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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 January 2014 (23.01.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/014934 A1

(51) International Patent Classification:
*B60R 25/20* (2013.01) *B60R 25/10* (2013.01)
*B60R 25/22* (2013.01) *E05B 65/12* (2006.01)

(21) International Application Number:
PCT/US2013/050716

(22) International Filing Date:
16 July 2013 (16.07.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

| | | |
|---|---|---|
| 61/672,463 | 17 July 2012 (17.07.2012) | US |
| 61/672,474 | 17 July 2012 (17.07.2012) | US |
| 13/942,367 | 15 July 2013 (15.07.2013) | US |


(71) Applicant: **TEXAS INSTRUMENTS INCORPORATED** [US/US]; P. O. Box 655474, Mail Station 3999, Dallas, TX 75264-5474 (US).

(71) Applicant *(for JP only)*: **TEXAS INSTRUMENTS JAPAN LIMITED** [JP/JP]; 24-1, Nishi-shinjuku 6-chome, Shinjuku-ku, 160-8366 (JP).

(72) Inventors: **HO, Jin-meng**; 7700 Cherry Creek Drive, Plano, TX 75025 (US). **PEETERS, Eric**; 9820 Crown Ridge Dr., Frisco, TX 75035 (US).

(74) Agents: **FRANZ, Warren, L.** et al.; Texas Instruments Incorporated, Deputy General Patent Counsel, P.O. Box 655474, Mail Station 3999, Dallas, TX 75265-5474 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, 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, 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, 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 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))*

WO 2014/014934 A1

(54) Title: CERTIFICATE-BASED CONTROL UNIT KEY FOB PAIRING

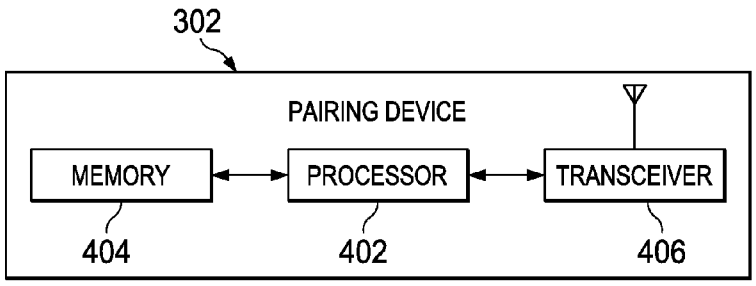


FIG. 4

(57) Abstract: A key fob-control unit pairing device (302) that includes a transceiver (406) to transmit and receive signals, a memory (404) to store a certificate of authenticity (CertVD) associated with the pairing device and a public key (PKVM), and a processor (402) coupled to the transceiver and memory. The processor (402) is configured to receive a public key (PKKF) from a key fob and associated with the key fob and a certificate of authenticity (CertKF) associated with the key fob, verify the CertKF with the PKVM, and transmit an encrypted PKKF to a control unit.

# CERTIFICATE-BASED CONTROL UNIT KEY FOB PAIRING

## BACKGROUND

**[0001]** Wireless key fobs and their respective vehicles may use encrypted operational keys to authenticate communications that occur between the two. For the key fob and the vehicle to be able to communicate, they must be paired at some point in either the manufacturing or the sales process. The pairing of wireless key fobs and their respective vehicles conventionally requires the vehicle manufacturer to deliver to the various vehicle dealers a secret key associated with each key fob where the secret key is a cryptographic key. A key fob's secret key may be then be used to associate the key fob with a vehicle, or pair the key fob and the vehicle. Multiple key fobs are typically paired with each vehicle. This step of delivering to the vehicle dealers the secret key may and the fact that each of these key fobs must store the secret key, however, open a means for theft of the secret key leading to unauthorized key fobs and potential theft.

## SUMMARY

**[0002]** The problems noted above are solved in large part by a key fob-control unit pairing device that includes a transceiver to transmit and receive signals, a memory to store a certificate of authenticity (CertVD) associated with the pairing device and a public key (PKVM), and a processor coupled to the transceiver and memory. The processor is to receive a public key (PKKF) from a key fob and associated with the key fob and a certificate of authenticity (CertKF) associated with the key fob, verify the CertKF with the PKVM, and transmit an encrypted PKKF to a control unit.

**[0003]** The solution may also involve a key fob that includes a transceiver to receive and send signals, a memory to store a public key (PKKF) and a certificate of authenticity (CertKF) associated with the key fob, and a processor coupled to the transceiver and memory. The processor is to transmit the PKKF and the CertKF to a pairing device, execute a public key agreement protocol to generate a common secret

encryption key, and receive, from a control unit, an operation key encrypted with the common secret encryption key.

**[0004]** Another solution to the above problem may be a method to pair a key fob and a control unit of a vehicle that includes reading, by a pairing device, a public encryption key (PKKF) and a certificate of authenticity (CertKF) from a key fob, verifying, by the pairing device, the CertKF using a public encryption key of a vehicle manufacturer (PKVM), transmitting, by the pairing device, a certificate of authenticity (CertVD) to a control unit, verifying, by the control unit, the CertVD using the PKVM, executing, by the pairing device and the control unit, a public key agreement to generate an encryption key DHKey1, encrypting, by the pairing device, the PKKF using the DHKey1, transmitting, by the pairing device, the encrypted PKKF to the control unit, executing, by the control unit and the key fob, a public key agreement to generate an encryption key DHKey2, encrypting, by the control unit, an operational key using the DHKey2, and transmitting, by the control unit, the encrypted operational key to the key fob.

BRIEF DESCRIPTION OF THE DRAWINGS

**[0005]** FIG. 1 shows an example vehicle manufacturing flow from sub-unit manufacturing to the vehicle dealership implementing a certificate-based authentication key fob-control unit pairing in accordance with various examples as discussed herein;

**[0006]** FIG. 2 is an example key fob and control unit pre-pairing conditioning process for certificate-based authentication in accordance with various examples as described herein;

**[0007]** FIG. 3 shows an example of an initial pairing process of a control unit and a key fob using certificate-based authentication in accordance with various embodiments as discussed herein;

**[0008]** FIGS. 4 is a block diagram of an example pairing device in accordance with various examples discussed herein;

**[0009]** FIGS. 5 is a block diagram of an example key fob in accordance with various examples discussed herein;

**[0010]** FIGS. 6 is a block diagram of an example control unit in accordance with various examples discussed herein;

**[0011]** FIG. 7 shows an example operation of a paired key fob and control unit after pairing in accordance with various examples as discussed herein;

**[0012]** FIG. 8 shows an example of an operational key change by a CU in accordance with various examples as discussed herein;

**[0013]** FIG. 9 is an example flow diagram of a method for the certificate-based authentication in accordance with various examples discussed herein; and

DETAILED DESCRIPTION OF EXAMPLE EMBODIMENTS

**[0014]** The pairing of key fobs and vehicles (e.g., automobiles, motorcycles, boats, scooters, etc.) may entail the transport and use of secure information to ensure imposter key fobs are not paired with vehicles, which may lead to theft. The full conventional process may be kept secret by vehicle manufacturers to ensure the security of their vehicles. This process, however, may require the manufacturer to develop an expensive and dedicated IT system to generate secret keys and to maintain their security. Yet, when vehicles are delivered to dealerships, the secret keys are passed along so that multiple key fobs may be paired at the final destination. The transportation of the secret keys from manufacturer to dealer may present an opportunity for the secret keys to be stolen leading to rogue and imposter key fobs.

**[0015]** In addition to vehicles, the disclosed methods may also be used to pair a key fob with any type of control unit that allows for wireless connectivity and control. For instance, the disclosed techniques and devices may be part of a garage door system, hotel entrance system, or a remote entry for a home. As such, the scope of this disclosure is not limited to control units of vehicles. The use of vehicles and the pairing of key fobs with one or all the control units of a vehicle is mainly for descriptive purposes.

