(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 108698563 B
(45)授权公告日 2022.02.11

(21)申请号 201780015910.9
(22)申请日 2017.03.07
(65)同一申请的已公布的文献号
申请公布号 CN 108698563 A
(43)申请公布日 2018.10.23
(30)优先权数据
62/305515 2016.03.08 US
(85)PCT国际申请进入国家阶段日
2018.09.07
(86)PCT国际申请的申请数据
PCT/US2017/021109 2017.03.07
(87)PCT国际申请的公布数据
WO2017/155960 EN 2017.09.14
(73)专利权人 大陆智能交通系统有限责任公司
地址 美国加利福尼亚州
(72)发明人 N.伯格霍夫 R.阿胡贾
(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 张凌苗 申屠伟进
(51)Int.Cl.
B60R 25/24(2006.01)
(56)对比文件
CN 103874061 A,2014.06.18
CN 102713927 A,2012.10.03
CN 103339911 A,2013.10.02
US 2015045013 A1,2015.02.12
WO 2011053357 A1,2011.05.05
CN 101588945 A,2009.11.25
CN 103874061 A,2014.06.18
审查员 郑湘南

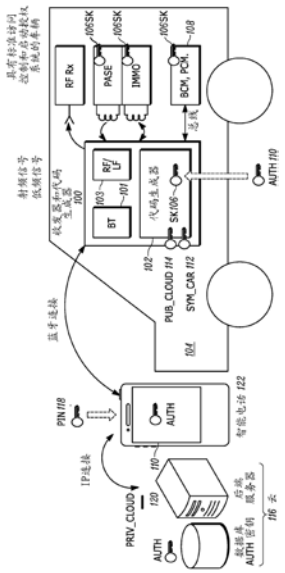
权利要求书1页 说明书5页 附图10页

(54)发明名称

用于车辆的基于安全智能电话的访问和启动授权系统

(57)摘要

一种访问和启动授权系统包括:收发器和代码生成器模块,其被配置为安装在车辆中,其中收发器和代码生成器模块包括:蓝牙收发器,其被配置为建立与智能电话的蓝牙连接;代码生成器,其被配置为:在向车辆学习代码生成器时将秘密密钥传送给一个或多个车辆电子控制单元,随后使用秘密密钥将在代码生成器和车辆之间的通信加密,并且不将未加密形式的秘密密钥存储在代码生成器存储器中,从而防止具有对车辆的访问的人经由代码生成器的对秘密密钥的未经授权的访问。



CN 108698563 B

1.一种用于车辆的装置,包括:

收发器和代码生成器模块,其被配置为安装在车辆中,其中收发器和代码生成器模块包括:

蓝牙收发器,其被配置为建立与智能电话的蓝牙连接;

代码生成器,其被配置为:

在对于车辆学习代码生成器时将秘密密钥传送到一个或多个车辆电子控制单元,

随后使用秘密密钥将在代码生成器和车辆之间的通信加密,以及

不在代码生成器存储器中存储未加密形式的秘密密钥,从而防止具有对车辆的访问的人经由代码生成器对秘密密钥的未经授权的访问。

2.根据权利要求1所述的装置,其中代码生成器存储用于加密和解密秘密密钥的加密密钥或加密形式的秘密密钥。

3.根据权利要求1所述的装置,其中经由后端服务使能智能电话,所述后端服务使用公钥/私钥基础设施以安全的方式分配用于将秘密密钥加密的唯一数或加密形式的秘密密钥。

4.根据权利要求1所述的装置,其中代码生成器被配置为经由周期性的轮询方案与智能电话保持联系。

5.根据权利要求4所述的装置,其中代码生成器被配置为使用接收的信号强度指示器准则来限制蓝牙连接的范围。

6.根据权利要求5所述的装置,其中代码生成器被配置为在蓝牙连接中断时,从存储器擦除解密形式的秘密密钥的任何存储的实例以防止对秘密密钥的未经授权的访问。

7.根据权利要求1所述的装置,其中代码生成器被配置为生成随机数AUTH。

8.根据权利要求1所述的装置,其中代码生成器被配置为利用随机数AUTH将秘密密钥加密并且将加密的秘密密钥存储在代码生成器存储器中。

9.根据权利要求1所述的装置,其中代码生成器被配置为将随机数AUTH加密并且将加密形式的随机数AUTH发送到后端服务。

10.根据权利要求9所述的装置,其中代码生成器被配置为从代码生成器存储器删除随机数AUTH。

11.根据权利要求1所述的装置,其中代码生成器被配置为生成和在本地存储器中存储随机数AUTH。

12.根据权利要求11所述的装置,其中代码生成器被配置为利用随机数AUTH和PUB_cloud两者将秘密密钥加密以及被配置为将加密的秘密密钥发送到云。

13.根据权利要求12所述的装置,其中利用散列的用户PIN将秘密密钥附加地加密。

14.根据权利要求12所述的装置,其中云被配置为存储加密的秘密密钥以及被配置为将加密的秘密密钥与相应的车辆识别号相关联。

15.根据权利要求14所述的装置,其中代码生成器被配置为从本地存储器删除秘密密钥。

用于车辆的基于安全智能电话的访问和启动授权系统

背景技术

[0001] 本发明的实施例一般地涉及用于车辆的访问控制和启动授权系统。

发明内容

[0002] 根据本发明的实施例，可以以安全和平安的方式将蓝牙使能的智能电话用于访问控制和启动授权两者，并且实施例与常规的车辆访问和启动系统向后兼容。

[0003] 根据本发明的实施例，智能电话充当对于代码生成器的中介(intermediary)授权设备，其实际上类似于安装在车辆中的车钥匙。将蓝牙收发器和代码生成器，以及可选地针对改装(retrofit)解决方案的RF/LF收发器添加到车辆。蓝牙收发器与智能电话通信。代码生成器与控制访问、反移动(immobilization)以及引擎启动的车辆中的电子控制单元通信。所述通信可以经由有线连接发生，或在改装解决方案的情况中经由RF/LF收发器发生，所述RF/LF收发器模仿向车辆编程的附加的车钥匙。

附图说明

[0004] 图1-3描绘了根据本发明的实施例的用于车辆的基于安全智能电话的访问和启动授权系统的第一示例实现。

[0005] 图4-6描绘了根据本发明的实施例的用于车辆的基于安全智能电话的访问和启动授权系统的第二示例实现。

[0006] 图7描绘了根据本发明的实施例的用于车辆的基于安全智能电话的访问和启动授权系统的第三示例实现。

[0007] 图8-10描绘了根据本发明的实施例的用于车辆的基于安全智能电话的访问和启动授权系统的、是第二和第三示例实现的组合的第四示例实现。

具体实施方式

[0008] 根据本发明的实施例，可以以安全和平安的方式将蓝牙使能的智能电话用于访问控制和启动授权两者，并且实施例与常规的车辆访问和启动系统向后兼容。

[0009] 本发明的目的包括但不限于：使用具有蓝牙功能的“普通的”智能电话来提供与利用现代车钥匙/钥匙扣(key fob)类似的用户体验；提供在车辆的原始制造日期之后向车辆添加/删除充当车钥匙的智能电话的能力；为系统提供“离线”工作很长时间或甚至几乎无限的时间段的能力，即，在智能电话和车辆都不具有到后端/互联网的连接性时；通过修改现有的车辆架构使系统与新的车辆一起工作；使系统与现有的车辆一起工作，即，现有的车辆架构保持不变(“改装解决方案”)；防止安装在车辆中的系统部件向获得对车辆的物理访问的攻击者暴露用于如下内容的方式：将车辆中的系统部件用作合法的车钥匙或从系统部件提取数据，所述数据将允许对将提供未经授权的访问和/或启动车辆的未经授权的能力的未经授权的车钥匙的创建。

