(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 103201996 B
(45)授权公告日 2016.03.23

(21)申请号 201180039545.8
(22)申请日 2011.08.05
(30)优先权数据
102010037013.4 2010.08.16 DE
102010037271.4 2010.09.01 DE
(85)PCT国际申请进入国家阶段日
2013.02.16
(86)PCT国际申请的申请数据
PCT/EP2011/063551 2011.08.05
(87)PCT国际申请的公布数据
WO2012/022637 DE 2012.02.23
(73)专利权人 胡夫·许尔斯贝克和福斯特有限及两合公司
地址 德国费尔伯特
(72)发明人 斯特凡·莫尼格 维特·席洛德
(74)专利代理机构 深圳中一专利商标事务所 44237
代理人 张全文
(51)Int.Cl.
H04L 29/06(2006.01)
B60R 25/24(2013.01)
G07C 9/00(2006.01)
(56)对比文件
EP 1281588 A2,2003.02.05,
EP 0931979 A1,1999.07.28,
审查员 颜悦

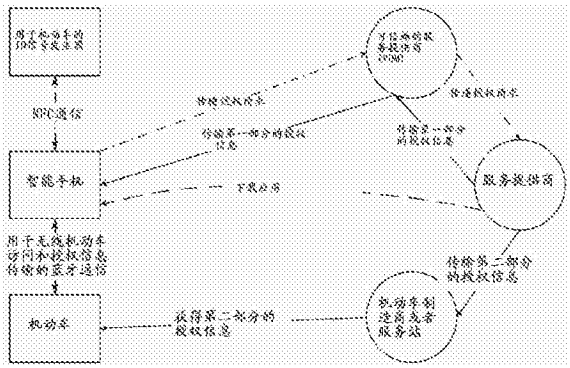
权利要求书1页 说明书7页 附图2页

(54)发明名称

提供无线机动车访问的方法

(57)摘要

本发明涉及一种用于提供机动车无线访问的方法，其中，在对应于机动车的ID信号发生器和无线通信装置之间建立连接。存储在ID信号发生器中的第一识别标识被传输给通信装置并且在无线通信装置和服务提供商之间的连接通过公共通信网络建立。识别标识与第二识别标识一同发送给服务提供商，该第二识别标识对无线通信装置进行识别。服务提供商产生多部分的授权信息并且部分的授权信息被发送给无线通信装置，同时部分的授权信息也被传输给机动车中的控制装置。基于来自机动车和通信装置的授权信息的部分通过在无线通信装置和机动车的控制装置之间的连接来检验通信装置的访问授权。



CN 103201996 B

1. 一种用于提供对机动车进行无线机动车访问的方法，包括以下步骤：

在对应于所述机动车的 ID 信号发生器和无线通信装置之间建立连接，

将在所述 ID 信号发生器中存储明确的第一识别标识从所述 ID 信号发生器传输给通信装置，

通过公共的通信网络在所述无线通信装置和服务提供商之间建立连接，以及

将所述 ID 信号发生器的第一识别标识与第二识别标识共同从所述无线通信装置传输给所述服务提供商，所述第二识别标识对所述无线通信装置进行识别，

通过服务提供商产生多部分的授权信息，

将多个部分的所述授权信息传输给所述无线通信装置，

将多个部分的所述授权信息传输给所述机动车中的控制装置，

在所述无线通信装置和所述机动车的所述控制装置之间建立连接并且根据来自所述机动车和所述通信装置的所述部分的授权信息检验所述通信装置的访问授权。

2. 如权利要求 1 所述的方法，其特征在于，在所述 ID 信号发生器和所述无线通信装置之间的连接为短程的无线连接，尤其是根据 NFC 标准的连接。

3. 如权利要求 1 或 2 所述的方法，其特征在于，在所述无线通信装置和所述机动车的所述控制装置之间的连接是短程的无线连接，尤其是根据蓝牙标准的连接。

4. 如权利要求 1 所述的方法，其特征在于，在所述访问授权的认证成功时，所述通信装置根据明确的标识作为被授权的访问设备存储在所述机动车的控制装置中。

5. 如权利要求 1 所述的方法，其特征在于，所述部分的授权信息通过公共的无线网络传输到所述机动车中。

6. 如权利要求 1 所述的方法，其特征在于，在使用可与所述控制装置连接的服务设备的情况下，所述部分的授权信息被传递给所述控制装置。

7. 如权利要求 1 所述的方法，其特征在于，能够由用于管理在所述 ID 信号发生器和所述无线通信装置之间的连接的所述服务提供商调出可执行的应用，所述应用可传输到所述无线通信装置上。

