

***Kia Corp. and Toyota Motor Corp. v.
Emerging Automotive LLC***

IPR2024-01167

U.S. Patent No. 11,738,659

Petitioner's Demonstratives

Hearing: October 27, 2025

Table of Contents

Topic	Slide
'659 Patent Overview	8
Summary of Prior Art	10
Ground 1: Kleve discloses that the e-key “request includes condition of use” and that an e-key is “assigned” with that condition (All claims)	26
Ground 3: Mikan renders obvious an e-key associated with “coded data” that includes “privilege settings” (All claims)	75
Dependent Claim 6: Kleve and Mikan render obvious “sharing of said eKey with a recipient user”	94
Dependent Claims 12, 13, and 20: Kleve and Mikan Disclose or Render Obvious a “server” or “application” “associated with a vehicle manufacturer”	102

Summary: Grounds

Ground	Claim(s) challenged
1. Kleve + Hatton	1, 3-21
2. Kleve + Hatton + Sekiyama	2
3. Mikan	1-3, 5, 8-10
4. Mikan + Xiao	4, 11-18, 20-21
5. Mikan + Sekiyama	6-7
6. Mikan + Xiao + Sekiyama	19

Summary: Disputed Issues (Independent Claims)

- **Kleve disputed issues:**
 - *“the coded data includes privilege settings”* (1[e], 11[e], 18[e]):
 - Issue: Whether it would be obvious to send Kleve’s “privilege settings” as coded data associated with an E-key.
 - Kleve discloses an E-key that is transmitted and authenticated using coded data
 - Obvious to include the privilege settings as part of the coded data
 - *Motivation to combine Kleve and Hatton* (cls. 1, 11, 18):
 - PO argues a POSITA would not combine Kleve and Hatton because Hatton discloses using encryption for “authentication” and not “confidentiality”
 - The Petition relies on Kleve, not Hatton, for disclosure of encryption and coded data
 - Hatton adds the use of wireless communication protocols for communicating eKey information directly between the mobile device and the vehicle
 - PO’s argument is also an improper bodily incorporation argument: nothing in Hatton prevents its encryption teachings from being used to secure privilege settings

Summary: Disputed Issues (Dependent Claims)

- Klevé disputed issues:
 - *“enable sharing of said eKey with a recipient user”* (cl. 6):
 - Issue: Whether Klevé prohibits allowing authorized users to share an eKey with each other
 - Klevé discloses sharing an eKey from an owner’s device to a temporary user’s device
 - Obvious to use the same techniques to enable sharing from one user’s device to another
 - *“server” or “application” “associated with a manufacturer of the vehicle”* (cls. 12, 13, 20):
 - Petition argues these limitations are not entitled to patentable weight, but are nonetheless disclosed/rendered obvious
 - PO argues the limitations should be given weight, but does not rebut obviousness
 - Klevé and other contemporaneous references (Xiao, Hatton) disclose servers/applications associated with vehicle manufacturers

Summary: Disputed Issues (Independent Claims)

- Mikan disputed issues:
 - “*the coded data includes privilege settings*” (1[e], 11[e], 18[e]):
 - Issue: Whether Mikan permits or renders obvious transmitting privilege settings via the mobile device
 - PO argues Mikan only discloses transmitting privilege settings from the server to the vehicle
 - This argument narrowly treats Mikan’s exemplary embodiments as limiting
 - Other disclosures in Mikan suggest that privilege settings may be stored as coded data in the wireless device
 - At a minimum, obvious to transmit privilege settings via the mobile device as coded data
 - PO’s argument that Mikan “discourages” sending privilege settings via the mobile device is legally incorrect: disclosure of alternative designs is not a teaching away
 - Mikan and PO’s expert both admit disadvantages that are solved by the proposed combination

Summary: Disputed Issues (Dependent Claims)

- Mikan disputed issues:
 - *“enable sharing of said eKey with a recipient user”* (cl. 6):
 - Issue: Whether Mikan prohibits allowing authorized users to share an eKey with each other
 - Mikan similarly discloses sharing and embedding an eKey in a mobile device
 - Obvious to use the same techniques to enable sharing from one user’s device to another
 - *“server” or “application” “associated with a manufacturer of the vehicle”* (cls. 12, 13, 20):
 - Petition argues these limitations are not entitled to patentable weight, but are nonetheless disclosed/rendered obvious
 - PO argues the limitations should be given weight, but does not rebut obviousness
 - Kleve and other contemporaneous references (Xiao, Hatton) disclose servers/applications associated with vehicle manufacturers

'659 Patent Overview

Patent Overview

- '659 Patent, Claim 1:

1. A sub-system of a vehicle, the vehicle having an on-board computer interfaced with the sub-system for processing instructions to enable use of an electronic key (eKey), the sub-system comprising:

memory associated with the on-board computer of the vehicle having program instructions for instructing unlocking and starting of the vehicle; and

communications circuitry of the vehicle interfaced with the on-board computer of the vehicle and the sub-system, the communications circuitry is configured to process program instructions to enable communication with a server, the communications circuitry includes wireless communication circuitry for enabling local connection with a mobile device, the mobile device is configured to use the eKey for said unlocking and said starting the vehicle;

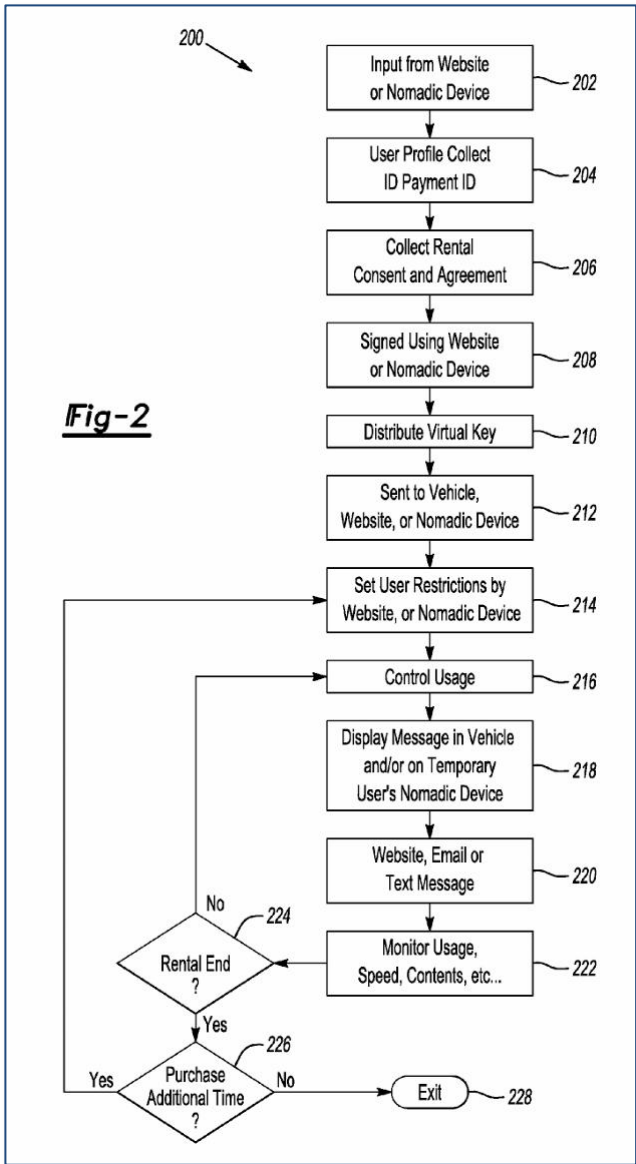
wherein the wireless communications circuitry of the vehicle is configured to receive coded data from the mobile device when using the eKey, the coded data enables functions of said eKey for said unlocking and use of the vehicle, the coded data is associated to the eKey for use by the mobile device, and the coded data includes privilege settings associated with the eKey for limiting types of use of the vehicle when using the eKey with the vehicle;

wherein use of the vehicle using the eKey is tracked to identify and log actions taken using the vehicle while the eKey is used.