[0010] 根据本发明的实施例，智能电话充当对于代码生成器的中介授权设备，其实际上

类似于安装在车辆中的车钥匙。将蓝牙收发器和代码生成器，以及可选地针对改装解决方案的RF/LF收发器添加到车辆。蓝牙收发器与智能电话通信。代码生成器与控制访问、制动以及引擎启动的车辆中的电子控制单元通信。通信可以经由有线连接发生，或在改装解决方案的情况中经由RF/LF收发器发生，所述RF/LF收发器模仿向车辆编程的附加的车钥匙。

[0011] 在车辆中的代码生成器和电子控制单元之间的通信被以如同通常在合法电子密钥设备和此类电子控制单元之间完成的那样的常规方式加密。

[0012] 不同于普通的车钥匙，用于代码生成器的加密的(一个或多个)秘密密钥SK不存储在代码生成器的存储器中。相反地，将SK的加密版本以及用于加密和解密SK的相应密钥AUTH进行存储：该二者之一被存储在代码生成器中并且另外一个被存储在智能电话中。在该文件中，具有包括“PRIV”或“PUB”的名称的任何密钥指代用在非对称加密中的加密密钥，非对称加密诸如是2,048-比特RSA或256-比特ECC加密。在另一方面，在其名称中不具有“PRIV”或“PUB”的加密密钥被用在诸如256-比特AES之类的对称加密中。

[0013] 经由后端服务使能将被用作车钥匙的智能电话一次，所述的后端服务使用公钥/私钥基础设施以安全的方式分配AUTH或者加密的SK。

[0014] 对于启动授权和车辆上的防盗器(immobilizer)和防盗设备(例如，转向柱锁、变速箱换档锁)的禁用，代码生成器经由周期性的轮询方案与智能电话保持联系。可以添加接收信号强度指示器(RSSI)准则以限制蓝牙连接的范围。如果连接被中断，则代码生成器从其存储器擦除SK的解密版本，致使车辆中的设备对于攻击者而言是无用的。

[0015] 现在将参考图1-3讨论第一示例实现。特别地，现在将参考图1讨论学习。收发器和代码生成器100包括蓝牙收发器101和RF/LF(射频/低频)发射器/收发器103。对于车辆104，学习代码生成器102：SK 106在一个或多个相应的车辆ECU 108和代码生成器之间交换。代码生成器创建随机数AUTH 110。代码生成器利用AUTH加密SK并且将加密的SK存储在本地存储器中。代码生成器将AUTH传送到云：首先利用SYM_car 112并且然后利用PUB_cloud 114加密AUTH。然后将加密的AUTH发送到云116。利用SYM_car的加密确保了其可以仅由车辆解密。利用PUB_cloud的加密确保了其可以仅由云正确地接收。可以利用(散列的)用户PIN 118将加密的AUTH附加地加密。

[0016] 云利用PRIV_cloud 120将AUTH解密。云存储了AUTH(仍利用SYM_car和可选的用户PIN加密)并且与VIN相关联。

[0017] 代码生成器从存储器删除AUTH。

[0018] 简言之，SK不被存储在代码生成器中。替代地，仅将SK的加密版本存储在代码生成器中。因此，假使攻击者获得对设备的物理访问，代码生成器也不能被滥用。这包括无电池-跛行回家模式(在改装版本中)，其不能被利用，因为未以明文形式存储SK。AUTH未被永久地存储在代码生成器中，仅被暂存在RAM中，用于在学习期间加密并且在操作期间解密，如下面更详细地讨论的那样。

[0019] 现在将参考图1讨论使能。电话122在云处注册并且提交车辆的车辆识别号码(VIN)。将AUTH(仍利用SYM_car和可选的用户PIN加密)传送到电话。电话存储AUTH。

[0020] 现在将参考图2和图3讨论操作。图2描绘了根据本发明的实施例的改装系统。

[0021] 现在将讨论访问(示例：主动解锁(UNLOCK))。用户开启电话/应用程序(app)并且输入PIN、指纹或诸如此类。电话与代码生成器(蓝牙，不需要配对)连接。代码生成器可以以

下面结合第三实现示例讨论的方式检查电话身份。用户按下应用程序中的解锁(UNLOCK)按钮。如果利用用户PIN加密了AUTH,则电话利用用户PIN将AUTH解密。电话将解锁(UNLOCK)命令与AUTH一起传输到代码生成器。代码生成器利用SYM_car将AUTH解密。代码生成器利用AUTH将SK解密(并且将解密的SK保持在RAM中)。代码生成器生成利用SK加密的解锁(UNLOCK)电报并且将解锁(UNLOCK)电报传输到RF接收器202。然后代码生成器从RAM存储器删除解密的SK和AUTH。

[0022] 现在将讨论启动(示例:在已使用了主动解锁(UNLOCK)之后的被动启动(START))。步骤与结合访问的上文类似,但是具有以下修改:代码生成器利用AUTH将SK解密。现在代码生成器准备好用于启动的常规挑战-响应(challenge-response)通信。注意到:与用于PASE系统(规章(regulatory))和Thatcham(可保险性)的NHTSAFMVSS 114解释相类比,现在可以认为物理钥匙在乘客舱内部,因为代码生成器已经承担该任务。电话与代码生成器"保持联系"并且每t_1(例如,3秒)周期性地重发AUTH。可以添加RSSI准则以限制蓝牙连接的范围。以这种方式,代码生成器可以在电话保持联系时使SK在存储器中被解密。如果代码生成器没有在时间T_max(T_max大于t_1)中接收AUTH或"心跳(heartbeat)",则代码生成器利用AUTH将SK加密、将加密的SK存储在存储器中并且将AUTH从RAM删除。用户按下启动按钮。被动启动和进入(PASE)204/防盗器(IMMO)206 ECU经由LF发送挑战。代码生成器使用SK计算响应。代码生成器将响应发送到RF接收器或IMMO。电源模式从关闭(off)到ACC循环或引擎启动(取决于实现细节)。注意:与用于PASE系统(规章)的NHTSA FMVSS 114解释相类比,现在将认为钥匙在点火开关中,即,电子代码(响应)处于系统中。

[0023] 简言之,电话需要与代码生成器保持联系以使启动功能使能。虽然在该情况下电话可以在车辆的外部,但是"钥匙"(具有有效SK的代码生成器)在内部。

[0024] 注意:如果用户驶离而遗留智能电话(外部),或智能电话电池放电,则车辆将发出"钥匙丢失警告"。在改装解决方案中,这发生在车辆对有效的钥匙扫描但因为代码生成器不再具有SK的解密版本而未接收到恰当响应时。

[0025] 现在将结合图3讨论原始装备系统。原始装备系统以类似于上面讨论的方式操作,但是不需要RF/LF。替代地可以发生与车身控制模块(BCM)、动力系统(powertrain)控制模块(PCM)或诸如此类的直接通信。

[0026] 参考图4-6讨论第二实现示例。现在将参考图4讨论学习。对于车辆,学习代码生成器:在相应的车辆电子控制单元(ECU)和代码生成器之间交换SK。代码生成器创建随机数、AUTH并且将AUTH存储在本地存储器中。代码生成器利用AUTH将SK加密。代码生成器将加密的SK传送到云:利用PUB_cloud将利用AUTH加密的SK再次加密。然后将加密的SK发送到云。可以利用(散列的)用户PIN将加密的SK附加地加密。云存储加密的SK(并且将加密的SK与VIN关联)。代码生成器从存储器删除SK。

[0027] 简言之,代码生成器存储加密/解密密钥AUTH,但不存储SK。假使攻击者获得对设备的物理访问,则代码生成器也不能被滥用(由于不存储SK,所以不能采用无电池-跛行回家模式(改装版本))。AUTH不离开代码生成器。如下面更详细地讨论的那样,针对学习并且在操作期间,SK仅暂时存在于代码生成器的存储器中。

