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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 April 2019 (11.04.2019)

WIPO | PCT

(10) International Publication Number
WO 2019/069129 A1

(51) International Patent Classification:
H04W 4/40 (2018.01) *G08C 17/02* (2006.01)
B60R 25/102 (2013.01) *H04W 12/06* (2009.01)
B60R 25/20 (2013.01)

(21) International Application Number:
PCT/IB2018/001213

(22) International Filing Date:
03 October 2018 (03.10.2018)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/568,242 04 October 2017 (04.10.2017) US

(71) Applicant: **KEYFREE TECHNOLOGIES INC.** [CA/CA]; 37 Advance Road, Suite 100, Toronto, ON M8Z 2S6 (CA).

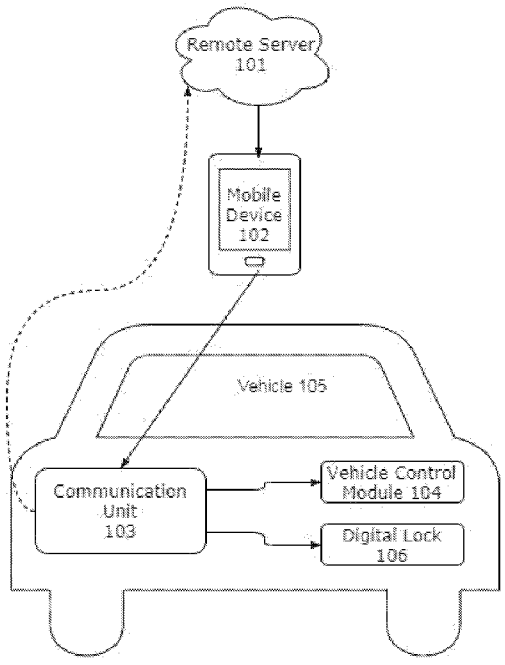
(72) Inventors: **WRIGHT, Shane, Adrian**; 100 Dunedin Drive, Toronto, Ontario, M8X 2K5 (CA). **SMITH, Cameron, Kenneth**; 3085 Swansea Drive, Oakville, ON L6L 6H7 (CA). **KESHWANI, Rahim, Fateali**; 70 Greendale Crescent, Kitchener, ON N2A 2R6 (CA). **LOCKHART, Daniel, Freeman**; 18b-50 Howe Drive, Kitchener, ON N2E 0A3 (CA). **SITEK, David**; 319 Bushview Circle, Waterloo, ON N2V 2A6 (CA).

(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, JO, 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).

(54) Title: METHODS AND DEVICES FOR MANAGING ACCESS TO A VEHICLE

FIG. 1



(57) Abstract: Described are mobile device based systems and methods for granting authorization to control a vehicle and allow a user to open and start the vehicle by a mobile device, which are currently carried by a vast majority of vehicle owners, and which allows a user to grant access to vehicle to others without physical device transference. Some embodiments of the mobile device bases systems are able to function when the mobile device does or does not have access to a wireless or cellular data.

WO 2019/069129 A1

[Continued on next page]

Declarations under Rule 4.17:

— *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))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

METHODS AND DEVICES FOR MANAGING ACCESS TO A VEHICLE

CROSS-REFERENCE

[0001] This application claims the benefit of U.S. Provisional Application No. 62/568,242, filed October 4, 2017, which application is incorporated herein by reference.

BACKGROUND OF THE INVENTION

[0002] In recent years, the usage of conventional keys in the automotive industry has diminished as new methods for enabling access to vehicles are being developed. Typical vehicle keys may be easily lost, misplaced, and forgotten, and are costly and burdensome to replace.

[0003] Many currently available vehicles have been configured for remote keyless entry, wherein the vehicle is capable of being wirelessly opened by a keyfob, but requires a key, that is usually attached to the keyfob, to start the vehicle. Additionally, many passive entry/start systems such as push-to start cars can be opened and started by a keyfob, as long as the vehicle detects that a keyfob is within, or within a set distance from, the vehicle. These systems, however, still require a user to carry a keyfob at all times, and do not allow a user to grant access to others without physically relinquishing the keyfob. As such, there is a current unmet need for a secure vehicle system capable of being opened and started by a mobile device, which are currently carried by a vast majority of vehicle owners, which allows a user to grant access to vehicle to others without physical device transference.

SUMMARY OF THE INVENTION

[0004] A first aspect provided herein is a mobile device based system for granting authorization to control a vehicle comprising: a communication unit; a vehicle control module that is separate and distinct from the communication unit; and a mobile device capable of receiving a user input and a first signal, and sending a second signal, wherein the mobile device comprises at least one mobile application including executable instructions to control the vehicle, wherein the executable instructions comprise: receiving the first signal from an internet, a cellular network, a server, or any combination thereof; storing the first signal; receiving the user input; and sending the second signal to the communication unit in response to receiving the user input; wherein the first and second signals both comprise a common unique identifier; wherein the communication unit is capable of receiving the second signal from the mobile device and sending a third signal to the vehicle control module; and wherein the vehicle control module is capable of receiving the third signal and sending a command to a receiver within the vehicle.

[0005] In some embodiments, the mobile device is capable of performing the executable instruction of sending the second signal to the communication unit without access to the internet, the cellular network, or the server. In some embodiments, the mobile device is capable of receiving and storing the first signal before receiving the user input. In some embodiments, the communication unit is capable of receiving the second signal from a variety of mobile devices. In some embodiments, the communication unit is capable of sending the third signal to a variety of vehicle control modules. In some embodiments, the vehicle control module is capable of functionally communicating with both the communication unit and the receiver. In some embodiments, at least one of the vehicle control module and the receiver are associated with a specific vehicle. In some embodiments, at least one of the communication unit and the vehicle control module is removably or non-removably mounted to the vehicle. In some embodiments, at least one of the communication unit and the vehicle control module is removably or non-removably mounted to an OBD port of the vehicle. In some embodiments, at least one of the communication unit and the vehicle control module are powered by the OBD port of the vehicle, a primary battery, a rechargeable battery, an energy generator, or any combination thereof. In some embodiments, the communication unit is further capable of receiving a fourth signal comprising a vehicle status, from the vehicle. In some embodiments, the communication unit is capable of receiving the fourth signal from the OBD port of the vehicle. In some embodiments, the communication unit is capable of receiving the fourth signal from a variety of specific vehicles. In some embodiments, the vehicle status comprises an OBD code. In some embodiments, the unique identifier is associated with the vehicle, the receiver, the mobile device, the communication unit, the vehicle control module, or any combination thereof. In some embodiments, the unique identifier comprises an encrypted identifier. In some embodiments, the unique identifier comprises a signed identifier. In some embodiments, the communication unit is further capable of decrypting the encrypted identifier. In some embodiments, the communication unit is capable of decrypting the encrypted identifier without access to the internet, the cellular network, or the server. In some embodiments the communication unit is further capable of validating the identifier. In some embodiments the communication unit is capable of validating the encrypted identifier without access to the internet, the cellular network, or the server. In some embodiments the mobile device is capable of receiving the first signal, storing the first signal, and sending the second signal without generating, validating, or decrypting the unique identifier. In some embodiments the executable instructions further comprises authenticating the first signal. In some embodiments at least one of the first signal and the second signal further comprises an access time range. In some embodiments the mobile device is capable of receiving and storing the first signal before receiving the user input. In some embodiments the executable

instructions of the mobile application are configured to receive and store the first signal before receiving the user input. In some embodiments the communication unit is further capable of receiving a fifth signal, equivalent to the second signal, from a source other than the mobile device. In some embodiments the source comprises the internet, the cellular network, the server, or any combination thereof. In some embodiments the mobile device receives the first signal from the internet, the cellular network, the server, or any combination thereof. In some embodiments the mobile application is capable of performing the executable instruction of sending the second signal to the communication unit without access to the internet, the cellular network, or the server. In some embodiments, the communication unit is further capable of sending a sixth signal to a user, the sixth signal comprising at least one of the sensor data, and a status data correlated to the fourth signal. In some embodiments the communication unit sends the sixth signal to the user via the internet, the cellular network, the server, the mobile device, or any combination thereof. In some embodiments, wherein the communication unit comprises a sensor capable of measuring a sensor data, In some embodiments the sensor comprises a GPS sensor, an accelerometer, an inclinometer, a vibration sensor, a motion detector, a microphone, a camera, or any combination thereof. In some embodiments, the sixth signal further comprises a sensor data measured by the sensor. In some embodiments the authorization to control the vehicle comprises authorization to unlock a vehicle door, lock the door, open the door, close the door, open a vehicle trunk, close the trunk, open a vehicle window, close the window, start a vehicle engine, stop the engine, enable a vehicle keyless start, disable the keyless start, start a vehicle air conditioning, stop the air conditioning, sound a vehicle alarm, disarm the alarm, honk a vehicle horn, turn on a vehicle headlight, turn off the headlight, or any combination thereof. In some embodiments the mobile application further comprises an executable instruction of granting a second user the authorization to control the vehicle. In some embodiments, the vehicle is a push-to-start vehicle. The system of any one of the preceding claims, wherein the second signal further comprises a request from the mobile device to the communication unit for a challenge. In some embodiments, the second signal further comprises the challenge sent from the communication unit to the mobile device. In some embodiments, the first signal further comprises a request to sign the challenge from the mobile device to the internet, cellular network, server, or any combination thereof. In some embodiments, the first signal further comprises a signed challenge from the internet, cellular network, server, or any combination thereof to the mobile device. In some embodiments, the second signal further comprises the signed challenge. In some embodiments, the first signal further comprises a key, and wherein the mobile device signs the challenge with the key.

[0006] A second aspect provided herein is method of granting authorization to control a vehicle comprising: a mobile device receiving a first signal, and sending a second signal; the mobile device storing the first signal; a user submitting an input to the mobile device; the mobile device sending a second signal to a communication unit; the communication unit receiving the second signal from the mobile device; the communication unit sending a third signal to a vehicle control module; the vehicle control module receiving the third signal; and the vehicle control module sending a command to a receiver within the vehicle; wherein the first and second signals both comprise a common unique identifier; and wherein the vehicle control module is in wired or wireless connection with the communication unit and the vehicle. In some embodiments, the mobile device sends the second signal to the communication unit without accessing the internet, the cellular network, or the server. In some embodiments, the mobile device receives and stores the first signal before the user submits the input. In some embodiments, the mobile device comprises a variety of one or more mobile devices. In some embodiments, at least one of the vehicle control module and the receiver are associated with a specific vehicle. Some embodiments further comprise charging at least one of the communication unit and the vehicle control module with an OBD port of the vehicle, a primary battery, a rechargeable battery, an energy generator, or any combination thereof. Some embodiments further comprise the communication unit receiving a fourth signal comprising a vehicle status, from the vehicle. In some embodiments, the communication unit receives the fourth signal from the OBD port of the vehicle. In some embodiments, the vehicle status comprises an OBD code. In some embodiments, the unique identifier is associated with the vehicle, the receiver, the mobile device, the communication unit, the vehicle control module, or any combination thereof. In some embodiments, the unique identifier comprises an encrypted identifier. In some embodiments, the unique identifier comprises a signed identifier. Some embodiments further comprise the communication unit decrypting the encrypted identifier. In some embodiments the communication unit is capable of decrypting the encrypted identifier without access to the internet, the cellular network, or the server. Some embodiments further comprise the communication unit validating the identifier. In some embodiments the communication unit is capable of validating the encrypted identifier without access to the internet, the cellular network, or the server. Some embodiments further comprise the communication unit authenticating the first signal. In some embodiments the mobile device receives the first signal, stores the first signal, and sends the second signal without generating, validating, or decrypting the unique identifier. In some embodiments at least one of the first signal and the second signal further comprises an access time range. In some embodiments the mobile device receives and stores the first signal before receiving the user input. Some embodiments further comprise the

communication unit receiving a fifth signal, equivalent to the second signal, from a source other than the mobile device. In some embodiments the source comprises the internet, the cellular network, the server, or any combination thereof. In some embodiments the mobile device receives the first signal from the internet, the cellular network, the server, or any combination thereof. Some embodiments further comprise the communication unit sending a sixth signal to a user, the sixth signal comprising at least one of the sensor data, and a status data correlated to the fourth signal. In some embodiments the communication unit sends the sixth signal to the user via the internet, the cellular network, the server, the mobile device, or any combination thereof. In some embodiments, the sixth signal further comprises a sensor data measured by a sensor. In some embodiments the authorization to control the vehicle comprises authorization to unlock a vehicle door, lock the door, open the door, close the door, open a vehicle trunk, close the trunk, open a vehicle window, close the window, start a vehicle engine, stop the engine, enable a vehicle keyless start, disable the keyless start, start a vehicle air conditioning, stop the air conditioning, sound a vehicle alarm, disarm the alarm, honk a vehicle horn, turn on a vehicle headlight, turn off the headlight, or any combination thereof. Some embodiments further comprise granting a second user the authorization to control the vehicle. In some embodiments the vehicle is a push-to-start vehicle. In some embodiments, the second signal further comprises a request from the mobile device to the communication unit for a challenge. In some embodiments, the second signal further comprises the challenge sent from the communication unit to the mobile device. In some embodiments, the first signal further comprises a request to sign the challenge from the mobile device to the internet, cellular network, server, or any combination thereof. In some embodiments, the first signal further comprises a signed challenge from the internet, cellular network, server, or any combination thereof to the mobile device. In some embodiments, the second signal further comprises the signed challenge. In some embodiments, the first signal further comprises a key, and wherein the mobile device signs the challenge with the key.

[0007] A third aspect provided herein is a mobile device based system for granting authorization to control a vehicle comprising: a communication unit; a vehicle control module that is separate and distinct from the communication unit; and a mobile device capable of receiving a user input and a first signal, and sending a second signal, wherein the mobile device comprises at least one mobile application including executable instructions to control the vehicle, wherein the executable instructions comprise: receiving the first signal from an internet, a cellular network, a server, or any combination thereof; storing the first signal; receiving the user input; and sending the second signal to the communication unit in response to receiving the user input; wherein the first and second signals both comprise a common unique identifier; wherein

the communication unit is capable of receiving the second signal from the mobile device and sending a third signal to the vehicle control module; and wherein the vehicle control module is capable of receiving the third signal and sending a command to a receiver within the vehicle; and wherein the mobile device is capable of performing the executable instruction of sending the second signal to the communication unit without access to the internet, the cellular network, or the server. In some embodiments, the mobile device is capable of receiving and storing the first signal before receiving the user input. In some embodiments, the communication unit is capable of receiving the second signal from a variety of mobile devices. In some embodiments, the communication unit is capable of sending the third signal to a variety of vehicle control modules. In some embodiments, the vehicle control module is capable of functionally communicating with both the communication unit and the receiver. In some embodiments, at least one of the vehicle control module and the receiver are associated with a specific vehicle. In some embodiments, at least one of the communication unit and the vehicle control module is removably or non-removably mounted to the vehicle. In some embodiments, at least one of the communication unit and the vehicle control module is removably or non-removably mounted to an OBD port of the vehicle. In some embodiments, at least one of the communication unit and the vehicle control module are powered by the OBD port of the vehicle, a primary battery, a rechargeable battery, an energy generator, or any combination thereof. In some embodiments, the communication unit is further capable of receiving a fourth signal comprising a vehicle status, from the vehicle. In some embodiments, wherein the communication unit is capable of receiving the fourth signal from the OBD port of the vehicle. In some embodiments, the communication unit is capable of receiving the fourth signal from a variety of specific vehicles. In some embodiments, the vehicle status comprises an OBD code. In some embodiments, the unique identifier is associated with the vehicle, the receiver, the mobile device, the communication unit, the vehicle control module, or any combination thereof. In some embodiments, the unique identifier comprises an encrypted identifier. In some embodiments, the unique identifier comprises a signed identifier. In some embodiments, the communication unit is further capable of decrypting the encrypted identifier. In some embodiments, the communication unit is capable of decrypting the encrypted identifier without access to the internet, the cellular network, or the server. In some embodiments, the communication unit is further capable of validating the identifier. In some embodiments, the communication unit is capable of validating the identifier without access to the internet, the cellular network, or the server. In some embodiments, the executable instructions further comprises authenticating the first signal. In some embodiments, the mobile device is capable of receiving the first signal, storing the first signal, and sending the second signal without generating, validating, or decrypting the unique identifier. In some embodiments, at least one of

the first signal and the second signal further comprises an access time range. In some embodiments, the mobile device is capable of receiving and storing the first signal before receiving the user input. In some embodiments, the executable instructions of the mobile application are configured to receive and store the first signal before receiving the user input. In some embodiments, the communication unit is further capable of receiving a fifth signal, equivalent to the second signal, from a source other than the mobile device. In some embodiments, source comprises the internet, the cellular network, the server, or any combination thereof. In some embodiments, the mobile device receives the first signal from the internet, the cellular network, the server, or any combination thereof. In some embodiments, the mobile application is capable of performing the executable instruction of sending the second signal to the communication unit without access to the internet, the cellular network, or the server. In some embodiments, the communication unit is further capable of sending a sixth signal to a user, the sixth signal comprising at least one of the sensor data, and a status data correlated to the fourth signal. In some embodiments, the communication unit sends the sixth signal to the user via the internet, the cellular network, the server, the mobile device, or any combination thereof. In some embodiments, the communication unit comprises a sensor capable of measuring a sensor data. In some embodiments, the sensor comprises a GPS sensor, an accelerometer, an inclinometer, a vibration sensor, a motion detector, a microphone, a camera, or any combination thereof. In some embodiments, the sixth signal further comprises a sensor data measured by the sensor. In some embodiments, the authorization to control the vehicle comprises authorization to unlock a vehicle door, lock the door, open the door, close the door, open a vehicle trunk, close the trunk, open a vehicle window, close the window, start a vehicle engine, stop the engine, enable a vehicle keyless start, disable the keyless start, start a vehicle air conditioning, stop the air conditioning, sound a vehicle alarm, disarm the alarm, honk a vehicle horn, turn on a vehicle headlight, turn off the headlight, or any combination thereof. In some embodiments, the mobile application further comprises an executable instruction of granting a second user the authorization to control the vehicle. In some embodiments, the vehicle is a push-to-start vehicle. The system of any one of the preceding claims, wherein the second signal further comprises a request from the mobile device to the communication unit for a challenge. In some embodiments, the second signal further comprises the challenge sent from the communication unit to the mobile device. In some embodiments, the first signal further comprises a request to sign the challenge from the mobile device to the internet, cellular network, server, or any combination thereof. In some embodiments, the first signal further comprises a signed challenge from the internet, cellular network, server, or any combination thereof to the mobile device. In some embodiments, the second signal further comprises the signed challenge. In some

embodiments, the first signal further comprises a key, and wherein the mobile device signs the challenge with the key.