Summary of Prior Art

Summary of Prior Art: Kleve (Ex. 1005)

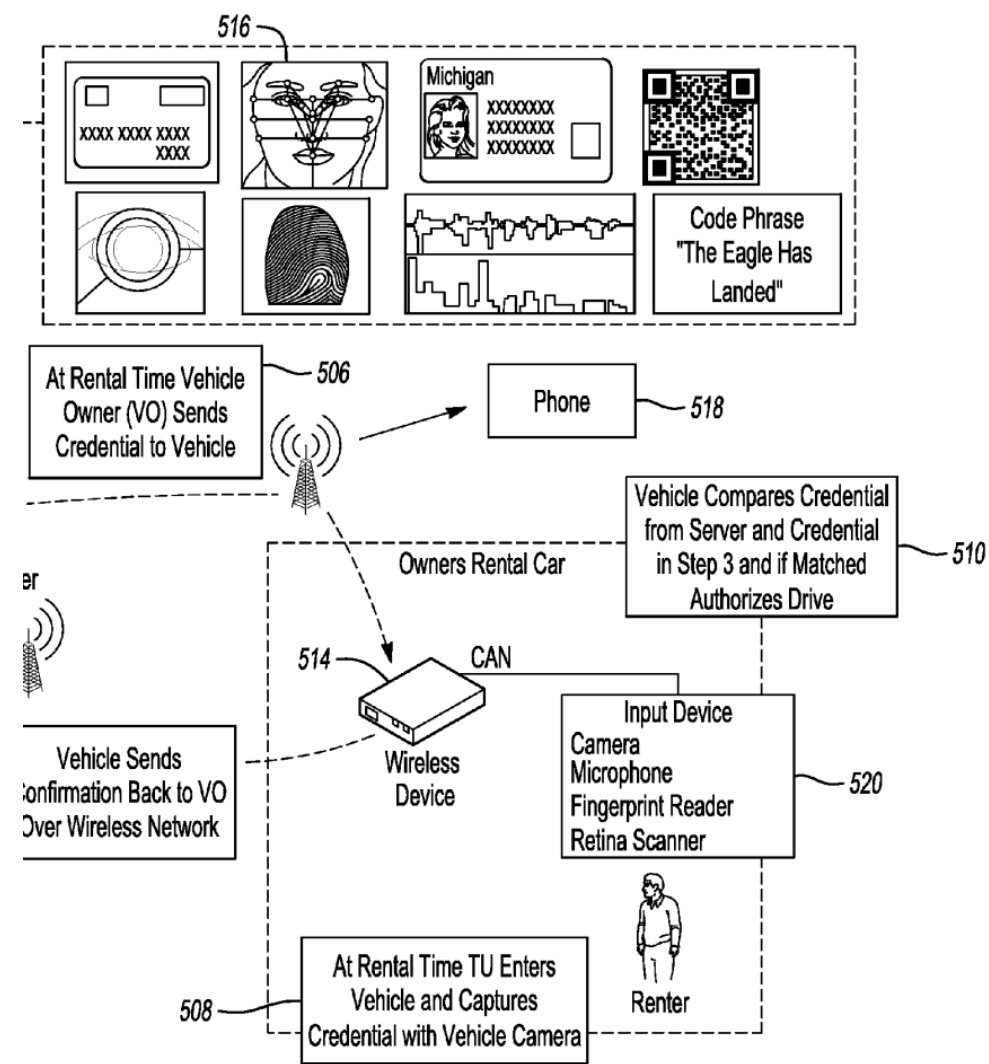
[0039] “At step 210, once the Temporary User selects the vehicle, pays the appropriate amount and signs a consent agreement, than the system may generate a virtual key to distribute to the Temporary User and VCS. The virtual key may be sent to, but not limited to, the website for the Temporary User to view, sent through an email, or to the Temporary User's nomadic device at step 212. The virtual key may also be sent to the vehicle configuring the VCS to enable the keyless drive system for the appropriate Temporary User during a given rental period.”



Ex. 1005 (Kleve) at ¶39, Fig. 2; Pet. 15, 24-25

Summary of Prior Art: Kleve (Ex. 1005)

