥类型
权限设定
所有者密钥ID

图7

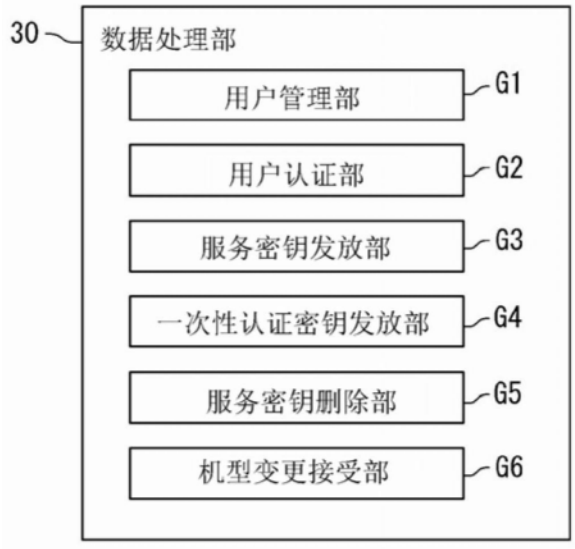

30
数据处理部
用户管理部
G1
用户认证部
G2
服务密钥发放部
G3
一次性认证密钥发放部
G4
服务密钥删除部
G5
机型变更接受部
G6

图8

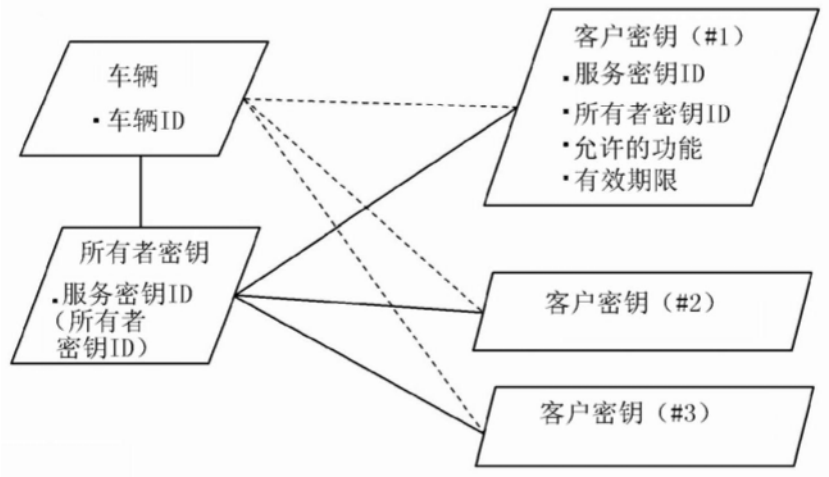

车辆
·车辆ID
所有者密钥
·服务密钥ID
（所有者
密钥ID）
客户密钥（#1）
·服务密钥ID
·所有者密钥ID
·允许的功能
·有效期限
客户密钥（#2）
客户密钥（#3）

图9

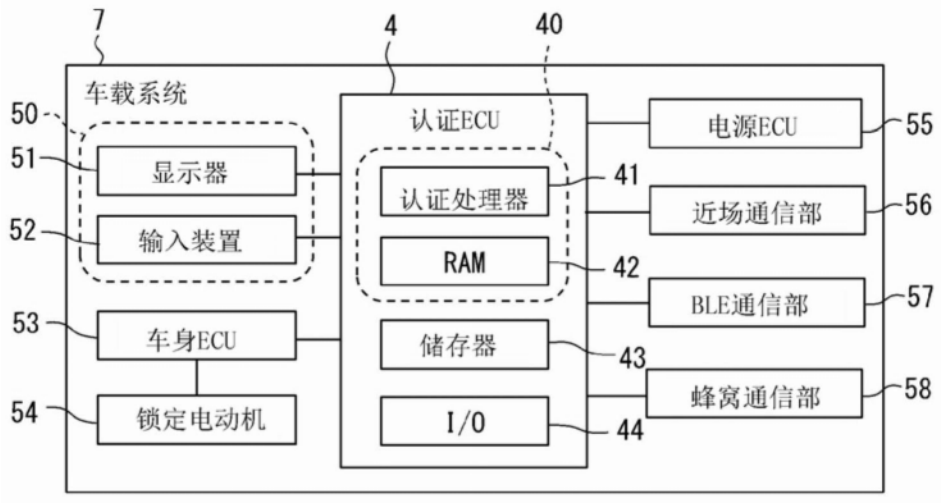

7
4
40
车载系统
50
51
显示器
52
输入装置
53
车身ECU
54
锁定电动机
认证ECU
认证处理器
41
RAM
42
储存器
43
I/O
44
电源ECU
55
近场通信部
56
BLE通信部
57
蜂窝通信部
58

