(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 September 2017 (14.09.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/155960 A1

(51) International Patent Classification:
B60R 25/24 (2013.01)

(21) International Application Number:
PCT/US2017/021109

(22) International Filing Date:
7 March 2017 (07.03.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/305,515 8 March 2016 (08.03.2016) US

(71) Applicant: **CONTINENTAL INTELLIGENT TRANSPORTATION SYSTEMS, LLC** [US/US]; 5201 Great America Parkway, Suite 320, Santa Clara, California 95054 (US).

(72) Inventors: **BERGERHOFF, Nikolas**; 2940 Jones Ave, North Vancouver, British Columbia B7N3V7 (CA). **AHUJA, Ritesh**; 10060 Carmen Rd, Cupertino, California 95014 (US).

(74) Agents: **KLEIN, William** et al.; 21440 W Lake Cook Rd, 7th floor, Deer Park, Illinois 60010 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to the identity of the inventor (Rule 4.17(i))*

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

— *with international search report (Art. 21(3))*

(54) **Title**: SECURE SMARTPHONE BASED ACCESS AND START AUTHORIZATION SYSTEM FOR VEHICLES

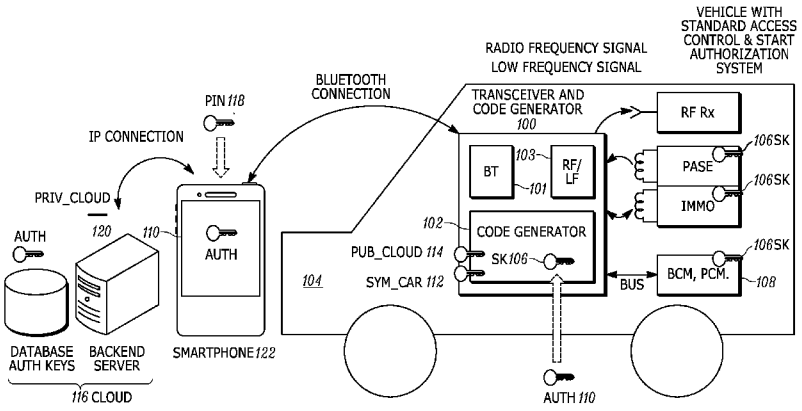

Figure 1

(57) **Abstract**: An access and start authorization system comprises: a transceiver-and-code-generator module that is configured to be installed in a vehicle, wherein the transceiver-and-code-generator module includes: a Bluetooth transceiver configured to establish a Bluetooth connection with a smartphone; a code generator that is configured to: communicate a secret key to one or more vehicle electronic control units while learning the code generator to the vehicle, subsequently use the secret key to encrypt communications between the code generator and the vehicle, and not store in code-generator memory the secret key in unencrypted form thereby preventing unauthorized access, via the code generator, to the secret key by a person who has access to the vehicle.

WO 2017/155960 A1

SECURE SMARTPHONE BASED ACCESS AND START AUTHORIZATION SYSTEM FOR VEHICLES

BACKGROUND

[0001] Embodiments of the invention relate generally to access control and start authorization systems for vehicles.

BRIEF SUMMARY

[0002] In accordance with embodiments of the invention, a Bluetooth enabled Smartphone may be used for both access control and start authorization in a secure and safe way, and embodiments are backward-compatible with conventional vehicle access and start systems.

[0003] In accordance with embodiments of the invention, a smart phone acts as an intermediary authorization device to a code generator which effectively resembles a car key that is installed in a vehicle. A Bluetooth transceiver and the code generator—and, optionally, for the retrofit solution, an RF/LF transceiver—are added to the vehicle. The Bluetooth transceiver communicates with the smart phone. The code generator communicates with electronic control units in the vehicle that control access, immobilization, and engine start. The communication may happen via a wired connection or, in the case of the retrofit solution, via an RF/LF transceiver that mimics an additional car key programmed to the vehicle.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] Figures 1-3 depict a first example implementation of a secure smartphone based access and start authorization system for vehicles in accordance with embodiments of the invention.

[0005] Figures 4-6 depict a second example implementation of a secure smartphone based access and start authorization system for vehicles in accordance with embodiments of the invention.

[0006] Figure 7 depicts a third example implementation of a secure smartphone based access and start authorization system for vehicles in accordance with embodiments of the invention.

[0007] Figures 8-10 depict a fourth example implementation, which is a combination of the second and third example implementations, of a secure smartphone based access and start authorization system for vehicles in accordance with embodiments of the invention.

DETAILED DESCRIPTION

[0008] In accordance with embodiments of the invention, a Bluetooth enabled Smartphone may be used for both access control and start authorization in a secure and safe way, and embodiments are backward-compatible with conventional vehicle access and start systems.

[0009] Objects of the invention include, but are not limited to: using a "regular" smart phone with Bluetooth capability to provide a similar user experience as with a modern car key / key fob; providing the ability to add / delete smart phones acting as a car key to the vehicle after the vehicle's original date of manufacture; providing the ability for the system to work "offline" for a long or even virtually infinite time period, i.e. while neither the smart phone nor the vehicle has connectivity to a backend / internet; making the system work with new vehicles by modifying the existing vehicle architecture; making the system work with existing vehicles, i.e. the existing vehicle architecture remains unchanged ("retrofit solution"); preventing system components installed in the vehicle from exposing a way for an attacker, who gets physical access to the vehicle, to use the system components in the vehicle as a legitimate car key or to extract data

from the systems components that would allow creation of an unauthorized car key that would provide unauthorized access and/or the unauthorized ability to start the vehicle.

[0010] In accordance with embodiments of the invention, a smart phone acts as an intermediary authorization device to a code generator which effectively resembles a car key that is installed in a vehicle. A Bluetooth transceiver and the code generator—and, optionally, for the retrofit solution, an RF/LF transceiver—are added to the vehicle. The Bluetooth transceiver communicates with the smart phone. The code generator communicates with electronic control units in the vehicle that control access, immobilization, and engine start. The communication may happen via a wired connection or, in the case of the retrofit solution, via an RF/LF transceiver that mimics an additional car key programmed to the vehicle.

[0011] The communication between the code generator and the electronic control units in the vehicle is encrypted in a conventional manner as is typically done between a legitimate electronic key device and such electronic control units.

[0012] Unlike in a regular car key, the secret key(s) SK used for encryption by the code generator are **not** stored in the code generator's memory. Contrarily, an encrypted version of the SK and a corresponding key AUTH to encrypt and decrypt SK are stored: one of the two is stored in the code generator and the other is stored in the smart phone. In this document, any key with a name including "PRIV" or "PUB" refers to an encryption key used in asymmetric encryption, such as 2,048-bit RSA or 256-bit ECC encryption. On the other hand, encryption keys that do not have "PRIV" or "PUB" in their names are used in symmetric encryption, such as 256-bit AES.

[0013] Smart phones to be used as car keys are enabled once via a backend service which distributes either AUTH or the encrypted SK in a secure manner using a public/private key infrastructure.

[0014] For start authorization and disabling of the immobilizer and anti theft devices on the vehicle (e.g., steering column lock, transmission shift lock) the code generator maintains contact with the smart phone via a periodic polling scheme. Received Signal Strength Indicator (RSSI) criteria may be added to limit the range of the Bluetooth connection. If the contact is interrupted, the code generator erases the decrypted version of SK from its memory rendering the device in the vehicle useless for an attacker.

[0015] A first example implementation will now be discussed with reference to Figures 1-3. In particular, learning will now be discussed with reference to Figure 1. A transceiver-and-code-generator 100 includes a Bluetooth transceiver 101 and an RF/LF (Radio Frequency / Low Frequency) transmitter/transceiver 103. The code generator 102 is learned to the vehicle 104: the SK 106 is exchanged between one or more corresponding vehicle ECUs 108 and the code generator. The code generator creates a random number AUTH 110. The code generator encrypts the SK with AUTH and stores the encrypted SK in local memory. The code Generator transfers AUTH to the cloud: AUTH is first encrypted with SYM_car 112 and then with PUB_cloud 114. Then the encrypted AUTH is sent to the cloud 116. Encryption with SYM_car ensures that it can only be decrypted by the vehicle. Encryption with PUB_cloud ensures that it can only be properly received by the cloud. The encrypted AUTH may be additionally encrypted with a (hashed) user PIN 118.

[0016] The cloud decrypts AUTH with PRIV_cloud 120. The cloud stores AUTH (still encrypted with SYM_car and optionally user PIN) and associates with VIN.

[0017] The code generator deletes AUTH from memory.