[0028] 现在将参考图4讨论使能。电话在云处注册并且提交VIN。加密的SK被传送到电话。电话存储加密的SK。

[0029] 现在将参考图5和图6讨论操作。现在将参考图5讨论改装系统。

[0030] 现在将讨论访问(示例:主动解锁(UNLOCK))。用户开启电话/应用程序(app)(输入PIN、指纹或诸如此类)。电话与代码生成器(蓝牙,不需要配对)连接。如下面结合第三示例实现更详细地讨论那样,代码生成器可以检查电话的身份。用户按下应用程序中的解锁(UNLOCK)按钮。电话将解锁(UNLOCK)命令与加密的SK一起传送到代码生成器。代码生成器利用AUTH将SK解密(并且将解密的SK保持在RAM中)。代码生成器生成利用SK加密的解锁(UNLOCK)电报并且将解锁(UNLOCK)电报传送到RF接收器。然后代码生成器从存储器删除解密的SK。

[0031] 现在将讨论启动(示例:在使用了主动解锁(UNLOCK)之后的被动启动(START))。步骤与上面类似,但是具有以下修改:代码生成器利用AUTH将SK解密。现在代码生成器已准备好用于启动的常规的挑战-响应通信。注意:与用于PASE系统(规章)和Thatcham(可保险性)的NHTSAFMVSS 114解释相类比,现在可以认为物理钥匙在乘客舱的内部,因为代码生成器已经承担该任务。电话与代码生成器"保持联系"并且每t_1(例如,3秒)周期性地重发SK。可以添加RSSI准则以限制蓝牙连接的范围。以这种方式,代码生成器可以在电话保持联系时使SK在存储器中被解密。如果代码生成器没有在时间T_max(T_max大于t_1)中接收AUTH或"心跳",则代码生成器从存储器删除SK。用户按下启动按钮。PASE/ IMMO ECU经由LF发送挑战。代码生成器使用SK计算响应。代码生成器将响应发送到RF接收器或IMMO。电源模式从关闭到ACC循环或引擎启动(取决于实现细节)。注意:与用于PASE系统(规章)的NHTSA FMVSS 114解释相类比,现在将认为钥匙在点火开关中,即,电子代码(响应)处于系统中。

[0032] 简言之,电话需要与代码生成器保持联系以使启动功能使能。虽然在该情况下电话可以在车辆的外部,但是"钥匙"(具有有效SK的代码生成器)在内部。

[0033] 注意:如果用户驶离而遗留智能电话(外部),或智能电话电池放电,则车辆将发出"钥匙丢失警告"。在改装解决方案中,这发生在车辆对有效的钥匙扫描但因为代码生成器不再具有SK的解密版本而未接收到恰当响应时。

[0034] 现在将结合图6讨论原始装备系统。原始装备系统以类似于上面讨论的方式操作,但是不需要RF/LF。替代地可以发生与车身控制模块(BCM)、动力系统控制模块(PCM)或诸如此类的直接通信。

[0035] 现在将参考图7讨论第三示例实现。该第三示例可以与前两个示例实现中的任一个组合。云是受信任的服务管理器。利用PUB_cloud 702将代码生成器工厂预编程。

[0036] 现在将参考图7讨论学习。代码生成器利用PUB_cloud将唯一数加密并且将加密的唯一数发送到云。云利用PRIV_cloud 704将唯一数解密并且将解密的唯一数存储在数据库中。唯一数可以是来自上面讨论的示例实现的AUTH或SK。

[0037] 现在将参考图7讨论使能电话。电话在云处注册(经由多个因素的认证)、提交VIN并且提交PUB_phone 706。云利用PRIV_cloud签署PUB_phone并且将其发送回到电话。电话将签署的PUB_phone发送到代码生成器。代码生成器通过使用PUB_cloud标识PUB_phone的真实性。代码生成器将PUB_phone存储在列表中并且在未来将使用PUB_phone来检查注册的电话的身份:电话将利用PRIV_phone 708向代码生成器签署命令。

[0038] 在图8中示出了是第二和第三示例实现的组合的第四示例实现,在图9和图10中示

出了第四示例实现的操作。如图8-10中所示，代码生成器存储AUTH，并且加密形式的SK被存储在智能电话上以及被存储在云中。这导致使得最初不受信任的电话可信任的不太复杂和更灵活的技术方案。

[0039] 为减轻重放攻击，尤其减轻在蓝牙链路上的重放攻击，从智能电话到代码生成器的消息可以合并滚动代码。替代地，这也可以被实现为具有由电话应用程序签署的响应的挑战响应方案。

[0040] 为允许车的基于时间的使用，例如，对于车共享，由云向智能电话提供的密钥可以包含可以由对实时时钟具有访问的代码生成器评估的附加的时间信息。

[0041] 虽然通过对各种实施例的描述已经说明了本发明并且虽然已经很详细地描述了这些实施例，但是本申请的意图不是将所附权利要求的范围约束或以任何方式限制为此类细节。附加的优势和修改对于本领域中的技术人员而言将容易显现。因此，本发明在其更广泛的方面不限于具体的细节、代表性的装置和方法以及示出和描述的说明性示例。因此，在不脱离申请人的一般发明性概念的精神或范围的情况下，可以从此类细节背离。