[0008] A fourth aspect provided herein is a method of granting authorization to control a vehicle comprising: a mobile device receiving a first signal, and sending a second signal; the mobile device storing the first signal; a user submitting an input to the mobile device; the mobile device sending a second signal to a communication unit; the communication unit receiving the second signal from the mobile device; the communication unit sending a third signal to a vehicle control module; the vehicle control module receiving the third signal; and the vehicle control module sending a command to a receiver within the vehicle; wherein the first and second signals both comprise a common unique identifier; wherein the vehicle control module is in wired or wireless connection with the communication unit and the vehicle; and wherein the mobile device sends the second signal to the communication unit without accessing the internet, the cellular network, or the server In some embodiments, the mobile device receives and stores the first signal before the user submits the input. In some embodiments, the mobile device comprises a variety of one or more mobile devices. In some embodiments, at least one of the vehicle control module and the receiver are associated with a specific vehicle. Some embodiments further comprise charging at least one of the communication unit and the vehicle control module with an OBD port of the vehicle, a primary battery, a rechargeable battery, an energy generator, or any combination thereof. Some embodiments further comprise the communication unit receiving a fourth signal comprising a vehicle status, from the vehicle. In some embodiments, the communication unit receives the fourth signal from the OBD port of the vehicle. In some embodiments, the vehicle status comprises an OBD code. In some embodiments, the unique identifier is associated with the vehicle, the receiver, the mobile device, the communication unit, the vehicle control module, or any combination thereof. In some embodiments, the unique identifier comprises an encrypted identifier. In some embodiments, the unique identifier comprises a signed identifier. Some embodiments further comprise the communication unit decrypting the encrypted identifier. In some embodiments, the communication unit is capable of decrypting the encrypted identifier without access to the internet, the cellular network, or the server. Some embodiments further comprise the communication unit validating the identifier. In some embodiments, the communication unit is capable of validating the identifier without access to the internet, the cellular network, or the server. Some embodiments further comprise the communication unit authenticating the first signal. In some embodiments, the mobile device receives the first signal, stores the first signal, and sends the second signal without generating, validating, or decrypting the unique identifier. In some embodiments, at least one of the first signal and the second signal further comprises an access time range. In some embodiments, the

mobile device receives and stores the first signal before receiving the user input. Some embodiments further comprise the communication unit receiving a fifth signal, equivalent to the second signal, from a source other than the mobile device. In some embodiments, the source comprises the internet, the cellular network, the server, or any combination thereof. In some embodiments, the mobile device receives the first signal from the internet, the cellular network, the server, or any combination thereof. Some embodiments further comprise the communication unit sending a sixth signal to a user, the sixth signal comprising at least one of the sensor data, and a status data correlated to the fourth signal. In some embodiments, the communication unit sends the sixth signal to the user via the internet, the cellular network, the server, the mobile device, or any combination thereof. In some embodiments, the sixth signal further comprises a sensor data measured by a sensor. In some embodiments, the authorization to control the vehicle comprises authorization to unlock a vehicle door, lock the door, open the door, close the door, open a vehicle trunk, close the trunk, open a vehicle window, close the window, start a vehicle engine, stop the engine, enable a vehicle keyless start, disable the keyless start, start a vehicle air conditioning, stop the air conditioning, sound a vehicle alarm, disarm the alarm, honk a vehicle horn, turn on a vehicle headlight, turn off the headlight, or any combination thereof.

[0009] Some embodiments further comprise granting a second user the authorization to control the vehicle. In some embodiments, the vehicle is a push-to-start vehicle.

[0010] In another aspect, disclosed herein are computer-implemented methods of granting authorization to control a vehicle comprising: a mobile device receiving a first signal, and sending a second signal; the mobile device storing the first signal; a user submitting an input to the mobile device; the mobile device sending a second signal to a communication unit; the communication unit receiving the second signal from the mobile device; the communication unit sending a third signal to a vehicle control module; the vehicle control module receiving the third signal; and the vehicle control module sending a command to a receiver within the vehicle; wherein the first and second signals both comprise a common unique identifier; and wherein the vehicle control module is in wired or wireless connection with the communication unit and the vehicle. In some embodiments, the mobile device sends the second signal to the communication unit without accessing the internet, the cellular network, or the server. In some embodiments, the mobile device receives and stores the first signal before the user submits the input. In some embodiments, the mobile device comprises a variety of one or more mobile devices. In some embodiments, at least one of the vehicle control module and the receiver are associated with a specific vehicle. Some embodiments further comprise charging at least one of the communication unit and the vehicle control module with an OBD port of the vehicle, a primary battery, a rechargeable battery, an energy generator, or any combination thereof. Some

embodiments further comprise the communication unit receiving a fourth signal comprising a vehicle status, from the vehicle. In some embodiments, the communication unit receives the fourth signal from the OBD port of the vehicle. In some embodiments, the vehicle status comprises an OBD code. In some embodiments, the unique identifier is associated with the vehicle, the receiver, the mobile device, the communication unit, the vehicle control module, or any combination thereof. In some embodiments, the unique identifier comprises an encrypted identifier. In some embodiments, the unique identifier comprises a signed identifier. Some embodiments further comprise the communication unit decrypting the encrypted identifier. In some embodiments the communication unit is capable of decrypting the encrypted identifier without access to the internet, the cellular network, or the server. Some embodiments further comprise the communication unit validating the identifier. In some embodiments the communication unit is capable of validating the encrypted identifier without access to the internet, the cellular network, or the server. Some embodiments further comprise the communication unit authenticating the first signal. In some embodiments the mobile device receives the first signal, stores the first signal, and sends the second signal without generating, validating, or decrypting the unique identifier. In some embodiments at least one of the first signal and the second signal further comprises an access time range. In some embodiments the mobile device receives and stores the first signal before receiving the user input. Some embodiments further comprise the communication unit receiving a fifth signal, equivalent to the second signal, from a source other than the mobile device. In some embodiments the source comprises the internet, the cellular network, the server, or any combination thereof. In some embodiments the mobile device receives the first signal from the internet, the cellular network, the server, or any combination thereof. Some embodiments further comprise the communication unit sending a sixth signal to a user, the sixth signal comprising at least one of the sensor data, and a status data correlated to the fourth signal. In some embodiments the communication unit sends the sixth signal to the user via the internet, the cellular network, the server, the mobile device, or any combination thereof. In some embodiments, the sixth signal further comprises a sensor data measured by a sensor. In some embodiments the authorization to control the vehicle comprises authorization to unlock a vehicle door, lock the door, open the door, close the door, open a vehicle trunk, close the trunk, open a vehicle window, close the window, start a vehicle engine, stop the engine, enable a vehicle keyless start, disable the keyless start, start a vehicle air conditioning, stop the air conditioning, sound a vehicle alarm, disarm the alarm, honk a vehicle horn, turn on a vehicle headlight, turn off the headlight, or any combination thereof. Some embodiments further comprise granting a second user the authorization to control the vehicle. In some embodiments the vehicle is a push-to-start vehicle. In some embodiments, the second

signal further comprises a request from the mobile device to the communication unit for a challenge. In some embodiments, the second signal further comprises the challenge sent from the communication unit to the mobile device. In some embodiments, the first signal further comprises a request to sign the challenge from the mobile device to the internet, cellular network, server, or any combination thereof. In some embodiments, the first signal further comprises a signed challenge from the internet, cellular network, server, or any combination thereof to the mobile device. In some embodiments, the second signal further comprises the signed challenge. In some embodiments, the first signal further comprises a key, and wherein the mobile device signs the challenge with the key.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] The novel features of the disclosure are set forth with particularity in the appended claims. A better understanding of the features and advantages of the present disclosure will be obtained by reference to the following detailed description that sets forth illustrative embodiments, in which the principles of the disclosure are utilized, and the accompanying drawings of which:

[0012] **FIG. 1** shows a non-limiting illustration of an exemplary first mobile device based system for granting authorization to control a vehicle.

[0013] **FIG. 2** shows a non-limiting illustration of an exemplary second mobile device based system for granting authorization to control a vehicle.

[0014] **FIG. 3** shows an exemplary flowchart for a process of communication unit configuration.

[0015] **FIG. 4** shows an exemplary flowchart for a first process for a new owner activating a communication unit after installation in a vehicle.

[0016] **FIG. 5** shows an exemplary flowchart for a first process of connecting to, authenticating the communication unit.

[0017] **FIG. 6** shows an exemplary flowchart for a process of locking and unlocking doors.

[0018] **FIG. 7** shows an exemplary flowchart for a second process of connecting to and authenticating the communication unit.

[0019] **FIG. 8** shows an exemplary flowchart for a second process for a new owner activating a communication unit after installation in a vehicle.

[0020] **FIG. 9** shows an exemplary flowchart for a second process of connecting to and authenticating the communication unit.

[0021] **FIG. 10** shows an exemplary flowchart of communication signals between an internet or cellular network, a mobile device, a communications unit, a vehicle module, and a receiver within a vehicle.

[0022] **FIG. 11** shows a non-limiting example of a digital processing device; in this case, a device with one or more CPUs, a memory, a communication interface, and a display.

[0023] **FIG. 12** shows a non-limiting example of a web/mobile application provision system; in this case, a system providing browser-based and/or native mobile user interfaces.

[0024] **FIG. 13** shows a non-limiting example of a cloud-based web/mobile application provision system; in this case, a system comprising an elastically load balanced, auto-scaling web server and application server resources as well synchronously replicated databases.

DETAILED DESCRIPTION OF THE INVENTION

[0025] The disclosure provided herein provides for aftermarket devices and systems for car sharing, car rental and ride sharing that are far more scalable and easier to install than current solutions. The disclosure herein further provides a higher level of security by eliminating or reducing the risk of hacking of cellular transmission to a vehicle. The methods and systems herein are applicable for use with all makes and models of vehicles, and minimize the battery drain on the vehicle by utilizing alternative wireless technologies, such Bluetooth Low Energy.

Mobile device based systems for granting authorization to control a vehicle

[0026] Per **FIGs. 1** and **2**, a mobile device based system for granting authorization to control a vehicle **105** is presented herein comprising a communication unit **103**, a vehicle control module **104** that is separate and distinct from the communication unit **103**, and a mobile device **102** capable of receiving a user input and a first signal, and sending a second signal. In some embodiments, the mobile device comprises at least one mobile application including executable instructions to control the vehicle **105**, wherein the executable instructions comprise receiving the first signal from an internet, a cellular network, a remote server **101**, or any combination thereof; storing the first signal; receiving the user input; and sending the second signal to the communication unit **103** in response to receiving the user input. In some embodiments, the first and second signals both comprise a common unique identifier, wherein the communication unit **103** is capable of receiving the second signal from the mobile device **102** and sending a third signal to the vehicle control module **104**; and wherein the vehicle control module **104** is capable of receiving the third signal and sending a command to a receiver within the vehicle **105**. In some embodiments, per **FIG. 1**, the communication unit **103** is capable of sending a command to open or close a digital lock **106**.

[0027] **FIG. 1** shows a non-limiting illustration of an exemplary "direct wired" first mobile device based system for granting authorization to control a vehicle. In some embodiments, the remote server **101** comprises a secure web-based service. In some embodiments, the mobile device **102** is carried by the owner or renter and runs an application "app" that is capable of communicating with the remote server **101** and the communication unit **103**. The mobile device **102** is not considered trusted and only stores, receives, or transmits encrypted and/or signed data from the remote server **101** and communication unit **103**. In some embodiments, established cryptography practices are used to ensure that secure data is not tampered with, stored and sent again later, or copied and sent from an unauthorized mobile device. In some embodiments, the mobile device **102** communicates with the remote server **101** over the internet using secure HTTP or HTTPS with the strongest available TLS version and cipher suite.

[0028] In some embodiments, the communication unit **103**, control module **104**, and digital lock **106** are installed in the vehicle **105** and are capable of secure data communication and storage. The communication unit **103** validates communication from the mobile unit **102** and controls features of the vehicle **105** through the control module **104**.

[0029] In some embodiments, the mobile device **102** communicates with the communication unit **103** using Bluetooth Low Energy (BLE), near-field communication (NFC) or any other short-range wireless technology. This communication path is not considered secure and may be susceptible to sniffing, tampering, and jamming. All data sent over this communication path is thus encrypted and/or signed to prevent spoofing, tampering, or information loss commonly associated with such means of communication.

[0030] In some embodiments, the communication unit **103** is wired to the vehicle **105** to supply power and ground, and comprises an integrated GPS module for tracking vehicle **105** position and speed, and an optional long-range wireless (GSM or LTE) module for reporting position, speed, or other diagnostic or status information to the remote server, either periodically or in real time.

[0031] In some embodiments, the control module **104** is capable of unlocking and locking the doors and controlling other vehicle **105** functions. Some control modules 104 are installed with aftermarket remote starters and car alarms. Bypass modules support a wide range of vehicle **105** models and model years. In some embodiments, the digital lock **106** is a circuit that prevents the vehicle **105** from being started if not authorized by the communication unit **103**.

[0032] **FIG. 2** shows a non-limiting illustration of an exemplary "plug-and-play" second mobile device based system for granting authorization to control a vehicle. In some embodiments, the second mobile device based system for granting authorization to control a vehicle is capable of enhanced security during factory configuration, employs a Diffie-Hellman

key exchange algorithm to ensure that the potentially insecure manufacturing station does not see the admin key, provides protection against rogue apps and mobile device cloning, and employs strong encryption and hashing algorithms using a true random number generator for enhanced device tampering prevention.

[0033] In the second mobile device based system for granting authorization to control a vehicle, the roles of the remote server **101**, mobile device **102**, and communication unit **103** are the same as in the first mobile device based system for granting authorization to control a vehicle.

[0034] In some embodiments, the communication unit **103** and vehicle control module **104** are wired to the vehicle control module **104** or connected using a secure wireless technology in the vehicle **105**, and are inaccessible to people outside of the vehicle **103**. In some embodiments, the communication unit **103** is plugged into the vehicle's OBD-II port for power and also possibly for reading diagnostic and status information such as fuel levels, speed, etc. from the vehicle's communication networks (e.g. CAN bus).

[0035] In some embodiments, the vehicle control module **104** contains similar circuitry that is present in a vehicle's OEM key fob, exposing an interface to enable the communication unit **103** to control the functionality present in the key fob circuitry of locking and unlocking doors, opening the trunk, and/or starting the vehicle. In some embodiments, the interface also allows the communication unit **103** to control the passive start functionality of the key fob circuitry to prevent the vehicle **103** from being started if not authorized by the communication unit **103**. In some embodiments, during installation, the vehicle control module is programmed with the vehicle **103** in the same way that a new OEM key fob is added to the vehicle **103**, by a dealer or locksmith.

[0036] As the vehicle control module **104** is physically separate from the communication unit **103**, the vehicle control module **104** may be manufactured separately by the original equipment manufacturer (OEM), wherein the communication unit **103** does not need to implement proprietary security technology that may be specific to particular vehicle's models or model years.

[0037] In some embodiments, although it is possible to unplug the communication unit **103** and the vehicle control module **104**, doing so will prevent the vehicle from being started because the passive start functionality will no longer be powered.

[0038] Per **FIG. 10**, a mobile device based system for granting authorization to control a vehicle **1005** is presented herein comprising a communication unit **1002**, a vehicle control module **1003** that is separate and distinct from the communication unit **1002**, and a mobile device **1001** capable of receiving a user input and a first signal **1011**, and sending a second signal

1012. In some embodiments, the mobile device **1001** comprises at least one mobile application including executable instructions to control the vehicle **1005**, wherein the executable instructions comprise receiving the first signal **1011** from an internet, a cellular network, a server **1006**, or any combination thereof; storing the first signal **1011**; receiving the user input; and sending the second signal **1012** to the communication unit **1001** in response to receiving the user input. In some embodiments, the first and second signals **1011 1012** both comprise a common unique identifier, wherein the communication unit **1002** is capable of receiving the second signal **1012** from the mobile device **1001** and sending a third signal **1013** to the vehicle control module **1003**; and wherein the vehicle control module **1003** is capable of receiving the third signal **1013** and sending a command **1017** to a receiver **1004** within the vehicle **1005**.