**[0016]** Disclosed herein are devices and methods for pairing key fobs with vehicles that may avoid the transport of the secret information to the dealerships and that may reduce the IT requirements of the vehicle manufacturers. One method, a certificate-based authentication process, may involve the use of authenticated certificates and public/private key pairs associated with the various components and actors involved in

the pairing process. In the certificate-based approach, a pairing device may receive the public key and the certificate from an associated key fob. The pairing device may also be authenticated by a vehicle control unit and establish a secret key between the pairing device and the control unit. The pairing device may then encrypt the public key of the key fob with the secret key and transmit the encrypted public key to the control unit. The control unit may then know what key fob with which to pair. The control unit and the key fob may then generate another secret key to use between themselves, which may then be used by the control unit to encrypt an operational key. The encrypted operational key may then be communicated to the key fob so to pair the two devices.

**[0017]** The certificate-based approach to pairing a key fob to a control unit may involve all actors (manufacturers, assemblers, dealerships, etc.) to obtain a public and secret (private) encryption key, which may be used to authenticate one another in the pairing process. That may mean that each vehicle dealership (or dealer/pairing device), the vehicle manufacturer, each key fob manufactured and assembled and each control unit manufactured and installed in a vehicle to have their own associated public/secret key pairs. Once the components involved have acquired their key pairs, the public keys may be certified by a trusted third party or a certificate authority (CA). The CA may receive the public key and identification from the associated component to prove their identity. After their identity is proven, the CA may then sign the party's public key with the trusted third party's secret key. The signed public key becomes the certificate of authenticity for the requesting party. To verify the identity of a certificate, another party needs to unlock the certificate using the trusted third party's public key. The CA, for example, may be the vehicle manufacturer or a third party designated by the car manufacturer.

**[0018]** The various components – key fobs, pairing devices, and control units – may use certain public/secret keys and certificates to authenticate one another and to generate secret encryption keys to use for passing information between one another. The generation of the secret keys may use a public key agreement protocol, such as elliptical curve Diffie-Hellman (ECDH) or Elliptic Curve Cryptography (ECC). A pair of

components, such as a key fob and a control unit, may use the secret encryption key as part of the pairing process.

**[0019]** FIG. 1 shows an example vehicle manufacturing flow 100 from sub-unit manufacturing to the vehicle dealership implementing a certificate-based authentication key fob-control unit pairing in accordance with various examples as discussed herein. The flow 100 may include a key fob manufacturer 102, a key fob assembly 104 (showing tier 1 of potentially multiple tiers), a control unit (CU) manufacturer 106, a CU assembly 108 (showing tier 1 of potentially multiple tiers), a vehicle manufacturer 110, and a vehicle dealer 112. The flow 100 shows the progression of components that may eventually be paired for operation and entrance into a corresponding vehicle. Each vehicle may have multiple CUs with each CU controlling a different function, i.e., ignition, braking, entrance, trunk, etc. An individual key fob may be paired with one, a few, or all of the CUs of a corresponding vehicle. Additionally, each vehicle and various numbers of the CUs may be paired with multiple key fobs. Further, each key fob associated with a vehicle may be deactivated if lost or stolen without affecting any other key fobs associated with that same vehicle.

**[0020]** Each key fob may have a public key ($PK_{KF}$) and a secret key ($SK_{KF}$) pair assigned to it and internally stored. The $PK_{KF}/SK_{KF}$ pair may be generated for and installed in each key fob by the key fob manufacturer 102, the key fob assembly 104 or the vehicle manufacturer 110. The vehicle manufacturer 110 may choose the most trusted entity for the generation and installation of the $PK_{KF}/SK_{KF}$ pairs to ensure secrecy and security. The same goes for each control unit that is manufactured and installed in a vehicle – each will have a key pair ($PK_{CU}/SK_{CU}$) generated and installed into an associated CU by a trusted party – the CU manufacturer 106, the CU assembly 108 or the vehicle manufacturer 110.

**[0021]** In addition to the key fobs and CUs including their respective PK/SK pairs, each unit may also include a certificate of authenticity (Cert) that authenticates the component's identity. Conventionally, a Cert is a verified and signed public key where the Cert is signed by a CA. The CA may sign a Cert with its secret key. For security reasons, the vehicle manufacturer 110 may be the trusted third party so they can control the flow and validity of Certs in the manufacturing and key fob-auto pairing

process. As such, the vehicle manufacturer 110 may sign all public keys with its secret key ($SK_{VM}$) to generate a corresponding certificate. For example, a $Cert_{KF}$ will be inserted into an associated key fob. A $Cert_{CU}$ may correspond to a CU.

**[0022]** The vehicle dealer 112 may also obtain a key pair ($PK_{VD}$ and $SK_{VD}$) in order to be verified in the key fob-CU pairing process. The vehicle dealer 112's key pair (and an associated $Cert_{VD}$ also signed by the vehicle manufacturer 110) may be associated with a dealer pairing device or simply a pairing device. For simplicity of discussion, the key fob-auto pairing will be described as occurring at the vehicle dealer 112, but the pairing may also occur at the vehicle manufacturer 110 without straying from the bounds of the disclosure.

**[0023]** Before any key fob-CU pairing may commence, some conditioning steps may take place at the various manufacturing and/or assembly locations. The conditioning may be performed to prime the separate components – key fobs, CUs, dealership (pairing device) – so that the pairing functions as intended. However, the conditioning and pairing steps may be done serially. If, for example, as is described herein, the pairing is performed at the vehicle dealer 112, then the conditioning may occur at the vehicle manufacturer 110.

**[0024]** FIG. 2 is an example key fob and control unit pre-pairing conditioning process 200 for certificate-based authentication in accordance with various examples as described herein. The conditioning process 200 may involve the vehicle manufacturer 110, the vehicle dealer 112, a CU 202 and a key fob 204. The steps of the conditioning process 200 are shown in a certain order but changes to the order are within the scope of the disclosure. The order shown is for illustrative purposes only. The goal of the conditioning process 200 may be to condition or prime the respective components to facilitate the initial pairing of a key fob and a CU, which may occur at the vehicle manufacturer 110's location or at a vehicle dealership 112.

**[0025]** The conditioning process 200 may begin at step 1a with the vehicle dealer 112 generating their encryption key pair – $PK_{VD}$ and $SK_{VD}$ – as discussed above. The dealer 112 may then transmit its $PK_{VD}$ in an authentic way to the vehicle manufacturer 110. Transmitting in an authentic way may ensure the vehicle dealer 112's identity to the vehicle manufacturer 110 and the authentic transmission may be physically

mailing the $PK_{VD}$ or delivering the $PK_{VD}$ by a courier or some other form of verified transmission. Upon receipt of the $PK_{VD}$, the vehicle manufacturer 110 may then certify the $PK_{VD}$ by signing the $PK_{VD}$ with the vehicle manufacturer 110's secret key, $SK_{VM}$, generating a certificate of authenticity ($Cert_{VD}$) for the vehicle dealer 112. The vehicle manufacturer 110 then sends the $Cert_{VD}$ back to the dealer 112, which may be inserted into the dealer's associated pairing device.

**[0026]** The conditioning process 200 may also include the vehicle manufacturer 110 inserting its public key, $PK_{VM}$, into each vehicle's CU(s) 202 and also into each key fob 204. The $PK_{VM}$ inserted into the key fob 204 and the CU 202 may be used at a later time to verify the authenticity/identity of another device since all certificates of authenticity should be signed by the vehicle manufacturer 110, which can be verified using the $PK_{VM}$.

**[0027]** Lastly, as part of the conditioning process 200, the dealer 112 may read each key fob 204's $PK_{KF}$, which is not secret. The dealer may receive numerous key fobs 204 at a time and may decide to read all of their associated public keys at once to store in the pairing device. Alternatively, the dealer 112 may read the $PK_{KF}$ of a single key fob as part of the initial pairing process, to be described below.