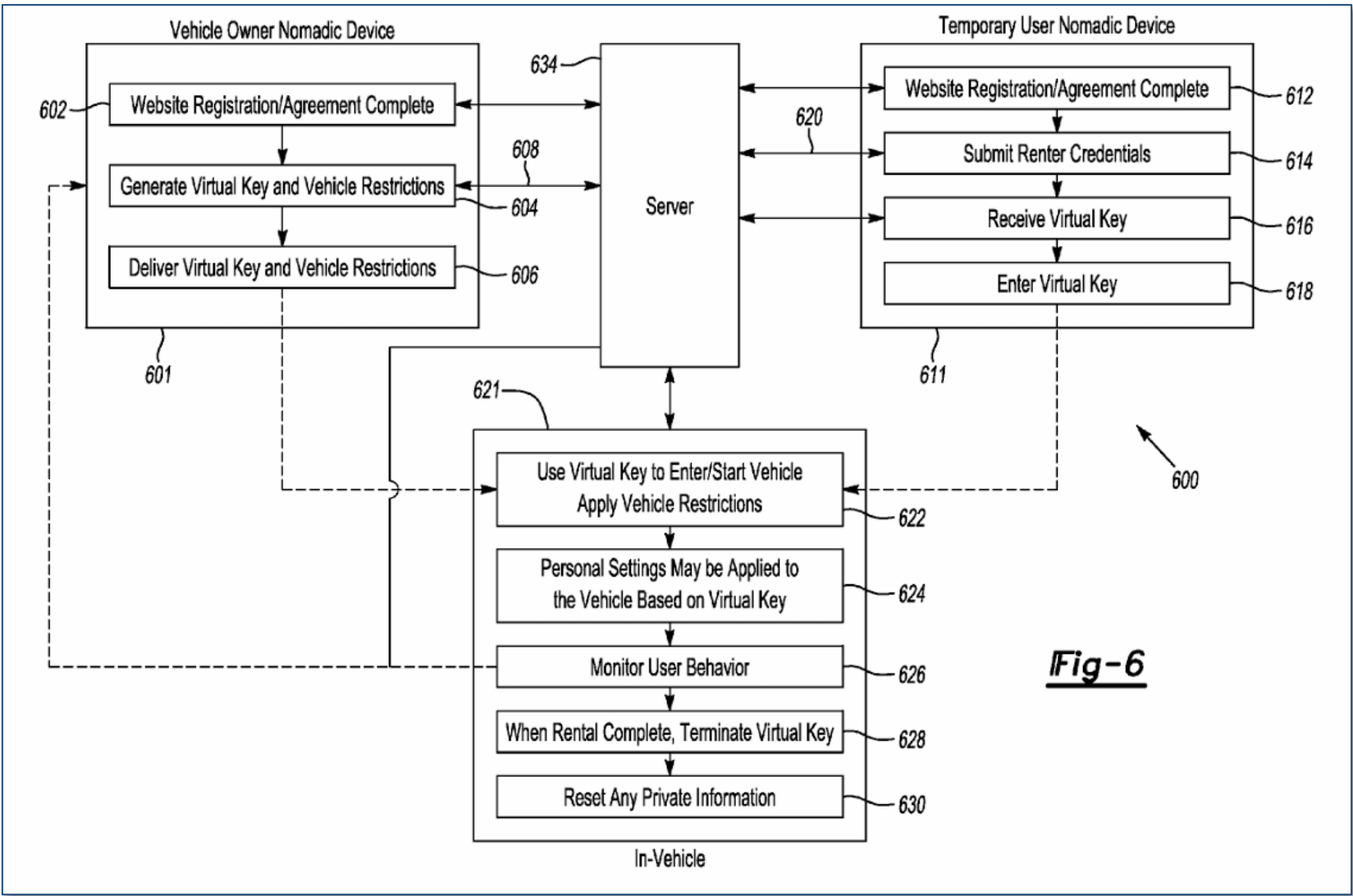
[0066] “When the scheduled rental period of time begins the vehicle Owner may send the credentials to the vehicle with the use of a server 506 and the vehicle may be able to receive the information using a wireless device 514.”



Summary of Prior Art: Kleve (Ex. 1005)

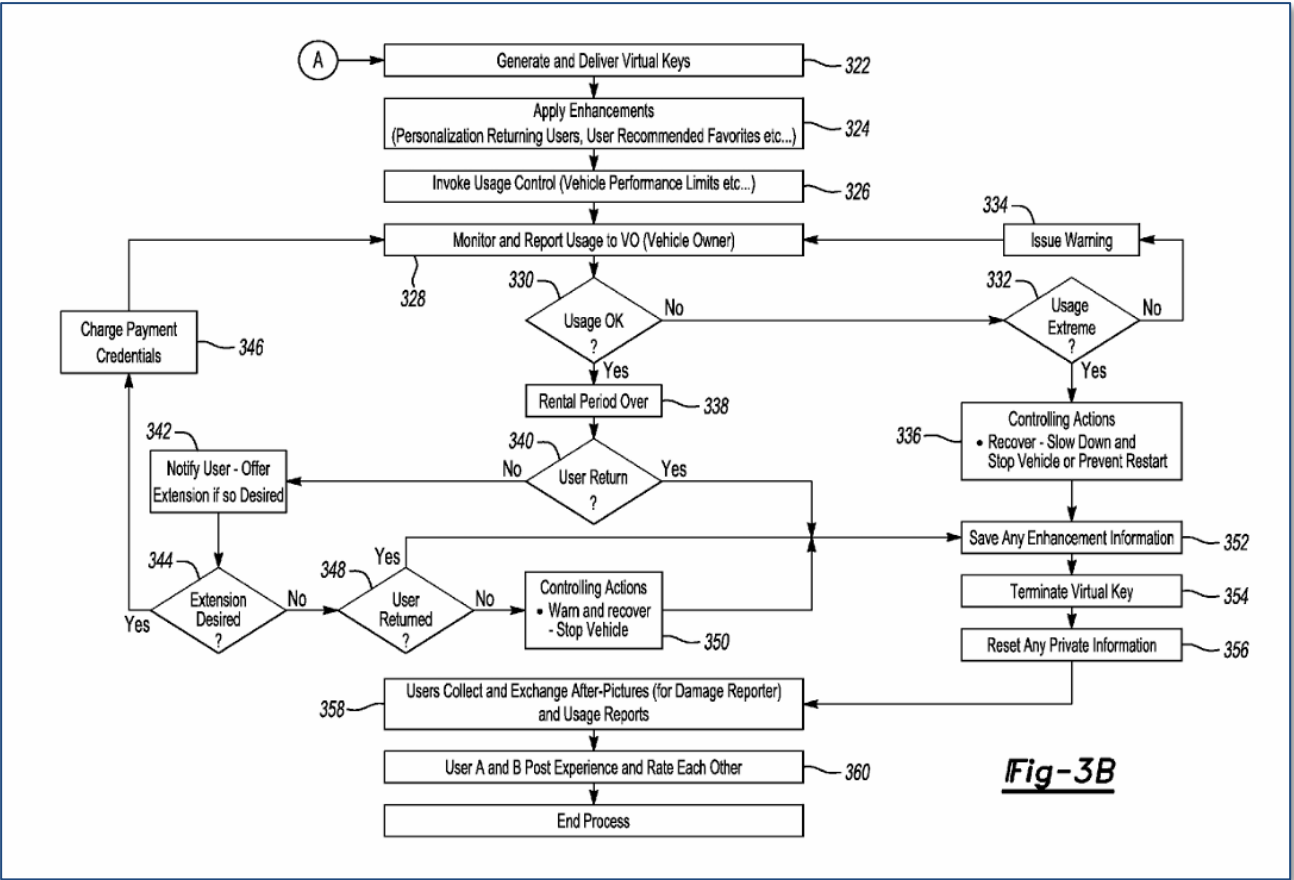
[0070] “At step 622, when the Temporary User arrives at the vehicle within the scheduled rental time, he or she may enter the virtual key using several methods. One method may include having the Temporary User scan their finger with the use of a fingerprint scanner integrated with the VCS to validate authorization to access the vehicle. The Temporary User's virtual key may be authorized several ways including, but not limited to, at the vehicle, communicated back to the vehicle rental authorization server using a telecommunications network, or by having the vehicle Owner verify access using their nomadic device.”