[0018] To summarize, the SK is not stored in the code generator. Instead, only an encrypted version of the SK is stored in the code generator. The code generator cannot, therefore, be misused in case an attacker gets physical

access to the device. This includes battery-less limp-home mode (in the retrofit version), which cannot be exploited because the SK is not stored in clear text form. AUTH is not stored permanently in the code generator, only temporary in RAM, for encryption during learning and decryption during operation, as is discussed in more detail below.

[0019] Enabling will now be discussed with reference to Figure 1. The phone 122 registers at the cloud and submits the vehicle's Vehicle Idenitification Number (VIN). The AUTH (still encrypted with SYM_car, and optionally the user PIN) is transferred to the phone. The phone stores the AUTH.

[0020] Operation will now be discussed with reference to Figures 2 and 3. Figure 2 depicts a retrofit system in accordance with embodiments of the invention.

[0021] Access (example: active UNLOCK) will now be discussed. The user switches on the phone/app and enters PIN, fingerprint, or the like. The phone connects with the code generator (Bluetooth, pairing not required). The code generator may check the phone identity, in the manner discussed below in connection with the third implementation example. The user pushes an UNLOCK button in the app. The phone decrypts the AUTH with the user PIN if the AUTH was encrypted with the user PIN. The phone transmits the UNLOCK command together with the AUTH to the code generator. The code generator decrypts the AUTH with the SYM_car. The code generator decrypts the SK with the AUTH (and keeps the decrypted SK in RAM). The code generator generates an UNLOCK telegram encrypted with the SK and transmits the UNLOCK telegram to the RF receiver 202. The code generator then deletes the decrypted SK and AUTH from RAM memory.

[0022] Start (example: passive START after active UNLOCK was used) will now be discussed. Steps like above in connection with Access, but with the following modifications: the code generator decrypts the SK with the

AUTH. Now Code Generator is ready for regular challenge-response communication for start. Note that, in analogy with NHTSA FMVSS 114 interpretations for PASE systems (regulatory) and Thatcham (insurability), the physical key could now be considered inside the passenger compartment, since the code generator has taken on this role. The phone "keeps in touch" with the code generator and resends the AUTH periodically every t_1 (e.g., 3 seconds). RSSI criteria may be added to limit the range of the Bluetooth connection. In this way, the code generator may leave the SK decrypted in memory while the phone is keeping in touch. If the code generator does not receive the AUTH or a "heartbeat" in time, T_max (T_max is greater than t_1), then the code generator encrypts the SK with the AUTH, stores the encrypted SK in memory, and deletes the AUTH from RAM. The user pushes start button. Passive Start and Entry (PASE) 204 / Immobilizer (IMMO) 206 ECU sends challenge via LF. The code generator calculates a response using the SK. The code generator sends a response to the RF receiver or the IMMO. The power mode is cycled from off to ACC or engine start (depending on implementation details). Note that, in analogy with NHTSA FMVSS 114 interpretations for PASE systems (regulatory), the key would now be considered to be in the ignition switch, i.e. the electronic code (response) is in the system.

[0023] To summarize, the phone needs to be in contact with the code generator to leave the start functionality enabled. While the phone may be outside of the vehicle in this situation, the "key" (code generator with valid SK) is inside.

[0024] Note that, if the user drives away leaving the smart phone behind (outside), or the smart phone battery is discharged, the vehicle will issue a "key lost warning". In a retrofit solution, this happens when the vehicle scans for a valid key but does not receive a proper response because the code generator no longer has a decrypted version of SK.

[0025] An original equipment system will now be discussed in connection with Figure 3. The original equipment system operates in a way similar to the discussion above, but RF/LF is not required. Direct communication with a Body Control Module (BCM), Powertrain Control Module (PCM) or the like may take place instead.

[0026] A second implementation example is discussed with reference to Figures 4-6. Learning will now be discussed with reference to Figure 4. The code generator is learned to the vehicle: the SK is exchanged between a corresponding vehicle Electronic Control Unit (ECU) and the code generator. The code generator creates a random number, AUTH, and stores the AUTH in local memory. The code generator encrypts the SK with the AUTH. The code generator transfers the encrypted SK to the cloud: the SK encrypted with the AUTH is again encrypted with PUB_cloud. Then the encrypted SK is sent to the cloud. The encrypted SK may be additionally encrypted with a (hashed) user PIN. The cloud stores the encrypted SK (and associates the encrypted SK with the VIN). The code generator deletes the SK from memory.

[0027] To summarize, the code generator stores the encryption/decryption key AUTH, but not the SK. The code generator cannot be misused in case an attacker gets physical access to the device (also battery-less limp-home mode (retrofit version) cannot be exploited since the SK is not stored). The AUTH does not leave the code generator. The SK exists only temporarily in the code generator's memory for learning and during operation, as is discussed in more detail below.

[0028] Enabling will now be discussed with reference to Figure 4. The phone registers at the cloud and submits the VIN. The encrypted SK is transferred to the phone. The phone stores the encrypted SK.

[0029] Operation will now be discussed with reference to Figures 5 and 6. A retrofit system will now be discussed with reference to Figure 5.

[0030] Access (example: active UNLOCK) will now be discussed. The user switches on the phone/app (enters PIN, fingerprint, or the like). The phone connects with the code generator (Bluetooth, pairing not required). The code generator may check the phone identity, as is discussed in more detail below in connection with the third example implementation. The user pushes an UNLOCK button in the app. The phone transmits an UNLOCK command together with the encrypted SK to the code generator. The code generator decrypts the SK with the AUTH (and keeps the decrypted SK in RAM). The code generator generates an UNLOCK telegram encrypted with the SK and transmits the UNLOCK telegram to the RF receiver. The code generator then deletes the decrypted SK from memory.

[0031] Start (example: passive START after active UNLOCK was used) will now be discussed. Steps like above, but with the following modifications: The code generator decrypts the SK with the AUTH. Now the Code Generator is ready for regular challenge-response communication for START. Note that, in analogy with NHTSA FMVSS 114 interpretations for PASE systems (regulatory) and Thatcham (insurability), the physical key could now be considered inside the passenger compartment, since the code generator has taken on this role. The phone "keeps in touch" with the code generator and resends the SK periodically every t_1 (e.g., 3 seconds). RSSI criteria may be added to limit the range of the Bluetooth connection. In this way, the code generator may leave the SK decrypted in memory while the phone is keeping in touch. If the code generator does not receive the AUTH or a "heartbeat" in time, T_max (T_max is greater than t_1), then the code generator deletes the SK from memory. The user pushes the start button. PASE/IMMO ECU sends challenge via LF. The code generator calculates a response using the SK. The code generator sends the response to the RF receiver or the IMMO. Power mode is cycled from Off to ACC or the engine starts (depending on implementation details). Note that, in analogy with NHTSA FMVSS 114 interpretations for PASE systems

(regulatory), the key would now be considered to be in the ignition switch, i.e. the electronic code (response) is in the system.

[0032] To summarize, the phone needs to stay in contact with the code generator to leave the start functionality enabled. While the phone may be outside of the vehicle in this situation, the "key" (the code generator with the valid SK) is inside.

[0033] Note that, if the user drives away leaving the smart phone behind (outside), or the smart phone battery is discharged, the vehicle will issue a "key lost warning". In a retrofit solution, this happens when the vehicle scans for a valid key, but does not receive a proper response because the code generator no longer has a decrypted version of SK.

[0034] An original equipment system will now be discussed in connection with Figure 6. The original equipment system operates in a way similar to the discussion above, but RF/LF is not required. Direct communication with a Body Control Module (BCM), Powertrain Control Module (PCM) or the like may take place instead.

[0035] A third example implementation will now be discussed with reference to Figure 7. This third example may be combined with either of the first two example implementations. The cloud is a trusted service manager. The code generator is factory pre-programmed with PUB_cloud 702.

[0036] Learning will now be discussed with reference to Figure 7. The code generator encrypts a unique number with PUB_cloud and sends the encrypted unique number to the cloud. The cloud decrypts the unique number with PRIV_cloud 704 and stores the decrypted unique number in a database. The unique number can be AUTH or SK from the example implementations discussed above.

[0037] Enabling the phone will be discussed with reference to Figure 7. The phone registers at the cloud (authentication via multiple factors), submits the

VIN, and submits PUB_phone 706. The cloud signs PUB_phone with PRIV_cloud and sends it back to the phone. The phone sends the signed PUB_phone to the code generator. The code generator identifies the authenticity of PUB_phone by using PUB_cloud. The code generator stores PUB_phone in a list and will use PUB_phone in the future to check the identity of registered phones: phones will sign commands to the code generator with PRIV_phone 708.