8. 如权利要求 1 所述的方法，其特征在于，在包含根据所述 ID 信号发生器的所述识别标识确定的机动车识别的情况下附加地确定所述授权信息。

9. 如权利要求 1 所述的方法，其特征在于，在通过公共的通信网络在所述无线通信装置和服务提供商之间的连接之前，主密钥作为另外的识别标识被存储在所述通信装置中，并且所述主密钥与所述第一识别标识和所述第二识别标识共同由所述无线通信装置传输给所述服务提供商。

10. 如权利要求 1 所述的方法，其特征在于检测是否在从将所述识别数据从所述无线通信装置传输给所述服务提供商开始的预设时间间隔内实现了在所述无线通信装置和所述机动车的所述控制装置之间的连接的建立。

11. 如权利要求 10 所述的方法，其特征在于，所述授权信息包含时间标识，所述时间标识说明了所述授权信息的产生或者所述授权信息的有效期。

提供无线机动车访问的方法

技术领域

[0001] 本发明涉及一种用于设置无线机动车访问的方法。本发明尤其涉及一种方法，在该方法中，用于从对应于机动车的 ID 信号发生器对独立的设备的无线机动车访问的权限被传输。

背景技术

[0002] 在当今多数的机动车中，对机动车的功能，例如车门的解锁或者机动车的启动的开启的功能的访问利用可能的（在授权装置或者权限设定装置之间的无线通信）例如 ID 信号发生器和机动车侧的控制装置执行。

[0003] 由机动车的使用者携带的设备在此包含识别数据，其可以通过机动车通过无线连接询问并且使用者被识别作为合法的使用者。如果以这种方式检验访问权限，那么可以释放或者锁定不同的机动车功能，而无需使用者主动进行操作。

[0004] 基本上除了期望之外已知的是，机动车的使用者希望平日尽可能少地受到用于机动车的随身携带的设备和钥匙拖累。另一方面，机动车钥匙和其功能展示出了用于机动车所有者的实际的辅助工具，尤其是在特殊的情况中（例如发送器装置的电池没电了或者用于对第三方的短期授权以访问机动车）。

[0005] 因此，机动车所有者产生通过一些设备来应用机动车的个别功能或者例如机动车的平常功能合法化的愿望，其中，这些设备无需随身携带。该设备例如可以是移动电话。然而，同时也要随时确保照顾到与安全重大相关的方面，由此可以阻止通过通常的可使用的装置和不值得信赖的授权位置对机动车钥匙和 ID 信号发生器的复制。

发明内容

[0006] 本发明的目的在于，通过可提供的通信装置来简化对机动车功能的操作和授权。

[0007] 本发明的目的通过具有权利要求 1 的特征的方法实现。

[0008] 根据本发明的用于提供无线机动车访问的方法，首先建立在对应于机动车的 ID 信号发生器和无线通信装置之间的连接。该无线通信连接可以使是任意的通信装置，例如移动电话。该移动电话必须携带与机动车钥匙协调一致的通信装置，从而在 ID 信号发生器和通信装置之间建立无线连接。为了建立该连接，或者使用通用的协议和存在于通信设备中的程序或者在通讯装置上提供特殊的程序，从而进行通信。为此，例如在通信装置上加载使用和应用，其被编程以用于与核实的 ID 信号发生器的通信。在通信的框架范围中，在 ID 信号发生器中存储的识别标识由 ID 信号发生器传送给通信装置。该被存储的识别标识表征 ID 信号发生器并且对其进行唯一地识别。该识别标识可以在 ID 信号发生器中加密地存在并且此外通过加密的连接传输给无线通信装置。此外，在 ID 信号发生器中加密的识别标识也以另外的加密形式传输给通信装置，从而使其在通信装置中完全不解密或者不可解密地存在。

[0009] 接下来，通过商业上的公共网络建立在通信装置和服务提供商或者服务提供商提

供的接口之间的连接。该连接不仅可以通过移动无线网络也可以例如通过互联网构建。服务提供商提供服务提供商方面的服务和设备，其可以随时相应于该连接的构建。联系到上下文，服务提供商可以被理解为所有类型的组织性的机构，其允许接收和处理被传输的数据。