[0039] In some embodiments, the mobile device **1001** is capable of performing the executable instruction of sending the second signal **1012** to the communication unit **1002** without access to the internet, the cellular network, or the server. In some embodiments, the mobile device **1001** is capable of receiving and storing the first signal **1011** before receiving the user input. In some embodiments, the communication unit **1002** is capable of receiving the second signal **1012** from a variety of mobile devices **1001**. In some embodiments, the communication unit **1002** is capable of sending the third signal **1013** to a variety of vehicle control modules **1003**. In some embodiments, the vehicle control module **1003** is capable of functionally communicating with both the communication unit **1002** and the receiver **1004**. In some embodiments, at least one of the vehicle control module **1003** and the receiver **1004** are associated with a specific vehicle **1005**. In some embodiments, at least one of the communication unit **1002** and the vehicle control module **1003** is removably or non-removably mounted to the vehicle **1005**. In some embodiments, at least one of the communication unit **1002** and the vehicle control module **1003** is removably or non-removably mounted to an OBD port of the vehicle **1005**. In some embodiments, at least one of the communication unit **1002** and the vehicle control module **1003** are powered by the OBD port of the vehicle **1005**, a primary battery, a rechargeable battery, an energy generator, or any combination thereof. In some embodiments, the communication unit **1002** is further capable of receiving a fourth signal **1014** comprising a vehicle status, from the vehicle **1005**. In some embodiments, the communication unit **1002** is capable of receiving the fourth signal **1014** from the OBD port of the vehicle **1005**. In some embodiments, the communication unit **1002** is capable of receiving the fourth signal **1014** from a variety of specific vehicles **1005**. In some embodiments, the vehicle status comprises an OBD code. In some embodiments, the unique identifier is associated with the vehicle **1005**, the receiver **1004**, the mobile device **1001**, the communication unit **1002**, the vehicle control module **1003**, or any combination thereof. In some embodiments, the unique identifier comprises an encrypted

identifier. In some embodiments, the unique identifier comprises a signed identifier. In some embodiments, the communication unit **1002** is further capable of decrypting the encrypted identifier. In some embodiments, the communication unit **1002** is capable of decrypting the encrypted identifier without access to the internet, the cellular network, or the server. In some embodiments, the communication unit **1002** is further capable of validating the identifier. In some embodiments, the communication unit **1002** is capable of validating the encrypted identifier without access to the internet, the cellular network, or the server. In some embodiments, the mobile device **1001** is capable of receiving the first signal **1011**, storing the first signal **1011**, and sending the second signal **1012** without generating, validating, or decrypting the unique identifier. In some embodiments, the executable instructions further comprise authenticating the first signal **1011**. In some embodiments, at least one of the first signal **1011** and the second signal **1012** further comprises an access time range. In some embodiments, the mobile device **1001** is capable of receiving and storing the first signal **1011** before receiving the user input. In some embodiments, the executable instructions of the mobile application are configured to receive and store the first signal **1011** before receiving the user input. In some embodiments, the communication unit **1002** is further capable of receiving a fifth signal **1015**, equivalent to the second signal **1012**, from a source other than the mobile device **1001**, wherein the source comprises the internet, the cellular network, the server, or any combination thereof. In some embodiments, the mobile device **1001** receives the first signal **1011** from the internet, the cellular network, the server, or any combination thereof. In some embodiments, the mobile application is capable of performing the executable instruction of sending the second signal **1012** to the communication unit **1002** without access to the internet, the cellular network, or the server. In some embodiments, the communication unit **1002** is further capable of sending a sixth signal **1016** to a user, the sixth signal **1016** comprising at least one of the sensor data, and a status data correlated to the fourth signal **1014**. In some embodiments, the communication unit **1002** sends the sixth signal **1016** to the user via the internet, the cellular network, the server, the mobile device, or any combination thereof. In some embodiments, the communication unit **1002** comprises a sensor capable of measuring a sensor data comprising a GPS sensor, an accelerometer, an inclinometer, a vibration sensor, a motion detector, a microphone, a camera, or any combination thereof. In some embodiments, the sixth signal **1016** further comprises a sensor data measured by the sensor. In some embodiments, the authorization to control the vehicle **1005** comprises authorization to unlock a vehicle door, lock the door, open the door, close the door, open a vehicle trunk, close the trunk, open a vehicle window, close the window, start a vehicle engine, stop the engine, enable a vehicle keyless start, disable the keyless start, start a vehicle air conditioning, stop the air conditioning, sound a vehicle alarm, disarm the

alarm, honk a vehicle horn, turn on a vehicle headlight, turn off the headlight, or any combination thereof. In some embodiments, the mobile application further comprises an executable instruction of granting a second user the authorization to control the vehicle **1005**. In some embodiments, the vehicle **1005** is a push-to-start vehicle.

[0040] In some embodiments, unlike many commercially available vehicle control systems, the communication unit does not require a direct communication link with the remote server because a remote link to control door locks or other vehicle functions may be compromised if the remotely server is hacked. As Bluetooth communications may not be secure, data sent over Bluetooth is signed and/or encrypted to prevent a potential attacker from trying to capture and replay, jam, or otherwise tamper with the wireless signals. Further, because a mobile device may be compromised, security policies are enforced within the remote server and the communication unit, and not on the app running on the mobile. As such, in some embodiments, unencrypted data is not stored, received, or sent on the mobile device.

Configuration of the communication unit

[0041] **FIG. 3** shows an exemplary flowchart for a process for communication unit configuration, comprising the communication generating a random admin key **301** on its first boot, a manufacturing station connecting to the communication unit **302**, and reading the admin key **303**, the communication unit sending the admin key **304** to the manufacturing station, the manufacturing station provisioning a new unit in its database **305** and sending a MAC ID and the admin key to a remote server for storage in a database **306**, and the manufacturing station sending a lockdown command **307** to the communication unit, which enters production mode and prevents the admin key from being read **308**.

[0042] On first boot, the communication unit generates a pseudorandom 128-bit administrative key **301**. During the configuration process, the manufacturing station wirelessly connects to the communication unit **302**, reads the admin key **303,** and sends a request, comprising the unit's unique MAC ID and the admin key that was read, to the remote server to provision the new unit in the database **304**. In some embodiments, a visible identifier such as a unit's serial number may also be sent. In some embodiments, the MAC ID is a unique and difficult to spoof identifier that is assigned to the wireless interface when the interface chip is manufactured and presented to other devices over the wireless network.

[0043] In some embodiments, the manufacturing station authenticates with the remote server using a secret API key which is also IP whitelisted by the server, to prevent others from creating fake devices. In some embodiments, prior to shipment, a lockdown command is sent to the unit

307 which enters the unit into production mode **307**. In some embodiments, the admin key may no longer be read by anyone, ensuring that it remains secret.

[0044] **FIG. 7** shows an exemplary flowchart for a second process of connecting to and authenticating the communication unit comprising the communication generating a random admin key **701** on its first boot, a manufacturing station connecting to the communication unit **702**, and reading the admin key **703**, the communication unit sending the admin key **704**, the manufacturing station creating a new unit in its database **705** and sending a MAC ID and the admin key to a remote server that generates random admin keys, calculates an admin shared secret, and sends a public key **706**, the manufacturing station writing a server public key **707**, and the communications unit calculating and sorting the admin shared secret **708**.

[0045] In some embodiments, the method shown in the exemplary flow chart per **FIG. 7** employs the Elliptic Curve Diffie-Hellman key agreement protocol to establish a shared secret between the communication unit and remote server over an insecure channel.

[0046] In some embodiments, on first boot, the communication unit generates random public and private keys using a true random number generator **701**. In some embodiments, during the factory configuration process, the manufacturing station connects to the communication unit **702** wirelessly and reads the unit's public key **703**, and sends a request to the remote server to provision the new unit in the database **705**. In some embodiments, the request comprises the unit's unique MAC ID and the public key that was read, and a visible identifier such as a unit's serial number.

[0047] In some embodiments, the remote server then generates its own random public and private keys for the unit, calculates the admin key using the server's public and private keys and the communication unit's public key, and sends back the server's public key **706**. In some embodiments, the mobile device then forwards the server's public key to the communication unit **707**, enabling the unit to calculate and store the admin key **708**.

New owner post-installation activation

[0048] **FIG. 4** shows an exemplary flowchart for a first "owner claim" process for new owner post-installation activation, comprising a mobile device receiving user credentials and logging into the server **401**, the remote server authenticating the user and sending a token **402** to the mobile device which scans for nearby communication units and obtains their MAC IDs **403**, receives a user pin **404**, establishes connection with the communication unit **405**, and requests an admin authentication challenge **406**, the communication unit generating a random challenge **407**, the mobile devices sending a MAC ID. PIN to request that the challenge is signed **408**, the remote server signing the challenge with the admin key **409**, the mobile device authenticating the

signed challenge **410**, the communication unit validating the signature **411**, the mobile device downloading a key **412**, the remote server generating random keys, which are stored in the database and sent in encrypted form to the mobile device **413**, which assigns the keys **414**, and the communication unit decrypting and storing the keys **415**.

[0049] Per the owner claim process in **FIG. 4**, where a newly installed unit is activated, after installation, the owner may be provided with a welcome card identifying the communication unit's MAC ID and unique PIN code. In some embodiments, the owner claim process is executed when the owner has Internet connectivity and is within short-range wireless range of the communication unit. In some embodiments, the owner begins the process by logging into the app on the mobile device **401**. In addition to the user credentials, the app also sends the mobile device's AppID in the login request to the remote server. In some embodiments, the AppID is a unique identifier for the app running on the particular mobile device, wherein the contents of the mobile device are backed up and restored on a different mobile device, or if the mobile device is wiped and the app is reinstalled, the AppID will change. In some embodiments, if the remote server detects a user login with a new AppID, it assumes the user is logging in with a different mobile device and triggers re-verification of the user's email address and phone number.

[0050] After a successful login, the remote server responds with a session token after validating the owner's credentials **402**, the app scans for nearby communication units **403**, and the owner identifies the unit with the matching MAC ID and enters the PIN from the welcome card **404**.

[0051] In some embodiments, the app then establishes a wireless connection to the communication unit **405**. The app requests an admin-level authentication challenge from the communication unit **406** which the unit generates pseudorandomly **407**. The app then asks the remote server to sign the challenge, passing along the challenge, MAC ID, and PIN **408**. If the PIN matches the expected value for the corresponding MAC ID, the server signs the challenge **409** with the unit's admin key and returns the signature to the app. The app then sends the signature to the communication unit **410**. If the unit verifies that the signature matches the expected signature (as calculated internally by the unit), the connection is considered authenticated with the admin access level **410**. During this process the admin key may not disclosed to the mobile device.

[0052] In some embodiments, the challenge-response approach avoids having to send keys in plain text. In some embodiments, a challenge is 128 bits in length and expires after about ten seconds. In some embodiments, challenges are signed using a keyed-hash message authentication code (HMAC). In some embodiments, each message (characteristic) type that the communication unit supports has a required access level for read operations and a required

access level for write operations, wherein the four possible access levels comprise admin, primary, secondary, and shared levels. In some embodiments, admin keys are used during the owner claim process, primary keys are used by the owner, and secondary keys and shared keys are similar, except that shared keys are time-limited.

[0053] In some embodiments, after authenticating with the communication unit, the app downloads the primary, secondary, and shared keys from the remote server **411**, the remote server generates the keys pseudorandomly, stores the keys in the database, and sends the keys back to the app in encrypted form **412**. In some embodiments, the keys are encrypted using AES-128 with the admin key, to prevent the keys from being disclosed to the app or during wireless transmission to the communication unit. In some embodiments, the app sends the encrypted keys to the communication unit **413** which then decrypts and stores the keys **414**.

[0054] **FIG. 8** shows an exemplary flowchart for a second "owner claim" process wherein a new owner activates a communication unit after installation in a vehicle comprising the user entering credentials and logging into the server **801** through the mobile device, the remote server authenticating the user and sending a token **802**, the mobile device scanning for nearby communications units and obtaining lists of MAC IDs **803**, receiving a user unit selection and pin **804**, establishing connection to the communication unit **805**, creating a communication session **806**, and sending a MAC ID to the remote server which generates a random owner key, encrypts a package containing the owner key and the AppID using an admin shared secret **807**, the mobile device forwarding the encrypted admin package and signing the package with the AppID **808**, the communication unit verifying that the AppID matches the signature **809**, storing the owner key, and encrypting the package **810**, and the mobile device forwarding the package **811** to the remote server, which stores the owner's AppID and MAC ID **812**.

[0055] In some embodiments, the second "owner claim" process, per **FIG. 8,** up to the wireless connection being established between the mobile device and the communication unit **805**, is identical to the second "owner claim" process. In some embodiments, after the connection to the communication unit is established, the app requests the remote server to establish a new encrypted communication session with the communication unit **806**, passing along the MAC ID and PIN. In some embodiments, if the PIN matches the expected value for the corresponding MAC ID, the server generates a random primary key then encrypts a package containing the primary key and owner's current AppID using the admin key generated during the factory configuration process **807**.

[0056] In some embodiments, a package comprises a message sent between the remote server and communication unit that cannot be inspected by the mobile device, wherein the mobile device passes the package along to the communication unit. In some embodiments, during the

owner claim process the package that initiates the communication session is signed with the admin key, wherein subsequent packages are signed using the primary key.

[0057] In some embodiments, after the mobile device receives the encrypted package the mobile devices signs the package with its AppID and sends the package to the communication unit **808**, wherein the communication unit decrypts the package using the admin key and verifies that the AppID in the package matches the AppID in the signature **809** to ensure that the package was sent by the same mobile device that was authorized by the remote server.

[0058] In some embodiments, the communication unit then stores the primary key and encrypts a new package containing the mobile device's MAC ID **8010**. The package is encrypted using the primary key. In some embodiments, the app forwards the package to the remote server **8011** which then stores the association between the AppID and the mobile device's MAC ID in the database.

Connecting the communications unit

[0059] **FIG. 5** shows an exemplary flowchart for a first process of connecting to and authenticating the communication unit comprising the mobile device receiving user credentials and logging into the server **501**, the server authenticating the user and sending a token and a vehicle key **502** to the mobile device, which stores the key **503**, the mobile device connecting to a vehicle **504**, establishing a connection to the communication unit **505** and requesting an authentication challenge **506**, the communication unit generating a random challenge **507**, the mobile device signing the challenge with the key **508** and authenticating the key with the signed challenge **509**, and the communications unit validating the signature **510** and authenticating the connection **511**.

[0060] In some embodiments, the exemplary connection processes shown in flowchart of **FIG. 5**, is followed for all connections to the communication unit except for during the owner claim process.

[0061] In some embodiments, the user initiates the process by logging into the app on the mobile device **501**. In some embodiments, the remote server responds with a session token after validating the user's credentials **502**, and sends back all of the vehicle keys to the user. In some embodiments, the app encrypts and stores the keys in the app's secure storage **503** for potential later offline use.

[0062] In some embodiments, the rest of the connection process in **FIG. 5** may occur with or without the mobile device having an Internet connection as long as the user has logged in and downloaded his or her keys, which is advantageous because a vehicle may be parked underground or in a remote location without cell connectivity.

[0063] In some embodiments, after the user selects the vehicle and initiates connection **504**, the app establishes a wireless connection to the communication unit **505** and requests an authentication challenge from the communication unit **506**,which the communications unit generates pseudorandomly **507**. In some embodiments, the challenge is specific to the access level of the user's key. In some embodiments, the app then signs the challenge using the key that was downloaded from the server **508** and sends the signature to the communication unit **509**. In some embodiments, if the communications unit verifies that the signature matches the expected signature **510**, the connection is considered authenticated with the appropriate access level **511**.

[0064] In some embodiments, shared keys are intended to be temporary and not reusable, even if the app or mobile device are compromised, wherein when shared keys are shared, the key is hashed together with an index by the remote server using a HMAC, which is incremented each time the key is shared. In some embodiments, during the owner claim process, the original (non-indexed) base key is encrypted and sent to the communication unit. In some embodiments of the shared key connection process, the hashed key is downloaded to the mobile device. In some embodiments, the communication unit independently maintains its own index based on the previously verified index, and increments its internal index up to 256 iterations past the current index when the signature is verified, generating a signature, and comparing it to the app's signature at each iteration. In some embodiments, if any of the generated signatures match, the app's signature is considered valid, otherwise, if the app sends a signature generated with a lower index value, validation will fail. Due to the mathematical nature of the HMAC algorithm, it is practically impossible to recover the base shared key from the signature or to change the index after the signature has been calculated. This effectively prevents past renters from reusing their key.

[0065] **FIG. 9** shows an exemplary flowchart for a second process of connecting to and authenticating the communication unit comprising the mobile device receiving user credentials and AppID, and logging into the server **901**, the remote server authenticating the user, sending a visual token and vehicle keys **902**, and encrypting a package containing the access control list (ACL) and the phone's AppID using the owner's key **903**, the mobile device storing the keys and ACL packages **904**, the mobile device connecting to a vehicle **905**, establishing connection to a communication unit **906**, and forwarding the encrypted ACL package that is signed with the AppID **907**, the communications unit decrypting the package and updating the ACL **908**, verifying that the AppID matches the signature **909**, verifying the phone's MAC ID if the ACL contains the MAC ID **910**, authenticating the connection **911**, encrypting the package containing the phone's MAC ID using the owner's key if the MAC ID is not in the ACL **912**, the mobile

device forwarding the encrypted package **913**, and the remote server storing the user's AppID and MAC ID **914**.