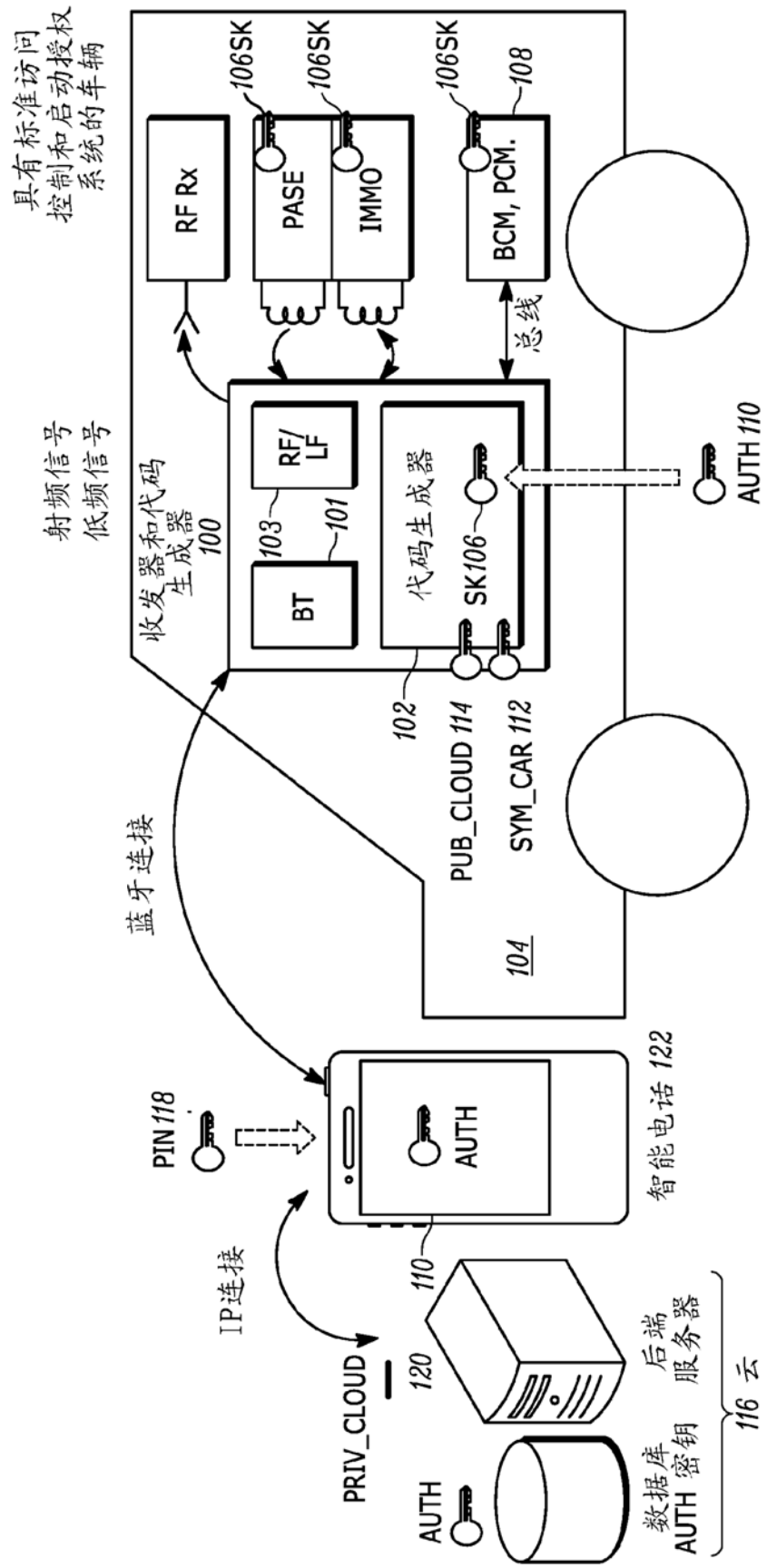

具有标准访问
控制和启动授权
系统的车辆
RF Rx
106SK
PASE
106SK
IMMO
106SK
BCM, PCM.
108
总线
射频信号
低频信号
收发器和代码
生成器
100
RF/
LF
103
101
BT
代码生成器
SK106
AUTH 110
102
PUB_CLOUD 114
SYM_CAR 112
104
蓝牙连接
PIN 118
AUTH
智能电话 122
IP连接
110
PRIV_CLOUD
120
后端
服务器
AUTH
数据库
AUTH 密钥
116 云

图 1

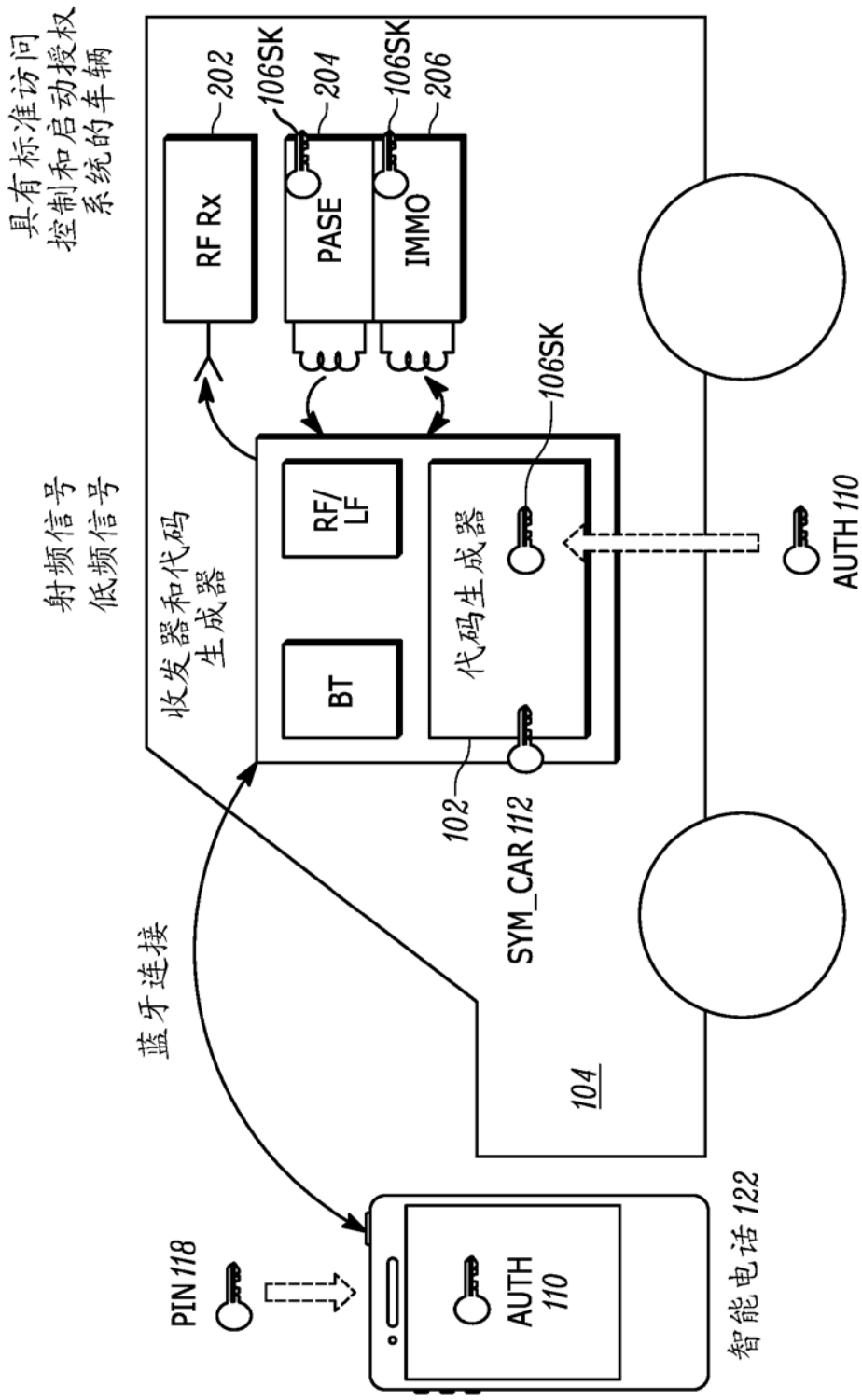

具有标准访问
控制和启动授权
系统的车辆
202
106SK
204
106SK
206
RF Rx
PASE
IMMO
106SK
射频信号
低频信号
收发器和代码
生成器
RF/
LF
BT
代码生成器
AUTH 110
102
SYM_CAR 112
104
蓝牙连接
PIN 118
AUTH
110
智能电话 122