**[0028]** FIG. 3 shows an example of an initial pairing process 300 of a control unit and a key fob using certificate-based authentication in accordance with various embodiments as discussed herein. The initial pairing process 300 may be performed at a vehicle manufacturer's location or at a vehicle dealership as shown. The initial pairing process 300 may include the vehicle manufacturer 110, a pairing device 302 associated with a vehicle dealer 112, the key fob 204 and the CU 202. The pairing device 302 may already contain the $PK_{VM}$, both may be used to verify the identities of the other components – the CU 202 and the key fob 204. The pairing device 302 may be in communication with the key fob 204 and the control unit 202 via a wireless connection, such as with Bluetooth, ultra-high frequency (UHF), or low frequency (LF), or they may be connected via a wire. Wireless and wired connections between the components are in the scope of this disclosure. Additionally or alternatively, the pairing device 302 may communicate wirelessly with one component, the key fob 204 for

instance, and communicate via a wire with another component, the CU 202 for instance.

**[0029]** Further, the pairing device 302 may be a handheld device, a fixed terminal, or a secure computer in a secure location of either the vehicle dealer 112 or the vehicle manufacturer 110 depending on where the pairing process is to occur. In either embodiment, the pairing device 302 may have a secure communication channel with the vehicle manufacturer 110. The secure communication channel may be a permanent connection or may be periodically established, nightly for example, to update lists and receive secure communications.

**[0030]** The initial pairing process 300 may begin by the pairing device 302 receiving from the key fob 204 the $PK_{KF}$ and the $Cert_{KF}$ associated with the key fob, step 1a. The information may be sent to the pairing device 302 from the key fob 204 as a result of a request sent by the pairing device 302. Alternatively, the key fob 204 may be periodically broadcasting its $PK_{KF}$ and $Cert_{KF}$. The pairing device 302 may then verify the identity of the key fob 204 by verifying the authenticity of the Cert KF, step 1b. The $Cert_{KF}$ may be verified by the pairing device using the stored $PK_{VM}$. The verification of the $Cert_{KF}$ may be performed by hashing the $Cert_{KF}$ with the $PK_{VM}$.

**[0031]** If the pairing device 302 is unable to verify the $Cert_{KF}$, the key fob 204 associated with that $Cert_{KF}$ may be deemed a rogue and further pairing steps halted. Additionally or alternatively, the pairing device 302 may verify that the received $Cert_{KF}$ is not on a certificate revocation list (CRL) maintained by the vehicle manufacturer 110, step 1c. This verification step may ensure that a specific $Cert_{KF}$ has not been used numerous times before, which may signal a fraudulent key fob. The CRL may be stored in the memory of the pairing device 302 and periodically updated or the pairing device 302 may have constant access to the CRL maintained on a server at the vehicle manufacturer 110.

**[0032]** The pairing device 302, before, after or simultaneously with verifying the key fob 204, may begin communications with the CU 202 so that the CU 202 may verify the identity of the pairing device 302. The pairing device 302, step 2a, sends its $Cert_{VD}$ to the CU 202. The CU 202, using the $PK_{VM}$, verifies the authenticity of the $Cert_{VD}$. Additionally or alternatively, the CU 202 may verify that the $Cert_{VD}$ is not on a CRL,

also maintained by the vehicle manufacturer 110. The CU 202 may use a wireless access point at the vehicle dealer 112 to access the internet and a server at the vehicle manufacturer 110 to determine if the $Cert_{VD}$ is on the revoke list, for example.

**[0033]** If the $Cert_{VD}$ is unverifiable or is on the CRL, then the CU 202 may determine the pairing device 302 and/or the dealer 112 is fraudulent. If deemed fraudulent, the CU 202 may cease communicating with the pairing device 302 and may alert the vehicle manufacturer 110.

**[0034]** If the CU 202 is able to verify the pairing device 302, then, step 3a, both the CU 202 and the pairing device 302 execute a key agreement protocol to generate a common secret key, DHKey1, which may only be known by the pairing device 302 and the CU 202. After generation of the DHKey1, the pairing device 302 may encrypt the $PK_{KF}$ of the key fob 202 and transmit the encrypted $PK_{KF}$ to the CU 202. Since the CU 202 knows the DHKey1 and can decrypt the message revealing the $PK_{KF}$, the CU 202 knows what key fob 204 with which to communicate and pair.

**[0035]** The CU 202 may initiate communication with the key fob 202, direct via wirelessly or through the pairing device 302. Once a communication link is established between the key fob 204 and the CU 202, the two components 202, 204, step 4a, may execute a key agreement protocol to generate a common secret key, DHKey2, known only by the CU 202 and the key fob 204. The CU 204, step 4b, may then generate an operational key (OpKey), encrypt the OpKey using DHKey2, and transmit the encrypted OpKey to the key fob 204. The OpKey may be a randomly generated 128-bit number.

**[0036]** The key fob 204 may then decrypt the message to learn the OpKey. At this point, the key fob 204 and the CU 202 may be deemed paired and normal operation may commence. The key fob 204 and the CU 202 may use the OpKey to authenticate one another in normal operation based on any standard private or public key authentication techniques, e.g. ISO 9798-2.

**[0037]** Pairing key fobs and control units may also be performed using identification (ID)-based authentication approach. The ID-based approach may use unique identification words associated with key fobs and CUs that may be used to both authenticate one another and to generate secret keys between the devices. The

secret keys would then be used to encrypt and decrypt information sent between the two components. The pairing of the key fob and the CU, again, may be facilitated by a pairing device located at either the vehicle dealership or at the vehicle manufacturer and which may be similar to the pairing device 302.

**[0038]** FIGS. 4, 5, and 6 show block diagrams of an example pairing device 302, key fob 204 and CU 202, respectively, in accordance with various examples discussed herein. The three devices/components – pairing device, key fob, and CU – may all comprise a processor (402, 502, 602), a memory (404, 504, 604), and a transceiver (406, 506, 606). The processors of the three devices/components may be used to perform the authentication computations and the common secret key generation computations associated with the certificate-based authentication pairing and the ID-based authentication pairing. The processors may be a standard CPU, a microcontroller, a low-power digital signal processor, etc. and may be capable of performing complex calculations in a short time.

**[0039]** The memories of the three devices may be used to store the public and private key pairs and the certificates of authenticity associated with their respective device for the certificate-based authentication pairing. Alternatively or additionally, the memories of the three devices may be used to store the IDs of their own or the other devices. For example, in the ID-based authentication pairing, the pairing device 302 may store both the KFID and the CUID before initiating a paring sequence. The KFID and CUID for those two associated devices may be stored in the memory 404 of the pairing device 302. The memories may be a non-volatile storage device such as flash memory or an EEPROM.

**[0040]** The transceivers for the three devices may be wired (not shown), wireless or capable of both. The transceivers may be used by the devices to communicate the IDs, public keys, and/or certificates of authenticity during the condition steps and the initial pairing steps for either authentication approach. The key fobs allowing for remote entry and control of vehicles may use a wireless technology such as Bluetooth, LF, or UHF for those transmissions but may also be able to communicate with the pairing device and/or the CUs via a wire during the initial pairing process.

**[0041]** Additionally, the pairing device 302 may include a wired connection to the vehicle manufacturer 110 so that the pairing device 302 may securely receive the CUIDs of the CUs 202 delivered to the dealer 112 for the ID-based authentication pairing. For the certificate-based authentication pairing the pairing device 302 may communicate with the vehicle manufacturer 110 when accessing a certification revoke list. Additionally, the CU 202 either via the pairing device 302 or some other connection may also access a CRL at the vehicle manufacturer 110 when checking the validity of the CertVD of the pairing device 302.