Summary of Prior Art: Kleve (Ex. 1005)



Summary of Prior Art: Kleve (Ex. 1005)

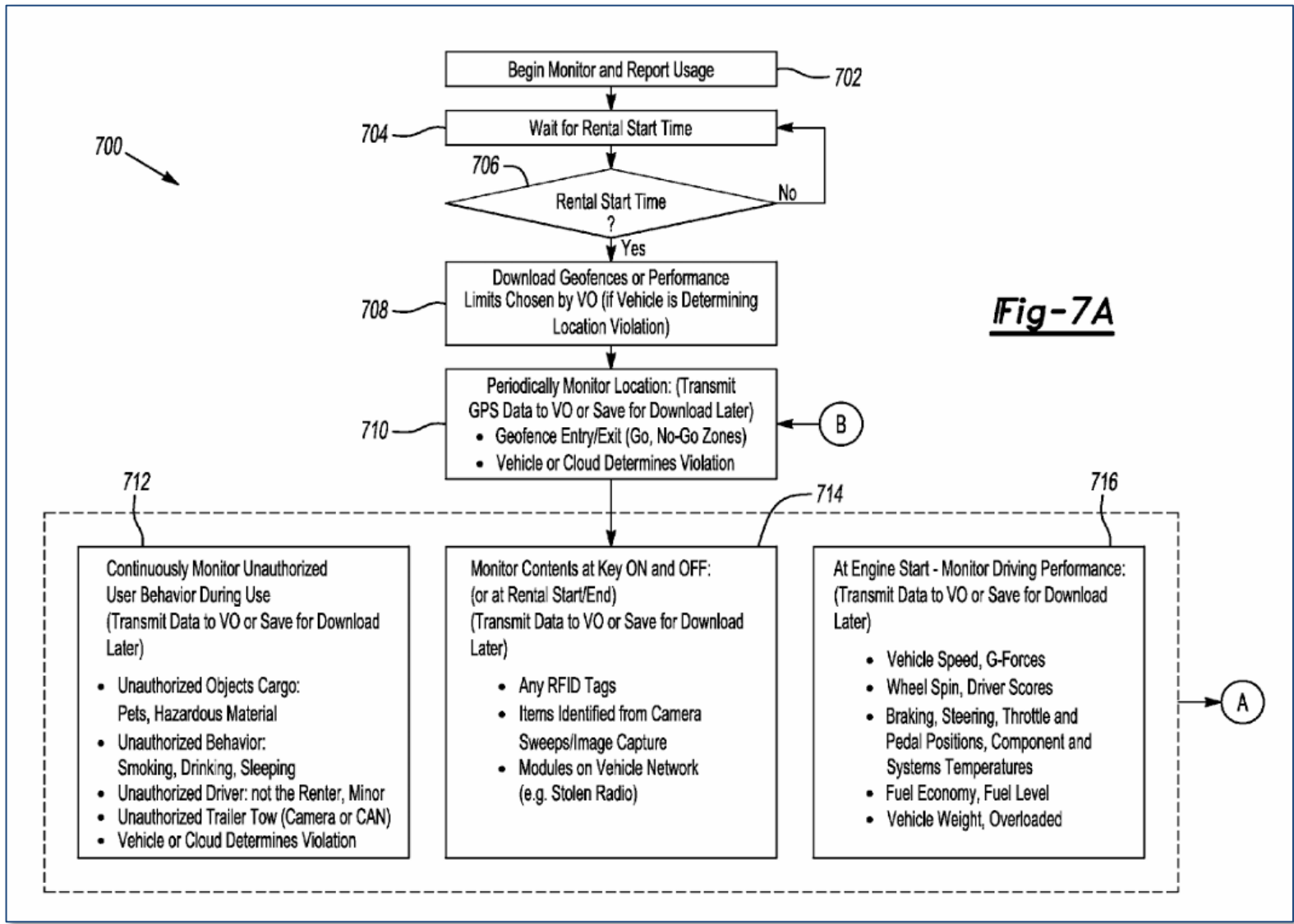
[0051] “At 326, the VCS may implement assigned vehicle control limitations during the use of the rental term by mitigating vehicle performance while preventing the Temporary User to exceed a limitation set by the Owner. The Owner may have the options to set rental restrictions based on, but not limited to, speed, destination location, or load weight limitations. Controlling usage to enforce compliance with the rental agreement terms may be of more importance to a vehicle rental micro-business owner as this may be the only vehicle the Owner possesses. These restrictions can be input using the vehicle rental website, a smart phone application or the Owner's nomadic device interacting with the VCS.”



Ex. 1005 (Kleve) at ¶51, Fig. 3B; Reply 3-4

Summary of Prior Art: Kleve (Ex. 1005)

[0075] “At step 702, the VCS may begin monitoring and report usage of the vehicle to the owner. The system may wait for the rental period to start at step 704.”



Summary of Prior Art: Hatton (Ex. 1008)