Locking and unlocking methods

[0066] **FIG. 6** shows an exemplary flowchart for a process of locking a door comprising a user generating a lock doors command **601** through the mobile device, which generates a random challenge **602**, and sends a lock door command **603** comprising a challenge to the communication unit which, upon receiving the lock doors command **604**, sends an instruction to the vehicle control module to lock the doors **605**, and signs the challenge with a key **606**, wherein the mobile device validates the signature **607**.

[0067] **FIG. 6** further shows an exemplary flowchart for a process of unlocking a door comprising a user generating a lock doors command **608** through the mobile device, which requests a random challenge **609**, the communication unit generating a random challenge **610**, the mobile device signing the challenge with the key **611** and sending an unlock door command **612** comprising a signature to the communication unit which validates the signature **613** and sends an unlock door command **614** to the vehicle control module to unlock the doors **615**.

[0068] As Bluetooth connections may not be secure, a challenge and response protocol is used in some embodiments for locking and unlocking doors. This approach prevents jamming and replay attacks and attempts to tamper with the data from being successful. For example, an unlock command might be captured over the air by an attacker and replayed later to unlock the vehicle. As another example, a lock command might be jammed, preventing the command from reaching the communication unit and leaving the vehicle unlocked.

[0069] In some embodiments, during the lock process **601**, the app generates a pseudorandom challenge **602** and sends it to the communication unit **603**. In some embodiments, after the communications unit instructs the vehicle control module to lock the doors **604**, the communications unit signs the challenge with same key used in the connection process **606**, and the app validates the signature **607**. In some embodiments, if the app fails to validate the signature the app may conclude that a "man-in-the-middle" intercepted or jammed the command and that the doors were not locked as intended.

[0070] In some embodiments, during the unlock process **608**, the app requests an unlock challenge from the communication unit **609**. In some embodiments, the communications unit generates a pseudorandom challenge **610** which the app then signs **611** and sends back **612**, wherein if the communications unit successfully validates the signature **612**, the communications unit sends the command to the vehicle control module to unlock the doors **614**. By involving a pseudorandom challenge with a ten-second timeout, an attacker capturing and replaying the

signature will fail to unlock the doors. Similar processes may be used for enabling and disabling the digital lock that prevents the vehicle from being started.

[0071] **FIG. 9** shows an exemplary flowchart for a second process of connecting to and authenticating the communication unit comprising the mobile device receiving user credentials and AppID, and logging into the server **901**, the remote server authenticating the user, sending a visual token and vehicle keys **902**, and encrypting a package containing the access control list (ACL) and the phone's AppID using the owner's key **903**, the mobile device storing the keys and ACL packages **904**, the mobile device connecting to a vehicle **905**, establishing connection to a communication unit **906**, and forwarding the encrypted ACL package that is signed with the AppID **907**, the communications unit decrypting the package and updating the ACL **908**, verifying that the AppID matches the signature **909**, verifying the phone's MAC ID if the ACL contains the MAC ID **910**, authenticating the connection **911**, encrypting the package containing the phone's MAC ID using the owner's key if the MAC ID is not in the ACL **912**, the mobile device forwarding the encrypted package **913**, and the remote server storing the user's AppID and MAC ID **914**.

[0072] In some embodiments, the second process of connecting to and authenticating the communication unit comprises the logging into the app on the mobile device **901**, The remote server responding with a session token after validating the user's credentials **902**, and the remote server sending back data for all of the vehicle keys to which the user has access **903**.

[0073] In some embodiments, the key data also includes encrypted packages containing an access control list (ACL) for each communication unit along with the user's current AppID, wherein the ACL comprises a table of multiple records, each consisting of an AppID, the mobile device's MAC ID, and the access level, and wherein the ACL is tagged with an incrementing version number. In some embodiments, a record would be included for the owner and all keys that have been shared, wherein the MAC ID is only included if it is known; that is, if a communication unit has previously communicated with the specific mobile device.

[0074] Storing the AppID to MAC ID associations in the database and including them in the ACL provides additional assurance that user data is not being transferred between mobile devices without authorization from the remote server. Both the AppID and MAC ID are required because some mobile device operating systems do not allow apps to query their own MAC IDs.

[0075] In some embodiments, the key data is stored on the mobile device **904** for potential later offline use, wherein the sensitive data is no longer encrypted (and not decryptable by the app) we no longer need to rely on the app to store it securely. In some embodiments, steps **905** to **913** may occur with or without the mobile device having an Internet connection.

[0076] In some embodiments, after the user selects the vehicle and initiates connection **905**, the app establishes a wireless connection to the communication unit **906**. The app then forwards the encrypted ACL to the communication unit, signing the package with its AppID **907**. The communication unit decrypts the package and stores the ACL if the version number is higher than the last version number that was received **908**. In some embodiments, the unit also verifies that the AppID in the package matches the AppID in the signature **909**, wherein if the MAC ID corresponding to the current mobile device's AppID is included in the ACL, the unit verifies that the connected mobile device's MAC ID matches the ACL MAC ID **910**. If these verification steps are successful, the connection is considered authenticated with the appropriate access level **911**.

[0077] In some embodiments, if the MAC ID corresponding to the current mobile device's AppID is not included in the ACL, the communication unit encrypts a new package containing the mobile device's MAC ID **912**, and the app forwards this package to the remote server **913** and the remote server stores the association between the AppID and the mobile device's MAC ID in the database.

[0078] In some embodiments, the above mentioned methods and systems for locking and unlocking a vehicle can be employed with the first or second mobile device based systems for granting authorization to control a vehicle.

Terms and Definitions

[0079] Unless otherwise defined, all technical terms used herein have the same meaning as commonly understood by one of ordinary skill in the art to which this disclosure belongs.

[0080] As used herein, the singular forms "a," "an," and "the" include plural references unless the context clearly dictates otherwise. Any reference to "or" herein is intended to encompass "and/or" unless otherwise stated.

[0081] As used herein, the term "about" refers to an amount that is near the stated amount by about 10%, 5%, or 1%, including increments therein.

[0082] As used herein, the term "vehicle" refers to a mobile machine that transports people or cargo, such as, for example, a wagon, a bicycle, a motor vehicle, a motorcycle, a car, a truck, a bus, a railed vehicle, a train, a tram, a watercraft, a ship, a boat, an aircraft or a spacecraft. In some embodiments, a vehicle comprises a door, a trunk, a window, an engine, a window, an air conditioning system, a horn, and a headlight.

[0083] As used herein, the term "mobile device" refers to a mobile computing device such as, for example, a laptop computer, a notebook computer, a sub-notebook computer, a netbook computer, a netpad computer, a set-top computer, a media streaming device, a handheld

computer, an Internet appliance, a mobile smartphone, a tablet computer, a personal digital assistant, or a video game console.

[0084] As used herein, the term "OBD port" refers to an on-board diagnostics port built into may vehicles that enables the vehicle to send a signal comprising a diagnosis or a status. In some embodiments, the OBD port is further capable of acting as a source of power.

[0085] As used herein, the term "access time range" refers to a specific time and/or date range wherein an item or resource can be accessed by a user.

[0086] As used herein, the term "push-to-start vehicle" refers to vehicle wherein ignition does not require a physical key, and wherein the engine can be turned on by the push of a button. In some embodiments, a push-to-start vehicle comprises a system to detect the proximity or signal from a key fob or authenticating device before starting the engine of the vehicle.

Digital processing device

[0087] In some embodiments, the platforms, systems, media, and methods described herein include a digital processing device, or use of the same. In further embodiments, the digital processing device includes one or more hardware central processing units (CPUs) or general purpose graphics processing units (GPGPUs) that carry out the device's functions. In still further embodiments, the digital processing device further comprises an operating system configured to perform executable instructions. In some embodiments, the digital processing device is optionally connected a computer network. In further embodiments, the digital processing device is optionally connected to the Internet such that it accesses the World Wide Web. In still further embodiments, the digital processing device is optionally connected to a cloud computing infrastructure. In other embodiments, the digital processing device is optionally connected to an intranet. In other embodiments, the digital processing device is optionally connected to a data storage device.

[0088] In accordance with the description herein, suitable digital processing devices include, by way of non-limiting examples, server computers, desktop computers, laptop computers, notebook computers, sub-notebook computers, netbook computers, netpad computers, set-top computers, media streaming devices, handheld computers, Internet appliances, mobile smartphones, tablet computers, personal digital assistants, video game consoles, and vehicles. Those of skill in the art will recognize that many smartphones are suitable for use in the system described herein. Those of skill in the art will also recognize that select televisions, video players, and digital music players with optional computer network connectivity are suitable for use in the system described herein. Suitable tablet computers include those with booklet, slate, and convertible configurations, known to those of skill in the art.

[0089] In some embodiments, the digital processing device includes an operating system configured to perform executable instructions. The operating system is, for example, software, including programs and data, which manages the device's hardware and provides services for execution of applications. Those of skill in the art will recognize that suitable server operating systems include, by way of non-limiting examples, FreeBSD, OpenBSD, NetBSD®, Linux, Apple® Mac OS X Server®, Oracle® Solaris®, Windows Server®, and Novell® NetWare®. Those of skill in the art will recognize that suitable personal computer operating systems include, by way of non-limiting examples, Microsoft® Windows®, Apple® Mac OS X®, UNIX®, and UNIX-like operating systems such as GNU/Linux®. In some embodiments, the operating system is provided by cloud computing. Those of skill in the art will also recognize that suitable mobile smart phone operating systems include, by way of non-limiting examples, Nokia® Symbian® OS, Apple® iOS®, Research In Motion® BlackBerry OS®, Google® Android®, Microsoft® Windows Phone® OS, Microsoft® Windows Mobile® OS, Linux®, and Palm® WebOS®. Those of skill in the art will also recognize that suitable media streaming device operating systems include, by way of non-limiting examples, Apple TV®, Roku®, Boxee®, Google TV®, Google Chromecast®, Amazon Fire®, and Samsung® HomeSync®. Those of skill in the art will also recognize that suitable video game console operating systems include, by way of non-limiting examples, Sony® PS3®, Sony® PS4®, Microsoft® Xbox 360®, Microsoft Xbox One, Nintendo® Wii®, Nintendo® Wii U®, and Ouya®.

[0090] In some embodiments, the device includes a storage and/or memory device. The storage and/or memory device is one or more physical apparatuses used to store data or programs on a temporary or permanent basis. In some embodiments, the device is volatile memory and requires power to maintain stored information. In some embodiments, the device is non-volatile memory and retains stored information when the digital processing device is not powered. In further embodiments, the non-volatile memory comprises flash memory. In some embodiments, the non-volatile memory comprises dynamic random-access memory (DRAM). In some embodiments, the non-volatile memory comprises ferroelectric random access memory (FRAM). In some embodiments, the non-volatile memory comprises phase-change random access memory (PRAM). In other embodiments, the device is a storage device including, by way of non-limiting examples, CD-ROMs, DVDs, flash memory devices, magnetic disk drives, magnetic tapes drives, optical disk drives, and cloud computing based storage. In further embodiments, the storage and/or memory device is a combination of devices such as those disclosed herein.

[0091] In some embodiments, the digital processing device includes a display to send visual information to a user. In some embodiments, the display is a liquid crystal display (LCD). In further embodiments, the display is a thin film transistor liquid crystal display (TFT-LCD). In

some embodiments, the display is an organic light emitting diode (OLED) display. In various further embodiments, on OLED display is a passive-matrix OLED (PMOLED) or active-matrix OLED (AMOLED) display. In some embodiments, the display is a plasma display. In other embodiments, the display is a video projector. In yet other embodiments, the display is a head-mounted display in communication with the digital processing device, such as a VR headset. In further embodiments, suitable VR headsets include, by way of non-limiting examples, HTC Vive, Oculus Rift, Samsung Gear VR, Microsoft HoloLens, Razer OSVR, FOVE VR, Zeiss VR One, Avegant Glyph, Freefly VR headset, and the like. In still further embodiments, the display is a combination of devices such as those disclosed herein.

[0092] In some embodiments, the digital processing device includes an input device to receive information from a user. In some embodiments, the input device is a keyboard. In some embodiments, the input device is a pointing device including, by way of non-limiting examples, a mouse, trackball, track pad, joystick, game controller, or stylus. In some embodiments, the input device is a touch screen or a multi-touch screen. In other embodiments, the input device is a microphone to capture voice or other sound input. In other embodiments, the input device is a video camera or other sensor to capture motion or visual input. In further embodiments, the input device is a Kinect, Leap Motion, or the like. In still further embodiments, the input device is a combination of devices such as those disclosed herein.

[0093] Referring to **FIG. 11**, in a particular embodiment, a digital processing device **1101** is programmed or otherwise configured to grant authorization to control a vehicle. In this embodiment, the digital processing device **1101** includes a central processing unit (CPU, also "processor" and "computer processor" herein) **1105**, which is optionally a single core, a multi core processor, or a plurality of processors for parallel processing. The digital processing device **1101** also includes memory or memory location **1110** (e.g., random-access memory, read-only memory, flash memory), electronic storage unit **1115** (e.g., hard disk), communication interface **1120** (e.g., network adapter) for communicating with one or more other systems, and peripheral devices **1125**, such as cache, other memory, data storage and/or electronic display adapters. The memory **1110**, storage unit **1115**, interface **1120** and peripheral devices **1125** are in communication with the CPU **1105** through a communication bus (solid lines), such as a motherboard. The storage unit **1115** comprises a data storage unit (or data repository) for storing data. The digital processing device **1101** is optionally operatively coupled to a computer network ("network") **1130** with the aid of the communication interface **1120**. The network **1130**, in various cases, is the internet, an internet, and/or extranet, or an intranet and/or extranet that is in communication with the internet. The network **1130**, in some cases, is a telecommunication and/or data network. The network **1130** optionally includes one or more computer servers, which

enable distributed computing, such as cloud computing. The network **1130**, in some cases, with the aid of the device **1101**, implements a peer-to-peer network, which enables devices coupled to the device **1101** to behave as a client or a server.

[0094] Continuing to refer to **FIG. 11**, the CPU **1105** is configured to execute a sequence of machine-readable instructions, embodied in a program, application, and/or software. The instructions are optionally stored in a memory location, such as the memory **1110**. The instructions are directed to the CPU **105**, which subsequently program or otherwise configure the CPU **1105** to implement methods of the present disclosure. Examples of operations performed by the CPU **1105** include fetch, decode, execute, and write back. The CPU **1105** is, in some cases, part of a circuit, such as an integrated circuit. One or more other components of the device **1101** are optionally included in the circuit. In some cases, the circuit is an application specific integrated circuit (ASIC) or a field programmable gate array (FPGA).

[0095] Continuing to refer to **FIG. 11**, the storage unit **1115** optionally stores files, such as drivers, libraries and saved programs. The storage unit **1115** optionally stores user data, e.g., user preferences and user programs. The digital processing device **1101**, in some cases, includes one or more additional data storage units that are external, such as located on a remote server that is in communication through an intranet or the internet.

[0096] Continuing to refer to **FIG. 11**, the digital processing device **1101** optionally communicates with one or more remote computer systems through the network **1130**. For instance, the device **1101** optionally communicates with a remote computer system of a user. Examples of remote computer systems include personal computers (e.g., portable PC), slate or tablet PCs (e.g., Apple® iPad, Samsung® Galaxy Tab, etc.), smartphones (e.g., Apple® iPhone, Android-enabled device, Blackberry®, etc.), or personal digital assistants.

[0097] Methods as described herein are optionally implemented by way of machine (e.g., computer processor) executable code stored on an electronic storage location of the digital processing device **101**, such as, for example, on the memory **1110** or electronic storage unit **1115**. The machine executable or machine readable code is optionally provided in the form of software. During use, the code is executed by the processor **1105**. In some cases, the code is retrieved from the storage unit **1115** and stored on the memory **1110** for ready access by the processor **1105**. In some situations, the electronic storage unit **1115** is precluded, and machine-executable instructions are stored on the memory **1110**.

Non-transitory computer readable storage medium

[0098] In some embodiments, the platforms, systems, media, and methods disclosed herein include one or more non-transitory computer readable storage media encoded with a program including instructions executable by the operating system of an optionally networked digital

processing device. In further embodiments, a computer readable storage medium is a tangible component of a digital processing device. In still further embodiments, a computer readable storage medium is optionally removable from a digital processing device. In some embodiments, a computer readable storage medium includes, by way of non-limiting examples, CD-ROMs, DVDs, flash memory devices, solid state memory, magnetic disk drives, magnetic tape drives, optical disk drives, cloud computing systems and services, and the like. In some cases, the program and instructions are permanently, substantially permanently, semi-permanently, or non-transitorily encoded on the media.

Computer program

[0099] In some embodiments, the platforms, systems, media, and methods disclosed herein include at least one computer program, or use of the same. A computer program includes a sequence of instructions, executable in the digital processing device's CPU, written to perform a specified task. Computer readable instructions may be implemented as program modules, such as functions, objects, Application Programming Interfaces (APIs), data structures, and the like, that perform particular tasks or implement particular abstract data types. In light of the disclosure provided herein, those of skill in the art will recognize that a computer program may be written in various versions of various languages.