[0010] 在建立连接之后，由 ID 信号发生器传输给通信设备的第一识别标识被传输给服务提供商。此外，另外的识别标识被发送给服务提供商，其自身用于识别无线通信装置并且唯一地进行表征。

[0011] 两个识别标识可以被加密地传输，为了可以在传输路径上中断对数据的未授权的访问。如果来自 ID 信号发生器的识别标识已经被加密的传输给通信装置，那么该通信装置可以附加地对加密的识别标识进行加密或者以原始的加密进一步传输，在该时间点，通信装置也完全不需要获知真实的识别标识，然而这同样是可以的。

[0012] 在服务提供商方面，对 ID 信号发生器进行真实性和可信性检验。为此，服务提供商可以访问数据储量，其包含对应于 ID 信号发生器的识别标识的信息。在这种类型的数据库中存储有在 ID 信号发生器和所属的机动车之间的链接。

[0013] 根据传输的数据，服务提供商的系统通过授权方法产生多部分的授权信息。该授权信息不仅考虑到了移动无线通信装置的识别标识，还考虑到 ID 信号发生器的识别标识。因此，该多部分的授权信息承载两个识别标识的链接。

[0014] 授权信息包含一些数据，这些数据对于释放机动车侧的无线通信装置的访问权限是必需的。该多部分的授权信息的一部分被传送回无线通信装置，其中可以使用任意类型的连接路径。尤其可以使用已经应用的公共通信网络，其已经被用于向装置传输数据。

[0015] 另外的一部分数据被传输给机动车中的控制装置。因此，授权信息以多个部分在两个不同的路径传输给不同的目标位置。在此，传输的部分逐步地与各自的目标位置相匹配，也具有数据交量(Datenschnittmenge)。可选的是，也可以传输完全不同的数据部分。向机动车或者机动车中的控制装置的部分的授权信息的传输通过通信的任意路径实现。如果机动车配备有合适形式的通信装置，那么该传输可以直接实现。然而，可选的是，该通信也可以通过可信任的位置中转地实现。因此，对于机动车中的控制装置的来说确定的部分的授权信息被传输给可选的车间或者机动车销售商或者其他的可信任的位置(例如加油站)，使用者必须向该处申请，以可以执行该部分的授权信息到其机动车上的传输。该步骤可以利用考虑到使用者和所属的无线通信设备的另外的验证检验来实现。

[0016] 在授权信息传输到无线通信装置以及传输到机动车中的控制装置上之后，在该两个组件之间建立连接，并且在机动车方面对于通信装置对于机动车的访问的授权根据现在完整存在的授权信息来验证。仅仅当部分的授权信息彼此匹配并且实现成功的检验时，由无线通信装置对机动车的访问才被设置和允许。该访问可以相对于 ID 信号发生器的功能来拓展部分功能或者完整的功能或者甚至另外的功能。

[0017] 部分的授权信息的产生可以通过任意的方法实现，然而尤其是对于信息传输来说已经通过验证的安全方法通过分布密钥来代替。因此，例如在服务提供商方面产生密钥对，该密钥对以不同的路径并且在通信装置与机动车连接之后添加。只有在该密钥对产生逻辑检验时，由授权的和未被腐化的连接来结束。这例如涉及密钥对，其中，待解密的信息利用一个密钥来加密并且与该密钥共同传输，并且仅仅可以通过另外的密钥来解密，从而验证

该授权信息(异步加密)。这种类型的概念在不同的技术领域都是已知的,并且例如已经在信息加密领域中应用很久了。

[0018] 这些非对称的加密系统尤其可以被使用,从而在服务提供商方面提供公共的密钥并且与加密的授权共同发送给通信装置并且将所属的第二私人密钥发送给机动车。通信装置可以以这种方式将通过公共密钥加密的信息发送给机动车,在该机动车处利用私人密钥来解密。除了授权外,这样的过程也被应用在用于控制命令的接下来的通信的安全方面。

[0019] 然而,可选的是,在机动车中存储的并且在那里再一次加密的秘密的密钥以可以在机动车生产时存储。这些秘密的密钥对于机动车系统是已知的,然而对于提供关于机动车的的详细数据的服务提供商来说也是已知的,类似的是机动车制造商提供以补充密钥为目的的密钥数据。信息的可用性通常通过盲码进行保护,因为 ID 信号发生器的识别标识被发送给服务提供商,其可以用于发现匹配的密钥。