图 2

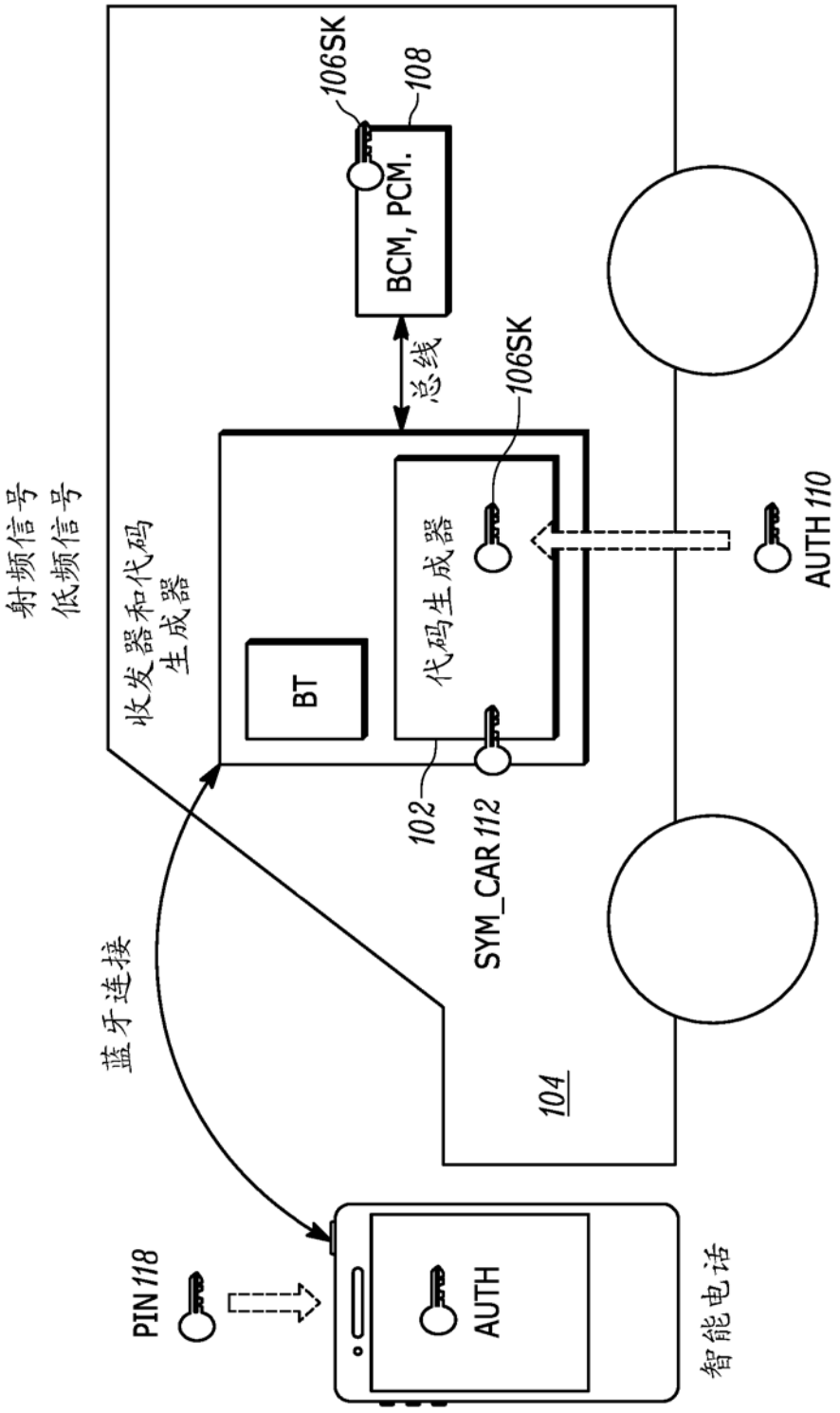

106SK
108
BCM, PCM.
总线
106SK
射频信号
低频信号
收发器和代码
生成器
BT
代码生成器
AUTH 110
102
SYM_CAR 112
蓝牙连接
104
PIN 118
AUTH
智能电话

图 3

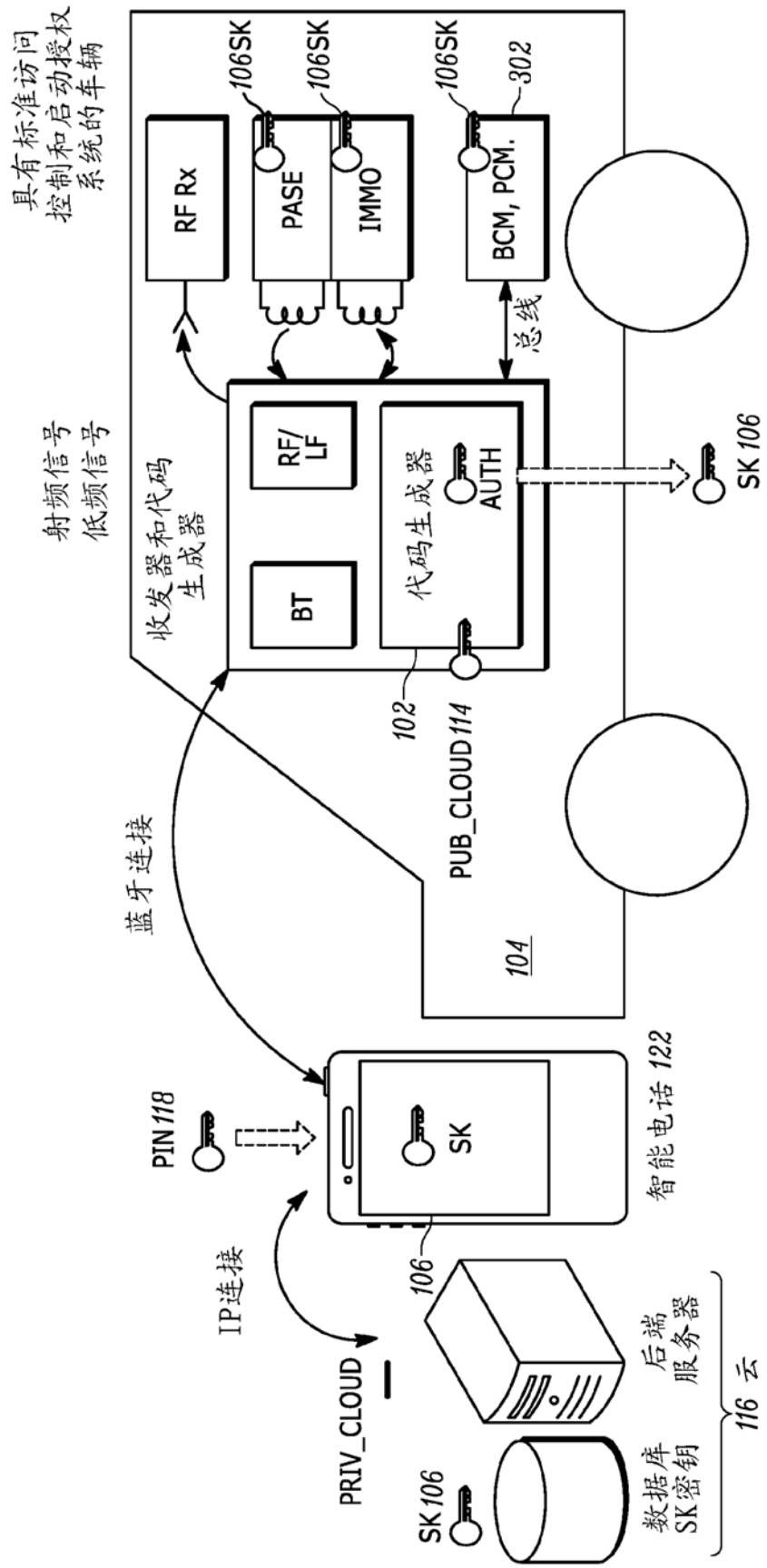

具有标准访问
控制和启动授权
系统的车辆
106SK
106SK
106SK
302
RF Rx
PASE
IMMO
BCM, PCM.
总线
射频信号
低频信号
收发器和代码
生成器
RF/
LF
BT
代码生成器
AUTH
SK 106
102
PUB_CLOUD 114
104
蓝牙连接
PIN 118
SK
智能电话 122
IP连接
106
PRIV_CLOUD
后端
服务器
SK 106
数据库
SK密钥
116 云