**[0042]** FIG. 7 shows an example normal operation of a paired key fob and CU in accordance with various examples as discussed herein. The normal operation depicted in FIG. 9 shows the interaction between a key fob 204 and a CU 202 post initial pairing by the process 300 (certificate-based). The key fob and CU, when communicating with one another upon a user's interaction with the key fob for example, may first authenticate one another by executing an OpKey authenticated challenge-response protocol based on AES-128, for example. Operation of the CU by the key fob may only be allowed when the response is valid. An invalid response may signify a rogue key fob and the CU may not perform commands sent from an invalid key fob.

**[0043]** FIG. 8 shows an example of an OpKey change by a CU in accordance with various examples as discussed herein. The CU 202 may change the OpKey when a key fob 206 is misplaced or is stolen. By changing the OpKey, the CU may prevent the missing or stolen key fob 206 from accessing the CU 202. The CU 202 may be initiated by an external signal that a new OpKey is desired. The external signal may come from the owner of the remaining key fob(s) 204 by performing a preset sequence with the key fob and vehicle or the external signal may come from the pairing device 302 of the dealer 112. Upon receiving the external signal, the CU 202 may encrypt a new OpKey using the old OpKey and then transmit the encrypted new OpKey to the remaining key fob(s) 204. After receiving the new OpKey, the old OpKey may be erased by all the CU 202 and the remaining key fobs 204. Normal operation between the devices may then continue without worry that the rogue key fob may interact with the CU.

**[0044]** FIG. 9 is a flow diagram of an example method 900 for the certificate-based authentication in accordance with various examples discussed herein. The method 900A may be one implementation of the initial pairing process 300 described in regards to FIG. 3. The method 900 begins at step 902 with the pairing device 302 reading a public encryption key ($PK_{KF}$) and a certificate of authenticity ($Cert_{KF}$) from the key fob 204. The method 900 continues at step 904 with the pairing device 302 verifying the $Cert_{KF}$ using a public encryption key ($PK_{VM}$) of the vehicle manufacturer 110. Step 906 continues the method 900 with the pairing device 302 transmitting the certificate of authenticity ($Cert_{VD}$) to the CU 202. The CU 202 at step 908 verifies the $Cert_{VD}$ using the $PK_{VM}$, which may be stored in the memory 804 of the CU 202. At step 910, the pairing device 302 and the CU 202 execute a public key agreement protocol to generate a common secret encryption key DHKey1, which may only be known by the pairing device and the CU.

**[0045]** The method 900 then continues at step 912 with the pairing device 302 encrypting the $PK_{KF}$ using the DHKey1 before the method 900 performs step 914 with the pairing device 302 transmitting the encrypted $PK_{KF}$ to the control unit 202. At step 916, the CU 202 and the key fob 204 execute a public key agreement protocol to generate a common secret encryption key DHKey2 to be shared between the CU 202 and the key fob 204. The method 900 ends with steps 918 and 920 with the CU 202 encrypting an operational key (OpKey) with DHKey2 and then transmitting the encrypted OpKey to the key fob 204. After the OpKey has been shared with the key fob 204, the CU 202 and the key fob 204 may be considered paired.

**[0046]** Those skilled in the art will appreciate that modifications may be made to the described embodiments, and also that many other embodiments are possible, within the scope of the claimed invention.

CLAIMS

What is claimed is:

1. A method to pair a key fob and a control unit of a vehicle, comprising:

reading, by a pairing device, a public encryption key (PKKF) and a certificate of authenticity (CertKF) from a key fob;

verifying, by the pairing device, the CertKF using a public encryption key of a vehicle manufacturer (PKVM);

transmitting, by the pairing device, a certificate of authenticity (CertVD) to a control unit;

verifying, by the control unit, the CertVD using the PKVM;

executing, by the pairing device and the control unit, a public key agreement to generate an encryption key DHKey1;

encrypting, by the pairing device, the PKKF using the DHKey1;

transmitting, by the pairing device, the encrypted PKKF to the control unit;

executing, by the control unit and the key fob, a public key agreement to generate an encryption key DHKey2;

encrypting, by the control unit, an operational key using the DHKey2; and

transmitting, by the control unit, the encrypted operational key to the key fob.

2. The method of claim 1, further comprising:

generating the $PK_{KF}$ for the key fob and inserting the $PK_{KF}$ into a storage device of the key fob;

generating the PKVM and a secret (SKVM) encryption key pair for the vehicle manufacturer and storing them in a vehicle manufacturer storage device; and

generating a public (PKVD) encryption key for a vehicle dealer and storing them in a vehicle dealer storage device.

3. The method of claim 1, further comprising:

generating a certificate of authenticity for the PKKF (CertKF) and PKVD (CertVD) by signing the respective public keys with the SKVM;

inserting the PKVM into a control unit storage device, into the key fob storage device, and into a storage device of the pairing device; and

inserting the CertKF into the key fob storage device and the CertVD into the pairing device storage device.

4. The method of claim 1, further comprising verifying, by the pairing device, that the CertKF is not on a certificate revocation list (CRL).

5. The method of claim 1, further comprising verifying, by the control unit, that the CertVD is not on a CRL.

6. A key fob-control unit pairing device, comprising:

a transceiver configured to transmit and receive signals;

a memory configured to store a certificate of authenticity (CertVD) associated with the pairing device and a public key (PKVM); and

a processor coupled to the transceiver and memory and configured to:

receive a public key (PKKF) from a key fob and associated with the key fob and a certificate of authenticity (CertKF) associated with the key fob;

verify the CertKF with the PKVM; and

transmit an encrypted PKKF to a control unit.

7. The device of claim 6, wherein the processor is configured to verify that the CertKF is not on a certificate revocation list.

8. The device of claim 6, wherein the processor, via the transceiver, is configured to transmit the CertVD of the pairing device to the control unit.

9. The device of claim 6, wherein the processor and the control unit is configured to co-execute a key agreement protocol to generate a common secret encryption key that is shared between the processor and the control unit.

10. The device of claim 9, wherein the processor is configured to encrypt the PKKF with the common secret encryption key.

11. The device of claim 9, wherein the key agreement protocol is based on elliptical curve Diffie-Hellman (ECDH) encryption.

12. The device of claim 9, wherein the key agreement protocol is based on elliptical curve cryptography (ECC).

13. The device of claim 6, wherein PKVM and the CertVM are associated with a certificate authority.

14. The device of claim 13, wherein the certificate authority is a vehicle manufacturer.

15. A key fob, comprising:

a transceiver configured to receive and send signals;

a memory configured to store a public key (PKKF) and a certificate of authenticity (CertKF) associated with the key fob; and

a processor coupled to the transceiver and memory and configured to:

transmit the PKKF and the CertKF to a pairing device;

execute a public key agreement protocol to generate a common secret encryption key; and

receive, from a control unit, an operation key encrypted with the common secret encryption key.

16. The key fob of claim 15, wherein the public key agreement protocol is based on elliptical curve Diffie-Hellman (ECDH) encryption.

17. The device of claim 15, wherein the key agreement protocol is based on elliptical curve cryptography (ECC).

18. The key fob of claim 15, wherein the processor is to decrypt the operation key with the common secret encryption key.