[00100] The functionality of the computer readable instructions may be combined or distributed as desired in various environments. In some embodiments, a computer program comprises one sequence of instructions. In some embodiments, a computer program comprises a plurality of sequences of instructions. In some embodiments, a computer program is provided from one location. In other embodiments, a computer program is provided from a plurality of locations. In various embodiments, a computer program includes one or more software modules. In various embodiments, a computer program includes, in part or in whole, one or more web applications, one or more mobile applications, one or more standalone applications, one or more web browser plug-ins, extensions, add-ins, or add-ons, or combinations thereof.

Web application

[00101] In some embodiments, a computer program includes a web application. In light of the disclosure provided herein, those of skill in the art will recognize that a web application, in various embodiments, utilizes one or more software frameworks and one or more database systems. In some embodiments, a web application is created upon a software framework such as Microsoft® .NET or Ruby on Rails (RoR). In some embodiments, a web application utilizes one or more database systems including, by way of non-limiting examples, relational, non-relational,

object oriented, associative, and XML database systems. In further embodiments, suitable relational database systems include, by way of non-limiting examples, Microsoft® SQL Server, mySQL™, and Oracle®. Those of skill in the art will also recognize that a web application, in various embodiments, is written in one or more versions of one or more languages. A web application may be written in one or more markup languages, presentation definition languages, client-side scripting languages, server-side coding languages, database query languages, or combinations thereof. In some embodiments, a web application is written to some extent in a markup language such as Hypertext Markup Language (HTML), Extensible Hypertext Markup Language (XHTML), or eXtensible Markup Language (XML). In some embodiments, a web application is written to some extent in a presentation definition language such as Cascading Style Sheets (CSS). In some embodiments, a web application is written to some extent in a client-side scripting language such as Asynchronous Javascript and XML (AJAX), Flash® Actionscript, Javascript, or Silverlight®. In some embodiments, a web application is written to some extent in a server-side coding language such as Active Server Pages (ASP), ColdFusion®, Perl, Java™, JavaServer Pages (JSP), Hypertext Preprocessor (PHP), Python™, Ruby, Tcl, Smalltalk, WebDNA®, or Groovy. In some embodiments, a web application is written to some extent in a database query language such as Structured Query Language (SQL). In some embodiments, a web application integrates enterprise server products such as IBM® Lotus Domino®. In some embodiments, a web application includes a media player element. In various further embodiments, a media player element utilizes one or more of many suitable multimedia technologies including, by way of non-limiting examples, Adobe® Flash®, HTML 5, Apple® QuickTime®, Microsoft® Silverlight®, Java™, and Unity®.

[00102] Referring to **FIG. 12**, in a particular embodiment, an application provision system comprises one or more databases **1200** accessed by a relational database management system (RDBMS) **1210**. Suitable RDBMSs include Firebird, MySQL, PostgreSQL, SQLite, Oracle Database, Microsoft SQL Server, IBM DB2, IBM Informix, SAP Sybase, SAP Sybase, Teradata, and the like. In this embodiment, the application provision system further comprises one or more application severs **1220** (such as Java servers, .NET servers, PHP servers, and the like) and one or more web servers **1230** (such as Apache, IIS, GWS and the like). The web server(s) optionally expose one or more web services via app application programming interfaces (APIs) **1240**. Via a network, such as the internet, the system provides browser-based and/or mobile native user interfaces.

[00103] Referring to **FIG. 13**, in a particular embodiment, an application provision system alternatively has a distributed, cloud-based architecture **1300** and comprises elastically load

balanced, auto-scaling web server resources **1310,** and application server resources **1320** as well synchronously replicated databases **1330**.

Mobile Application

[00104] In some embodiments, a computer program includes a mobile application provided to a mobile digital processing device. In some embodiments, the mobile application is provided to a mobile digital processing device at the time it is manufactured. In other embodiments, the mobile application is provided to a mobile digital processing device via the computer network described herein.

[00105] In view of the disclosure provided herein, a mobile application is created by techniques known to those of skill in the art using hardware, languages, and development environments known to the art. Those of skill in the art will recognize that mobile applications are written in several languages. Suitable programming languages include, by way of non-limiting examples, C, C++, C#, Objective-C, Java™, Javascript, Pascal, Object Pascal, Python™, Ruby, VB.NET, WML, and XHTML/HTML with or without CSS, or combinations thereof.

[00106] Suitable mobile application development environments are available from several sources. Commercially available development environments include, by way of non-limiting examples, AirplaySDK, alcheMo, Appcelerator®, Celsius, Bedrock, Flash Lite, .NET Compact Framework, Rhomobile, and WorkLight Mobile Platform. Other development environments are available without cost including, by way of non-limiting examples, Lazarus, MobiFlex, MoSync, and Phonegap. Also, mobile device manufacturers distribute software developer kits including, by way of non-limiting examples, iPhone and iPad (iOS) SDK, Android™ SDK, BlackBerry® SDK, BREW SDK, Palm® OS SDK, Symbian SDK, webOS SDK, and Windows® Mobile SDK.

[00107] Those of skill in the art will recognize that several commercial forums are available for distribution of mobile applications including, by way of non-limiting examples, Apple® App Store, Google® Play, Chrome WebStore, BlackBerry® App World, App Store for Palm devices, App Catalog for webOS, Windows® Marketplace for Mobile, Ovi Store for Nokia® devices, Samsung® Apps, and Nintendo® DSi Shop.

Standalone Application

[00108] In some embodiments, a computer program includes a standalone application, which is a program that is run as an independent computer process, not an add-on to an existing process, e.g., not a plug-in. Those of skill in the art will recognize that standalone applications are often compiled. A compiler is a computer program(s) that transforms source code written in a programming language into binary object code such as assembly language or machine code.

Suitable compiled programming languages include, by way of non-limiting examples, C, C++, Objective-C, COBOL, Delphi, Eiffel, Java™, Lisp, Python™, Visual Basic, and VB .NET, or combinations thereof. Compilation is often performed, at least in part, to create an executable program. In some embodiments, a computer program includes one or more executable complied applications.

Web Browser Plug-in

[00109] In some embodiments, the computer program includes a web browser plug-in (e.g., extension, etc.). In computing, a plug-in is one or more software components that add specific functionality to a larger software application. Makers of software applications support plug-ins to enable third-party developers to create abilities which extend an application, to support easily adding new features, and to reduce the size of an application. When supported, plug-ins enables customizing the functionality of a software application. For example, plug-ins are commonly used in web browsers to play video, generate interactivity, scan for viruses, and display particular file types. Those of skill in the art will be familiar with several web browser plug-ins including, Adobe® Flash® Player, Microsoft® Silverlight®, and Apple® QuickTime®.

[00110] In view of the disclosure provided herein, those of skill in the art will recognize that several plug-in frameworks are available that enable development of plug-ins in various programming languages, including, by way of non-limiting examples, C++, Delphi, Java™, PHP, Python™, and VB .NET, or combinations thereof.

[00111] Web browsers (also called Internet browsers) are software applications, designed for use with network-connected digital processing devices, for retrieving, presenting, and traversing information resources on the World Wide Web. Suitable web browsers include, by way of non-limiting examples, Microsoft® Internet Explorer®, Mozilla® Firefox®, Google® Chrome, Apple® Safari®, Opera Software® Opera®, and KDE Konqueror. In some embodiments, the web browser is a mobile web browser. Mobile web browsers (also called mircrobrowsers, mini-browsers, and wireless browsers) are designed for use on mobile digital processing devices including, by way of non-limiting examples, handheld computers, tablet computers, netbook computers, subnotebook computers, smartphones, music players, personal digital assistants (PDAs), and handheld video game systems. Suitable mobile web browsers include, by way of non-limiting examples, Google® Android® browser, RIM BlackBerry® Browser, Apple® Safari®, Palm® Blazer, Palm® WebOS® Browser, Mozilla® Firefox® for mobile, Microsoft® Internet Explorer® Mobile, Amazon® Kindle® Basic Web, Nokia® Browser, Opera Software® Opera® Mobile, and Sony® PSP™ browser.

Software Modules

[00112] In some embodiments, the platforms, systems, media, and methods disclosed herein include software, server, and/or database modules, or use of the same. In view of the disclosure provided herein, software modules are created by techniques known to those of skill in the art using machines, software, and languages known to the art. The software modules disclosed herein are implemented in a multitude of ways. In various embodiments, a software module comprises a file, a section of code, a programming object, a programming structure, or combinations thereof. In further various embodiments, a software module comprises a plurality of files, a plurality of sections of code, a plurality of programming objects, a plurality of programming structures, or combinations thereof. In various embodiments, the one or more software modules comprise, by way of non-limiting examples, a web application, a mobile application, and a standalone application. In some embodiments, software modules are in one computer program or application. In other embodiments, software modules are in more than one computer program or application. In some embodiments, software modules are hosted on one machine. In other embodiments, software modules are hosted on more than one machine. In further embodiments, software modules are hosted on cloud computing platforms. In some embodiments, software modules are hosted on one or more machines in one location. In other embodiments, software modules are hosted on one or more machines in more than one location.

Databases

[00113] In some embodiments, the platforms, systems, media, and methods disclosed herein include one or more databases, or use of the same. In view of the disclosure provided herein, those of skill in the art will recognize that many databases are suitable for storing information regarding users, vehicles, mobile devices, communication units, and vehicle control modules. In various embodiments, suitable databases include, by way of non-limiting examples, relational databases, non-relational databases, object oriented databases, object databases, entity-relationship model databases, associative databases, and XML databases. Further non-limiting examples include SQL, PostgreSQL, MySQL, Oracle, DB2, and Sybase. In some embodiments, a database is internet-based. In further embodiments, a database is web-based. In still further embodiments, a database is cloud computing-based. In other embodiments, a database is based on one or more local computer storage devices.

CLAIMS

WHAT IS CLAIMED IS:

1. A mobile device based system for granting authorization to control a vehicle comprising:
    a. a communication unit;
    b. a vehicle control module that is separate and distinct from the communication unit; and
    c. a mobile device capable of receiving a user input and a first signal, and sending a second signal, wherein the mobile device comprises at least one mobile application including executable instructions to control the vehicle, the mobile application configured for:
        i. receiving the first signal from an internet, a cellular network, a server, or any combination thereof;
        ii. storing the first signal;
        iii. receiving the user input; and
        iv. sending the second signal to the communication unit in response to receiving the user input;

    wherein the first and second signals both comprise a common unique identifier;

    wherein the communication unit is capable of receiving the second signal from the mobile device and sending a third signal to the vehicle control module; and

    wherein the vehicle control module is capable of receiving the third signal and sending a command to a receiver within the vehicle.

2. The system of claim 1, wherein the mobile application is configured for performing the executable instruction of sending the second signal to the communication unit with and without access to the internet, the cellular network, or the server.

3. The system of claim 1, wherein the communication unit is further capable of receiving a fourth signal comprising a vehicle status, from the vehicle.

4. The system of claim 1, wherein the unique identifier comprises an encrypted identifier, a signed identifier, or both.

5. The system of claim 4, wherein the communication unit is capable of decrypting the encrypted identifier, validating the identifier, or both without access to the internet, the cellular network, or the server.

6. The system of claim 4, wherein the mobile device is capable of receiving the first signal, storing the first signal, and sending the second signal without generating, validating, or decrypting the unique identifier.

7. The system of claim 1, wherein the communication unit is further capable of receiving a fifth signal, equivalent to the second signal, from a source other than the mobile device.

8. The system of claim 1, wherein the mobile application further comprises an executable instruction of granting a second user the authorization to control the vehicle.

9. The system of claim 1, wherein the second signal further comprises a request for a challenge from the communication unit.

10. The system of claim 9, wherein the first signal further comprises a key, and wherein the mobile device signs the challenge with the key.

11. A method of granting authorization to control a vehicle comprising:
    a. a mobile device receiving a first signal, and sending a second signal;
    b. the mobile device storing the first signal;
    c. a user submitting an input to the mobile device;
    d. the mobile device sending a second signal to a communication unit;
    e. the communication unit receiving the second signal from the mobile device;
    f. the communication unit sending a third signal to a vehicle control module;
    g. the vehicle control module receiving the third signal; and
    h. the vehicle control module sending a command to a receiver within the vehicle;

    wherein the first and second signals both comprise a common unique identifier; and

    wherein the vehicle control module is in wired or wireless connection with the communication unit and the vehicle.

12. The method of claim 11, wherein the mobile device sends the second signal to the communication unit with or without accessing the internet, the cellular network, or the server.

13. The method of claim 11, further comprising the communication unit receiving a fourth signal comprising a vehicle status, from the OBD port of the vehicle.

14. The method of claim 11, wherein the unique identifier comprises an encrypted identifier, a signed identifier, or both.

15. The method of claim 11, wherein the communication unit is capable of decrypting the encrypted identifier, validating the identifier, or both without access to the internet, the cellular network, or the server.

16. The method of claim 15, wherein the mobile device receives the first signal, stores the first signal, and sends the second signal without generating, validating, or decrypting the unique identifier.

17. The method of claim 11, further comprising the communication unit receiving a fifth signal, equivalent to the second signal, from a source other than the mobile device.

18. The method of claim 11, further comprising granting a second user the authorization to control the vehicle.

19. The method of claim 11, wherein the second signal further comprises a request for a challenge from the communication unit.

20. The method of claim 11 wherein the first signal further comprises a key, and wherein the mobile device signs the challenge with the key.

FIG. 1

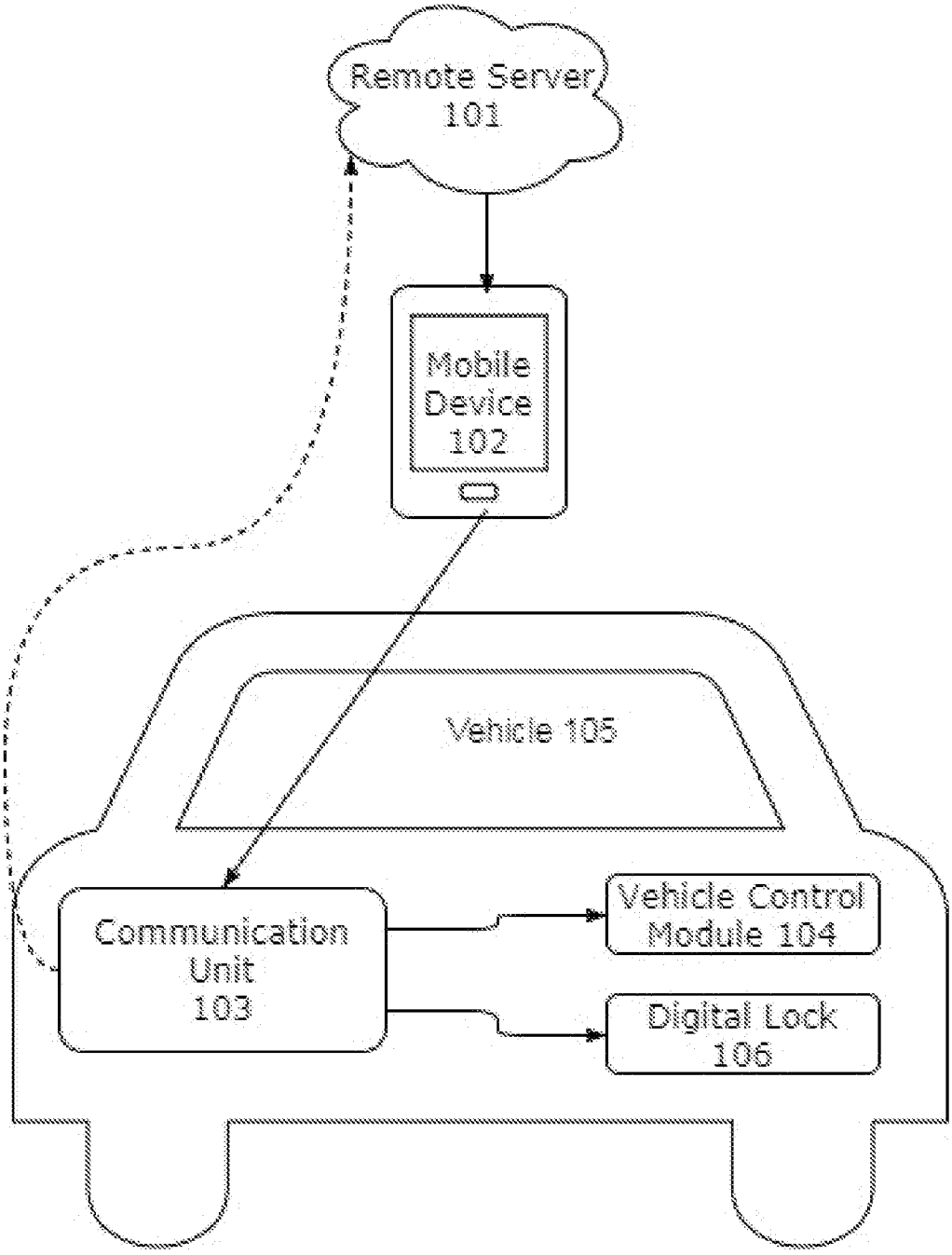

Remote Server
101
Mobile
Device
102
Vehicle 105
Communication
Unit
103
Vehicle Control
Module 104
Digital Lock
106