[0038] A fourth example implementation, which is a combination of the second and third example implementations, is shown Figure 8, and the operation of the fourth example implementation is shown in Figure 9 and 10. As shown in Figures 8-10, the code generator stores AUTH, and the SK in encrypted form is stored on the smart phone and in the cloud. This results in a less complicated and more flexible solution that enables making initially non-trusted phones trustable.

[0039] To mitigate replay attacks, especially on the Bluetooth link, the messages from the smart phone to the code generator may incorporate a rolling code. Alternatively, this may also be implemented as a challenge response scheme with the response signed by the phone app.

[0040] To allow time based usage of the car, e.g. for car sharing, the key provided by the cloud to the smart phone may contain additional time information which can be evaluated by the code generator having access to a real time clock.

[0041] While the present invention has been illustrated by a description of various embodiments and while these embodiments have been described in considerable detail, it is not the intention of the applicants to restrict or in any way limit the scope of the appended claims to such detail. Additional advantages and modifications will readily appear to those skilled in the art. The invention in its broader aspects is therefore not limited to the specific details, representative apparatuses and methods, and illustrative

examples shown and described. Accordingly, departures may be made from such details without departing from the spirit or scope of applicant's general inventive concept.

CLAIMS

1. An apparatus comprising:

a transceiver-and-code-generator module that is configured to be installed in a vehicle, wherein the transceiver-and-code-generator module includes:

a Bluetooth transceiver configured to establish a Bluetooth connection with a smartphone;

a code generator that is configured to:

communicate a secret key to one or more vehicle electronic control units while learning the code generator to the vehicle,

subsequently use the secret key to encrypt communications between the code generator and the vehicle, and

not store in code-generator memory the secret key in unencrypted form thereby preventing unauthorized access, via the code generator, to the secret key by a person who has access to the vehicle.

2. The apparatus of claim 1, wherein the code generator stores either an encryption key used to encrypt and decrypt the secret key or the secret key in encrypted form.

3. The apparatus of claim 1, wherein the smart phone is enabled via a backend service that distributes, in a secure manner using public/private key infrastructure, either a unique number used for encrypting the secret key or the secret key in encrypted form.

4. The apparatus of claim 1, wherein the code generator is configured to maintain contact with the smart phone via a periodic polling scheme.

5. The apparatus of claim 4, wherein the code generator is configured to use received signal strength indicator criteria to limit the range of the Bluetooth connection.

6. The apparatus of claim 5, wherein the code generator is configured to, upon interruption of the Bluetooth connection, erase from memory any stored instances of the secret key in decrypted form to prevent unauthorized access to the secret key.

7. The apparatus of claim 1, wherein the code generator is configured to generate a random number AUTH.

8. The apparatus of claim 1, wherein the code generator is configured to encrypt the secret key with the random number AUTH and store the encrypted secret key in code-generator memory.

9. The apparatus of claim 1, wherein the code generator is configured to encrypt the random number AUTH and send the random number AUTH in encrypted form to the backend service.

10. The apparatus of claim 9, wherein the code generator is configured to delete the random number AUTH from code-generator memory.

11. The apparatus of claim 1, wherein the code generator is configured to generate and store in local memory a random number AUTH.

12. The apparatus of claim 11, wherein the code generator is configured to encrypt the secret key with both the random number AUTH and with PUB_cloud and to send the encrypted secret key to the cloud.

13. The apparatus of claim 12, wherein the secret key is additionally encrypted with a hashed user PIN.

14. The apparatus of claim 12, wherein the cloud is configured to store the encrypted secret key and to associate the encrypted secret key with a corresponding vehicle identification number.

15. The apparatus of claim 14, wherein the code generator is configured to delete the secret key from local memory.

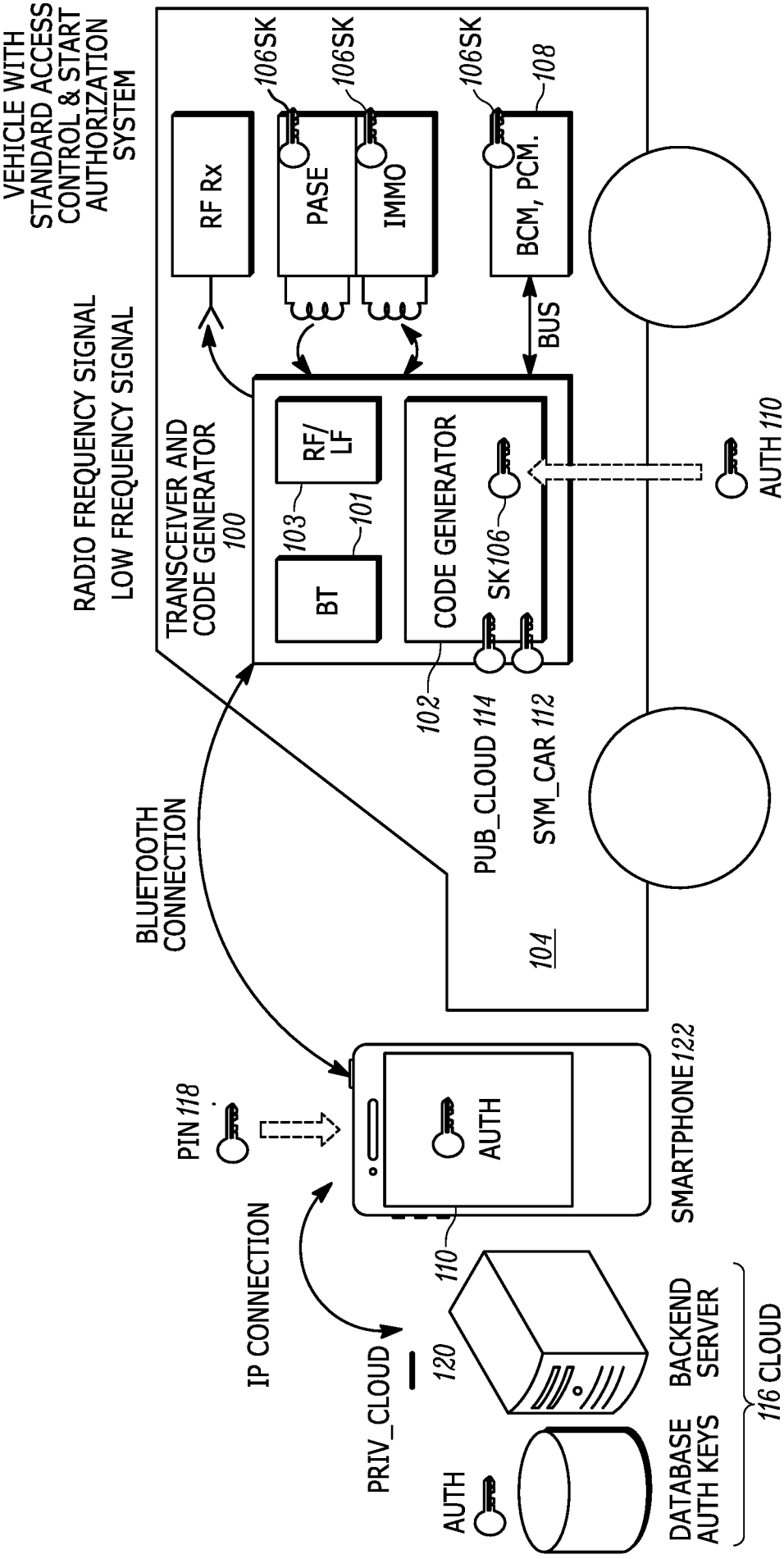
VEHICLE WITH STANDARD ACCESS CONTROL & START AUTHORIZATION SYSTEM
RADIO FREQUENCY SIGNAL
LOW FREQUENCY SIGNAL
TRANSCEIVER AND CODE GENERATOR 100
RF Rx
PASE
IMMO
BCM, PCM.
106SK
108
BUS
RF/ LF
BT
103
101
CODE GENERATOR
SK106
AUTH 110
102
PUB_CLOUD 114
SYM_CAR 112
104
BLUETOOTH CONNECTION
PIN 118
AUTH
SMARTPHONE 122
IP CONNECTION
110
PRIV_CLOUD
120
BACKEND SERVER
AUTH
DATABASE AUTH KEYS
116 CLOUD