图10

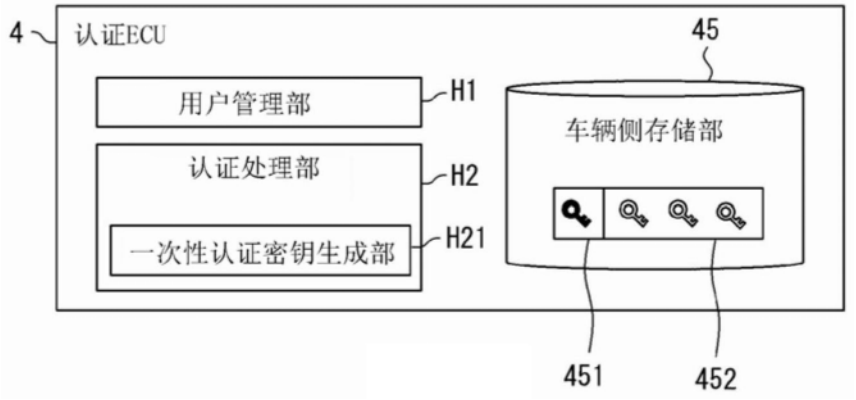

4
认证ECU
用户管理部
H1
认证处理部
H2
一次性认证密钥生成部
H21
45
车辆侧存储部
451
452

图11

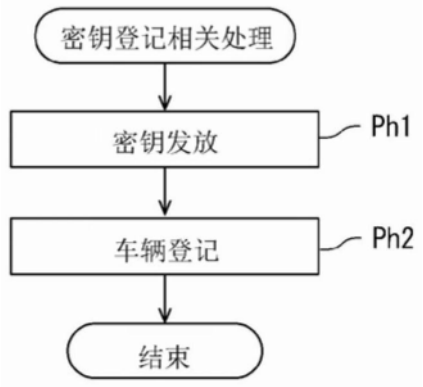

密钥登记相关处理
密钥发放
Ph1
车辆登记
Ph2
结束

图12

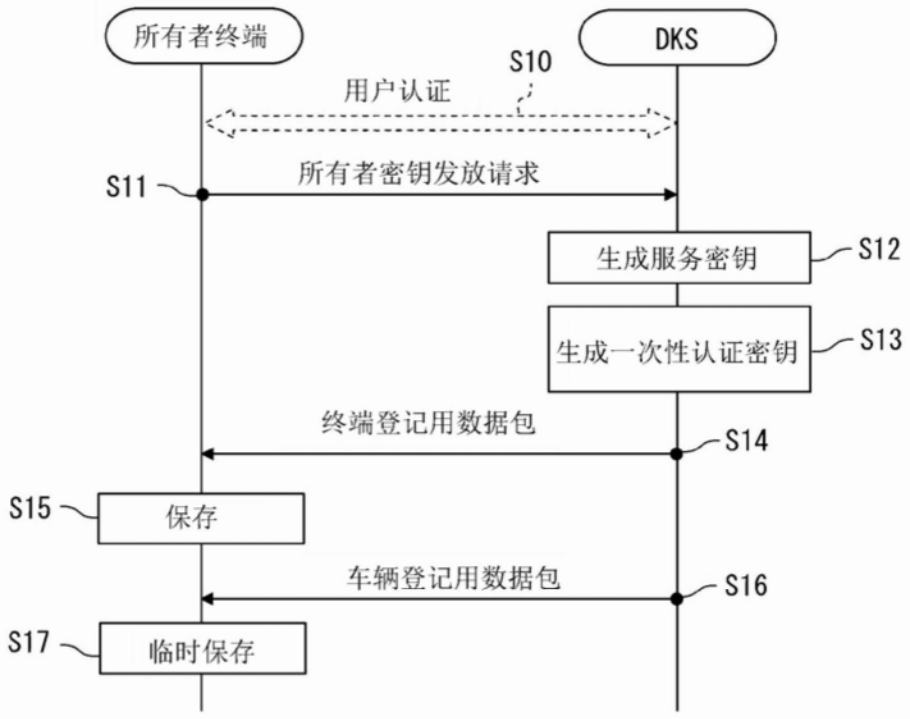

所有者终端
DKS
S10
用户认证
S11
所有者密钥发放请求
生成服务密钥
S12
生成一次性认证密钥
S13
终端登记用数据包
S14
S15
保存
车辆登记用数据包
S16
S17
临时保存

图13

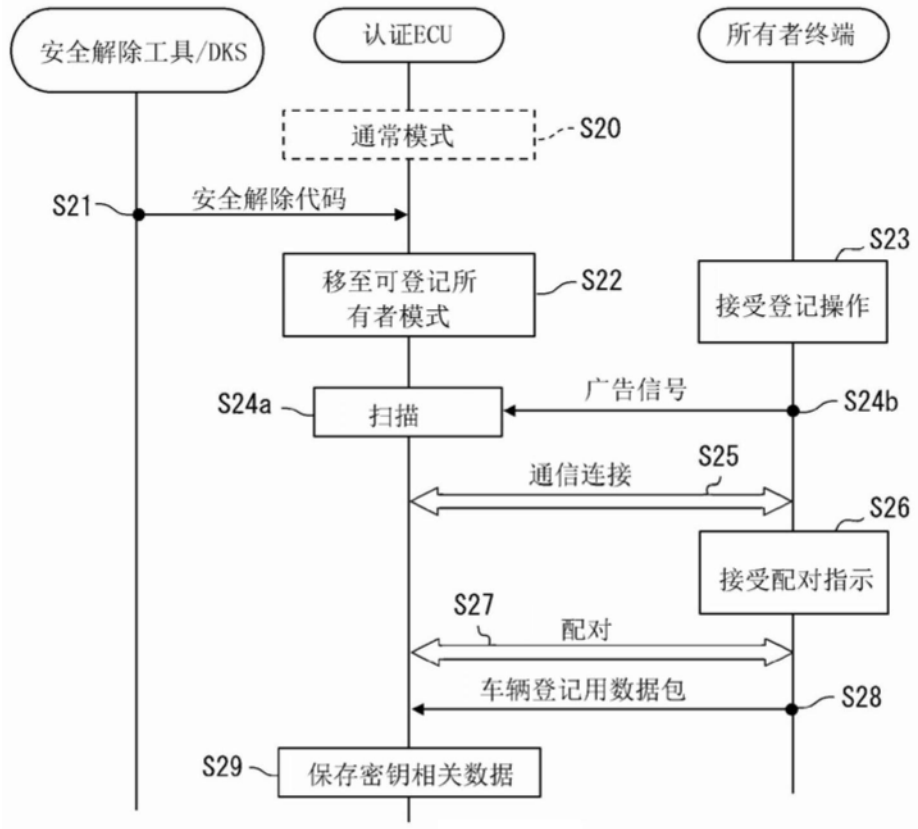

安全解除工具/DKS
认证ECU
所有者终端
通常模式
S20
S21
安全解除代码
S23
移至可登记所有者模式
S22
接受登记操作
S24a
扫描
广告信号
S24b
S25
通信连接
S26
接受配对指示
S27
配对
车辆登记用数据包
S28
S29
保存密钥相关数据