FIG. 2

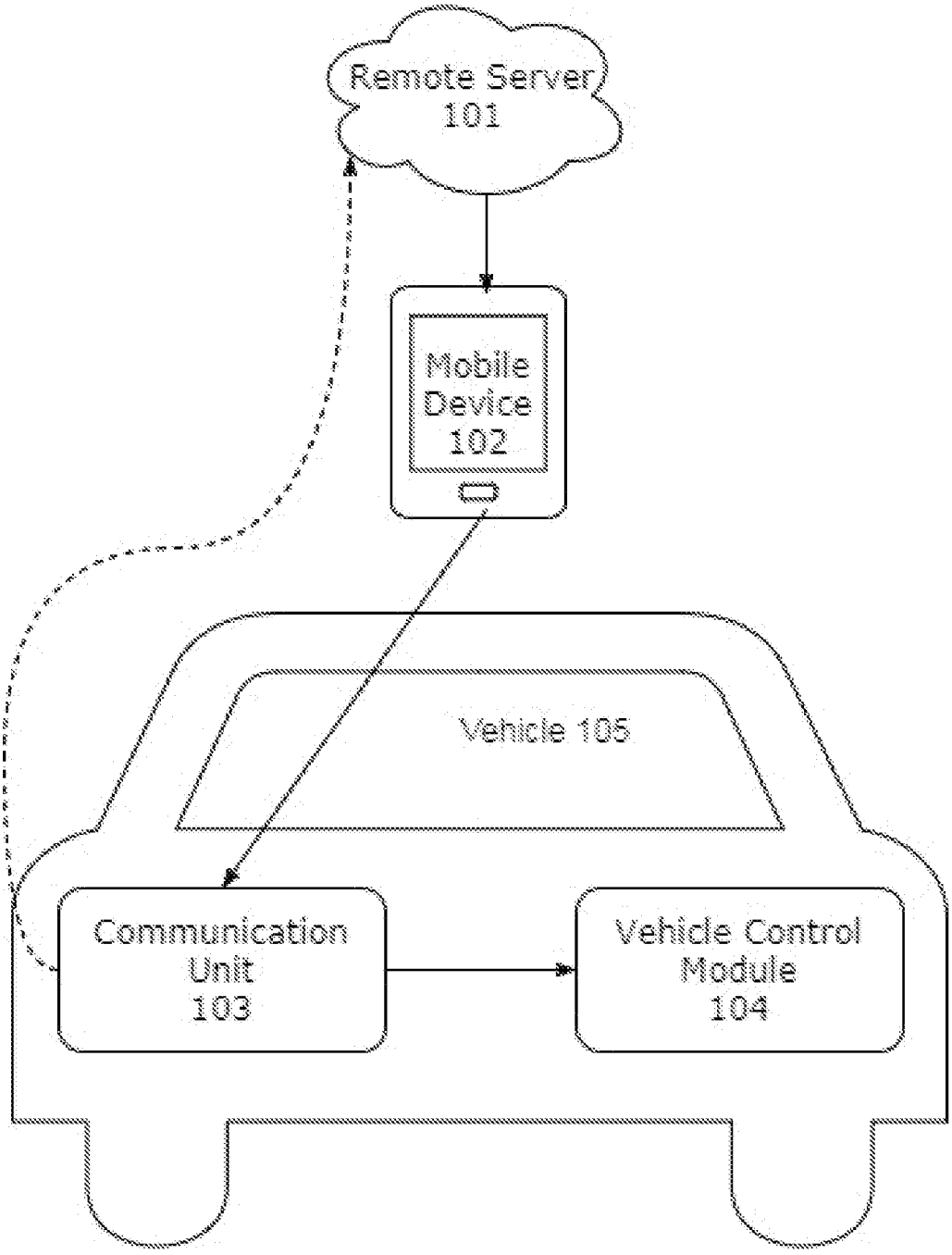

Remote Server
101
Mobile
Device
102
Vehicle 105
Communication
Unit
103
Vehicle Control
Module
104

FIG. 3

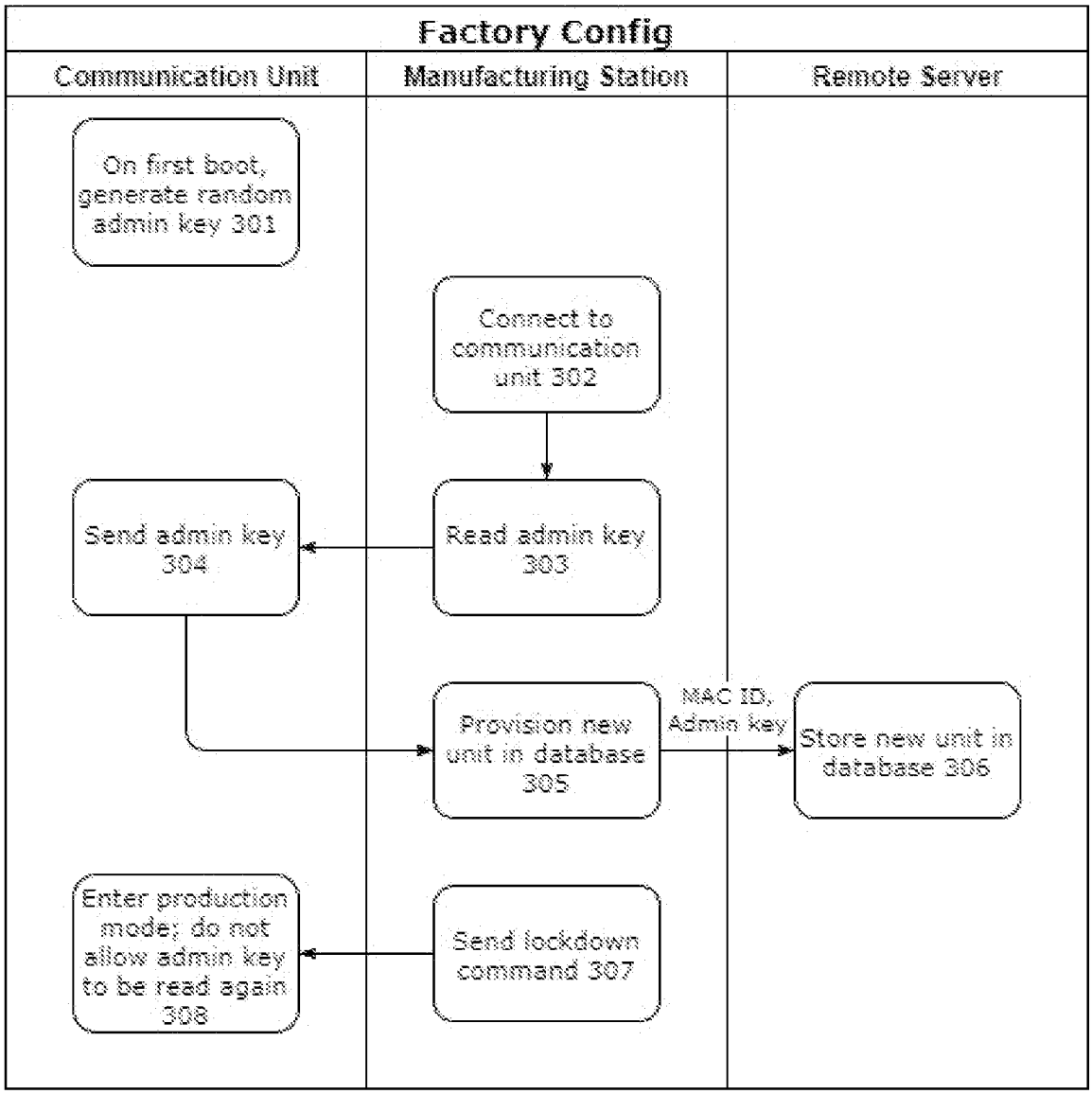

Factory Config
Communication Unit
Manufacturing Station
Remote Server
On first boot, generate random admin key 301
Connect to communication unit 302
Send admin key 304
Read admin key 303
Provision new unit in database 305
MAC ID, Admin key
Store new unit in database 306
Enter production mode; do not allow admin key to be read again 308
Send lockdown command 307

FIG. 4

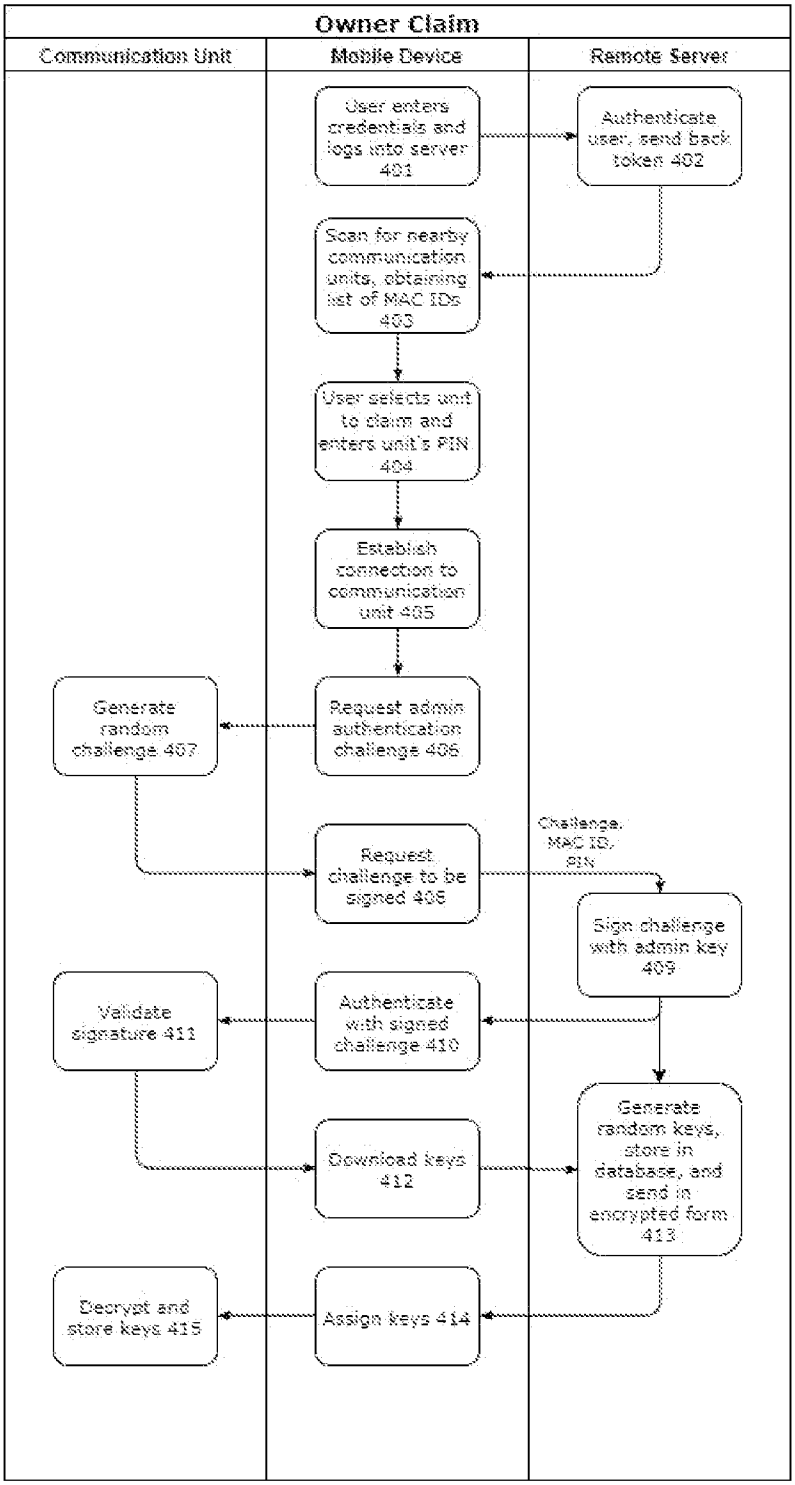

Owner Claim
Communication Unit
Mobile Device
Remote Server
User enters credentials and logs into server 401
Authenticate user, send back token 402
Scan for nearby communication units, obtaining list of MAC IDs 403
User selects unit to claim and enters unit's PIN 404
Establish connection to communication unit 405
Request admin authentication challenge 406
Generate random challenge 407
Request challenge to be signed 408
Challenge, MAC ID, PIN
Sign challenge with admin key 409
Authenticate with signed challenge 410
Validate signature 411
Download keys 412
Generate random keys, store in database, and send in encrypted form 413
Assign keys 414
Decrypt and store keys 415

FIG. 5

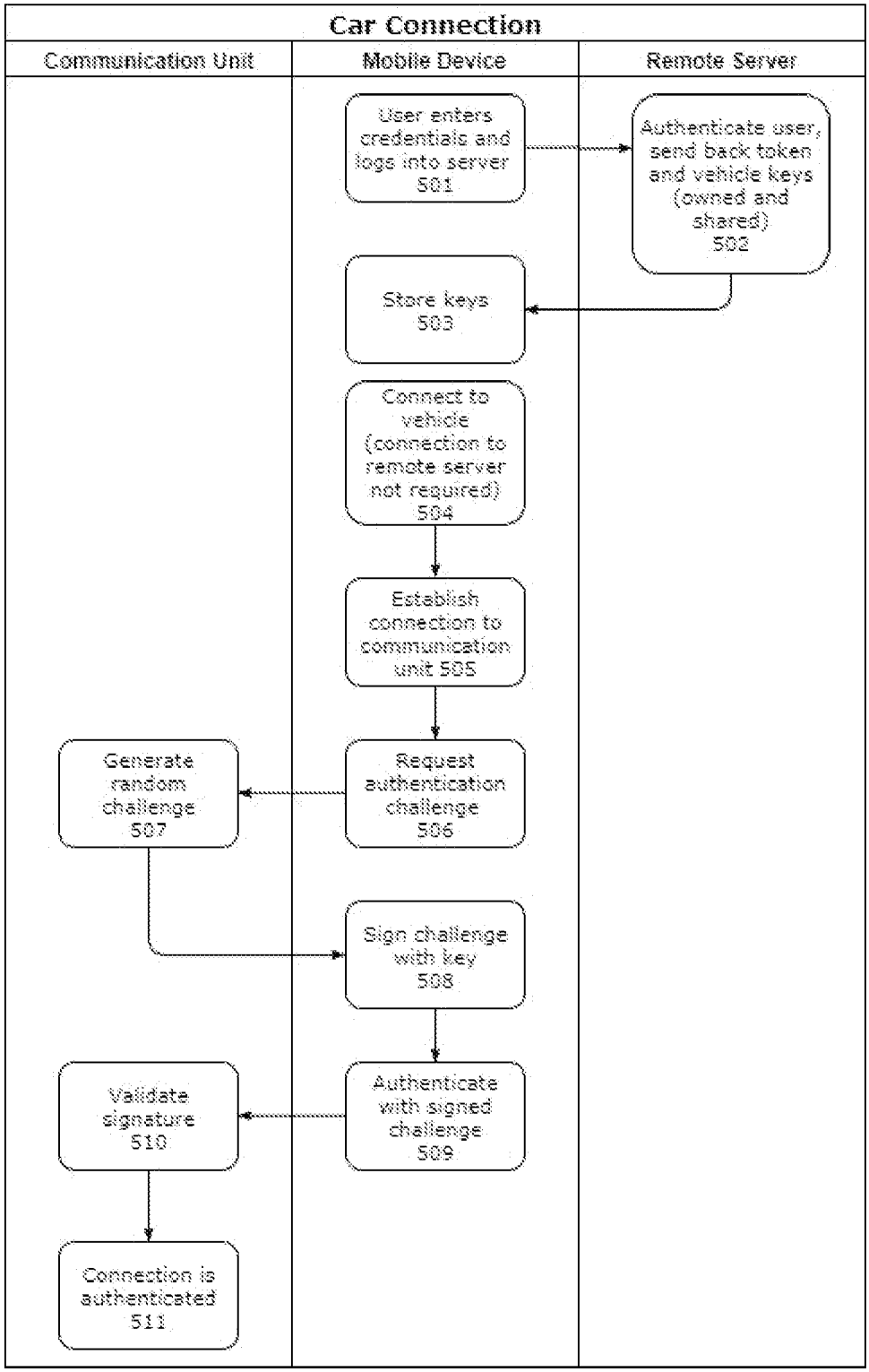

Car Connection
Communication Unit
Mobile Device
Remote Server
User enters credentials and logs into server 501
Authenticate user, send back token and vehicle keys (owned and shared) 502
Store keys 503
Connect to vehicle (connection to remote server not required) 504
Establish connection to communication unit 505
Request authentication challenge 506
Generate random challenge 507
Sign challenge with key 508
Authenticate with signed challenge 509
Validate signature 510
Connection is authenticated 511