图 4

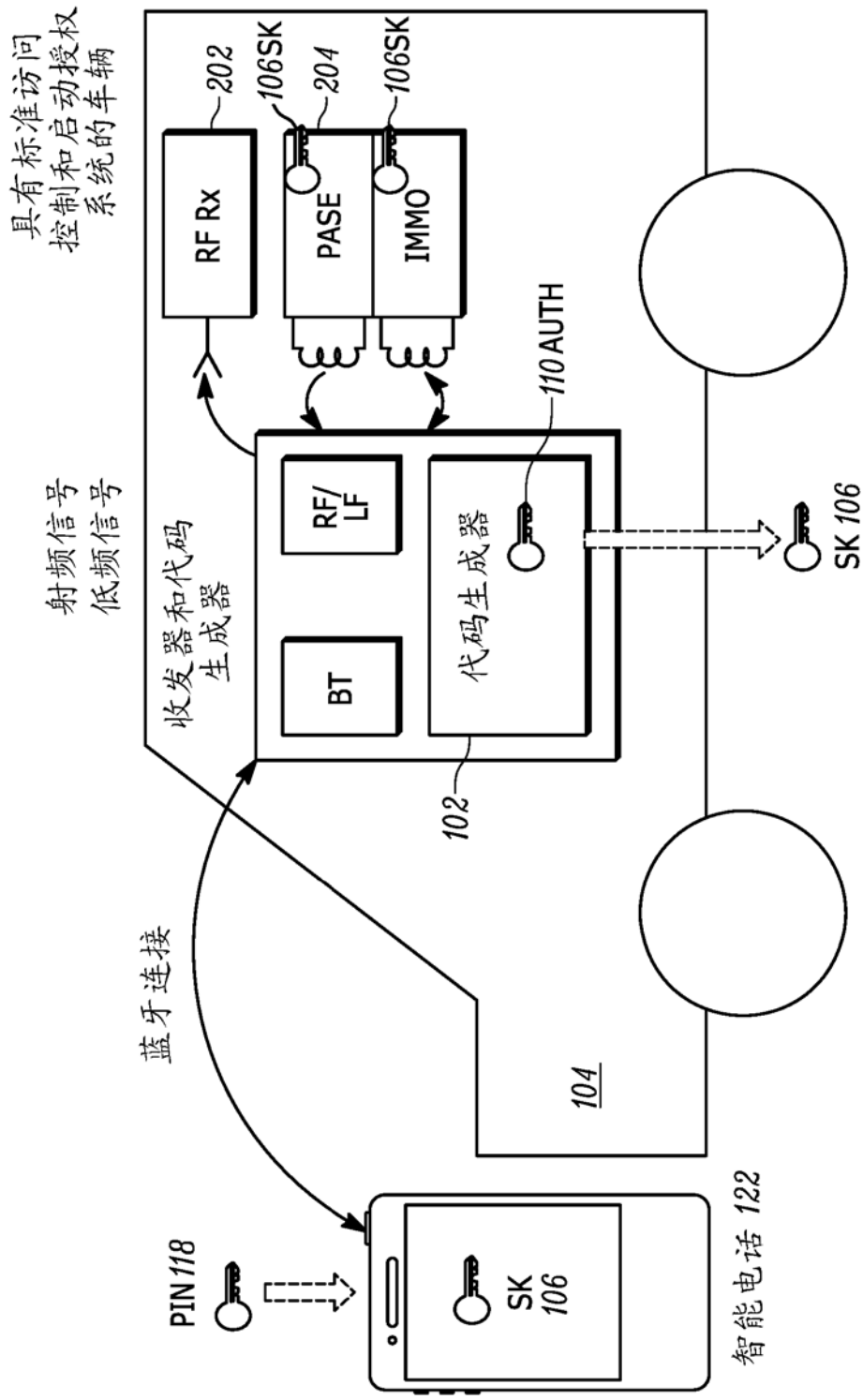

具有标准访问
控制和启动授权
系统的车辆
202
106SK
204
106SK
RF Rx
PASE
IMMO
110 AUTH
射频信号
低频信号
收发器和代码
生成器
RF/
LF
BT
代码生成器
SK 106
102
104
蓝牙连接
PIN 118
SK
106
智能电话 122

图 5

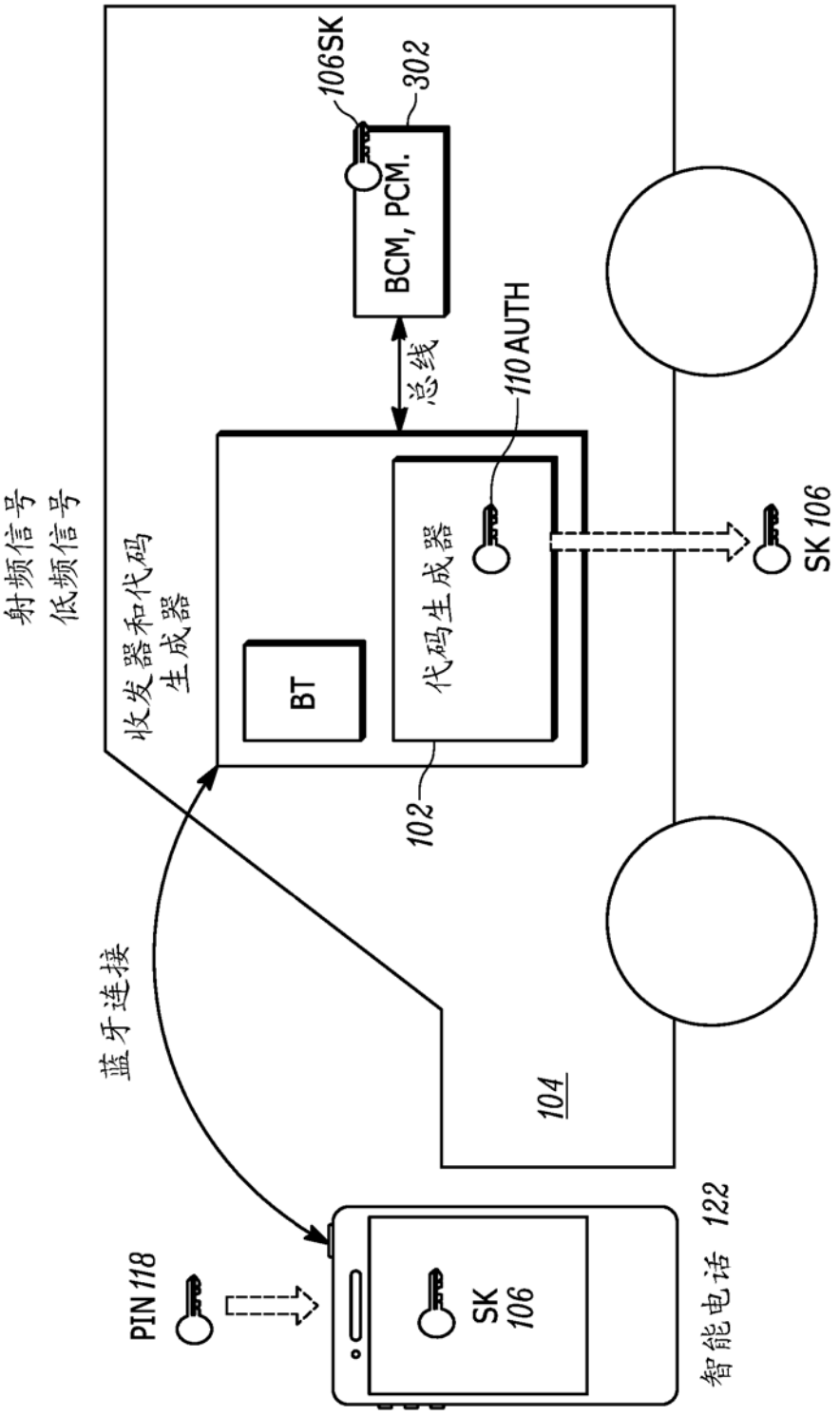

106SK
302
BCM, PCM.
总线
110 AUTH
射频信号
低频信号
收发器和代码
生成器
BT
代码生成器
SK 106
102
104
蓝牙连接
PIN 118
SK
106
智能电话 122