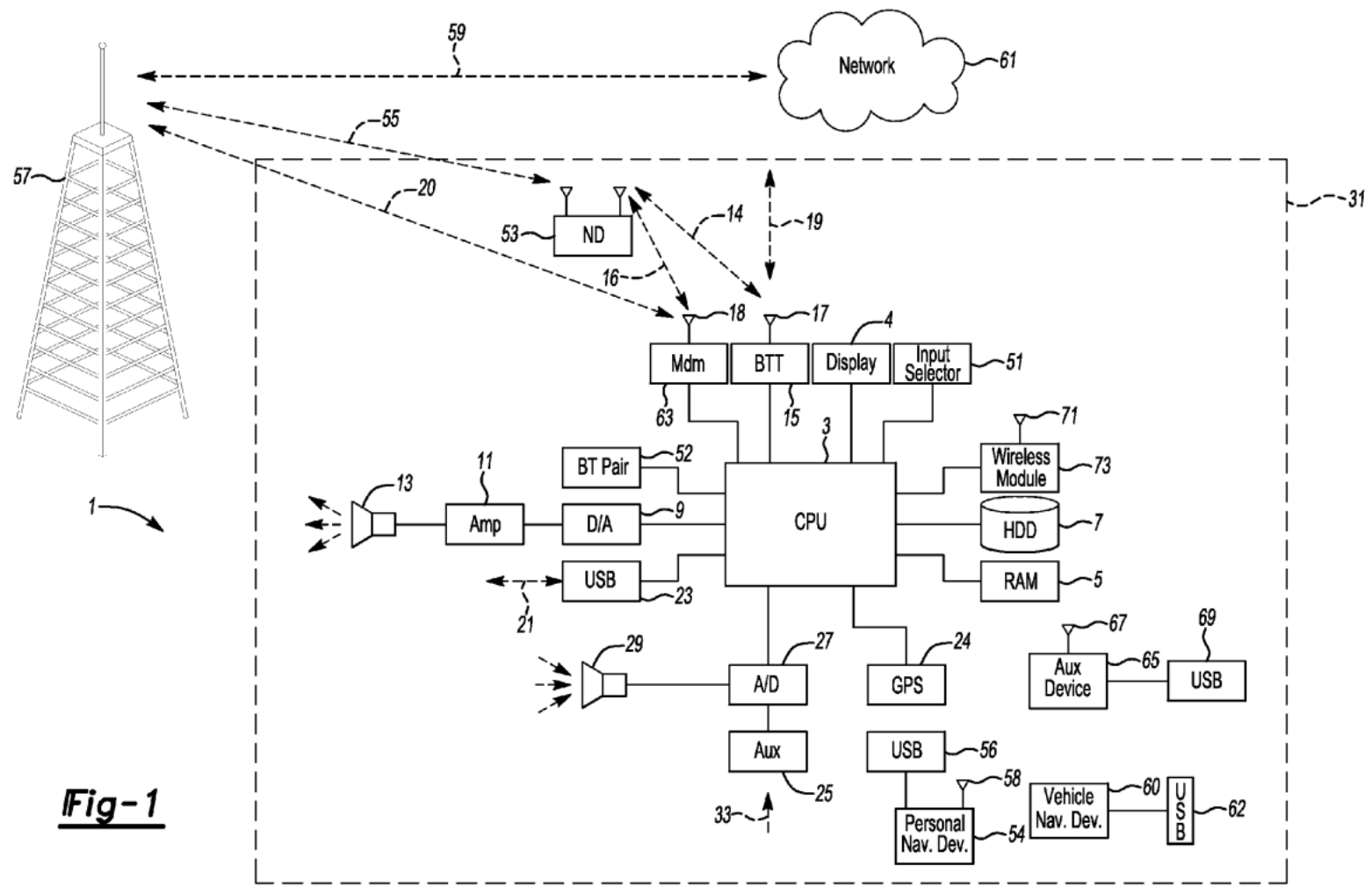


Fig-1

Ex. 1005 (Kleve) at Fig. 1 and Ex. 1008 (Hatton) at Fig. 1; Pet. 11-12

Summary of Prior Art: Hatton (Ex. 1008)

“The mobile device 124 may a software application 126 running in a processor 128 on the device to transmit a vehicle control signal using an onboard modem with antenna 128 to communicate with a vehicle. The PATS controller and/or VCS may recognize the mobile device associated to a user using one or more of the key serial number, manufacturing code in combination with the mobile device transmitted encrypted data. The PATS and/or VCS may recognize the paired mobile device from the received KEY ID signal using one or more wireless communication technologies including, but not limited to Bluetooth, WiFi, cellular, and/or near field communication.”

Ex. 1008 (Hatton) at 7:49-60; Pet. 20

Summary of Prior Art: Sekiyama (Ex. 1006)

“The function restriction unit 43 controls the enablement of execution or disablement of execution of various functions of the vehicle 40 based on the key information recognized by the electronic key recognition unit 42. The function restriction unit 43 outputs command signals to the door lock control unit 51, controlling the locking and unlocking of the door lock. ... The function restriction unit 43 outputs command signals to the trunk lock control unit 53, controlling the locking and unlocking of the trunk.”

Ex. 1006 (Sekiyama) at ¶18; Pet. 38-39

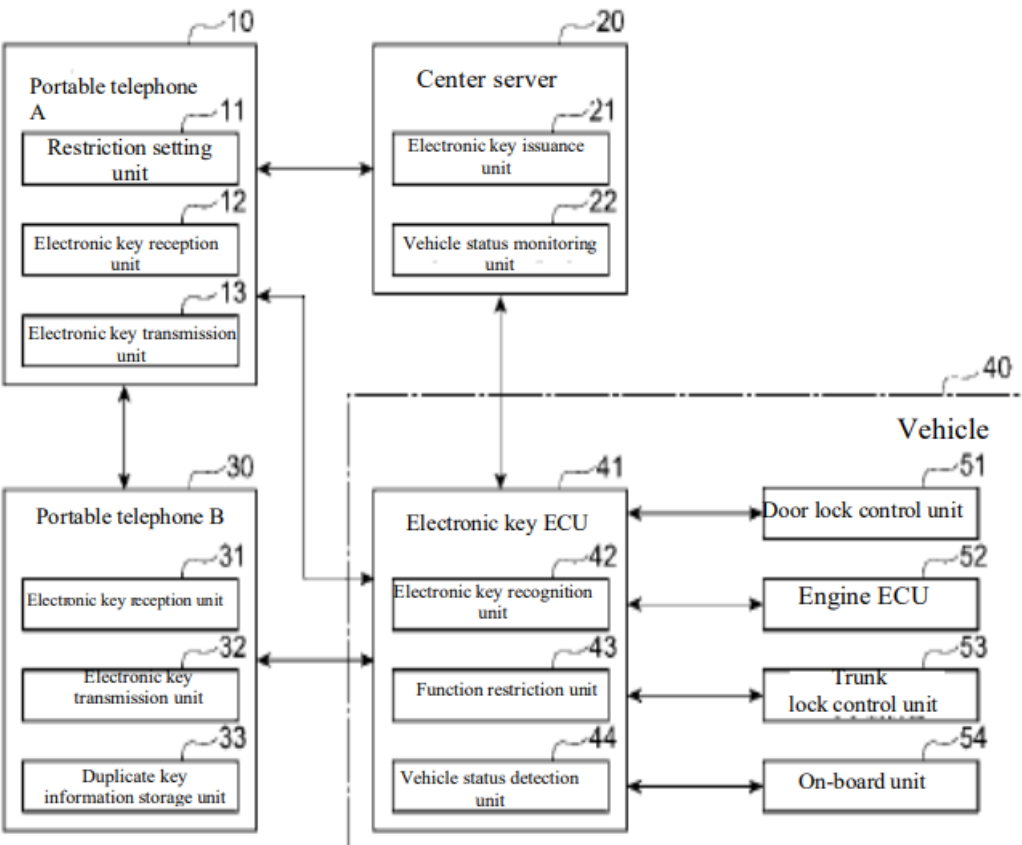
Summary of Prior Art: Sekiyama (Ex. 1006)

“The function restriction unit 43 controls the enablement of execution or disablement of execution of various functions of the vehicle 40 based on the key information recognized by the electronic key recognition unit 42. The function restriction unit 43 outputs command signals to the door lock control unit 51, controlling the locking and unlocking of the door lock. ... The function restriction unit 43 outputs command signals to the trunk lock control unit 53, controlling the locking and unlocking of the trunk.”

Ex. 1006 (Sekiyama) at ¶18; Pet. 38-39

Summary of Prior Art: Sekiyama (Ex. 1006)