Figure 1

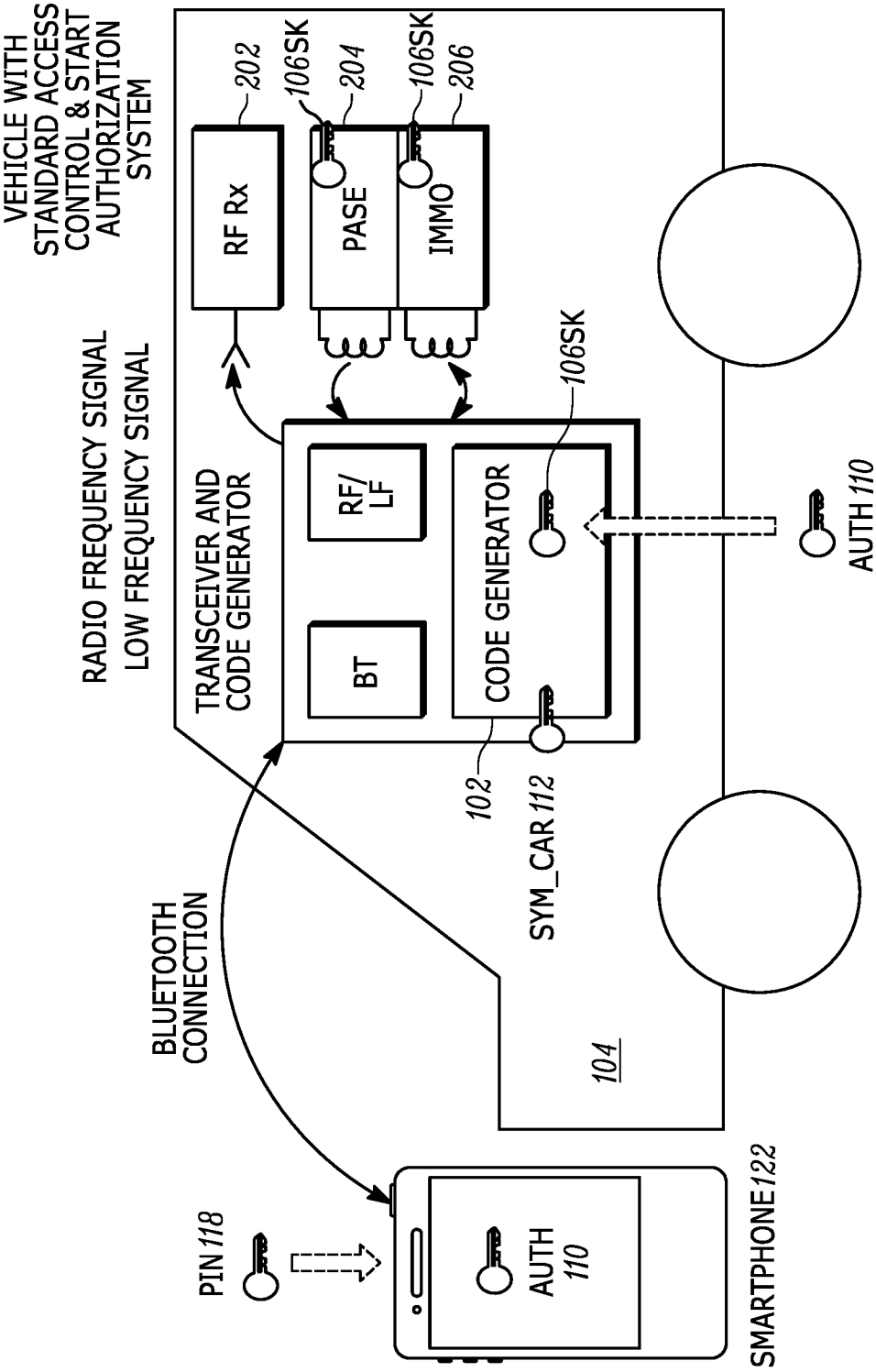
VEHICLE WITH STANDARD ACCESS CONTROL & START AUTHORIZATION SYSTEM
RADIO FREQUENCY SIGNAL
LOW FREQUENCY SIGNAL
TRANSCEIVER AND CODE GENERATOR
RF Rx
202
106SK
PASE
204
106SK
IMMO
206
RF/ LF
BT
CODE GENERATOR
106SK
AUTH 110
102
SYM_CAR 112
104
BLUETOOTH CONNECTION
PIN 118
AUTH 110
SMARTPHONE 122

Figure 2

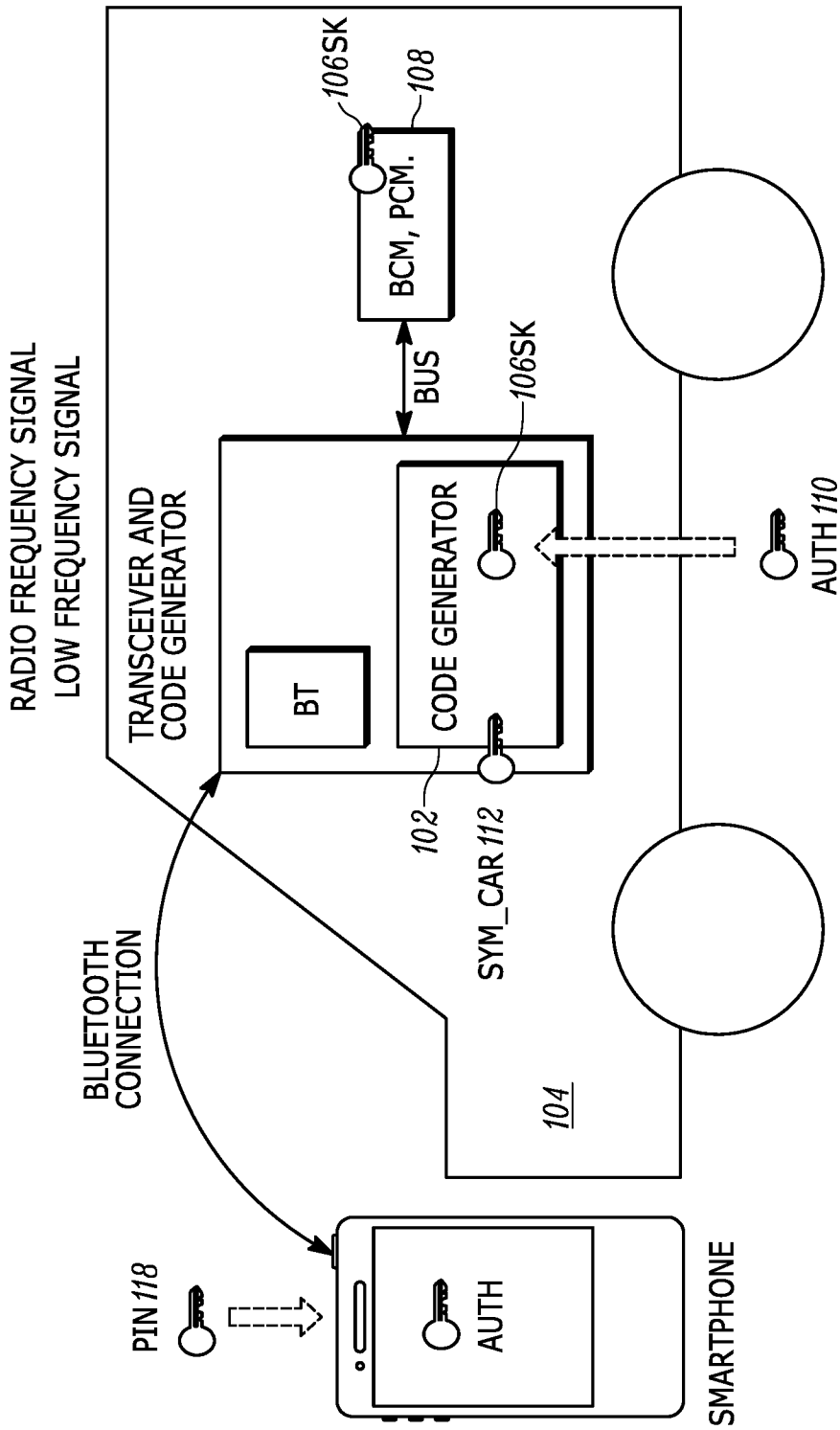
RADIO FREQUENCY SIGNAL
LOW FREQUENCY SIGNAL
TRANSCEIVER AND CODE GENERATOR
106SK
108
BCM, PCM.
BUS
106SK
BT
CODE GENERATOR
AUTH 110
102
SYM_CAR 112
104
BLUETOOTH CONNECTION
PIN 118
AUTH
SMARTPHONE