FIG. 6

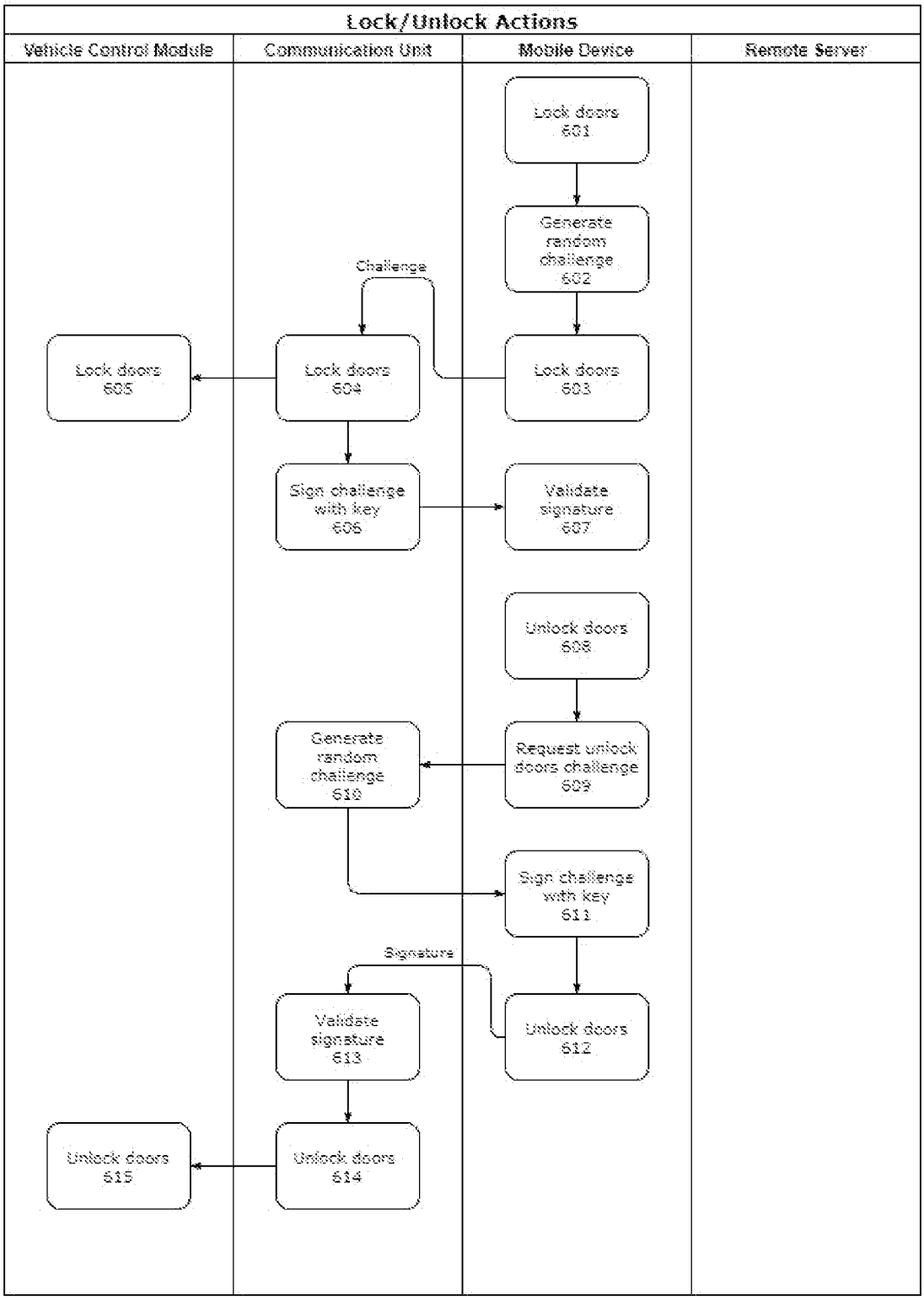

Lock/Unlock Actions
Vehicle Control Module
Communication Unit
Mobile Device
Remote Server
Lock doors 601
Generate random challenge 602
Challenge
Lock doors 603
Lock doors 604
Lock doors 605
Sign challenge with key 606
Validate signature 607
Unlock doors 608
Request unlock doors challenge 609
Generate random challenge 610
Sign challenge with key 611
Signature
Unlock doors 612
Validate signature 613
Unlock doors 614
Unlock doors 615

FIG. 7

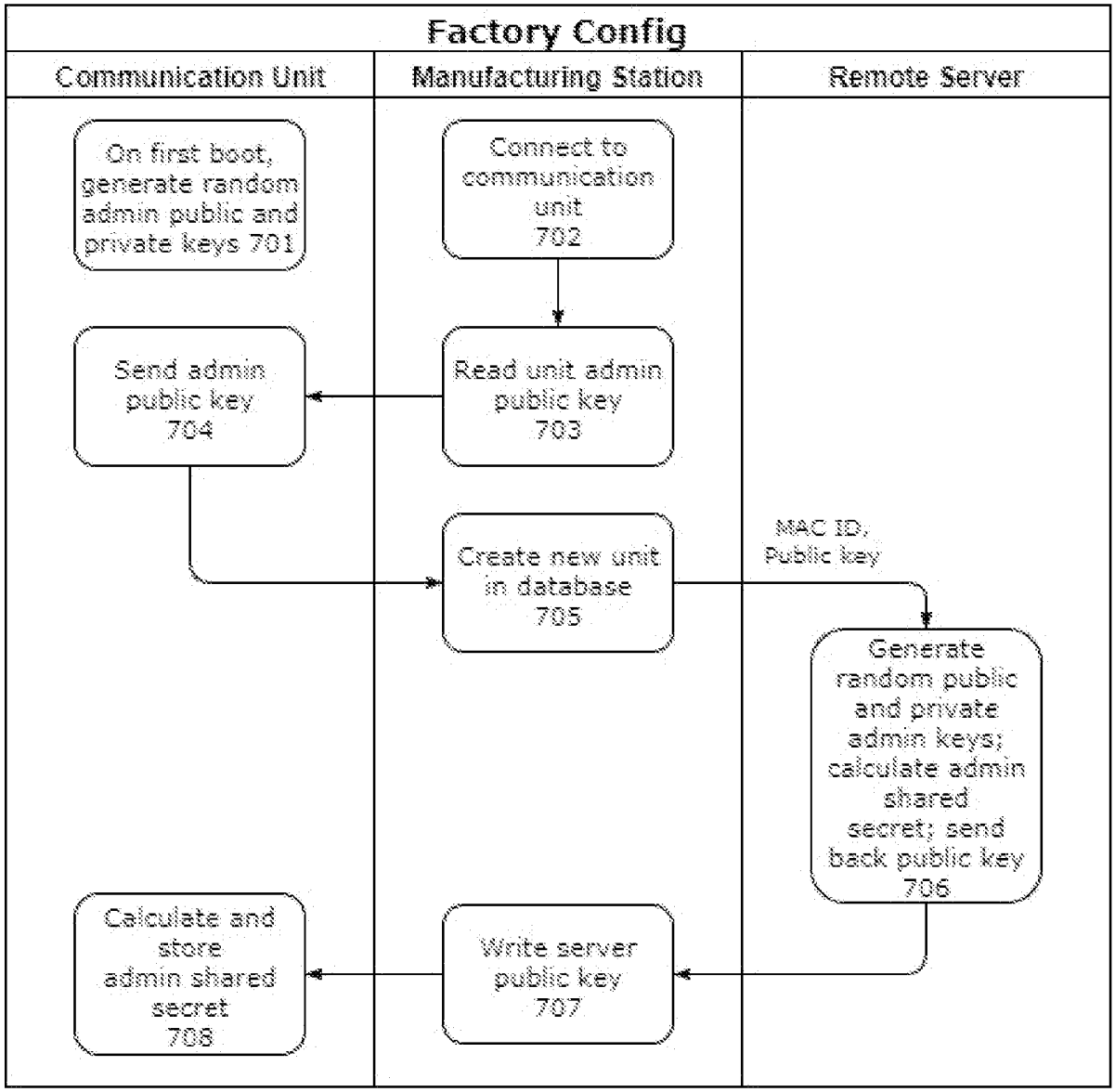

Factory Config
Communication Unit
Manufacturing Station
Remote Server
On first boot, generate random admin public and private keys 701
Connect to communication unit 702
Send admin public key 704
Read unit admin public key 703
Create new unit in database 705
MAC ID, Public key
Generate random public and private admin keys; calculate admin shared secret; send back public key 706
Calculate and store admin shared secret 708
Write server public key 707

FIG. 8

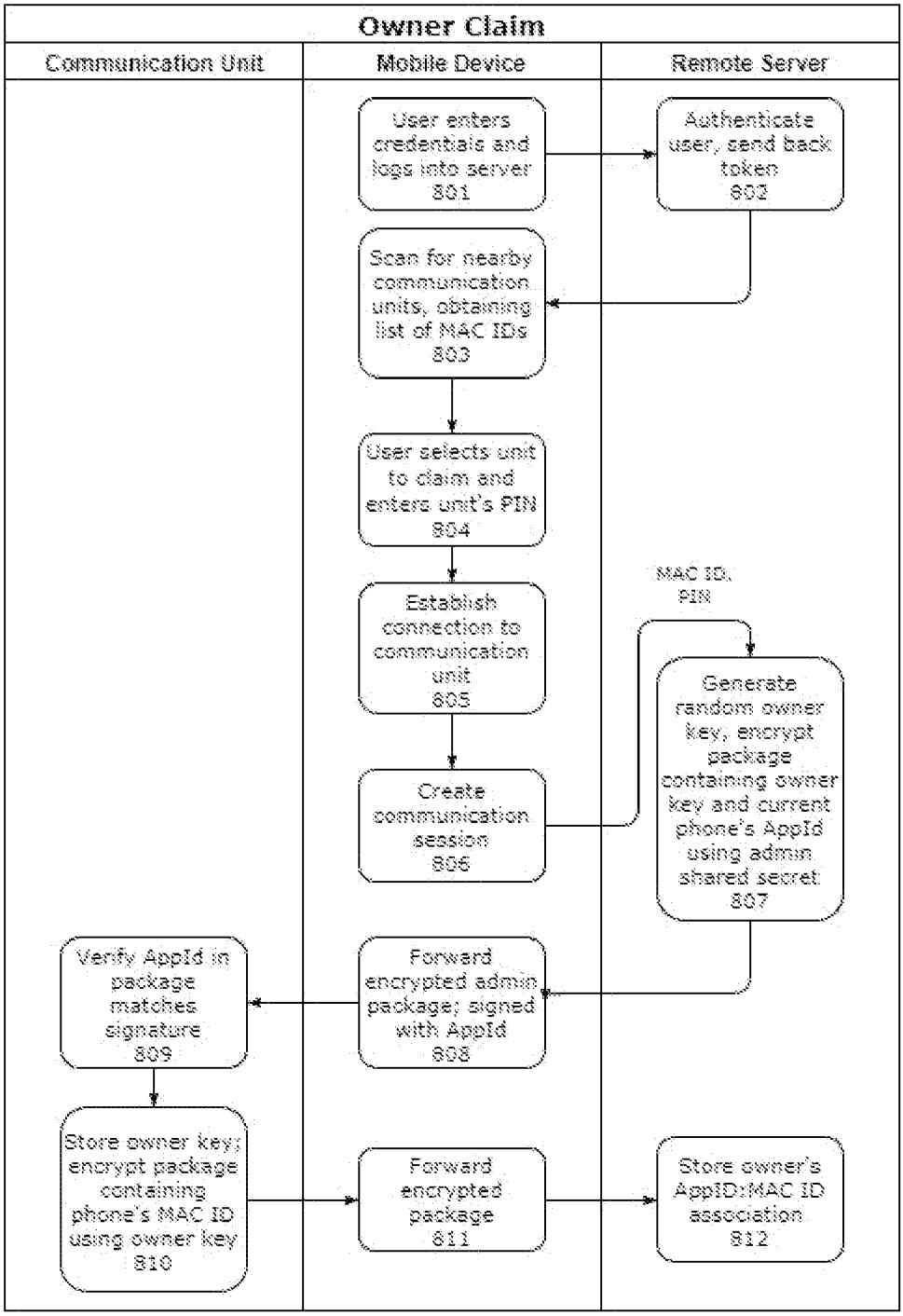

Owner Claim
Communication Unit
Mobile Device
Remote Server
User enters credentials and logs into server 801
Authenticate user, send back token 802
Scan for nearby communication units, obtaining list of MAC IDs 803
User selects unit to claim and enters unit's PIN 804
Establish connection to communication unit 805
Create communication session 806
MAC ID, PIN
Generate random owner key, encrypt package containing owner key and current phone's AppId using admin shared secret 807
Forward encrypted admin package; signed with AppId 808
Verify AppId in package matches signature 809
Store owner key; encrypt package containing phone's MAC ID using owner key 810
Forward encrypted package 811
Store owner's AppID:MAC ID association 812

FIG. 9

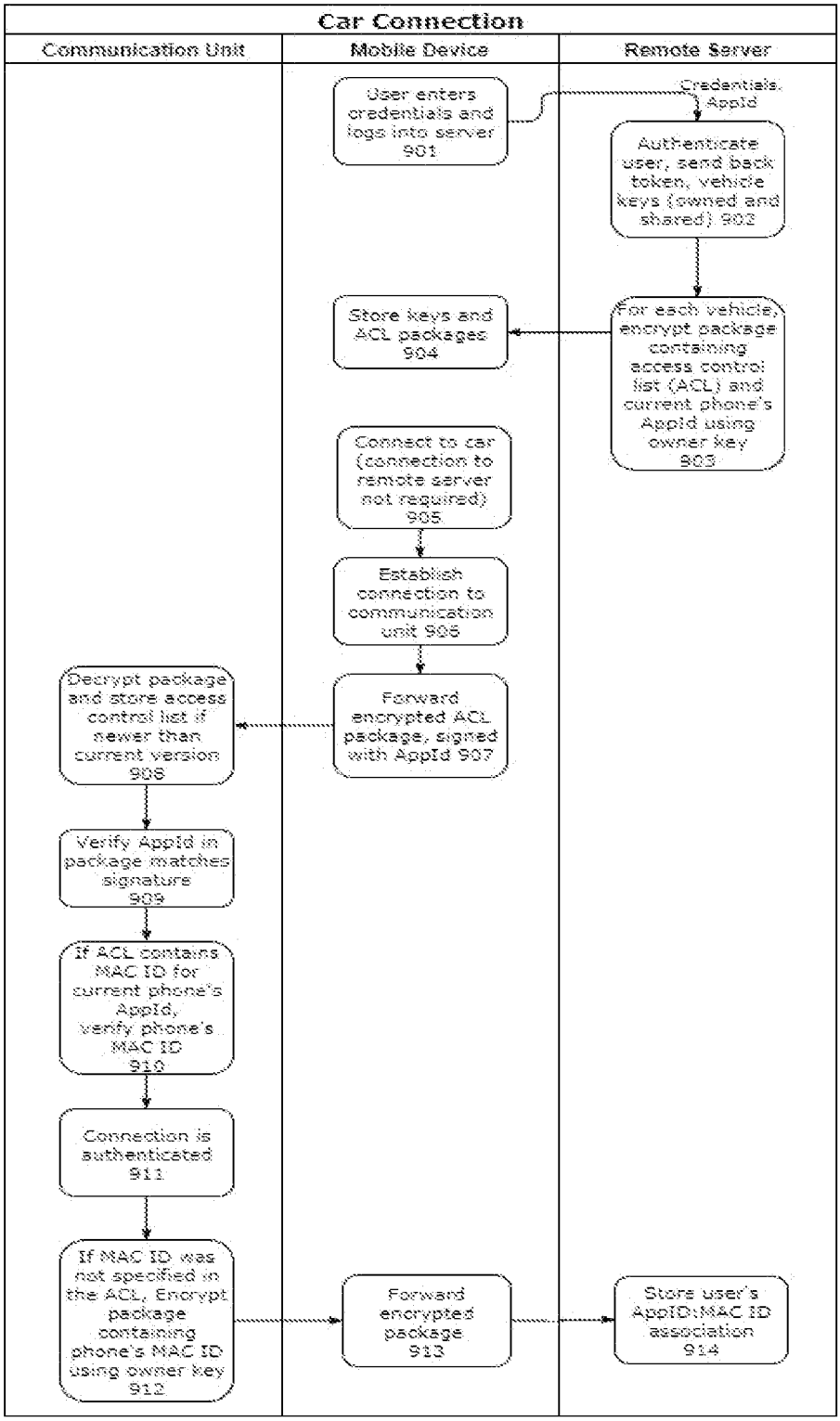

Car Connection
Communication Unit
Mobile Device
Remote Server
User enters credentials and logs into server 901
Credentials, AppId
Authenticate user, send back token, vehicle keys (owned and shared) 902
For each vehicle, encrypt package containing access control list (ACL) and current phone's AppId using owner key 903
Store keys and ACL packages 904
Connect to car (connection to remote server not required) 905
Establish connection to communication unit 906
Forward encrypted ACL package, signed with AppId 907
Decrypt package and store access control list if newer than current version 908
Verify AppId in package matches signature 909
If ACL contains MAC ID for current phone's AppId, verify phone's MAC ID 910
Connection is authenticated 911
If MAC ID was not specified in the ACL, Encrypt package containing phone's MAC ID using owner key 912
Forward encrypted package 913
Store user's AppID:MAC ID association 914