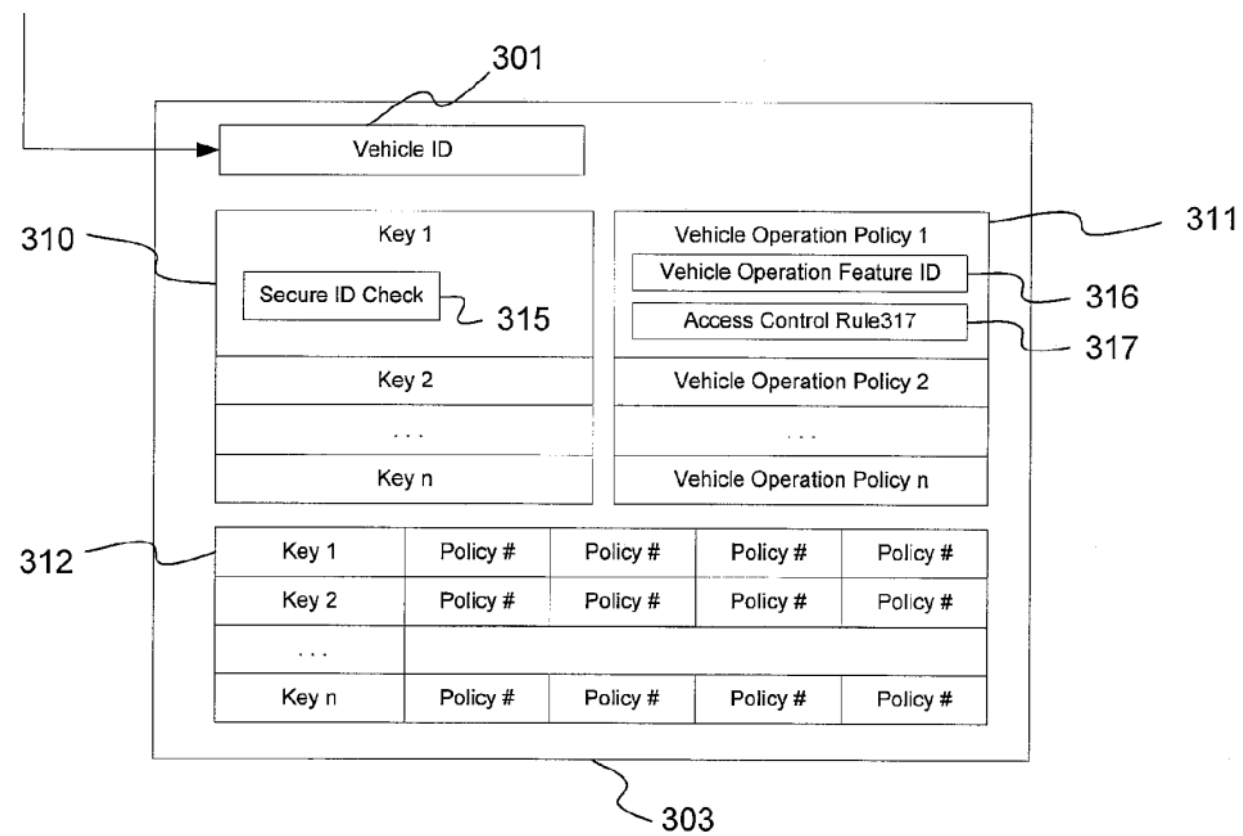
“The electronic key system shown in FIG. 1 is a keyless entry system using portable telephones, allowing for the unlocking of a door lock of a vehicle 40 using portable telephones 10, 30, which store key information, without possession of a dedicated key. As shown in FIG. 2, this electronic key system has a configuration that allows key information to be transmitted from portable telephone A (first terminal) 10, which functions as a master key, to portable telephone B (second terminal) 30, which functions as a duplicate electronic key.



Ex. 1006 (Sekiyama) at ¶11, Fig. 1; Pet. 65

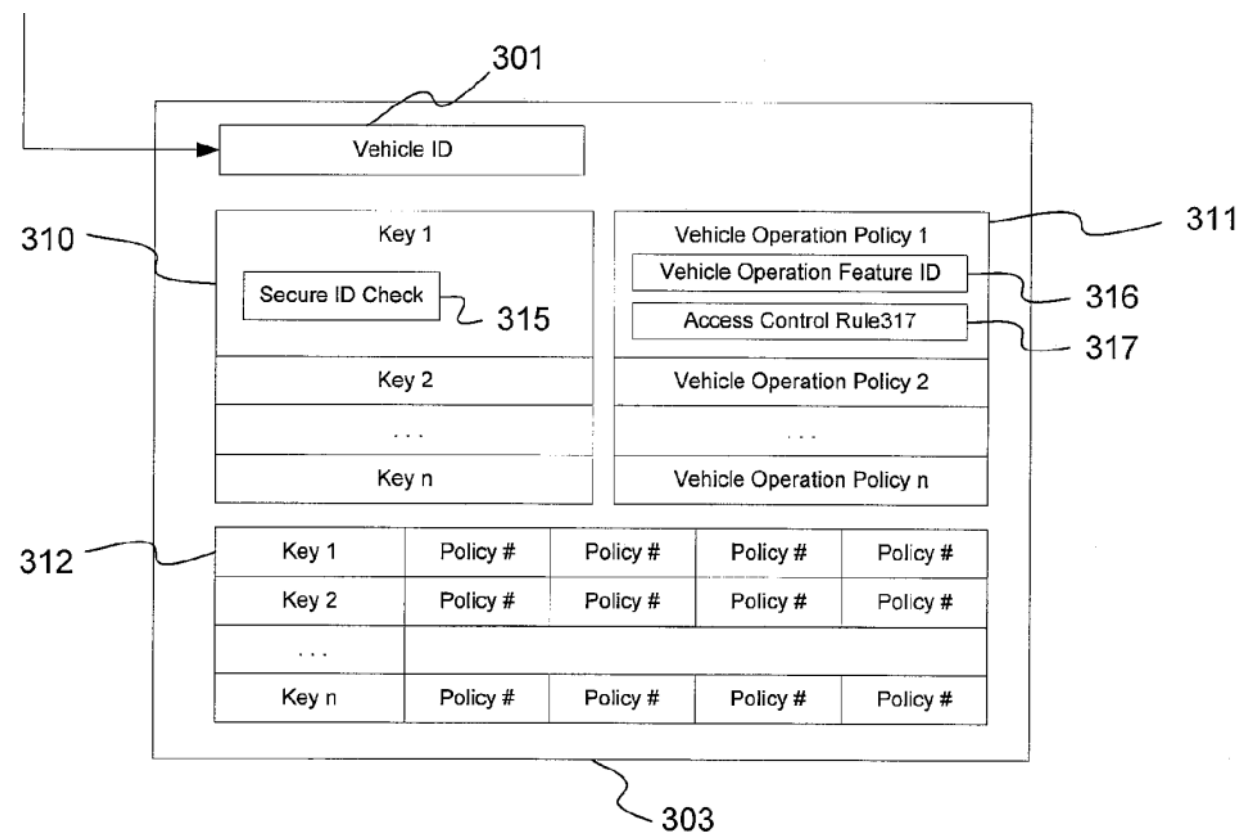
Summary of Prior Art: Mikan (Ex. 1007)

[0060] “Local database 303 may include vehicle operation policy 311. Vehicle operation policy 311 may include vehicle operation feature ID 316 and a related access control rule 317. ... Access control rule 317 may include a criterion relating to associated vehicle operation feature ID 316. For example, access control rule 317 may operate to enable, partially enable, or disable the related vehicle operation feature. Access control rule 317 may include advanced criteria relating to the manner and conditions under which the vehicle may be operated. For example, access control rule 317 may establish a maximum acceleration for the vehicle, a maximum distance traveled for the vehicle, a range of time within which the vehicle may be operated, a geographic range within which the vehicle may be operated and the like.”



Summary of Prior Art: Mikan (Ex. 1007)

[0060] “Local database 303 may include vehicle operation policy 311. Vehicle operation policy 311 may include vehicle operation feature ID 316 and a related access control rule 317. ... Access control rule 317 may include a criterion relating to associated vehicle operation feature ID 316. For example, access control rule 317 may operate to enable, partially enable, or disable the related vehicle operation feature. Access control rule 317 may include advanced criteria relating to the manner and conditions under which the vehicle may be operated. For example, access control rule 317 may establish a maximum acceleration for the vehicle, a maximum distance traveled for the vehicle, a range of time within which the vehicle may be operated, a geographic range within which the vehicle may be operated and the like.”