Figure 3

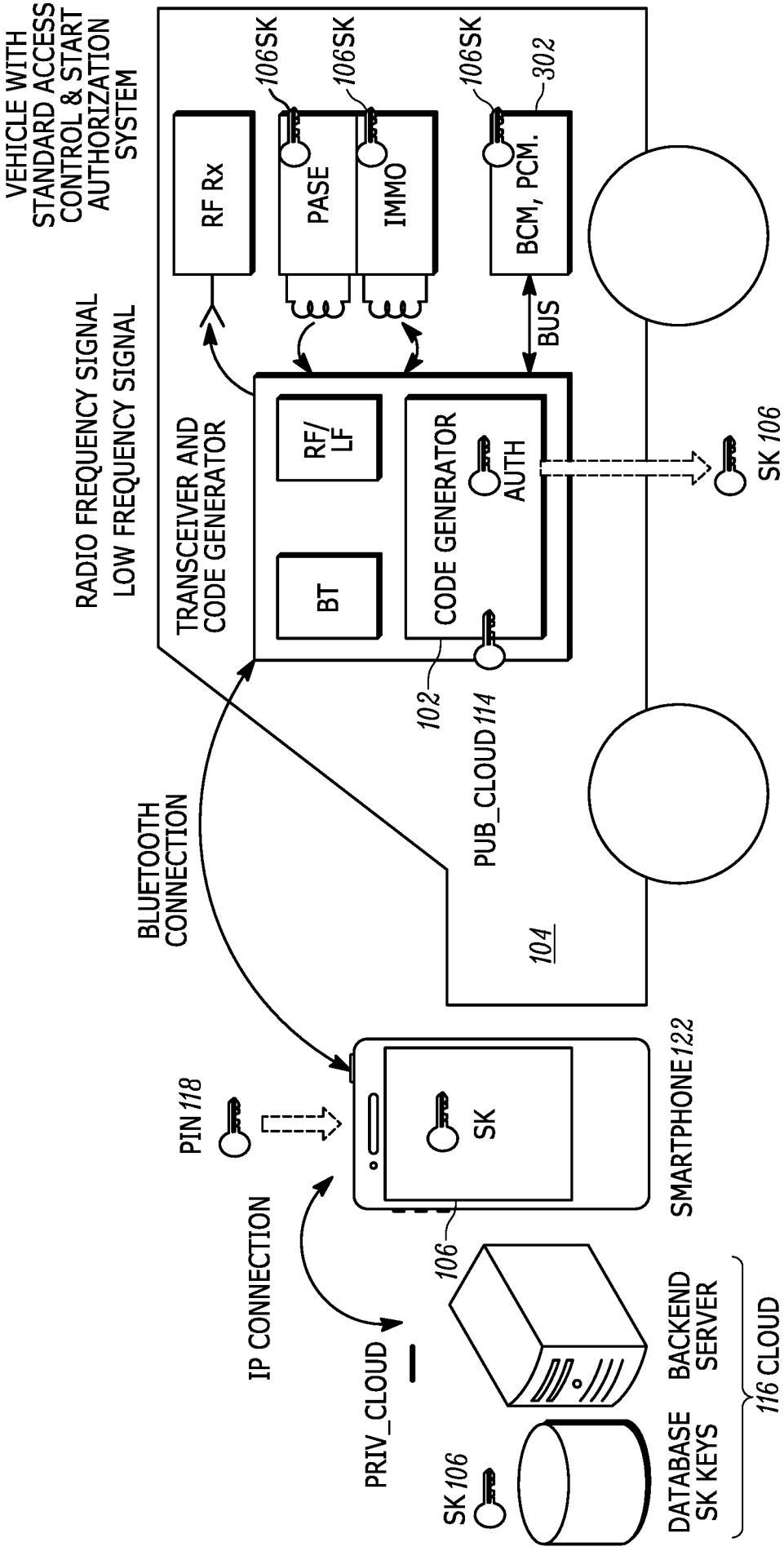
VEHICLE WITH STANDARD ACCESS CONTROL & START AUTHORIZATION SYSTEM
RADIO FREQUENCY SIGNAL
LOW FREQUENCY SIGNAL
TRANSCEIVER AND CODE GENERATOR
RF Rx
PASE
IMMO
BCM, PCM.
106SK
106SK
106SK
302
BUS
RF/ LF
BT
CODE GENERATOR
AUTH
SK 106
102
PUB_CLOUD 114
104
BLUETOOTH CONNECTION
PIN 118
SK
SMARTPHONE 122
106
IP CONNECTION
PRIV_CLOUD
BACKEND SERVER
DATABASE SK KEYS
SK 106
116 CLOUD

Figure 4

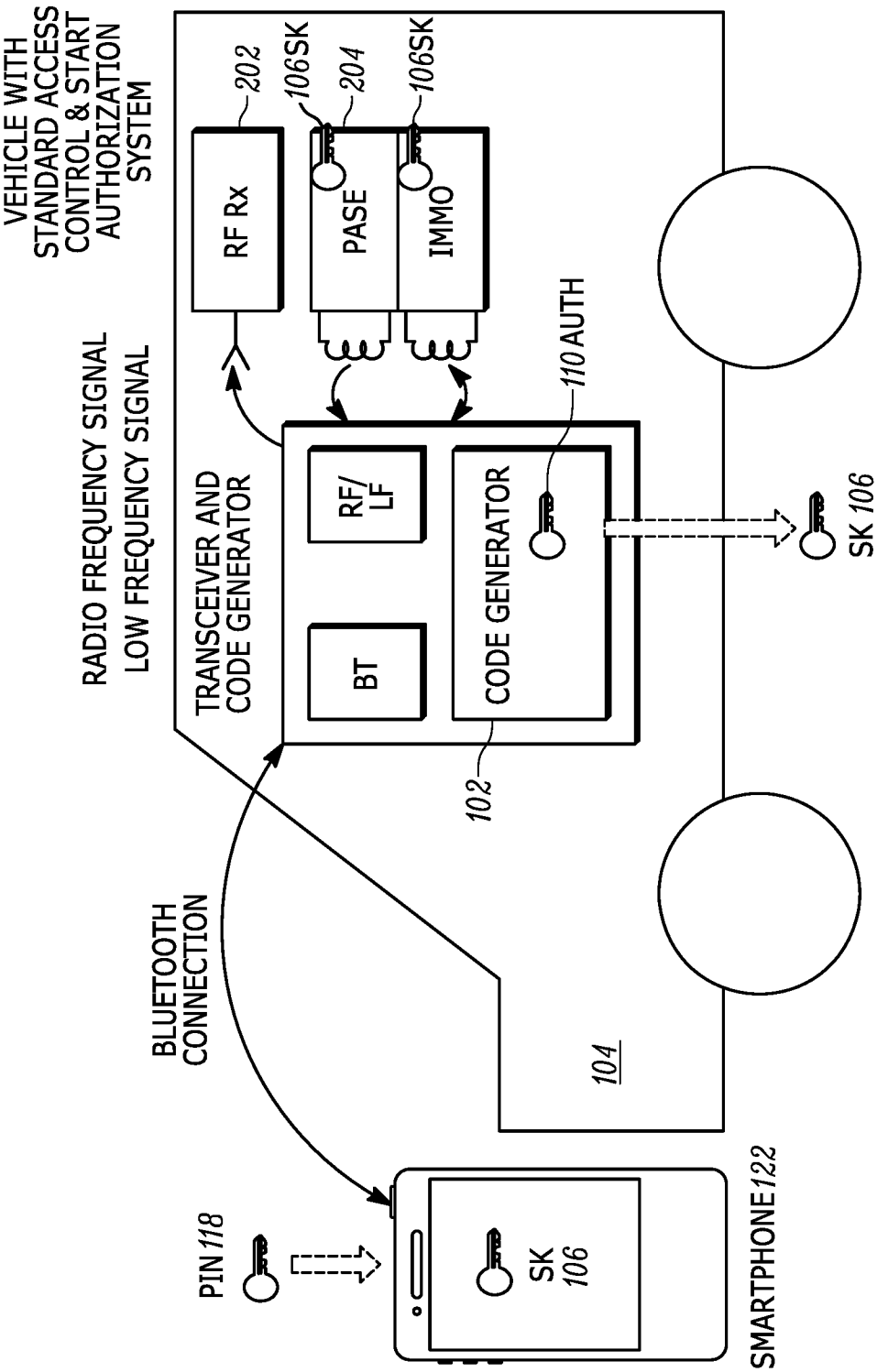
VEHICLE WITH STANDARD ACCESS CONTROL & START AUTHORIZATION SYSTEM
RADIO FREQUENCY SIGNAL
LOW FREQUENCY SIGNAL
202
106SK
204
106SK
RF Rx
PASE
IMMO
110 AUTH
TRANSCEIVER AND CODE GENERATOR
RF/ LF
BT
CODE GENERATOR
102
SK 106
BLUETOOTH CONNECTION
104
PIN 118
SK 106
SMARTPHONE 122