图14

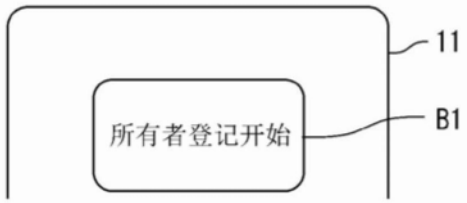

11
所有者登记开始
B1

图15

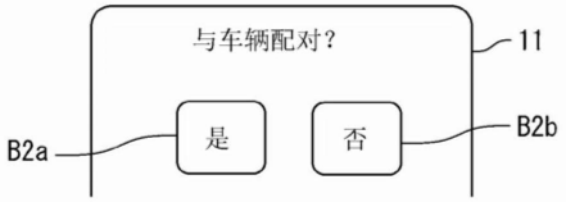

与车辆配对？
11
B2a
是
否
B2b

图16

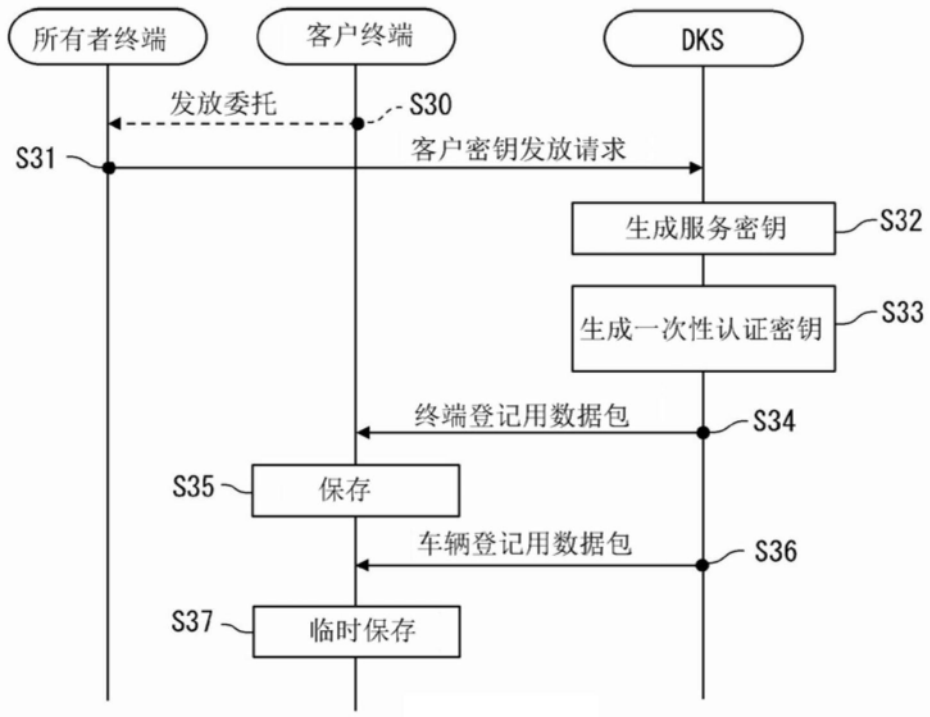

所有者终端
客户终端
DKS
发放委托
S30
S31
客户密钥发放请求
生成服务密钥
S32
生成一次性认证密钥
S33
终端登记用数据包
S34
S35
保存
车辆登记用数据包
S36
S37
临时保存

图17


请求源信息
对象车辆信息
对象用户ID
有效期限
权限设定
·客户密钥发放
·电源操作
·可使用车门

图18

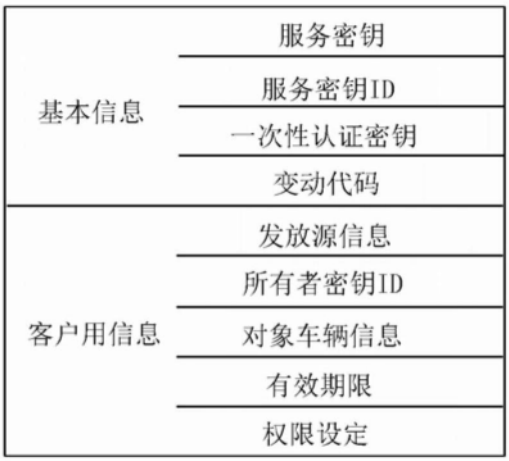

基本信息
服务密钥
服务密钥ID
一次性认证密钥
变动代码
客户用信息
发放源信息
所有者密钥ID
对象车辆信息
有效期限
权限设定

图19

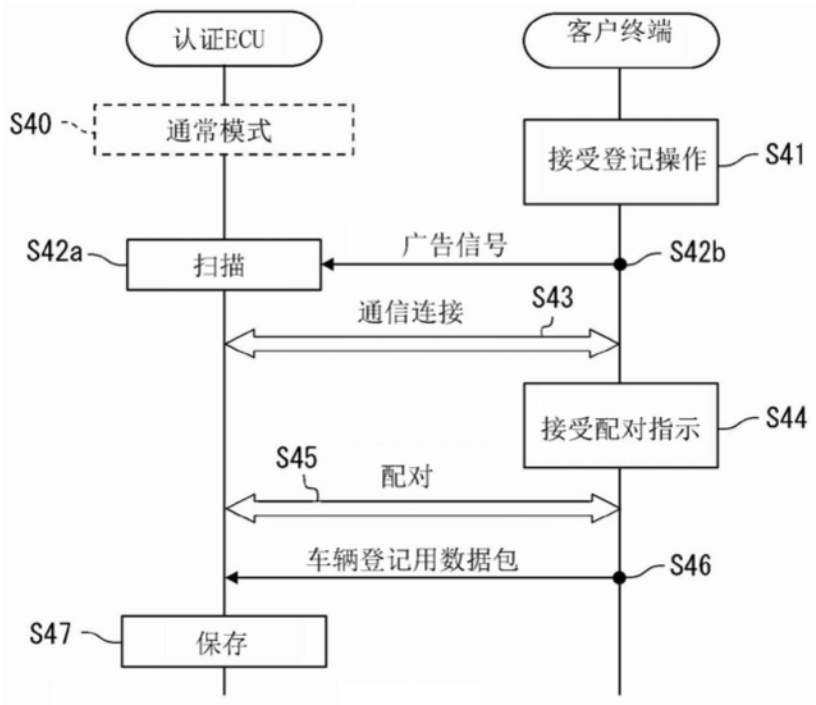

认证ECU
客户终端
S40
通常模式
接受登记操作
S41
S42a
扫描
广告信号
S42b
通信连接
S43
接受配对指示
S44
S45
配对
车辆登记用数据包
S46
S47
保存