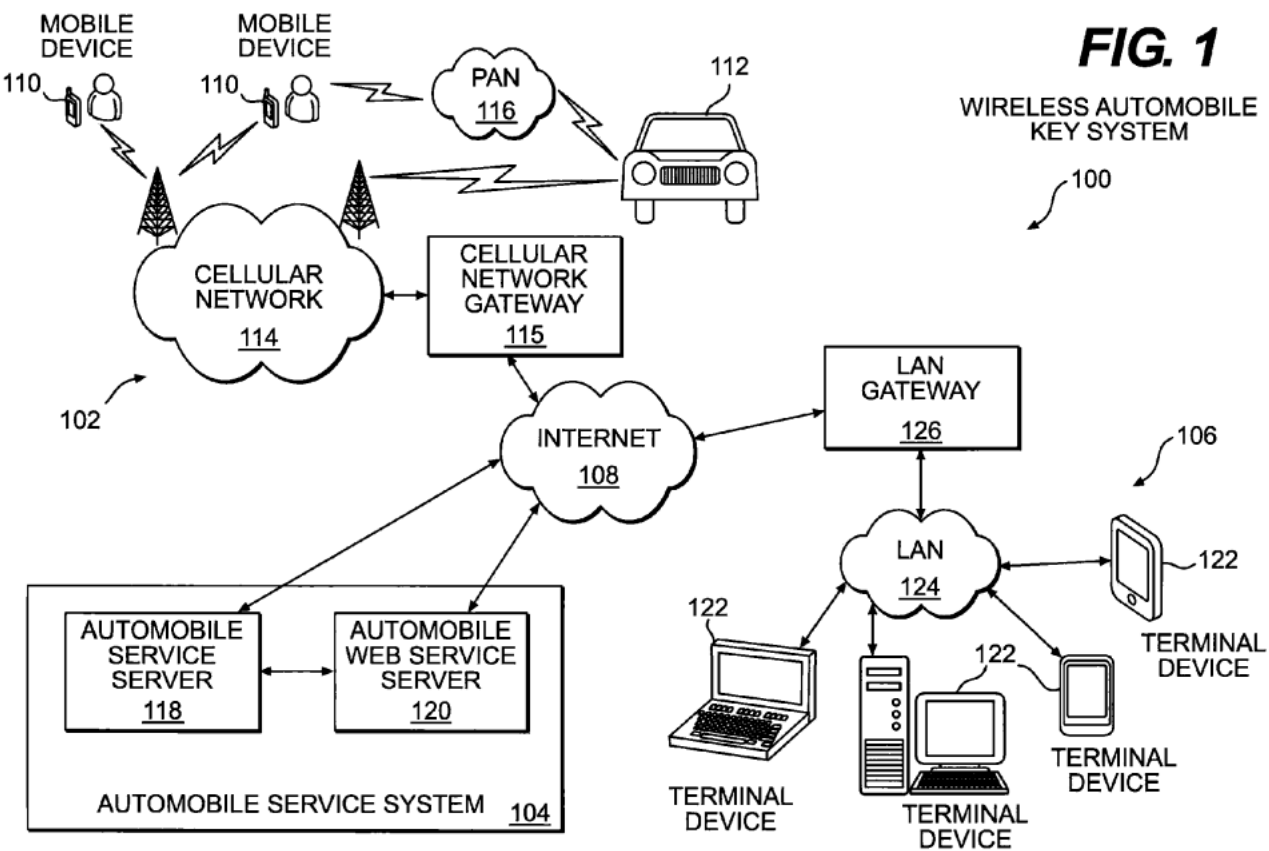


Summary of Prior Art: Mikan (Ex. 1007)

[0085] “Vehicle 201 may not always be in contact with wireless network 207, such as when vehicle 201 is parked underground and out of range of wireless network 207, for example. Where master database 208 pushes the synchronization to local database 203, master application 209 may establish communication with control unit 202 before initiating the synchronization. When communication cannot be established, master application 209 or master database 208 may queue the request for a later time.”

Summary of Prior Art: Xiao (Ex. 1010)

FIG. 1 illustrates an exemplary wireless automobile key system 100, consistent with the disclosed embodiments. System 100 may be associated with an Internet service provider, a wireless service provider, a telecommunications service provider, a content service provider, or another entity that provides the disclosed wireless automobile key service. In another embodiment, system 100 may be associated with an automobile company that provides the disclosed wireless automobile key service.



Ground 1: Kleve renders obvious an e-key associated with “coded data” that includes “privilege settings” (All claims)

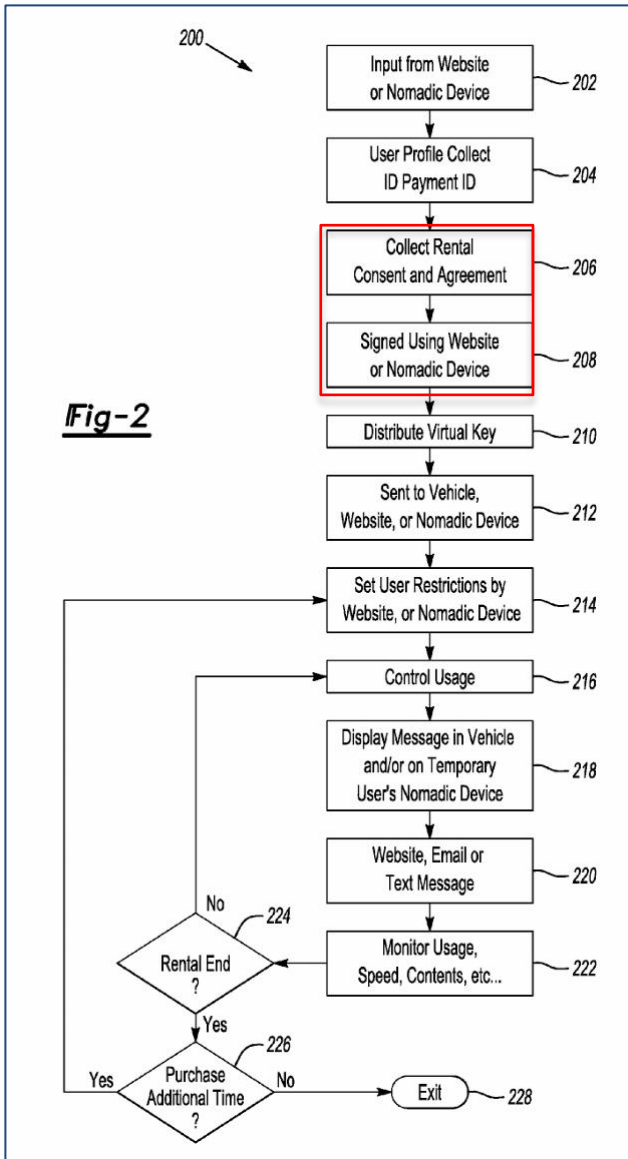
Ground 1: Kleve renders obvious “coded data” including “privilege settings”