Figure 5

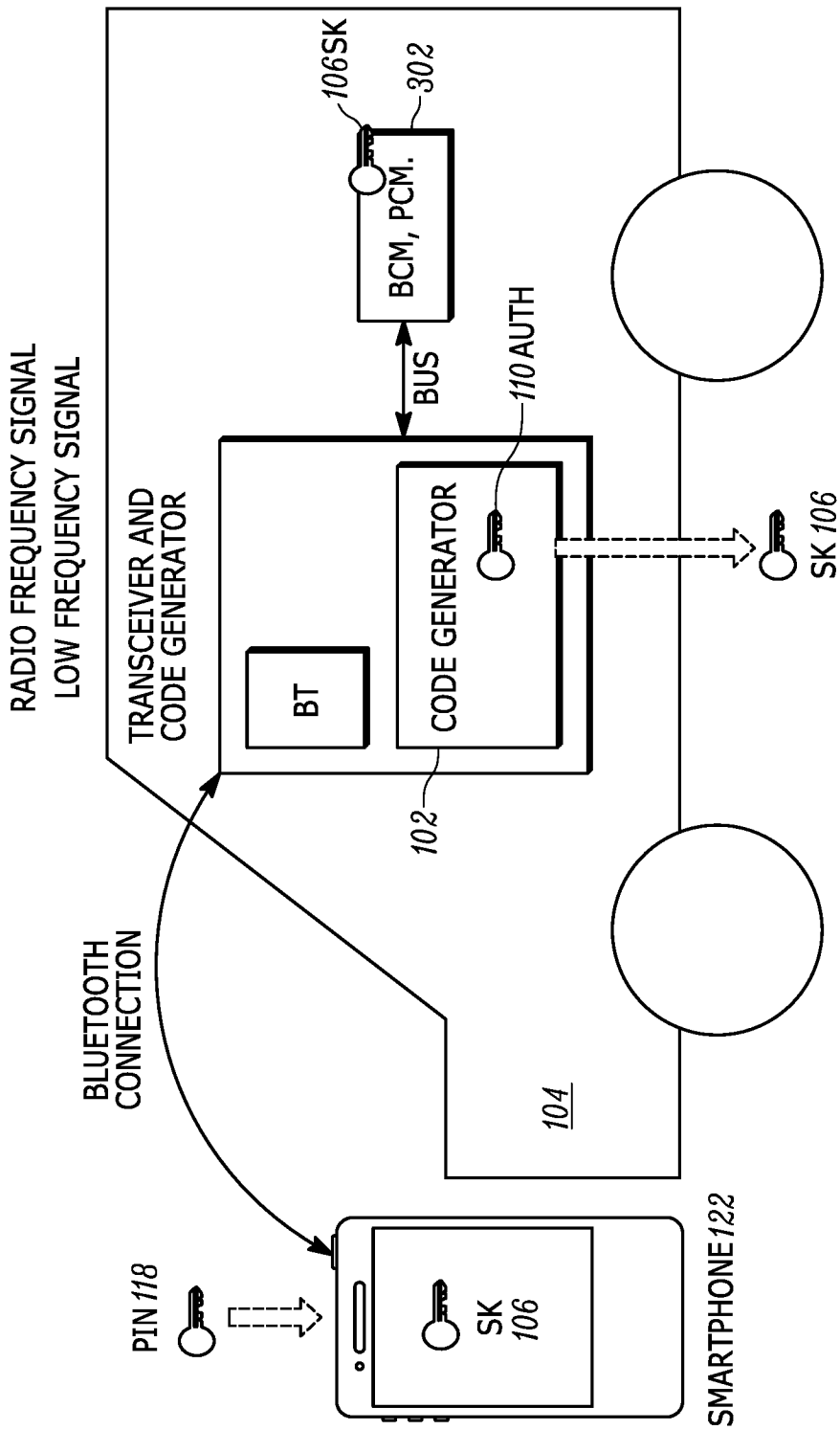
RADIO FREQUENCY SIGNAL
LOW FREQUENCY SIGNAL
TRANSCEIVER AND CODE GENERATOR
106SK
302
BCM, PCM.
BUS
110 AUTH
BT
CODE GENERATOR
102
SK 106
BLUETOOTH CONNECTION
104
PIN 118
SK 106
SMARTPHONE 122

Figure 6

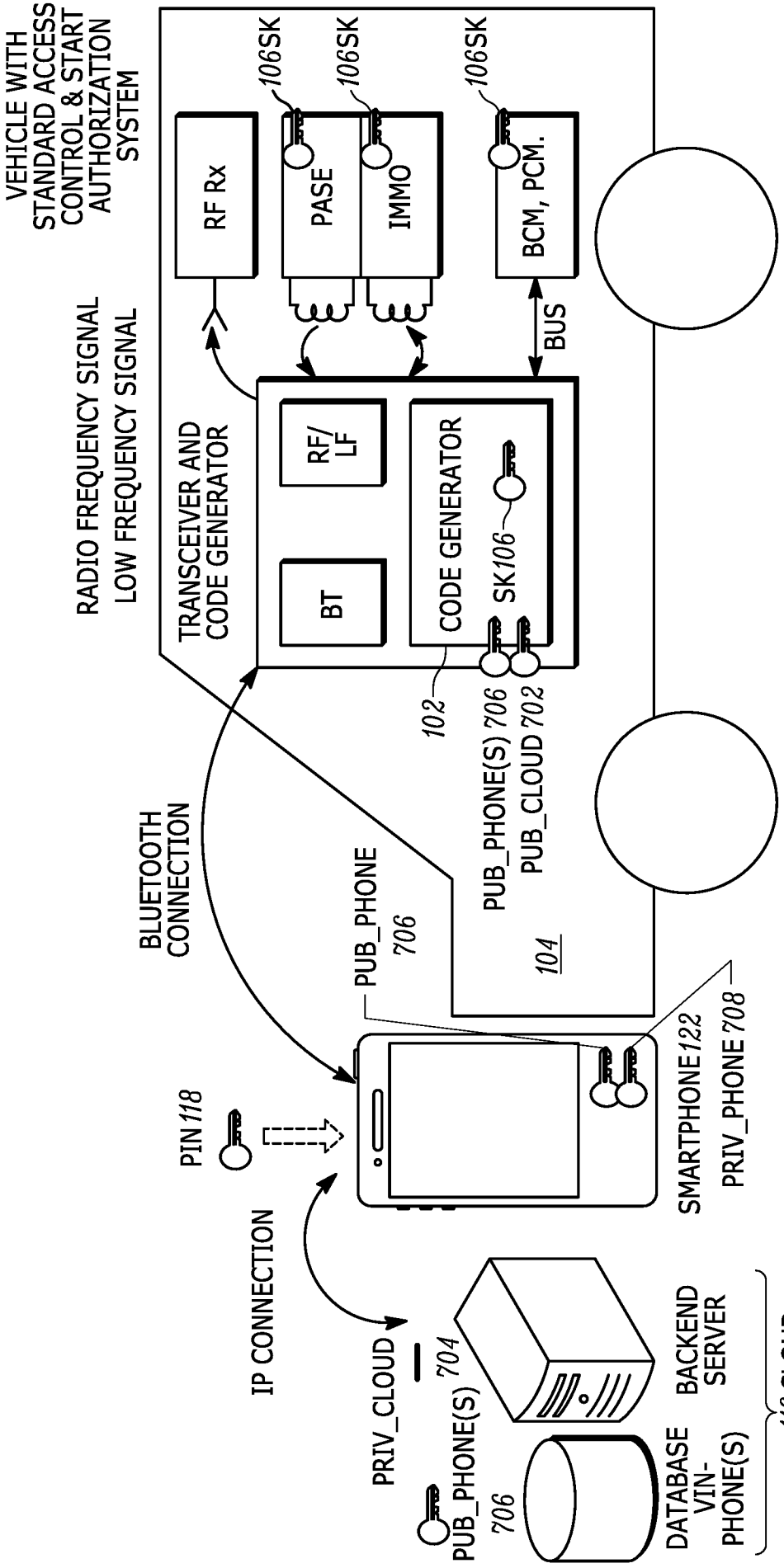
VEHICLE WITH STANDARD ACCESS CONTROL & START AUTHORIZATION SYSTEM
RADIO FREQUENCY SIGNAL
LOW FREQUENCY SIGNAL
RF Rx
106SK
PASE
106SK
IMMO
106SK
BCM, PCM.
BUS
TRANSCEIVER AND CODE GENERATOR
RF/ LF
BT
CODE GENERATOR
SK106
102
PUB_PHONE(S) 706
PUB_CLOUD 702
104
BLUETOOTH CONNECTION
PUB_PHONE 706
PIN 118
SMARTPHONE 122
PRIV_PHONE 708
IP CONNECTION
PRIV_CLOUD
PUB_PHONE(S) 706
704
BACKEND SERVER
DATABASE VIN-PHONE(S)
116 CLOUD