图 6

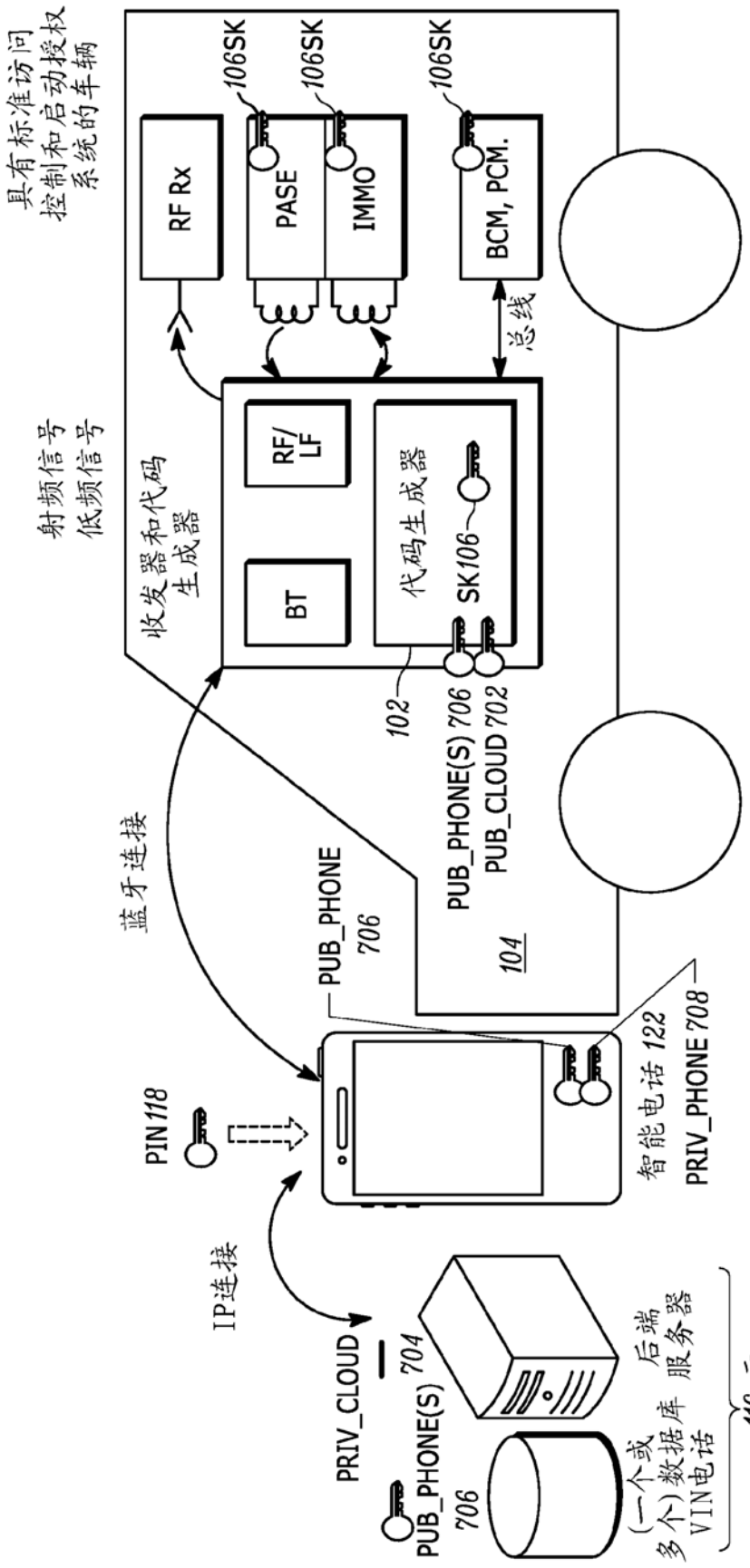

具有标准访问
控制和启动授权
系统的车辆
106SK
106SK
106SK
RF Rx
PASE
IMMO
BCM, PCM.
总线
射频信号
低频信号
收发器和代码
生成器
RF/
LF
BT
代码生成器
SK106
102
PUB_PHONE(S) 706
PUB_CLOUD 702
104
蓝牙连接
PUB_PHONE
706
PIN 118
智能电话 122
PRIV_PHONE 708
IP连接
PRIV_CLOUD
704
后端
服务器
PUB_PHONE(S)
706
(一个或
多个)数据库
VIN电话
116 云

图 7

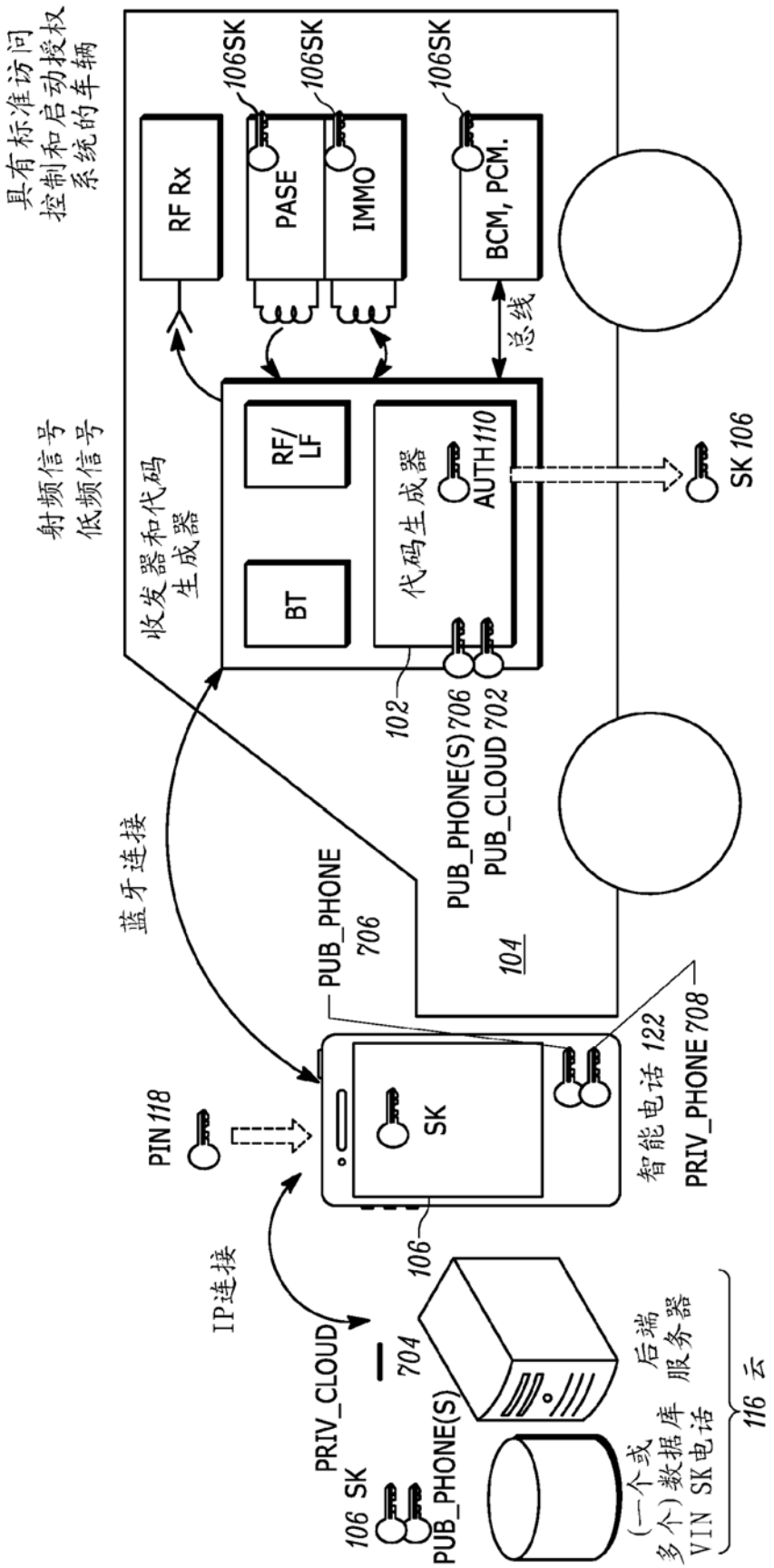

具有标准访问
控制和启动授权
系统的车辆
106SK
106SK
106SK
RF Rx
PASE
IMMO
BCM, PCM.
总线
射频信号
低频信号
收发器和代码
生成器
RF/
LF
BT
代码生成器
AUTH110
SK 106
102
PUB_PHONE(S)706
PUB_CLOUD 702
蓝牙连接
PUB_PHONE
706
104
PIN 118
SK
智能电话 122
PRIV_PHONE 708
IP连接
106
PRIV_CLOUD
704
106 SK
PUB_PHONE(S)
后端
服务器
(一个或
多个)数据库
VIN SK电话
116 云