19. The key fob of claim 15, wherein the CertKF is signed by a certificate authority.

20. The key fob of claim 19, wherein the certificate authority is a vehicle manufacturer.

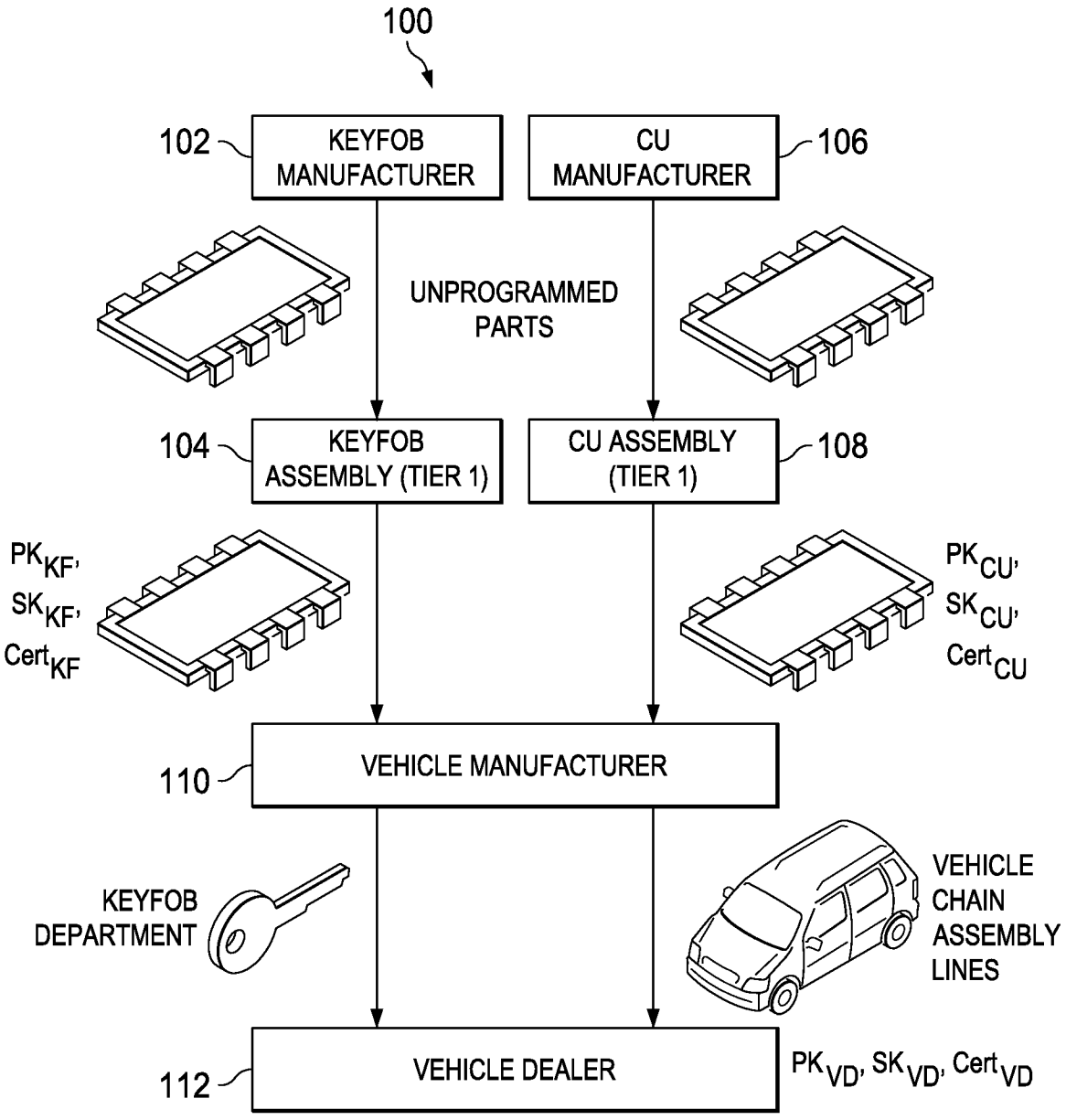
100
102
KEYFOB MANUFACTURER
CU MANUFACTURER
106
UNPROGRAMMED PARTS
104
KEYFOB ASSEMBLY (TIER 1)
CU ASSEMBLY (TIER 1)
108
PK_KF, SK_KF, Cert_KF
PK_CU, SK_CU, Cert_CU
110
VEHICLE MANUFACTURER
KEYFOB DEPARTMENT
VEHICLE CHAIN ASSEMBLY LINES
112
VEHICLE DEALER
PK_VD, SK_VD, Cert_VD

FIG. 1

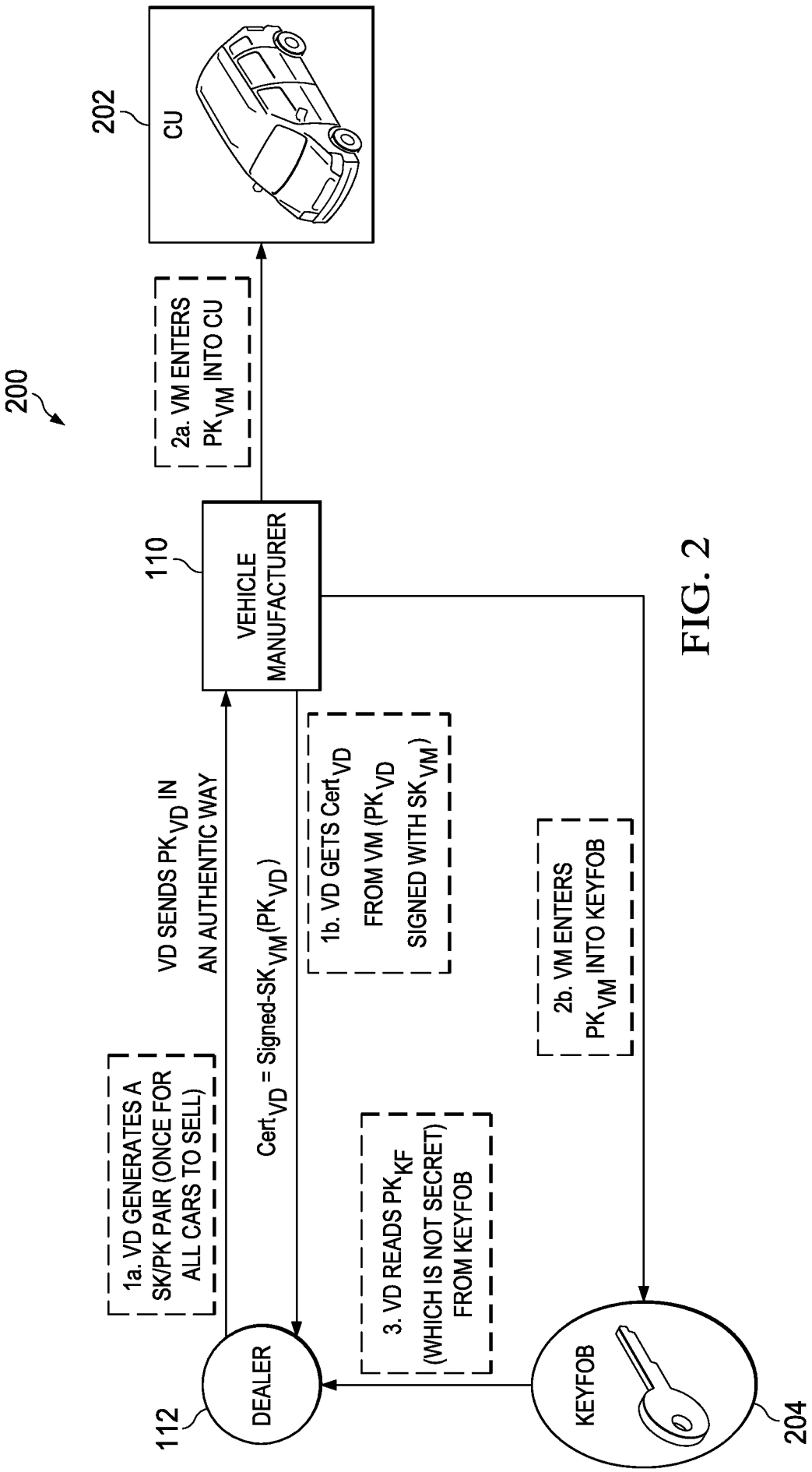
200
202
CU
2a. VM ENTERS $PK_{VM}$ INTO CU
110
VEHICLE MANUFACTURER
VD SENDS $PK_{VD}$ IN AN AUTHENTIC WAY
$Cert_{VD}$ = Signed-$SK_{VM}$($PK_{VD}$)
1b. VD GETS $Cert_{VD}$ FROM VM ($PK_{VD}$ SIGNED WITH $SK_{VM}$)
1a. VD GENERATES A SK/PK PAIR (ONCE FOR ALL CARS TO SELL)
2b. VM ENTERS $PK_{VM}$ INTO KEYFOB
3. VD READS $PK_{KF}$ (WHICH IS NOT SECRET) FROM KEYFOB
DEALER
112
KEYFOB
204