图20

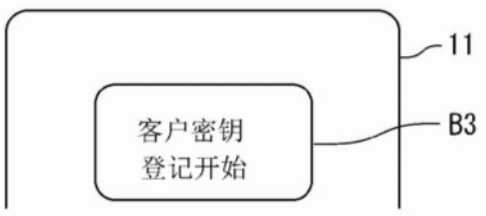

11
客户密钥
登记开始
B3

图21

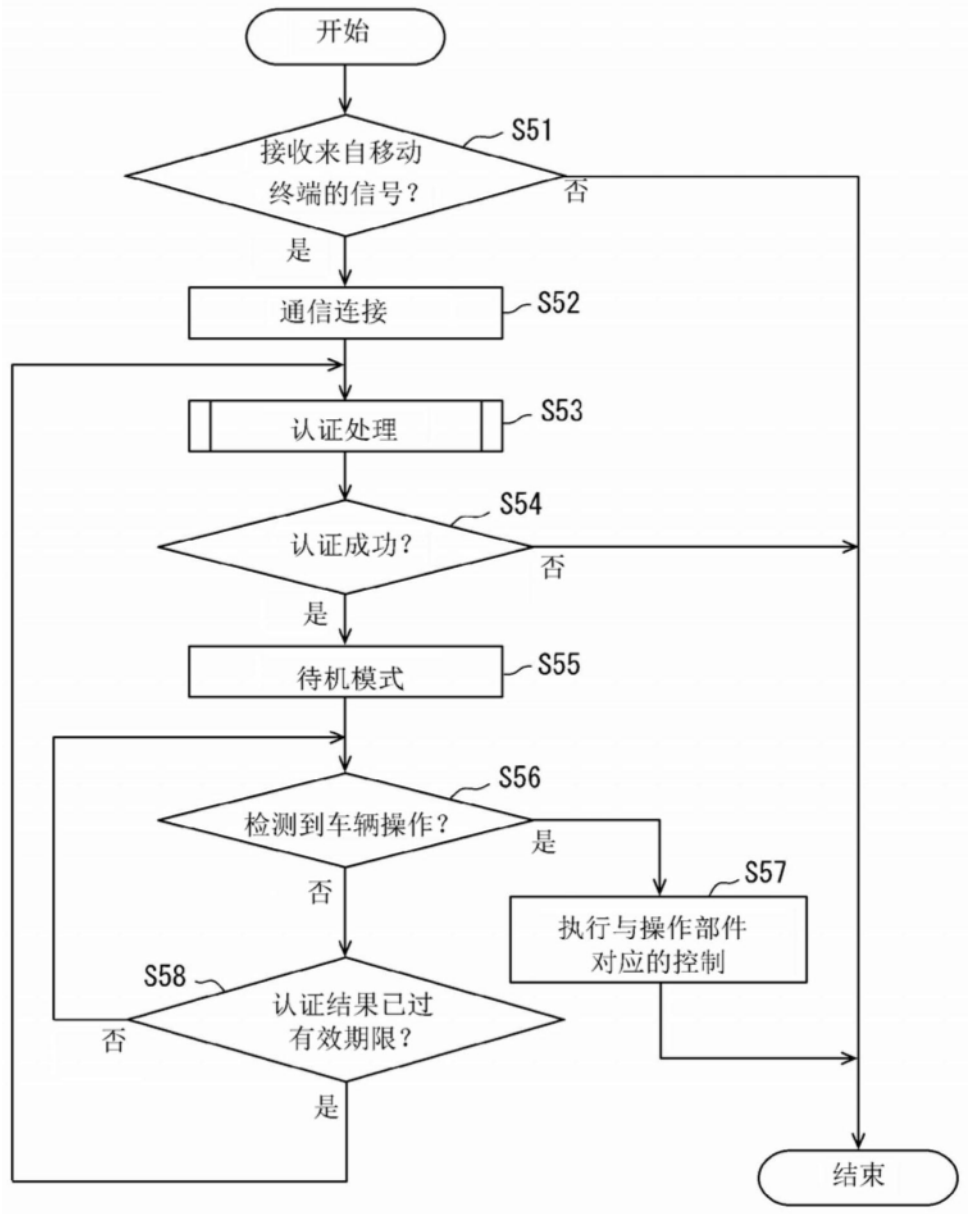

开始
S51
接收来自移动终端的信号？
否
是
S52
通信连接
S53
认证处理
S54
认证成功？
否
是
S55
待机模式
S56
检测到车辆操作？
是
否
S57
执行与操作部件对应的控制
S58
认证结果已过有效期限？
否
是
结束

图22

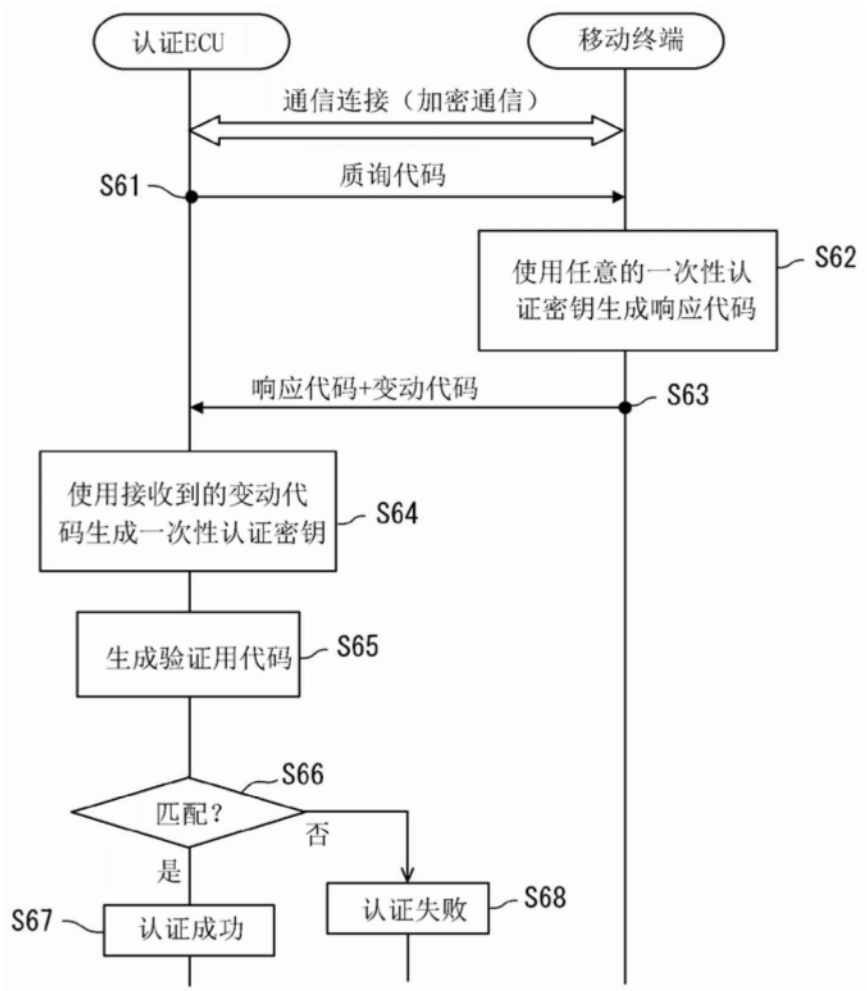

认证ECU
移动终端
通信连接（加密通信）
S61
质询代码
使用任意的一次性认证密钥生成响应代码
S62
响应代码+变动代码
S63
使用接收到的变动代码生成一次性认证密钥
S64
生成验证用代码
S65
S66
匹配？
否
是
S67
认证成功
认证失败
S68