Figure 7

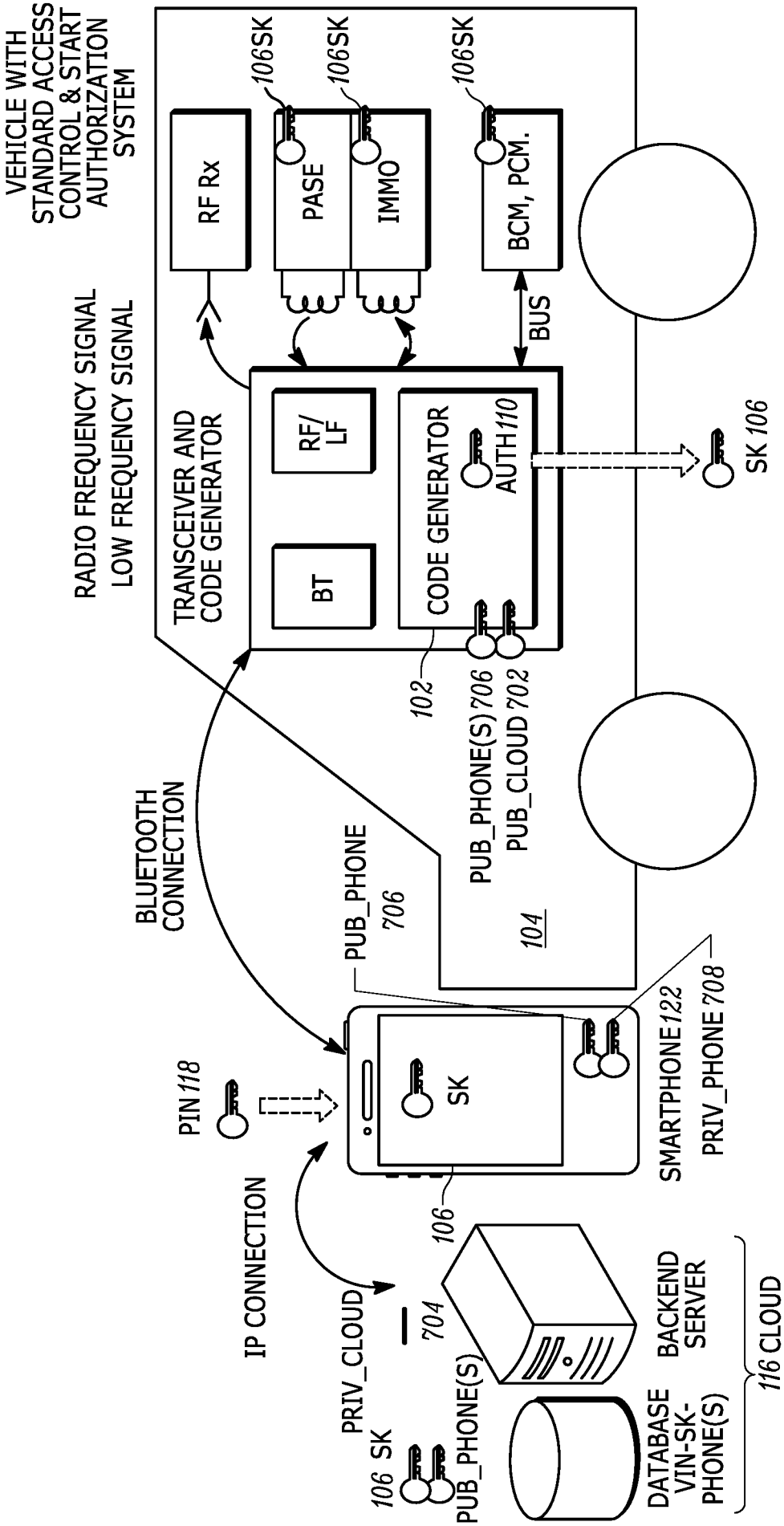
VEHICLE WITH STANDARD ACCESS CONTROL & START AUTHORIZATION SYSTEM
RADIO FREQUENCY SIGNAL
LOW FREQUENCY SIGNAL
RF Rx
106SK
PASE
106SK
IMMO
106SK
BCM, PCM.
BUS
TRANSCEIVER AND CODE GENERATOR
RF/ LF
BT
CODE GENERATOR
AUTH110
SK 106
102
PUB_PHONE(S) 706
PUB_CLOUD 702
104
BLUETOOTH CONNECTION
PUB_PHONE 706
PIN 118
SK
SMARTPHONE122
PRIV_PHONE 708
106
IP CONNECTION
PRIV_CLOUD
704
BACKEND SERVER
106 SK
PUB_PHONE(S)
DATABASE VIN-SK-PHONE(S)
116 CLOUD

Figure 8

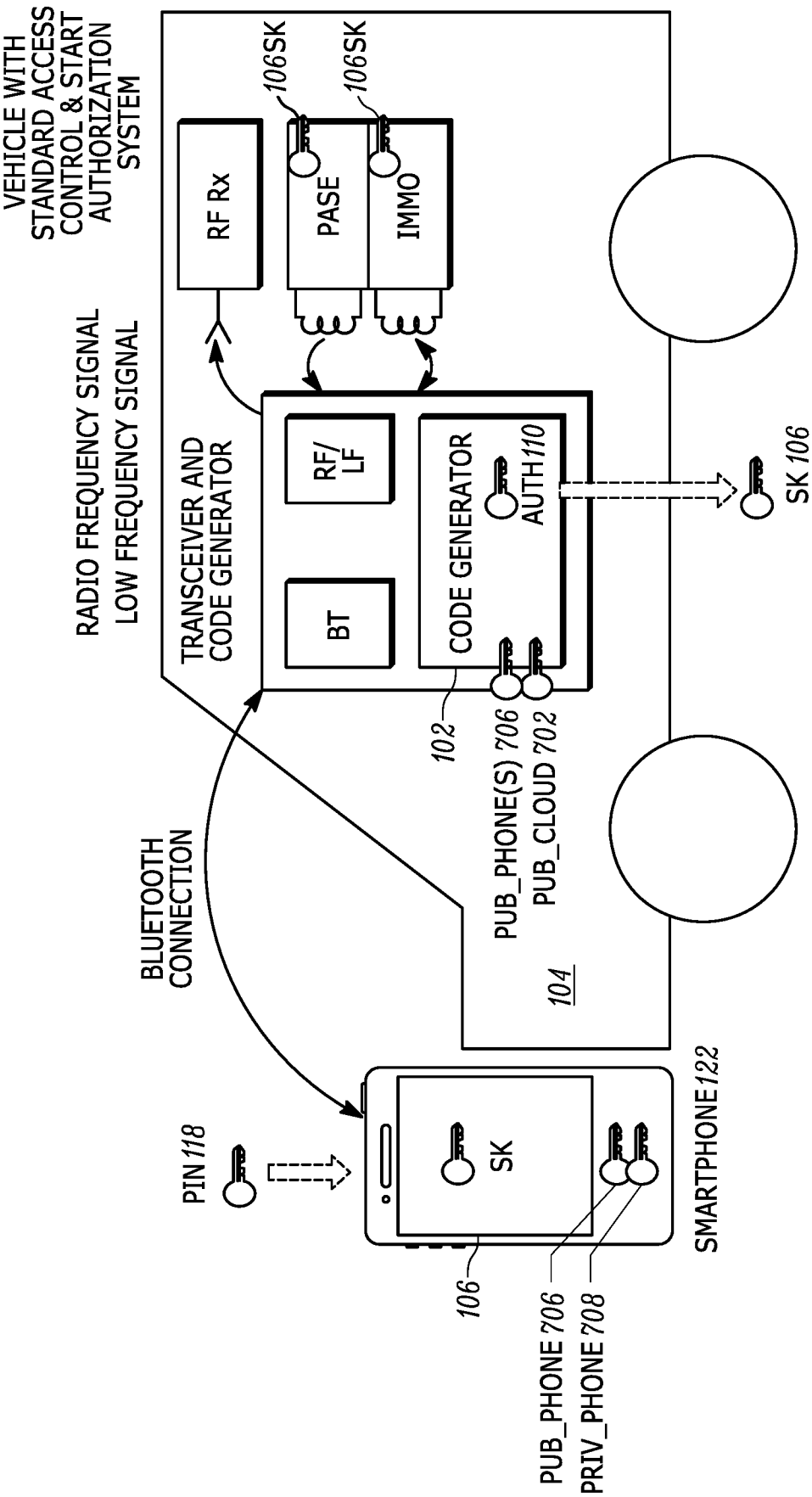
VEHICLE WITH STANDARD ACCESS CONTROL & START AUTHORIZATION SYSTEM
RADIO FREQUENCY SIGNAL
LOW FREQUENCY SIGNAL
TRANSCEIVER AND CODE GENERATOR
RF Rx
106SK
PASE
106SK
IMMO
RF/ LF
BT
CODE GENERATOR
AUTH110
SK 106
102
PUB_PHONE(S) 706
PUB_CLOUD 702
104
BLUETOOTH CONNECTION
PIN 118
SK
SMARTPHONE122
106
PUB_PHONE 706
PRIV_PHONE 708