FIG. 2

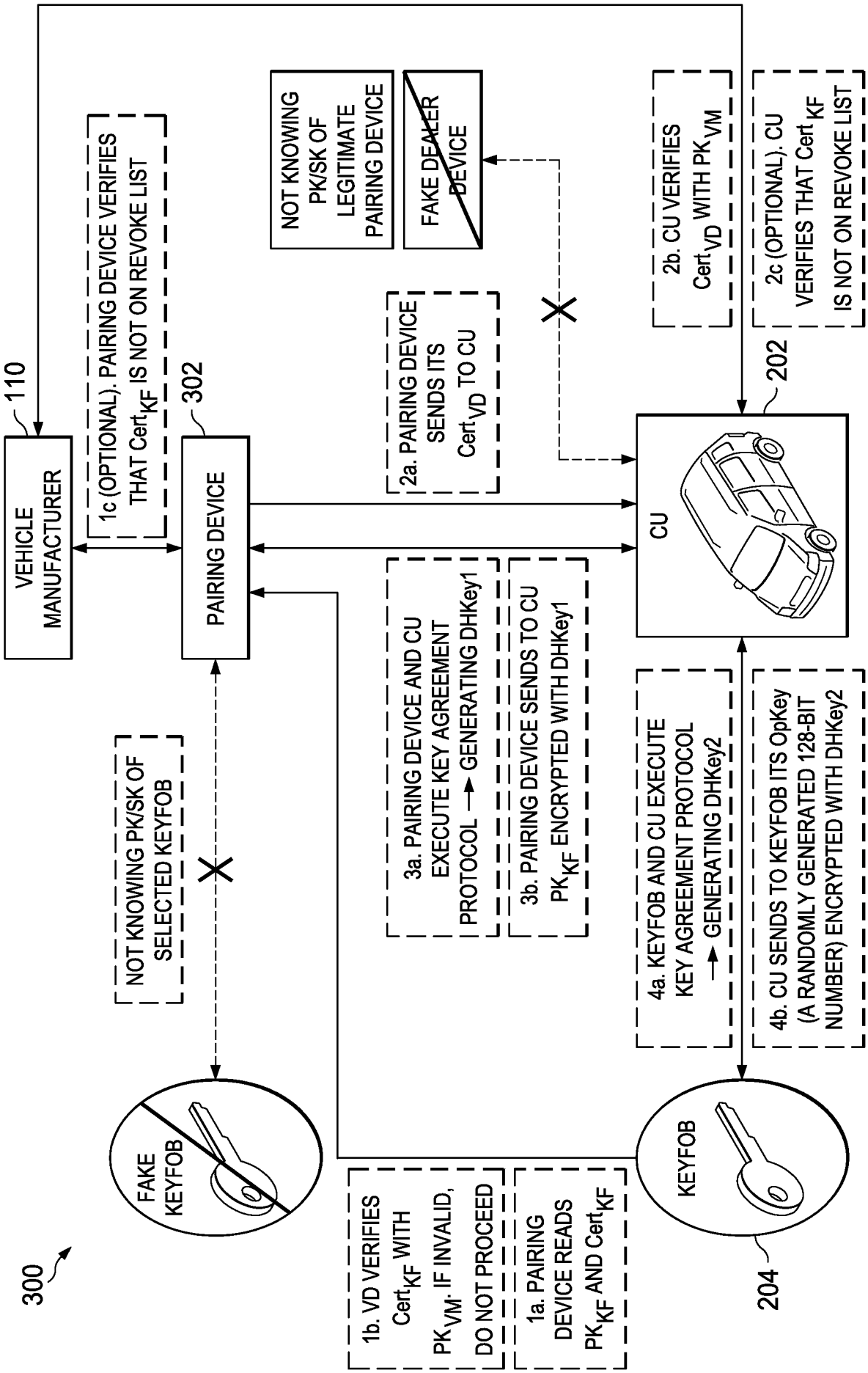
300
VEHICLE MANUFACTURER
110
PAIRING DEVICE
302
CU
202
FAKE KEYFOB
KEYFOB
204
1c (OPTIONAL). PAIRING DEVICE VERIFIES THAT Cert$_{KF}$ IS NOT ON REVOKE LIST
NOT KNOWING PK/SK OF LEGITIMATE PAIRING DEVICE
FAKE DEALER DEVICE
2a. PAIRING DEVICE SENDS ITS Cert$_{VD}$ TO CU
2b. CU VERIFIES Cert$_{VD}$ WITH PK$_{VM}$
2c (OPTIONAL). CU VERIFIES THAT Cert$_{KF}$ IS NOT ON REVOKE LIST
NOT KNOWING PK/SK OF SELECTED KEYFOB
3a. PAIRING DEVICE AND CU EXECUTE KEY AGREEMENT PROTOCOL → GENERATING DHKey1
3b. PAIRING DEVICE SENDS TO CU PK$_{KF}$ ENCRYPTED WITH DHKey1
4a. KEYFOB AND CU EXECUTE KEY AGREEMENT PROTOCOL → GENERATING DHKey2
4b. CU SENDS TO KEYFOB ITS OpKey (A RANDOMLY GENERATED 128-BIT NUMBER) ENCRYPTED WITH DHKey2
1b. VD VERIFIES Cert$_{KF}$ WITH PK$_{VM}$. IF INVALID, DO NOT PROCEED
1a. PAIRING DEVICE READS PK$_{KF}$ AND Cert$_{KF}$