图 8

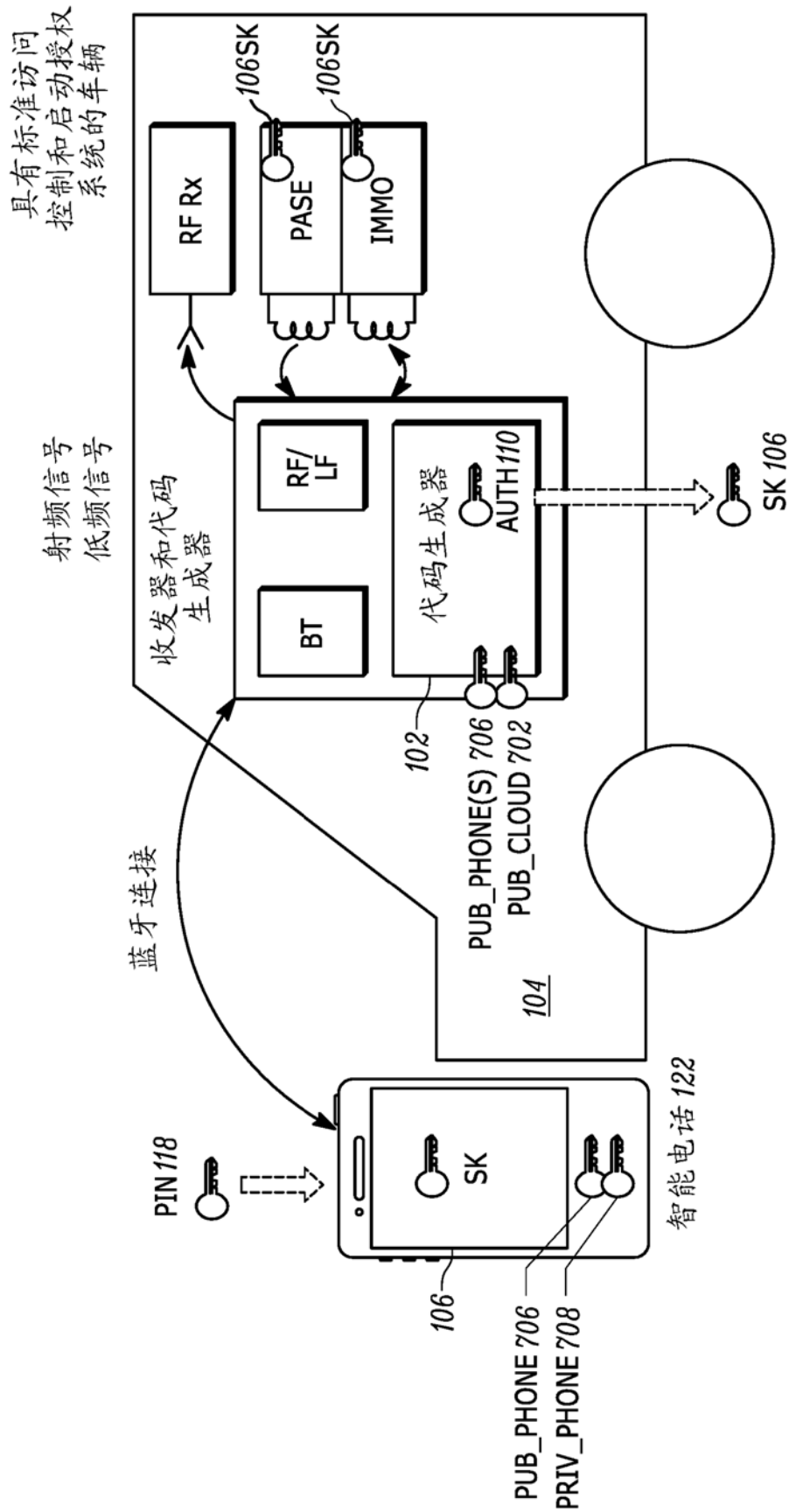

具有标准访问
控制和启动授权
系统的车辆
106SK
106SK
RF Rx
PASE
IMMO
射频信号
低频信号
收发器和代码
生成器
RF/
LF
BT
代码生成器
AUTH110
SK 106
102
PUB_PHONE(S) 706
PUB_CLOUD 702
104
蓝牙连接
PIN 118
SK
智能电话 122
106
PUB_PHONE 706
PRIV_PHONE 708

图 9

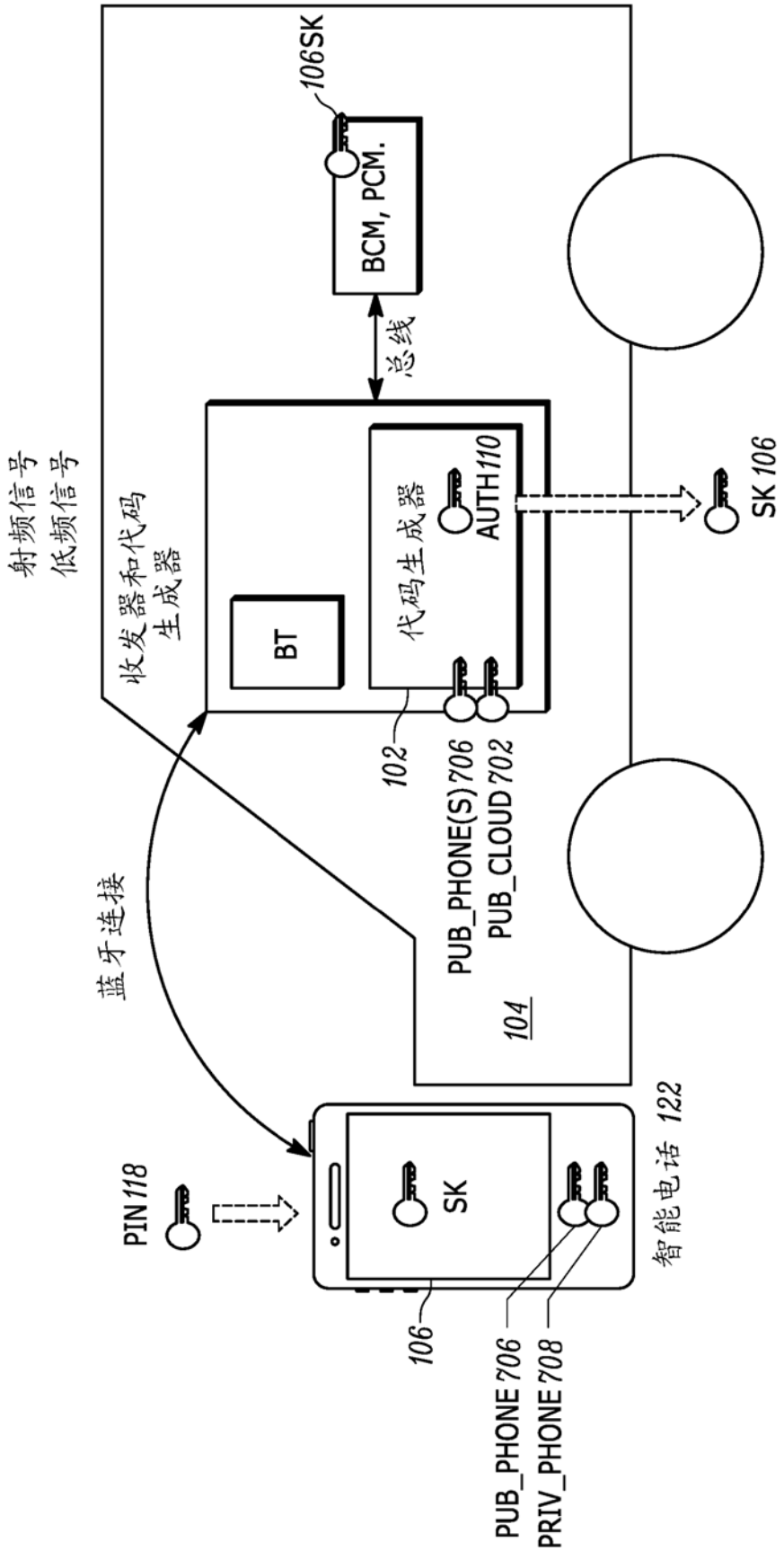

106SK
BCM, PCM.
总线
射频信号
低频信号
收发器和代码
生成器
BT
代码生成器
AUTH110
SK 106
102
PUB_PHONE(S)706
PUB_CLOUD 702
104
蓝牙连接
PIN 118
SK
智能电话 122
106
PUB_PHONE 706
PRIV_PHONE 708

图 10