[0020] 因此可以通过服务提供商向移动通信设备传输需要利用私人密钥解密的公告和授权通知,以及授权消息,该授权消息同样可利用秘密的密钥来解密并且被发送给机动车。

[0021] 在本发明的框架中给出了大量的其他可能性,以保护从服务提供商向两个目标位置的授权信息的传输,该两个目标位置一方面是通信装置并且另一方面是机动车。

[0022] 此外,在相应的授权通知生成之前,服务提供商也可以除了密钥和通信装置的被传输的识别数据之外还考虑到另外的数据。例如,这可以是必须的,即车主个人在服务提供商处报告(例如通过 Web 界面或者电话呼叫),并且通知其移动设备的授权申请。仅有当这样的通知存在时才可以在时间窗口内进行授权。

[0023] 重要的是,为了执行授权和为了向机动车传输相应的授权通知而设置有服务提供商的中间连接,其占据一个可信赖的位置并且其为机动车提供附加的数据。此外,通过该措施可以将数据可存储地上传到中央位置,这在取消授权,例如丢失移动设备时是具有优势的。

[0024] 根据本发明,在 ID 信号发生器和无线通信装置之间的通信这样地设置,即仅仅可以根据在 ID 信号发生器上协调一致的通信才能实现对 ID 信号发生器的重大相关的数据的访问。此外,基本上可以使用标准化的传输协议,然而对较高的协议层的数据的访问也可以通过相应的访问软件在移动设备方面进行管理。由此可以阻止利用标准设备进行不希望的攻击以对重大相关的信息进行访问。

[0025] 优选的是,在 ID 信号发生器和无线通信装置之间的连接是短程连接,尤其是根据 NFC 标准的连接。

[0026] NFC 标准(进场通信)是数据的短程传输标准。NFC 技术的作用距离仅仅是几个厘米并且由此确保对机动车密钥的不希望的访问,例如当对话伙伴或者饭店邻居携带相应的密钥时。根据本发明,通常可以提出,即在 ID 信号发生器的一侧不必进行操作输入,以实现在 ID 信号发生器和无线通信设备之间的通信。相应地具有 NFC 电路的 ID 信号发生器被带入到具有 NFC 功能的移动通信设备附近并且可以实现从 ID 信号发生器到移动设备的识别数据的传输。在市场上已经可以获得具有 NFC 功能的电话设备。这种类型的功能技术被考验和建立并且对于根据本发明的应用适合于进行识别报告的传输。

[0027] 通常,整个的概念和红外结构可以使用 NFC 技术,从而实施本发明。其标准也可以应用于本发明。然而,本发明也可以利用独立的结构和特殊的标准或者另外建立的标准来

代替。

[0028] 在本发明的改进方案中，在无线通信装置和机动车的控制装置之间的连接同样建立一个短程连接，在此然而尤其是根据蓝牙标准的连接。该连接类型也是经受考验和建立的连接技术，该连接技术已经提供给了标准的或者特殊的设计方案的机动车。蓝牙连接相对于 NFC 无线技术具有较大的作用距离并且允许移动通信设备与机动车进行舒适的连接，从而执行不能更改的授权。

[0029] 在改进方案中，在实现了对移动的通信设备的单次成功的授权之后将唯一的标识存储在机动车侧的控制装置中并且将该移动的通信装置视为长期的授权来存储。这样的长期的授权也可以设置具有时间期限，从而在预定的时间期限之后，例如几周之后重复进行授权或者必须进行更新。该方法的优点在于，在一次实现的长期授权之后，提供不依赖网络的和持久的对机动车的访问，而无需再规律地在通信装置和机动车之间进行授权连接。优选的是，仅仅在该方法多次以最小的预设时间间隔重复时才需要执行授权。当授权询问必须以几小时或者几天以相同的设备来重复时，这例如对于提高安全性来说是非常有意义的。由此可以杜绝短时占有 ID 信号发生器的非法者来执行授权。在之前描述的时间间隔中，ID 信号发生器的丢失被最大可能地引起注意并报告遗失，从而可以中断已经实现的授权。

[0030] 尤其有利的是，当部分的授权信息通过公共的移动无线网络从服务提供商传递给机动车中的控制装置时。需要机动车已经具有适合移动无线网络的通信装置，例如 GSM/GPRS 装置。该通信路径可以用于服务提供商，以将授权信息传输给机动车。应用现有的结构来设置特别舒适的传输。