FIG. 3

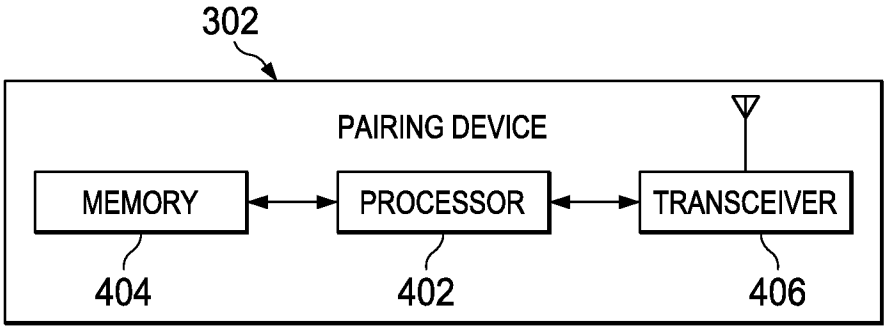


FIG. 4

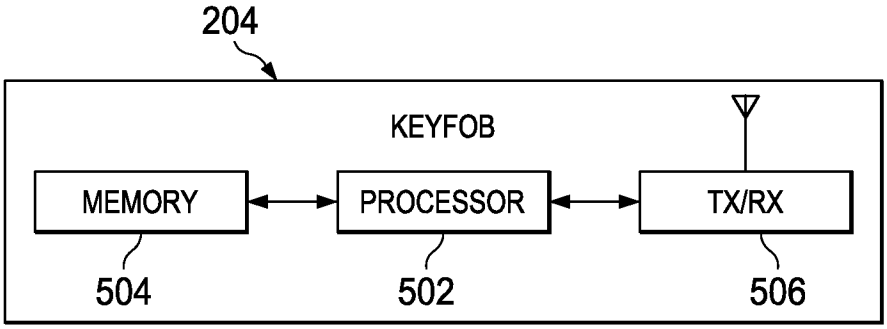


FIG. 5

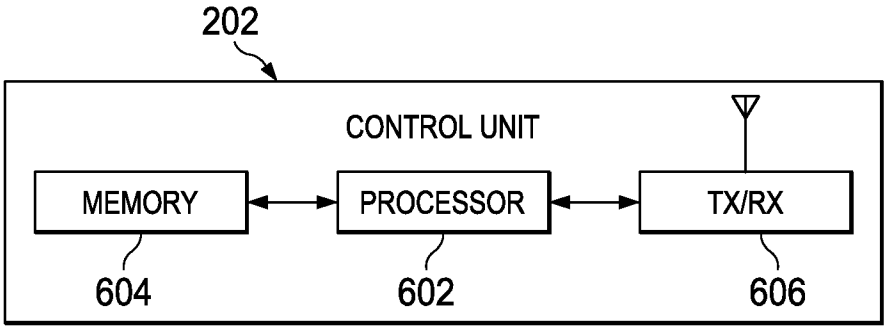


FIG. 6

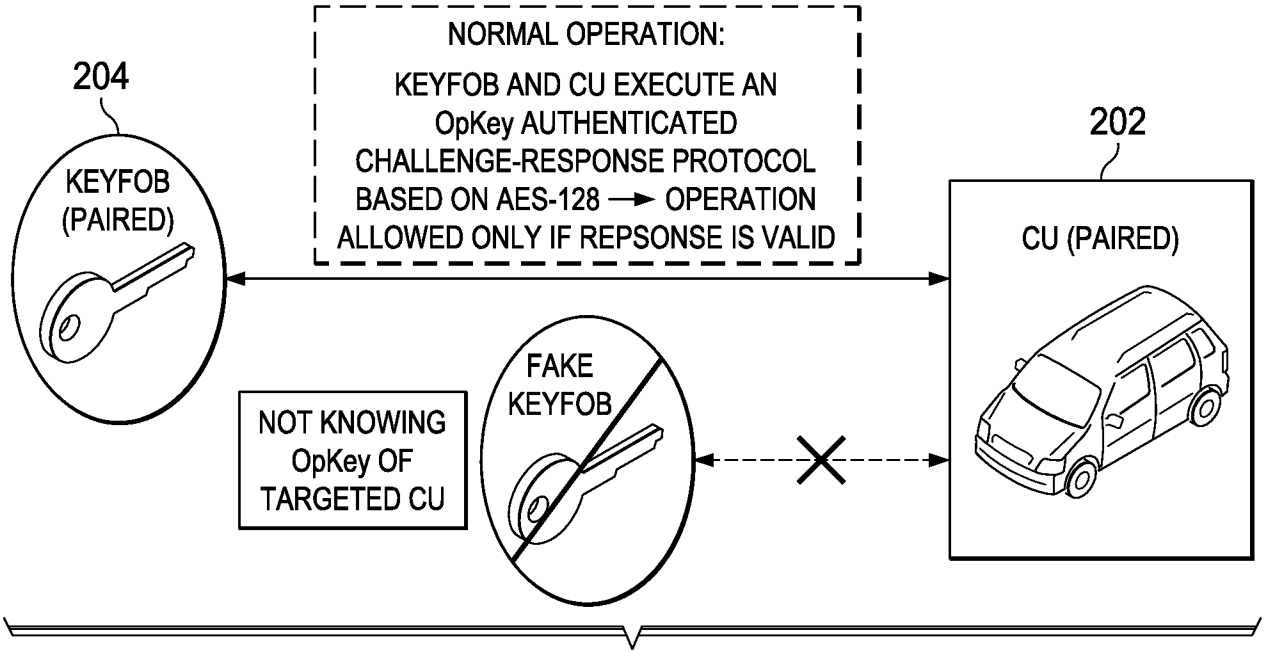
NORMAL OPERATION:
KEYFOB AND CU EXECUTE AN OpKey AUTHENTICATED CHALLENGE-RESPONSE PROTOCOL BASED ON AES-128 → OPERATION ALLOWED ONLY IF REPSONSE IS VALID
204
KEYFOB (PAIRED)
202
CU (PAIRED)
FAKE KEYFOB
NOT KNOWING OpKey OF TARGETED CU

FIG. 7

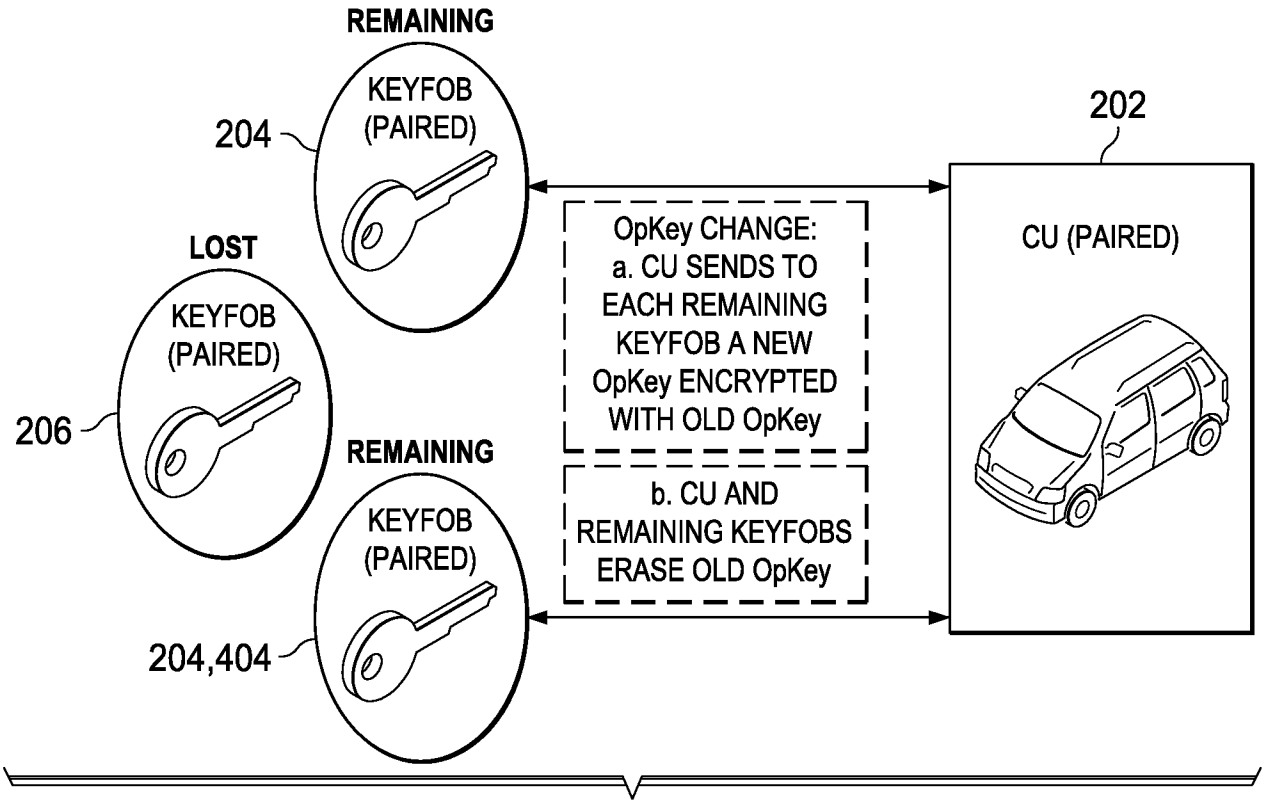
REMAINING
KEYFOB (PAIRED)
204
202
CU (PAIRED)
LOST
KEYFOB (PAIRED)
206
OpKey CHANGE:
a. CU SENDS TO EACH REMAINING KEYFOB A NEW OpKey ENCRYPTED WITH OLD OpKey
REMAINING
KEYFOB (PAIRED)
b. CU AND REMAINING KEYFOBS ERASE OLD OpKey
204,404