Figure 9

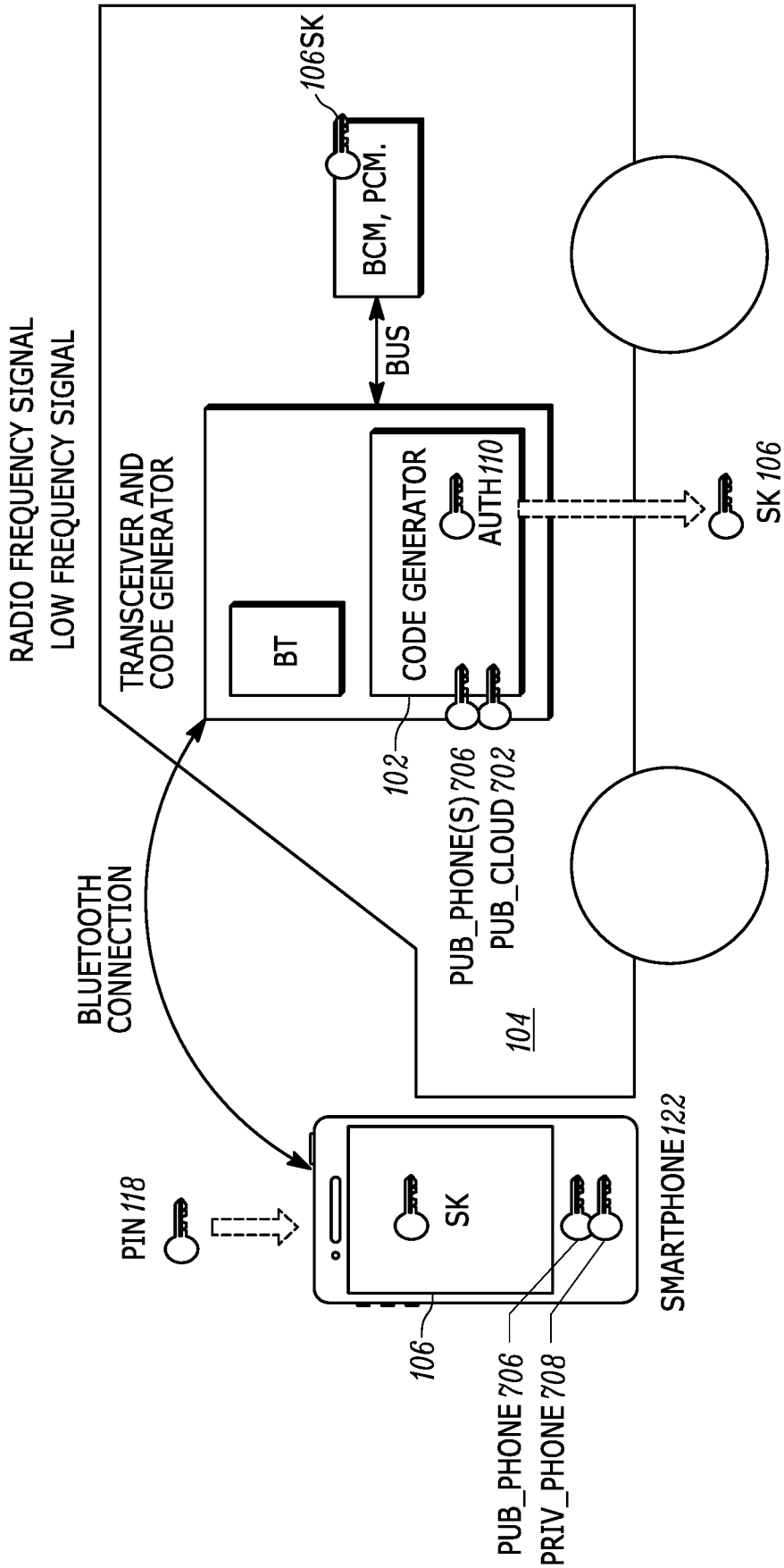
RADIO FREQUENCY SIGNAL
LOW FREQUENCY SIGNAL
TRANSCEIVER AND CODE GENERATOR
106SK
BCM, PCM.
BUS
BT
CODE GENERATOR
AUTH110
SK 106
102
PUB_PHONE(S)706
PUB_CLOUD702
104
BLUETOOTH CONNECTION
PIN118
SK
SMARTPHONE122
106
PUB_PHONE 706
PRIV_PHONE 708

Figure 10

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2017/021109

A. CLASSIFICATION OF SUBJECT MATTER
INV. B60R25/24
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
B60R G07C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2015/045013 A1 (SIMMONS MICHAEL S [US]) 12 February 2015 (2015-02-12) paragraphs [0014], [0020] - [0022]; figure 1	1
A	US 2014/169564 A1 (GAUTAMA NEERAJ R [CA] ET AL) 19 June 2014 (2014-06-19) paragraphs [0033] - [0037], [0068], [0093], [0094]	1,5
A	US 2011/112969 A1 (ZAID SAM [CA] ET AL) 12 May 2011 (2011-05-12) paragraphs [0123], [0125] - [0128]; figures 3,5	1

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 June 2017	20/06/2017

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Krieger, Philippe

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2017/021109

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2010/048244 A1 (GOREN NIR [IL]) 25 February 2010 (2010-02-25) paragraphs [0015], [0020], [0022]; figure 1	1
A	US 2013/259232 A1 (PETEL LAURENT [FR]) 3 October 2013 (2013-10-03) paragraphs [0100] - [0104], [0112] - [0114]; figures	1
A	US 2015/263860 A1 (LEBOEUF KARL B [CA] ET AL) 17 September 2015 (2015-09-17) paragraphs [0031], [0034], [0044]; figures	1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2017/021109

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2015045013 A1	12-02-2015	NONE	
US 2014169564 A1	19-06-2014	CN 103874061 A	18-06-2014
		DE 102013225742 A1	18-06-2014
		US 2014169564 A1	19-06-2014
US 2011112969 A1	12-05-2011	CN 102667655 A	12-09-2012
		CN 106515658 A	22-03-2017
		EP 2494418 A1	05-09-2012
		JP 5794997 B2	14-10-2015
		JP 2013509640 A	14-03-2013
		JP 2016007035 A	14-01-2016
		KR 20120116924 A	23-10-2012
		US 2011112969 A1	12-05-2011
		WO 2011053357 A1	05-05-2011
US 2010048244 A1	25-02-2010	BR PI0714644 A2	01-10-2013
		CA 2664063 A1	27-03-2008
		CN 101588945 A	25-11-2009
		EP 2064093 A1	03-06-2009
		RU 2009110755 A	27-10-2010
		US 2010048244 A1	25-02-2010
		WO 2008035351 A1	27-03-2008
US 2013259232 A1	03-10-2013	CN 103328278 A	25-09-2013
		EP 2621769 A1	07-08-2013
		FR 2965434 A1	30-03-2012
		JP 2013545907 A	26-12-2013
		US 2013259232 A1	03-10-2013
		WO 2012041885 A1	05-04-2012
US 2015263860 A1	17-09-2015	CN 104917745 A	16-09-2015
		DE 102015103020 A1	17-09-2015
		US 2015263860 A1	17-09-2015