[0031] 在一个可选的设计方案中，在使用可与控制装置连接的服务设备的情况下，授权信息被传递给机动车中的控制装置。这种类型的服务设备可以例如安装在支持点处，例如加油站或者机动车车间或者汽车销售商处，其通过总归存在的服务接口执行在机动车处的连接。该支持点调出属于机动车的、由服务提供商提供的部分的授权信息或者已经根据顾客选择为服务提供商将该部分预先传输。通过在机动车上的服务接口可以利用服务设备传输相应的授权信息。应该注意的是，其单独不意味着对通信装置的授权。利用该服务设备自身也绝不能产生对机动车的非法访问，也就是说密钥的拷贝。取而代之的是，所有部件的共同作用，尤其是服务提供商的介入是必须的。

[0032] 在本发明的优选的设计方案中，服务提供商在无线移动通信设备上调出或者存储一个应用，该应用执行认证和授权通信的整个过程。该应用可以由服务提供商自身执行或者提供并且可以例如也可以独立地根据使用者有目的地对仅仅与 ID 信号发生器的通信的需求来匹配。

[0033] 如果该应用一开始就在服务提供商处要求机动车的使用者提供其姓名和其机动车标识(车架号)，那么可以产生匹配于该特殊的 ID 信号发生器的应用，并且传输给使用者的无线通信设备。以这种方式可以阻止利用通常可使用的应用来进行利用多个密钥的通信。对于每个密钥都可能会产生特殊的应用和传输该特殊的应用。

[0034] 在本发明的改进方案中，在通过公共的通信网络在无线通信装置和服务提供商之间建立连接之前，一个主密钥作为另外的识别标识存储在通讯装置中，并且其与第一识别标识和第二识别标识共同从无线通信装置传输给服务提供商。

[0035] 该与机动车钥匙能够在一个安全的位置存储的主密钥提高了方法的安全性。在类似于移动电话卡中的 PUK 的主密匙在机动车的日常使用中无需随身携带，仅仅对于非正常的授权过程是必需的。这样的另外的标识码阻止了通过非法占有的密钥产生制造拷贝的风险。当该主密匙也如密钥的识别一样对于服务提供商是已知的，并且被精确地传输时，那么服务提供商就能设置授权信息。

[0036] 优选的是，在本发明的方法中还检测是否将识别数据从无线通信装置传输至服务提供商开始在预设的时间间隔内就实现了在无线通信装置和机动车的控制装置间建立了连接。

[0037] 将时间作为限定的参数包含在该方法中提高了安全性。预设的时间间隔可以根据用于传输数据的时间和用于回传授权信息的时间来选择。如果数据通过无线网络直接发送给通信装置和机动车，那么从申请对移动通信设备的访问权利直至通讯设备和机动车的配对的允许的时间总和被限制在几秒直至几分钟。之后，该权利失效并且彼此再次请求。该过程阻止了密钥信息大量地从密钥中读出并且实现了机动车的进入的延迟。

[0038] 在这种情况下，当授权信息包括时间标识时是特别优选的，该时间标识说明了授权信息的产生或者授权信息的有效期。

[0039] 根据时间标识可以追踪授权的有效性或者过期。此外，当一方面实现与机动车的系统时间和另一方面与通信装置的系统时间进行比较时，根据时间标识可以识别对时间的手动篡改。

附图说明

[0040] 以下根据附图进一步说明根据本发明的方法。

[0041] 图 1 示出了在执行了根据第一实施例的方法时关于各个组件的共同作用的示意图。

[0042] 图 2 示出了根据第一实施例的方法的流程图。

具体实施方式

[0043] 在图 1 中示出了参与到该方法中的装置及其作用。用于机动车的 ID 信号发生器 10、智能手机 20 和机动车 30 形成方法的实体功能单元。通过圆圈示出的方法参与者是可信任的服务中间商（VDM）40、服务提供商（SP）50 和机动车制造商及其服务站 60。该最后提到的装置可以代表复杂的功能系统，其也可以分散到另外的面区域和功能区域上。

[0044] 可信任的服务中间商（VDM）承担对使用者和服务提供商之间的联系数据的管理。在此，VDM 可以提供安全的管理和提供由服务提供商准备的应用。

[0045] 为此目的，VDM 与通信网络的运营者合作并且该运营商满足关于认证和可信度方面的要求。

[0046] 实体的方法参与者变换地存在于通信连接中。因此，在 ID 信号发生器 10 和智能手机 20 之间建立 NFC 通信 15。在智能手机 20 和机动车 30 之间可以建立蓝牙连接 25。