FIG. 10

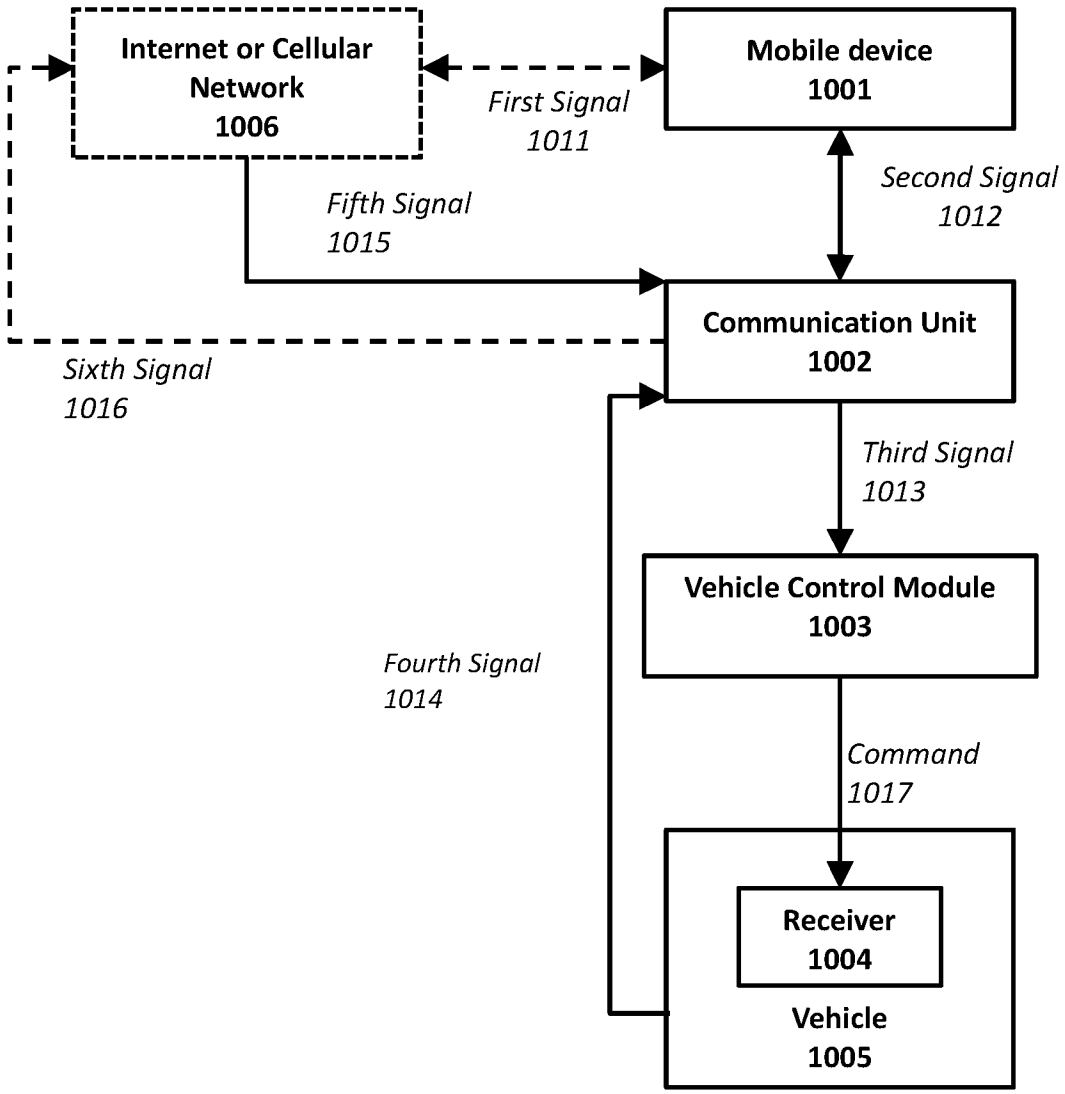

Internet or Cellular Network 1006
Mobile device 1001
First Signal 1011
Second Signal 1012
Fifth Signal 1015
Communication Unit 1002
Sixth Signal 1016
Third Signal 1013
Vehicle Control Module 1003
Fourth Signal 1014
Command 1017
Receiver 1004
Vehicle 1005

FIG. 11

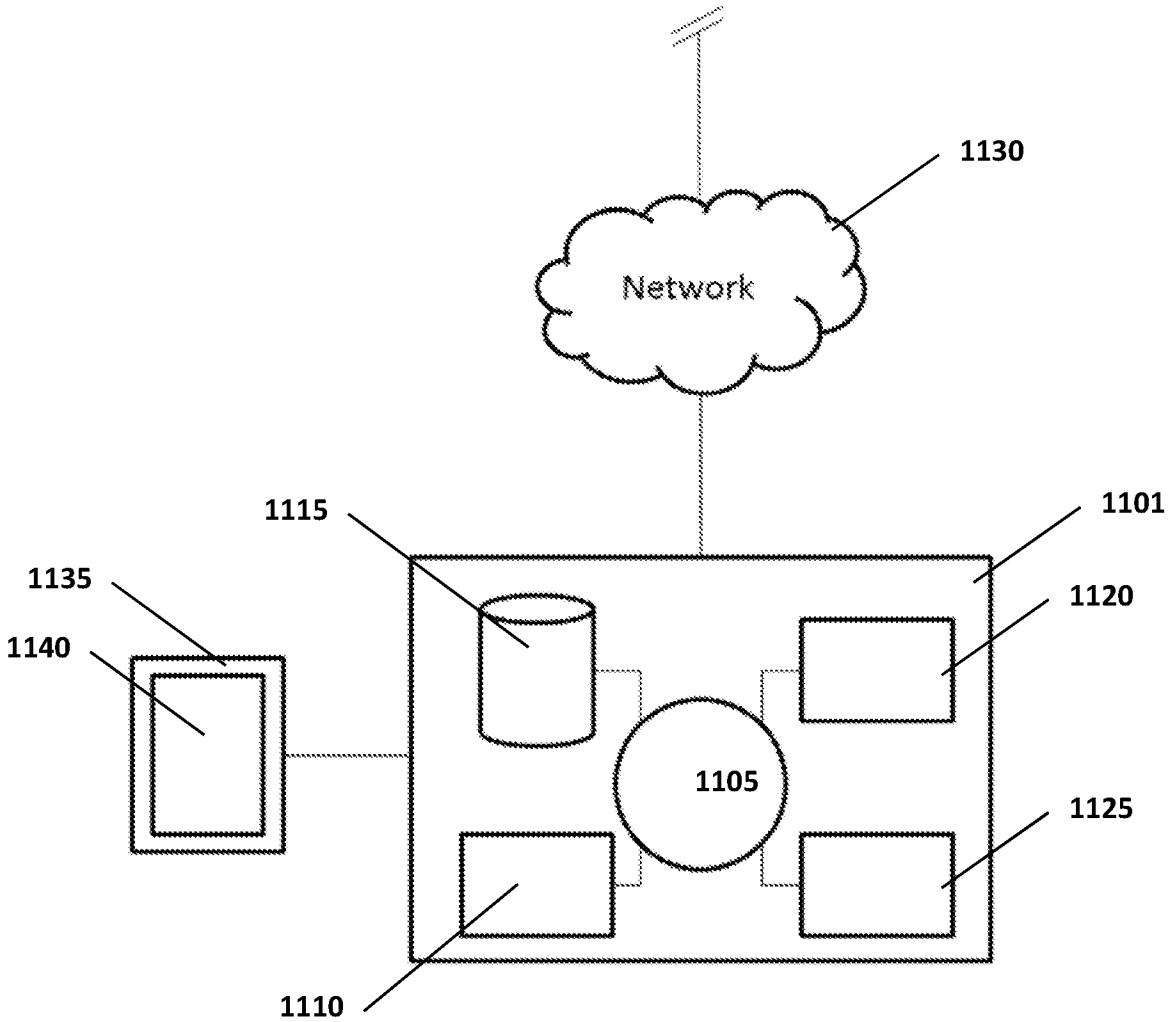


FIG. 12

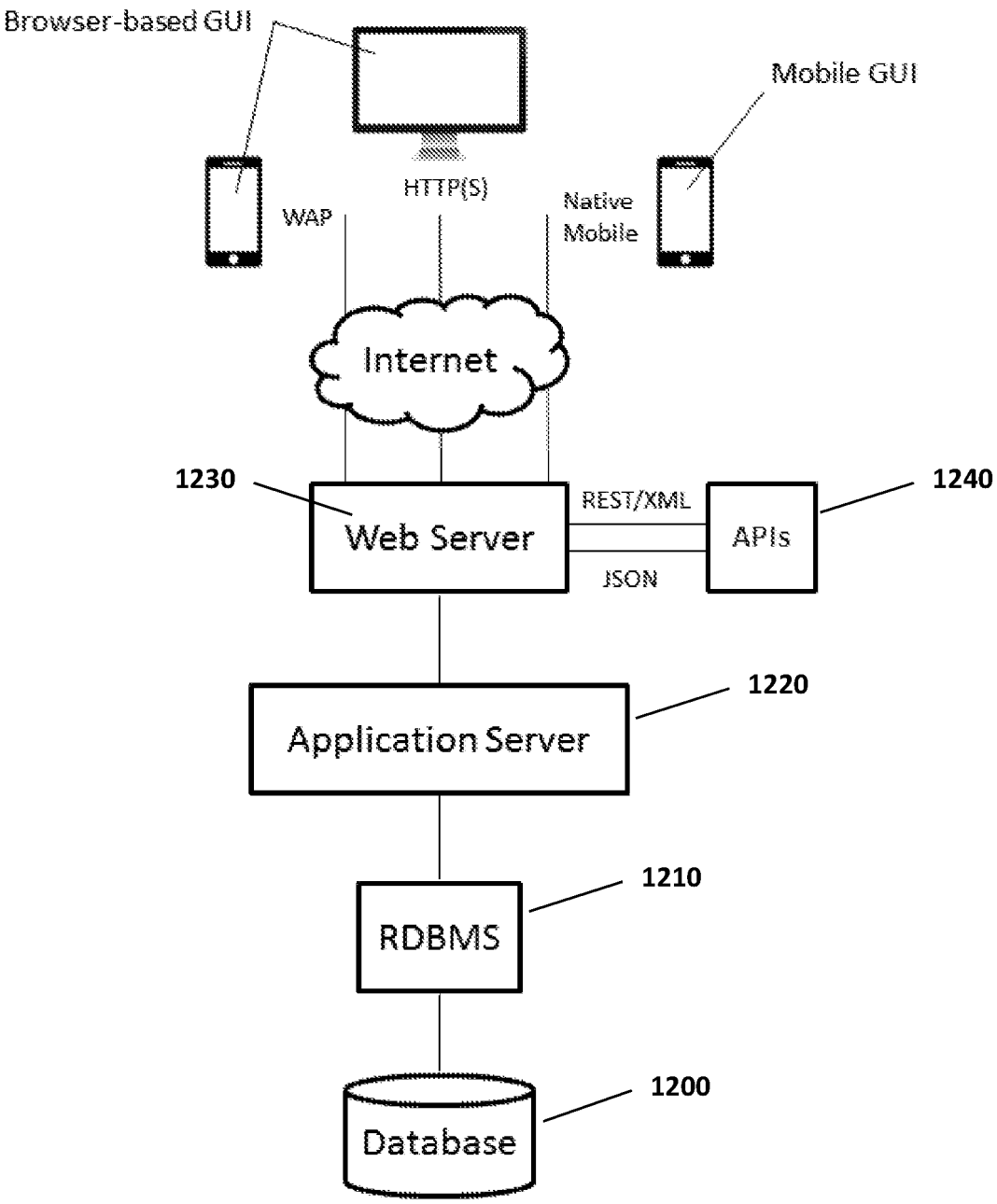
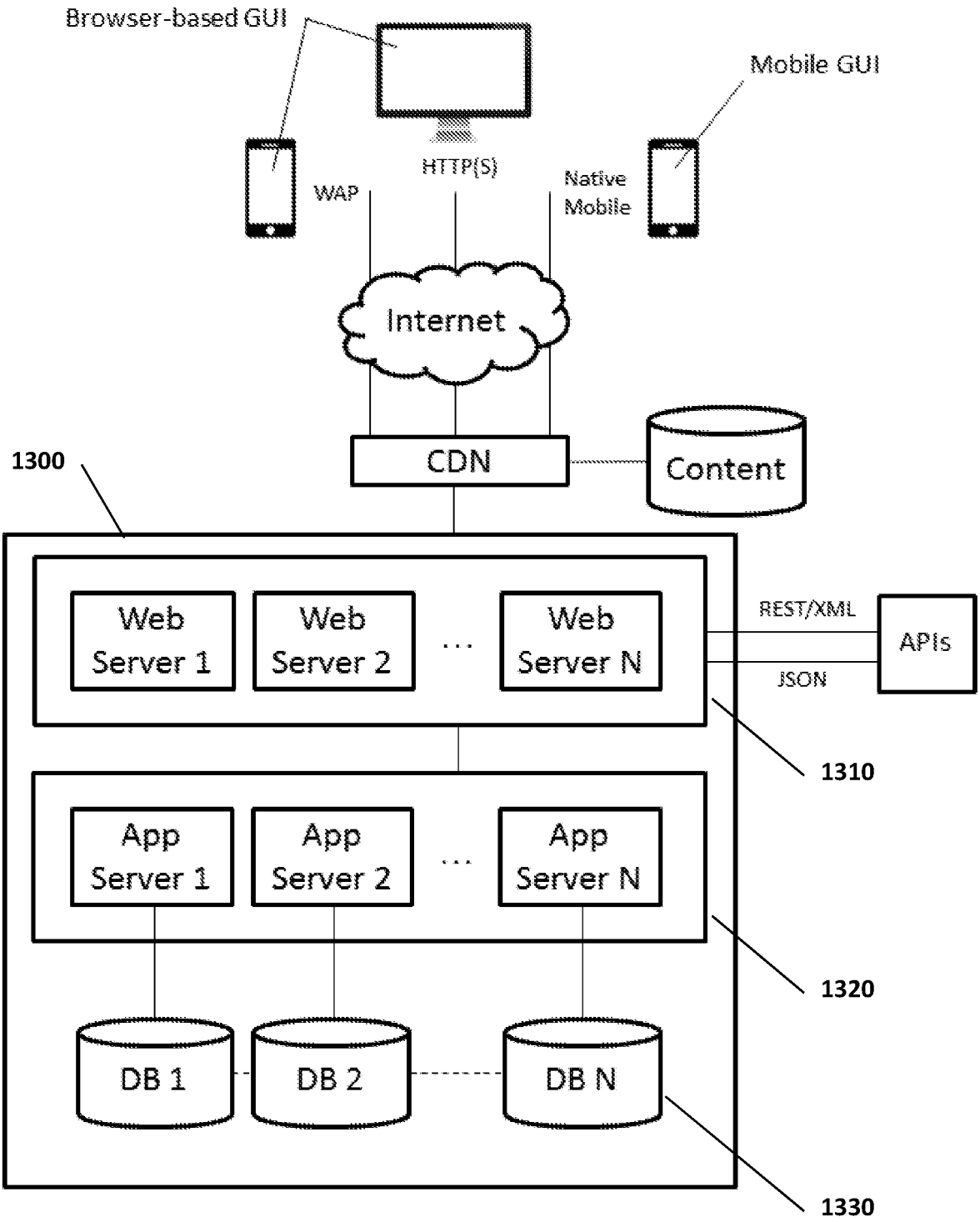

Browser-based GUI
Mobile GUI
HTTP(S)
WAP
Native
Mobile
Internet
1230
Web Server
REST/XML
JSON
APIs
1240
Application Server
1220
RDBMS
1210
Database
1200

FIG. 13


Browser-based GUI
Mobile GUI
HTTP(S)
WAP
Native Mobile
Internet
CDN
Content
1300
Web Server 1
Web Server 2
...
Web Server N
REST/XML
JSON
APIs
1310
App Server 1
App Server 2
...
App Server N
1320
DB 1
DB 2
DB N
1330

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB2018/001213

A. CLASSIFICATION OF SUBJECT MATTER
IPC: ***H04W 4/40*** (2018.01), ***B60R 25/102*** (2013.01), ***B60R 25/20*** (2013.01), ***G08C 17/02*** (2006.01), ***H04W 12/06*** (2009.01)

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)
H04W 4/40 (2018.01), B60R 25/102 (2013.01), B60R 25/20 (2013.01), G08C 17/02 (2006.01), H04W 12/06 (2009.01)

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

Electronic database(s) consulted during the international search (name of database(s) and, where practicable, search terms used)
Databases: Questel Orbit, Canadian Patent Database (Intellect), IEEE Xplore, Google Patents
Keywords: car, vehicle, auto, mobile, device, cellphone, phone, control, identifier, token, unique, encrypt, signature, key, challenge, engine, ignition, unlock, control, wireless, command, instruction, sign, signature

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	US8736438B1 (Vasquez et al.), 27 May 2014 (27-05-2014) *col 3, lines 28-39; col 4, lines 5-9, 13-21; col 5, line 21 to col 6, line 16; Col 7, lines 14-18; col 9, line 64 to col 10 line; col 11, lines 16-30; Abstract, claims 1, 18; Figures 1, 2*	11-20 1-10
Y	US8831224B2 (Bai et al.), 09 September 2014 (09-09-2014) *col 4, lines 41-53*	1-10

☐ 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 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 14 February 2019 (14-02-2019)	Date of mailing of the international search report 14 February 2019 (14-02-2019)
Name and mailing address of the ISA/CA Canadian Intellectual Property Office Place du Portage I, C114 - 1st Floor, Box PCT 50 Victoria Street Gatineau, Quebec K1A 0C9 Facsimile No.: 819-953-2476	Authorized officer Darren Cassidy (819) 635-4278

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/IB2018/001213

Patent Document Cited in Search Report	Publication Date	Publication Family Member(s)	Publication Date
US8736438B1	27 May 2014 (27-05-2014)		None
US8831224B2	09 September 2014 (09-09-2014)	US2014079217A1	20 March 2014 (20-03-2014)
		US8831224B2	09 September 2014 (09-09-2014)
		CN103686713A	26 March 2014 (26-03-2014)
		CN103686713B	26 April 2017 (26-04-2017)