图23

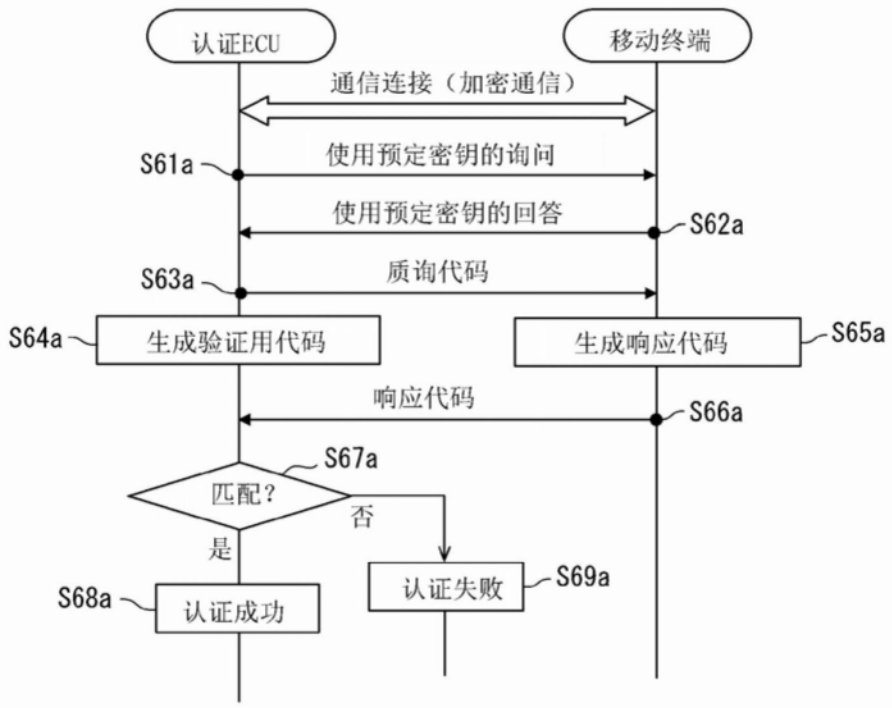

认证ECU
移动终端
通信连接（加密通信）
S61a
使用预定密钥的询问
使用预定密钥的回答
S62a
S63a
质询代码
S64a
生成验证用代码
生成响应代码
S65a
响应代码
S66a
S67a
匹配？
否
是
S68a
认证成功
认证失败
S69a

图24

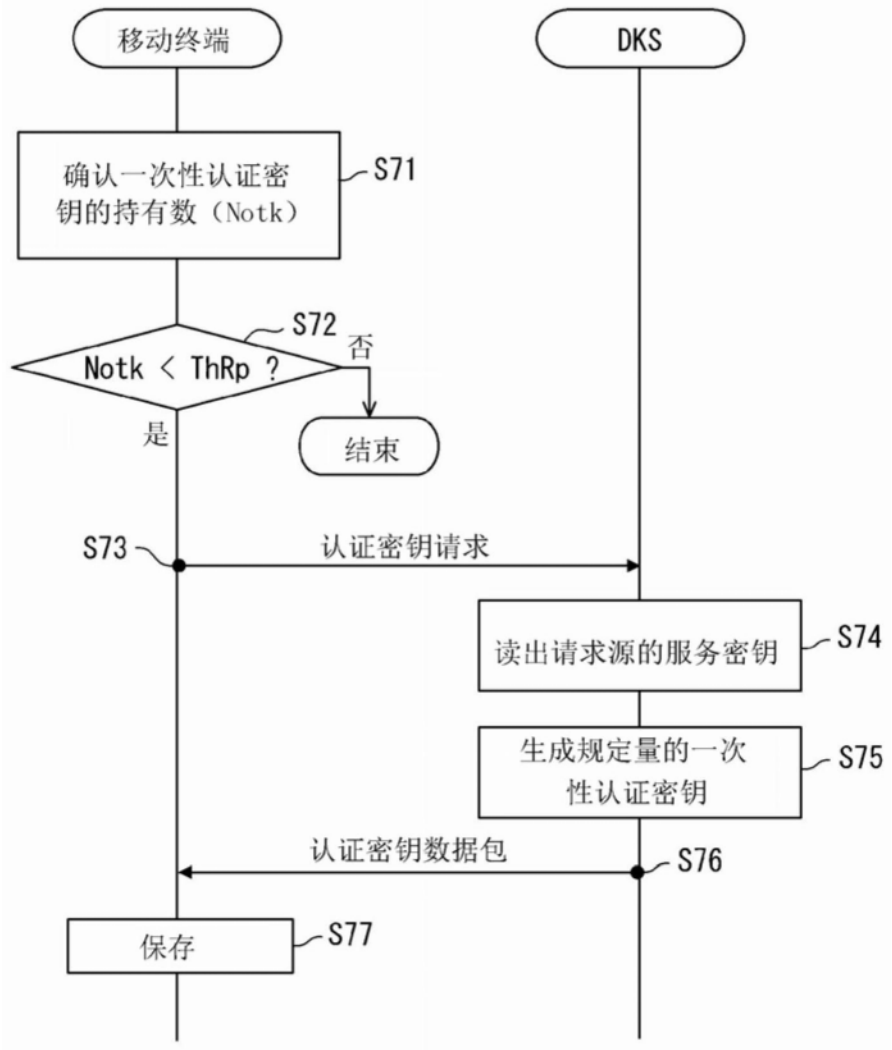

移动终端
DKS
确认一次性认证密钥的持有数（Notk）
S71
S72
Notk < ThRp ?
否
是
结束
S73
认证密钥请求
读出请求源的服务密钥
S74
生成规定量的一次性认证密钥
S75
认证密钥数据包
S76
保存
S77