[0047] 该通信路径为短程无线通信。与之相对的是，智能手机通过通信网络对 VDM 和 / 或对 SP 建立较大范围的通信连接。为此，尤其可以使用移动无线网络或者互联网。

[0048] 在图 2 中，描述了图 1 中的单元的共同作用的流程图。

[0049] 在方法可执行之前，用于执行智能手机 15 与 ID 信号发生器 10 之间的通信和另外的通信询问的应用被安装到智能手机 10 上。这可以通过从可提供的在线数据库中调出相应的应用程序来实现或者通过将智能手机 10 与存储有应用的相应的数据载体来实现。该应用不仅可以匹配于智能手机也可以匹配特定的机动车类型或者甚至特定的 ID 信号发生器。

[0050] 在图 2 示出的步骤 100 中，在智能手机 20 上启动该应用。ID 信号发生器 10 和智能手机 20 彼此被放置到附近。在智能手机 20 上的应用的流程起作用，即识别标识通过 NFC 连接 15 从 ID 信号发生器 10 传输至智能手机 20。这在图 2 示出的步骤 120 中实现。该数据立刻在智能手机 20 中进行可信度检测，从而排除传输错误以及对智能手机和在智能手机上的相应的应用与 ID 信号发生器 10 的兼容性进行检测。

[0051] 在步骤 130 中，从 ID 信号发生器 10 传输到智能手机 20 上的识别标识从智能手机 20 通过公共的通信网络发送给可信赖的服务中间商（VDM）40。VDM 的功能在于在使用全球可使用的网络来提供服务的安全性。VDM 的这种功能已经由在线支付过程所公开。VDM 形成一种在实际的服务提供商和最终用户之间的传递点。

[0052] VDM40 在步骤 140 中向 SP50 递交智能手机 20 的请求。该 SP 接下来验证传输的数据，尤其是传输的识别标识。根据密钥或者 ID 信号发生器 10 的唯一的识别标识，服务提供商 50 可以调用机动车 30 的相应的机动车数据并且在步骤 150 中产生多行的码序，其不仅匹配于机动车 30 也匹配于智能手机 20 并且考虑到 ID 信号发生器 10 的数据。

[0053] 现在分别将部分的码序以不同的路径反馈给待连接的设备。码序的第一部分由通过 VDM40 从 SP50 传输给智能手机 20。在步骤 160A，170A 和 180A 中实现。第一码序在目标设备，智能手机 20 中存储。

[0054] 另外的码序在步骤 160B 中根据数据从 SP50 传输给机动车制造商 60，SP50 根据用于机动车 30 的识别标识来确定这些数据。在步骤 170B 中，机动车制造商 60 将第二码序传输给机动车 30。这或者可以在服务站中保养机动车时通过连接至相应的服务设备实现，或者利用公共的通信网络通过无线传输实现，只要机动车 30 具有相应的通信部件。

[0055] 在步骤 180B 中，将第二码序存储在机动车中。

[0056] 在该步骤之后，在智能手机 20 中存储第一码序，而在机动车 30 中存储第二码序。在接下来的在智能手机 20 和机动车 30 之间的连接过程中，码序被传输和认证并且在码序的认证成功时产生连接释放 200。

[0057] 在此在智能手机和机动车之间的必需的通信能够以电缆连接的形式进行，然而也可以通过用于无线传输的蓝牙通信来实现。在两个组件，即智能手机和机动车 30 之间的必要的连接之后，智能手机的访问授权在机动车中存储在控制装置中（步骤 200）。接下来，完全无需 ID 信号发生器的存在既可以实现智能手机对机动车的开启的功能的访问。

[0058] 当在成功地执行连接之前，向机动车 30 的合法所有者报告智能手机的所属关系的通告时，根据本发明的方法在其安全性方面可以进一步提高。为此，该所有者例如可以通过呼叫智能手机 20 或者当其从该智能手机传输一个仅仅可由所有者访问的信息时，从智能手机 20 发送 SMS 给预设的号码，该号码的智能手机作为合法的通信设备提前被报告。这例如可以是信息或者标识，其在执行方法之前在应用的通信线路的情况下通过蓝牙从机动车传输至智能手机，其中，在该时间点，在机动车中，合法的 ID 信号发生器必须被插入到机