FIG. 8

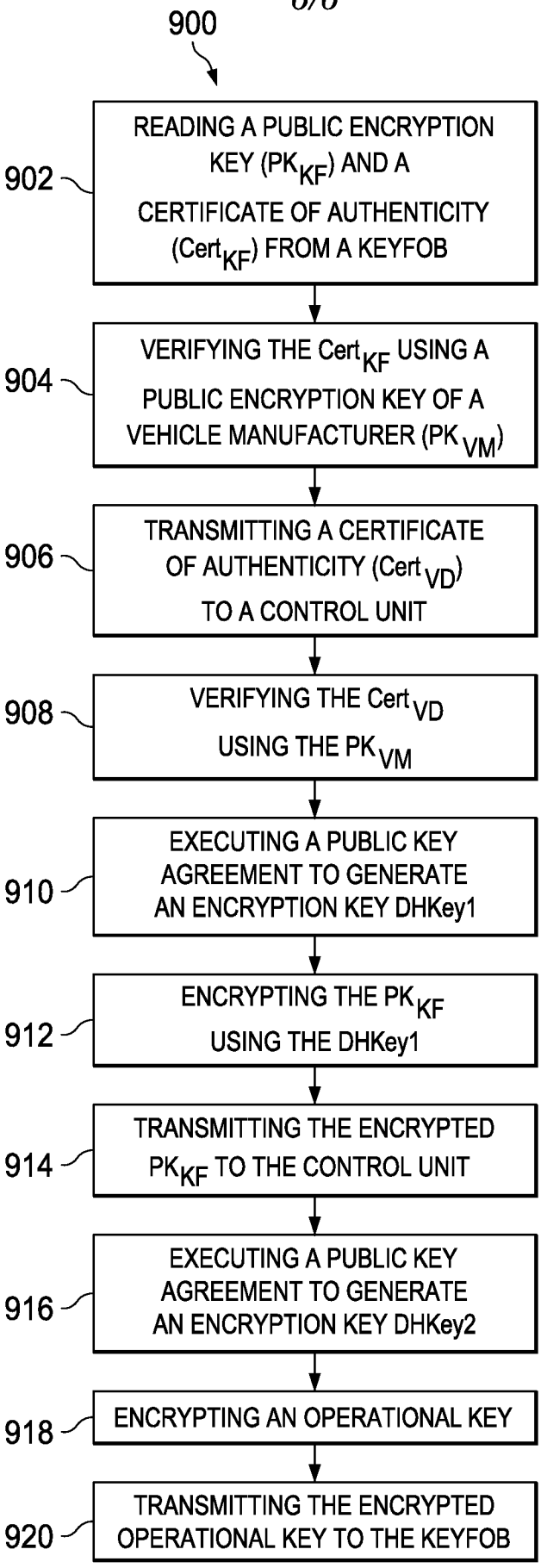
900
902
READING A PUBLIC ENCRYPTION KEY ($PK_{KF}$) AND A CERTIFICATE OF AUTHENTICITY ($Cert_{KF}$) FROM A KEYFOB
904
VERIFYING THE $Cert_{KF}$ USING A PUBLIC ENCRYPTION KEY OF A VEHICLE MANUFACTURER ($PK_{VM}$)
906
TRANSMITTING A CERTIFICATE OF AUTHENTICITY ($Cert_{VD}$) TO A CONTROL UNIT
908
VERIFYING THE $Cert_{VD}$ USING THE $PK_{VM}$
910
EXECUTING A PUBLIC KEY AGREEMENT TO GENERATE AN ENCRYPTION KEY DHKey1
912
ENCRYPTING THE $PK_{KF}$ USING THE DHKey1
914
TRANSMITTING THE ENCRYPTED $PK_{KF}$ TO THE CONTROL UNIT
916
EXECUTING A PUBLIC KEY AGREEMENT TO GENERATE AN ENCRYPTION KEY DHKey2
918
ENCRYPTING AN OPERATIONAL KEY
920
TRANSMITTING THE ENCRYPTED OPERATIONAL KEY TO THE KEYFOB

FIG. 9

**INTERNATIONAL SEARCH REPORT**

International application No.
**PCT/US2013/050716**

**A. CLASSIFICATION OF SUBJECT MATTER**

**B60R 25/20(2013.01)i, B60R 25/22(2013.01)i, B60R 25/10(2006.01)i, E05B 65/12(2006.01)i**

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 25/20; H04L 9/08; E05B 49/00; B60R 25/04; B60R 25/10; H04L 9/32; H04W 4/00; H04Q 9/00; H04B 1/38; B60R 25/22; E05B 65/12

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords: vehicle, key, pairing, and transceiver

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| Y | JP 2009-278506 A (PANASONIC CORP.) 26 November 2009<br>See paragraphs [0020]-[0023],[0025]; figure 1. | 6,8,13,14 |
| A | | 1-5,7,9-12,15-20 |
| Y | US 2012-0030467 A1 (SCHAEFER, MARK S.) 02 February 2012<br>See paragraphs [0027]-[0032],[0053],[0054]; figures 2-4. | 6,8,13,14 |
| A | US 2012-0115446 A1 (GAUTAMA et al.) 10 May 2012<br>See paragraphs [0017]-[0019]; figure 1. | 1-20 |
| A | US 7437183 B2 (MAKINEN, RAUNO) 14 October 2008<br>See column 5, line 35-column 6, line 14, column 8, lines 25-41; figures 1, 3. | 1-20 |
| A | WO 2004-085213 A1 (THOMPSON, MILTON) 07 October 2004<br>See page 11, lines 2-13, page 13, line 26-page 14, line 21; figure 1(b). | 1-20 |

☐ Further documents are listed in the continuation of Box C.

☒ 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 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 |
|---|---|
| 11 October 2013 (11.10.2013) | **14 October 2013 (14.10.2013)** |


Name and mailing address of the ISA/KR
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea
Facsimile No. +82-42-472-7140

Authorized officer
SONG Ho Keun
Telephone No. +82-42-481-5580

**INTERNATIONAL SEARCH REPORT**

Information on patent family members

International application No.
**PCT/US2013/050716**

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| JP 2009-278506 A | 26/11/2009 | None | |
| US 2012-0030467 A1 | 02/02/2012 | None | |
| US 2012-0115446 A1 | 10/05/2012 | CN 102572151 A | 11/07/2012 |
| | | DE 102011117499 A1 | 16/05/2012 |
| | | US 8326259 B2 | 04/12/2012 |
| US 7437183 B2 | 14/10/2008 | AT 391057 T | 15/04/2008 |
| | | DE 60225872 D1 | 15/05/2008 |
| | | DE 60225872 T2 | 09/04/2009 |
| | | EP 1270348 A2 | 02/01/2003 |
| | | EP 1270348 A3 | 10/03/2004 |
| | | EP 1270348 B1 | 02/04/2008 |
| | | FI 111494 B1 | 31/07/2003 |
| | | FI 20011415 A | 30/12/2002 |
| | | US 2003-0003892 A1 | 02/01/2003 |
| WO 2004-085213 A1 | 07/10/2004 | CN 1764562 A | 26/04/2006 |
| | | EP 1606149 A1 | 21/12/2005 |
| | | JP 2006-523572 A | 19/10/2006 |
| | | US 2006-0273885 A1 | 07/12/2006 |