图25

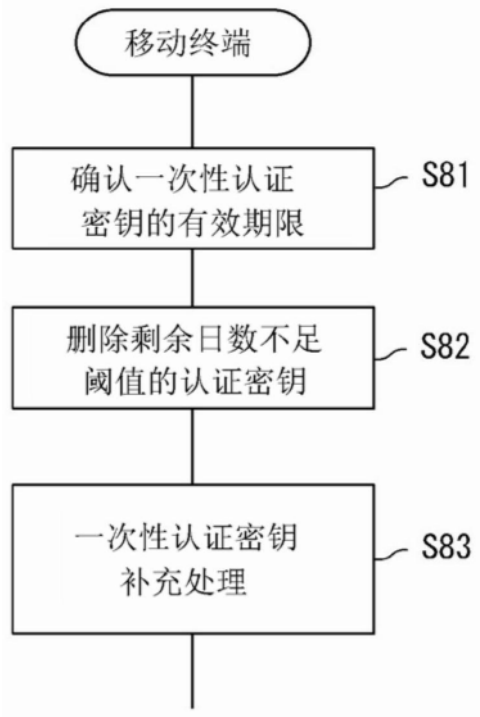

移动终端
确认一次性认证密钥的有效期限
S81
删除剩余日数不足阈值的认证密钥
S82
一次性认证密钥补充处理
S83

图26

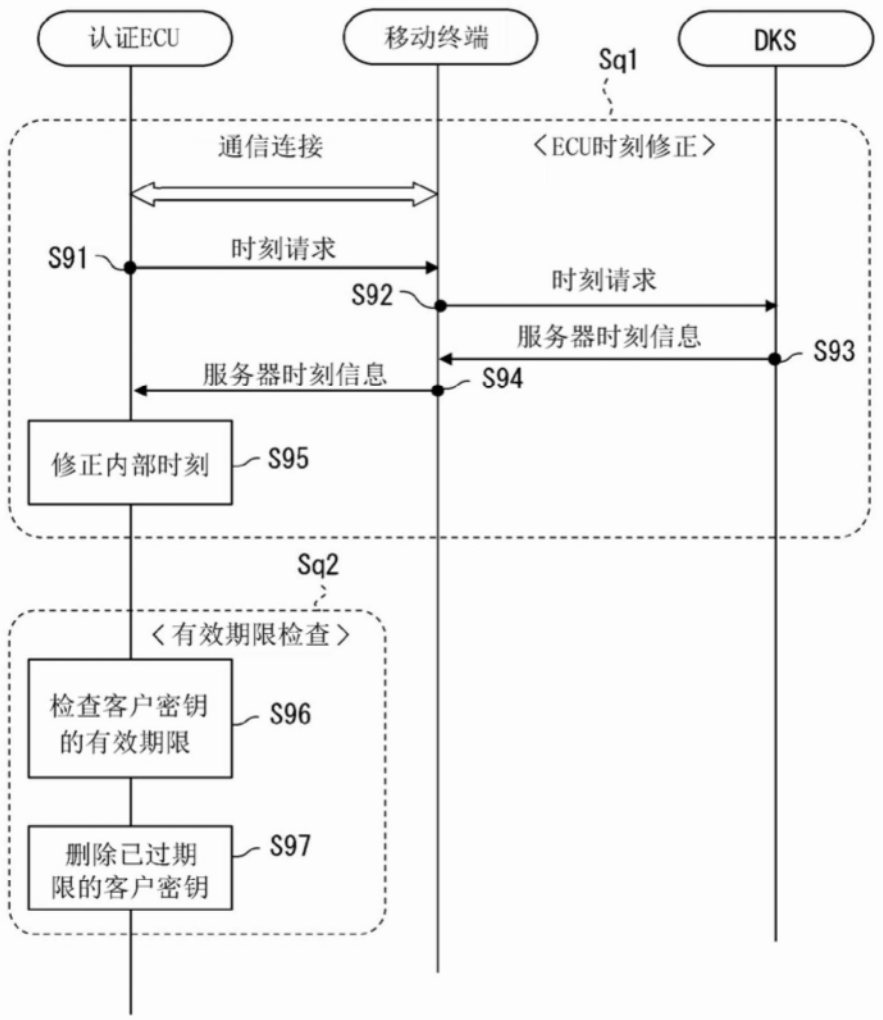

认证ECU
移动终端
DKS
Sq1
通信连接
〈ECU时刻修正〉
S91
时刻请求
S92
时刻请求
服务器时刻信息
S93
服务器时刻信息
S94
修正内部时刻
S95
Sq2
〈有效期限检查〉
检查客户密钥的有效期限
S96
删除已过期限的客户密钥
S97

图27

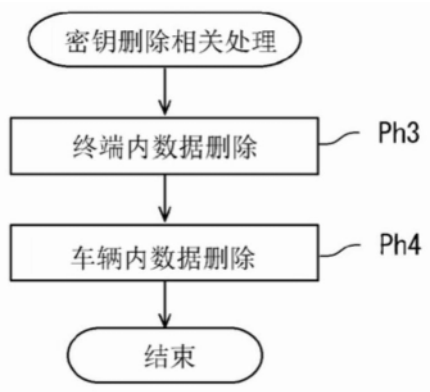

密钥删除相关处理
终端内数据删除
Ph3
车辆内数据删除
Ph4
结束

图28

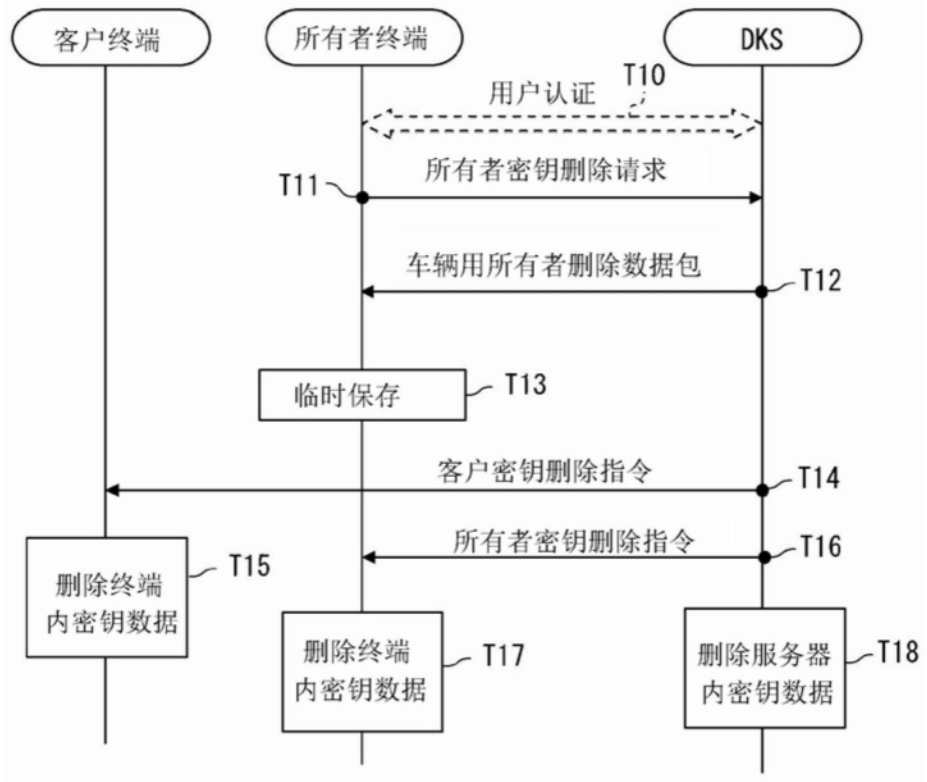

客户终端
所有者终端
DKS
T10
用户认证
所有者密钥删除请求
T11
车辆用所有者删除数据包
T12
临时保存
T13
客户密钥删除指令
T14
所有者密钥删除指令
T16
删除终端
内密钥数据
T15
删除终端
内密钥数据
T17
删除服务器
内密钥数据
T18