动车的点火钥匙中。在该状态中，机动车的控制装置通过蓝牙连接将唯一的标识传输给智能手机，其在执行根据本发明的方法时作为附加的识别标识发送给 SP。由此确保智能手机真正地在由机动车的所有者控制的情况下作为合法的用于执行相应的根据本发明的授权方法的装置来授权。

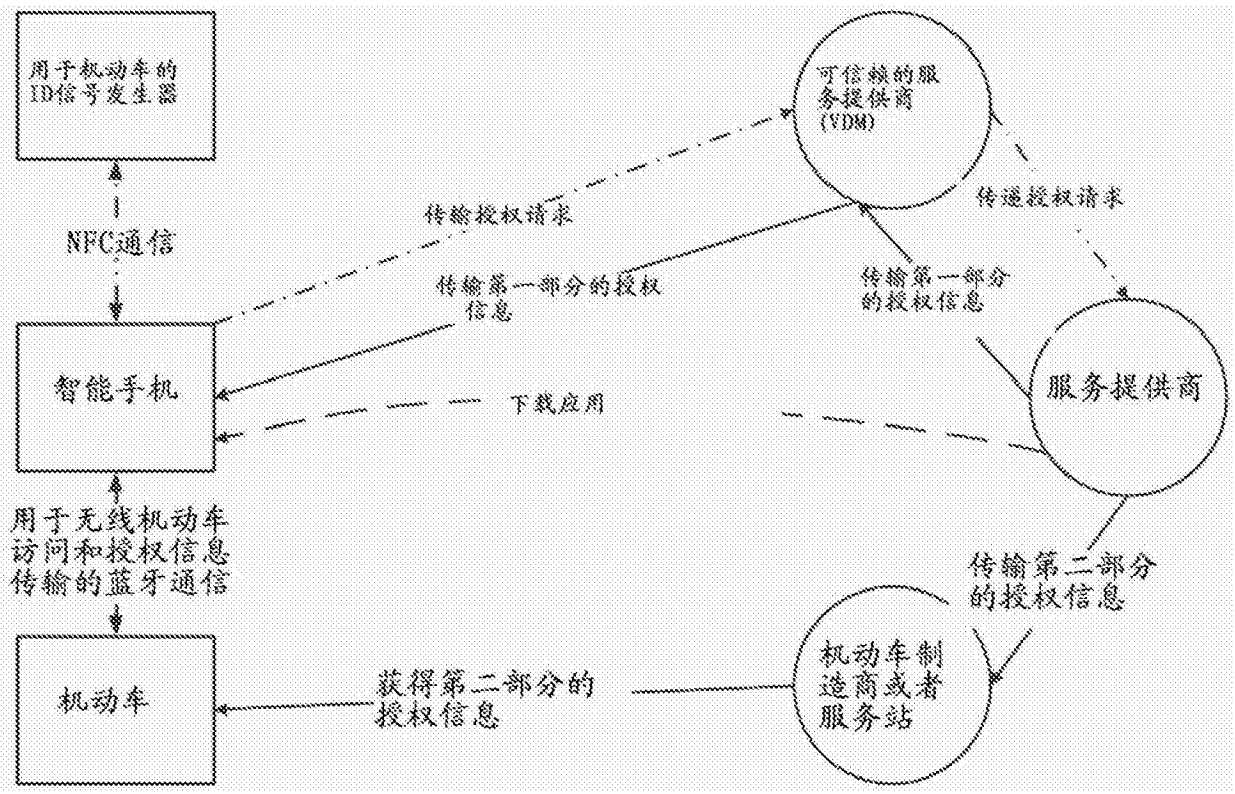

用于机动车的ID信号发生器
NFC通信
智能手机
用于无线机动车访问和授权信息传输的蓝牙通信
机动车
可信赖的服务提供商(VDM)
传输授权请求
传输第一部分的授权信息
传递授权请求
传输第一部分的授权信息
服务提供商
下载应用
传输第二部分的授权信息
机动车制造商或者服务站
获得第二部分的授权信息

图 1

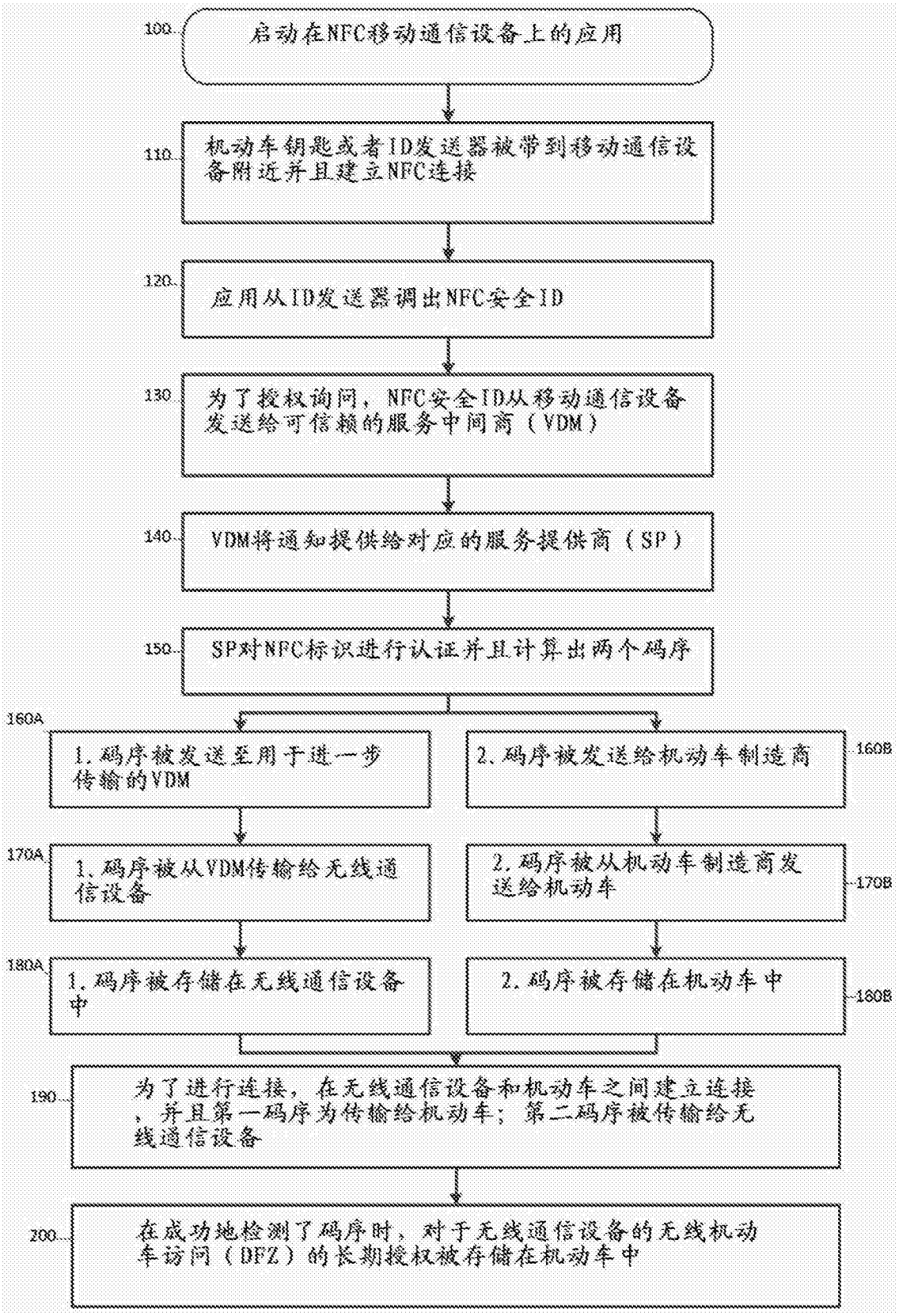

100
启动在NFC移动通信设备上的应用
110
机动车钥匙或者ID发送器被带到移动通信设备附近并且建立NFC连接
120
应用从ID发送器调出NFC安全ID
130
为了授权询问，NFC安全ID从移动通信设备发送给可信赖的服务中间商（VDM）
140
VDM将通知提供给对应的服务提供商（SP）
150
SP对NFC标识进行认证并且计算出两个码序
160A
1.码序被发送至用于进一步传输的VDM
160B
2.码序被发送给机动车制造商
170A
1.码序被从VDM传输给无线通信设备
170B
2.码序被从机动车制造商发送给机动车
180A
1.码序被存储在无线通信设备中
180B
2.码序被存储在机动车中
190
为了进行连接，在无线通信设备和机动车之间建立连接，并且第一码序为传输给机动车；第二码序被传输给无线通信设备
200
在成功地检测了码序时，对于无线通信设备的无线机动车访问（DFZ）的长期授权被存储在机动车中

图 2