图29

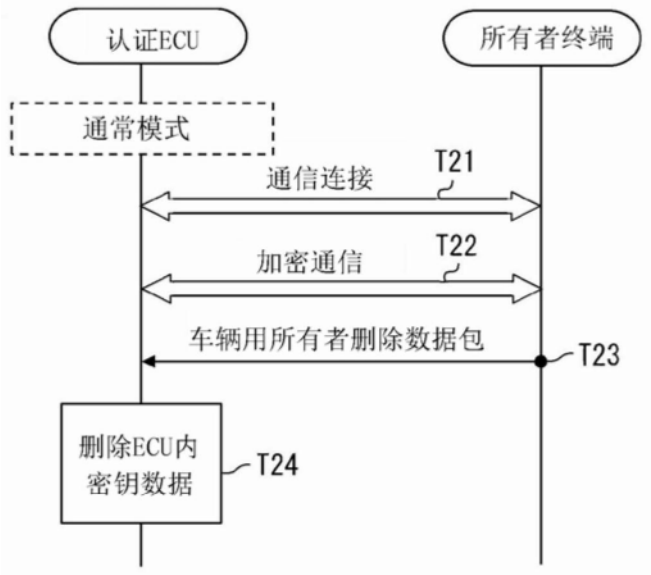

认证ECU
所有者终端
通常模式
通信连接
T21
加密通信
T22
车辆用所有者删除数据包
T23
删除ECU内
密钥数据
T24

图30

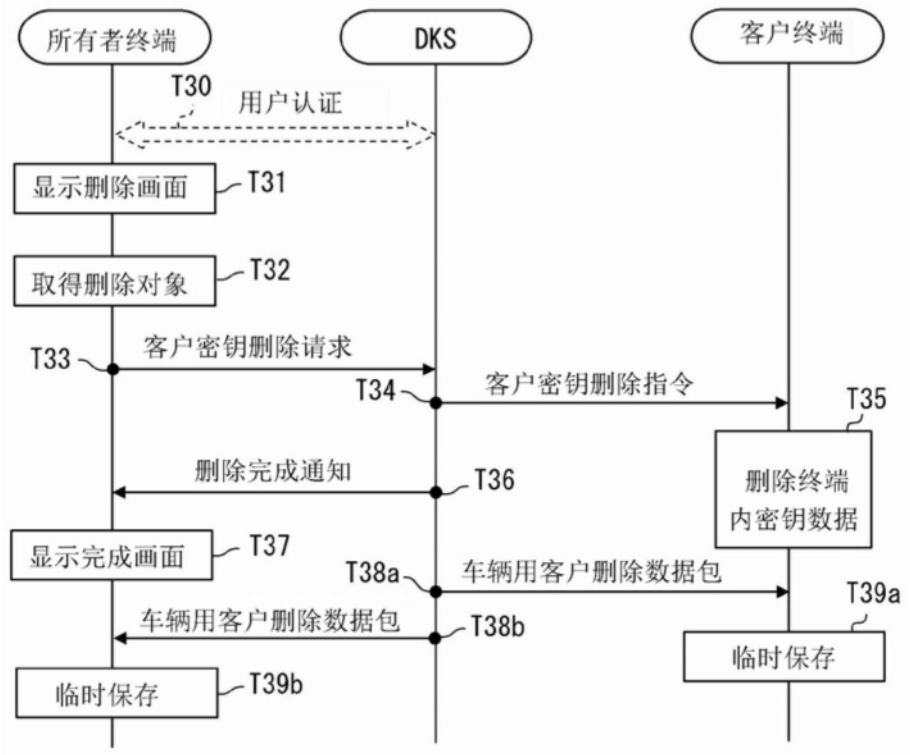

所有者终端
DKS
客户终端
T30
用户认证
显示删除画面
T31
取得删除对象
T32
T33
客户密钥删除请求
T34
客户密钥删除指令
T35
删除终端
内密钥数据
删除完成通知
T36
显示完成画面
T37
T38a
车辆用客户删除数据包
T39a
车辆用客户删除数据包
T38b
临时保存
临时保存
T39b

图31

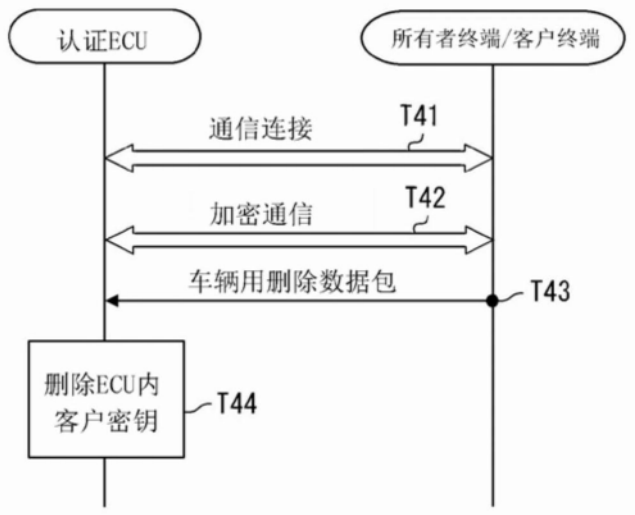

认证ECU
所有者终端/客户终端
通信连接
T41
加密通信
T42
车辆用删除数据包
T43
删除ECU内
客户密钥
T44

图32

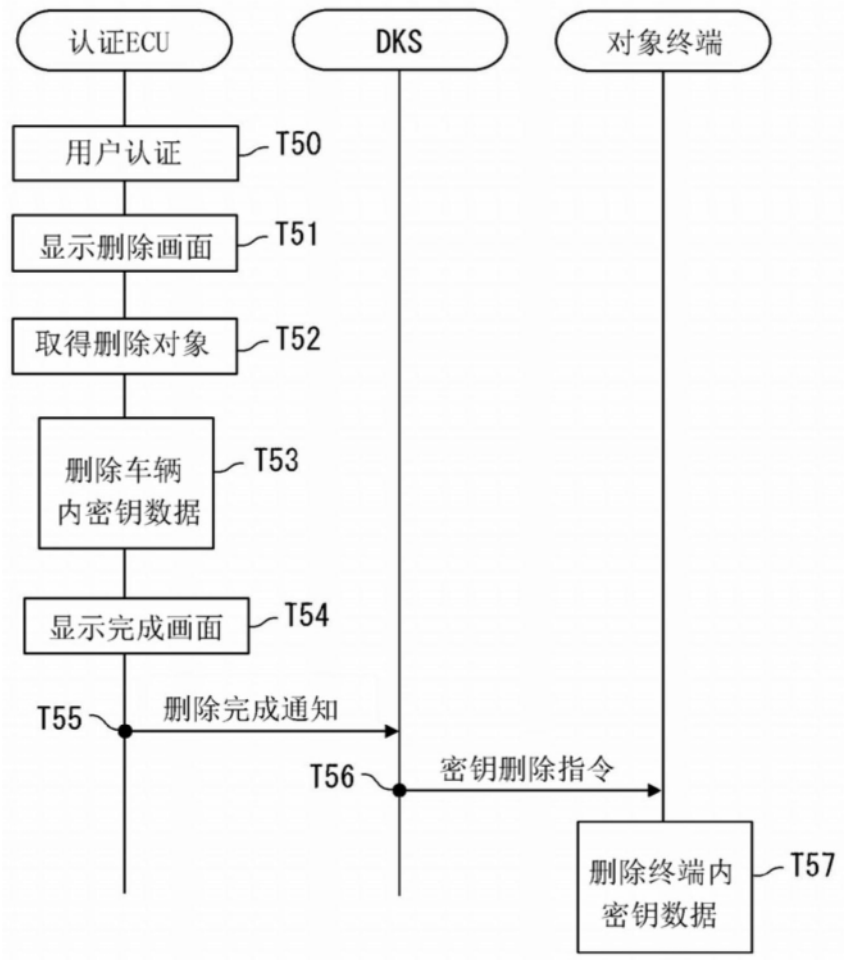

认证ECU
DKS
对象终端
用户认证
T50
显示删除画面
T51
取得删除对象
T52
删除车辆
内密钥数据
T53
显示完成画面
T54
T55
删除完成通知
T56
密钥删除指令
删除终端内
密钥数据
T57

图33

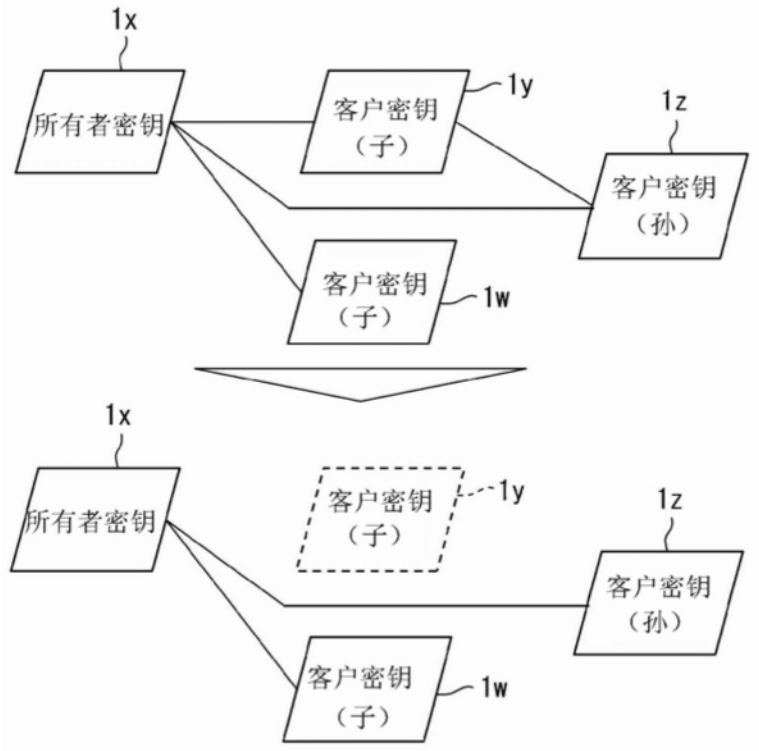

1x
所有者密钥
客户密钥
（子）
1y
1z
客户密钥
（孙）
客户密钥
（子）
1w
1x
所有者密钥
客户密钥
（子）
1y
1z
客户密钥
（孙）
客户密钥
（子）
1w

图34

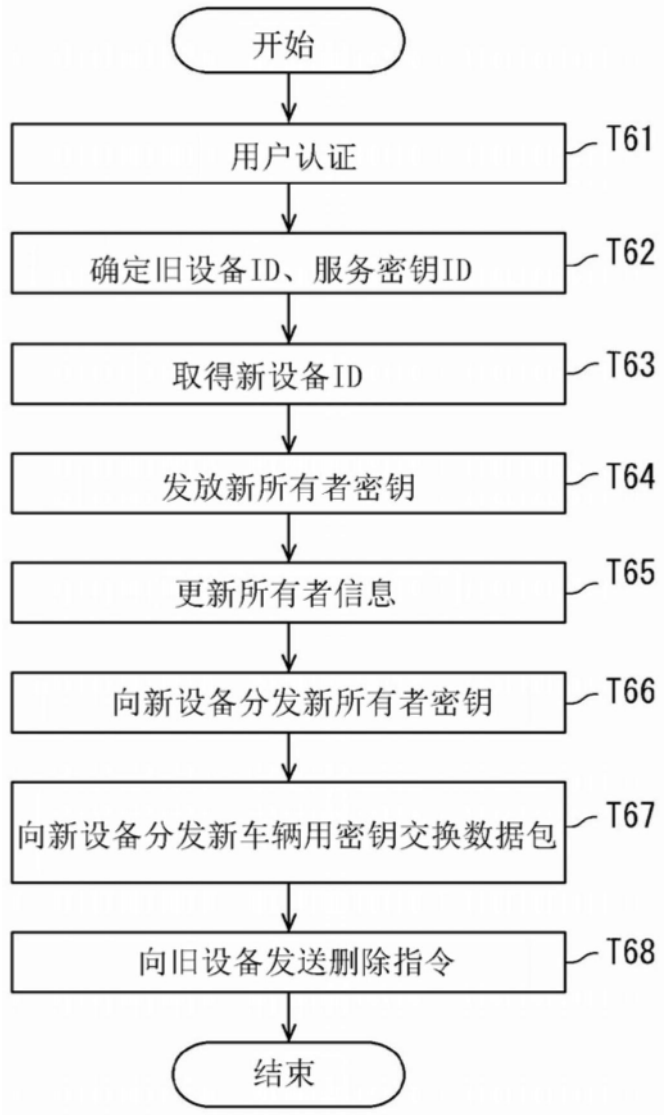

开始
用户认证
T61
确定旧设备ID、服务密钥ID
T62
取得新设备ID
T63
发放新所有者密钥
T64
更新所有者信息
T65
向新设备分发新所有者密钥
T66
向新设备分发新车辆用密钥交换数据包
T67
向旧设备发送删除指令
T68
结束

图35