- **Undisputed:**
 - Kleve discloses that owner and renter agree on use conditions, including rental period, in the rental agreement
 - Kleve discloses the eKey is sent to the renter’s mobile device as coded data
 - If privilege settings are sent to the renter’s device, it is obvious to use coded data
 - Kleve discloses that privilege settings are enforced
- **PO:**
 - POR: Kleve **only** discloses **owner** setting privilege settings at start of rental, **after** e-key is sent
 - Surreply: Kleve discloses privilege settings are only sent from the **server** to the vehicle
- PO is **incorrect:**
 - Kleve **expressly** discloses “enabl[ing]” the key for the “rental period” when it is sent
 - A POSITA would understand “enabl[ing]” the rental period includes the privilege setting being sent with the key
 - POSITA would have found it obvious for the privilege setting to be included as coded data to prevent tampering and other improper uses (as found in the ID)

Ground 1: Kleve Summary

- Owner and renter agree to terms and conditions, including rental period:

[0038] “At step 206, the Owner may collect the monetary compensation in exchange for the use of his vehicle. The Owner and Temporary User may agree to terms and conditions for the rental period using the website or nomadic device. The Owner may create a standard rental agreement form, or may develop a custom form based on the type of use the Temporary User is requesting to use the vehicle for. For example, if the Temporary User wants to use the Owner's vehicle to move furniture, the Owner can tailor the rental agreement to include what can and cannot be transported. The Temporary User and Owner can sign the consent and agreement using the website or the nomadic device at step 208.”



Ex. 1005 (Kleve) at ¶138, Fig. 2; Pet. 24-25; POR 5

Ground 1: Kleve Summary

- Owner and renter sign agreement with use conditions, including rental period:

[0062] “FIG. 5 shows an illustrative example of an overview of how the vehicle rental micro-business may be structured with a keyless transaction between the Owner of the vehicle and the Temporary User. This example illustrates the process after the vehicle Owner and Temporary User have already setup a user profile within the database and have both agreed to the rental agreement. At step 502, the vehicle Owner may enter in vehicle authorization credentials based on information received by the Temporary User to set up a virtual key. The virtual key may be sent to the vehicle allowing Temporary User access to the Owner's vehicle.”

Ex. 1005 (Kleve) at ¶¶62; Pet. 24-25

[0064] “The Temporary User's information for credential verification 516 may be collected and exchanged using several methods including . . .”

[0065] “An example for applying Temporary User credential verification at a vehicle may include, but not limited to, the use of additional hardware integrated with the VCS to allow collection and exchange of information to enable a keyless drive-away rental event. For example the Temporary User may use their credit card at a vehicle with the use of hardware integrated with the VCS to collect payment credentials, identify the user, and/or agree to rental terms.”

Ex. 1005 (Kleve) at ¶¶64-65; Reply 13, 15

Ground 1: Kleve Summary

- Owner and renter sign agreement with use conditions, including rental period:

[0047] “... When the Temporary User and vehicle Owner agree to terms 316 the website may generate the exchange or propose a rental agreement 318. The agreement between the Owner and Temporary User can be signed and payment made through the website at step 320. The agreement to rental terms and conditions between the parties may be done with the website using smart phones or a smart phone application, or any other type of nomadic device. Rental conditions may also be displayed on the vehicle's touchscreen visual display and accepted or rejected through the touchscreen visual display.”

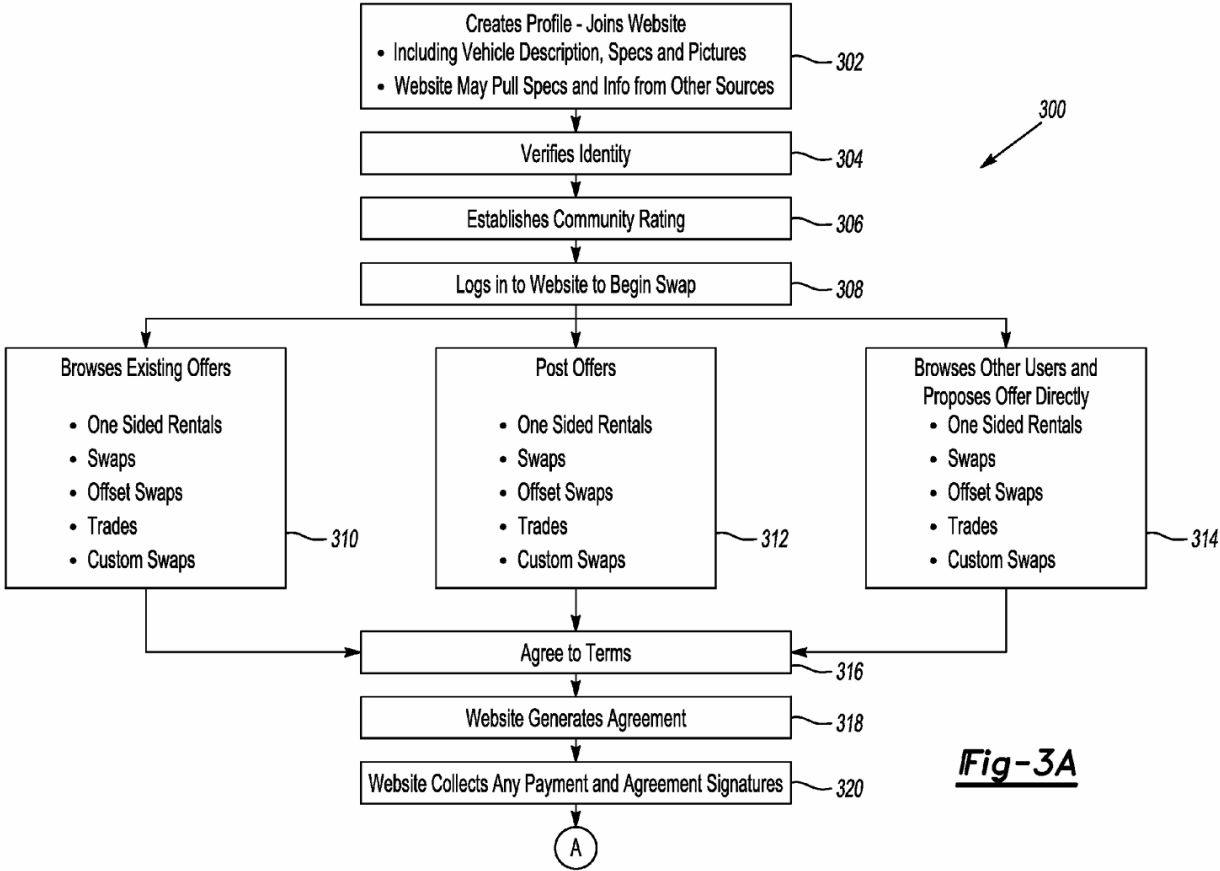
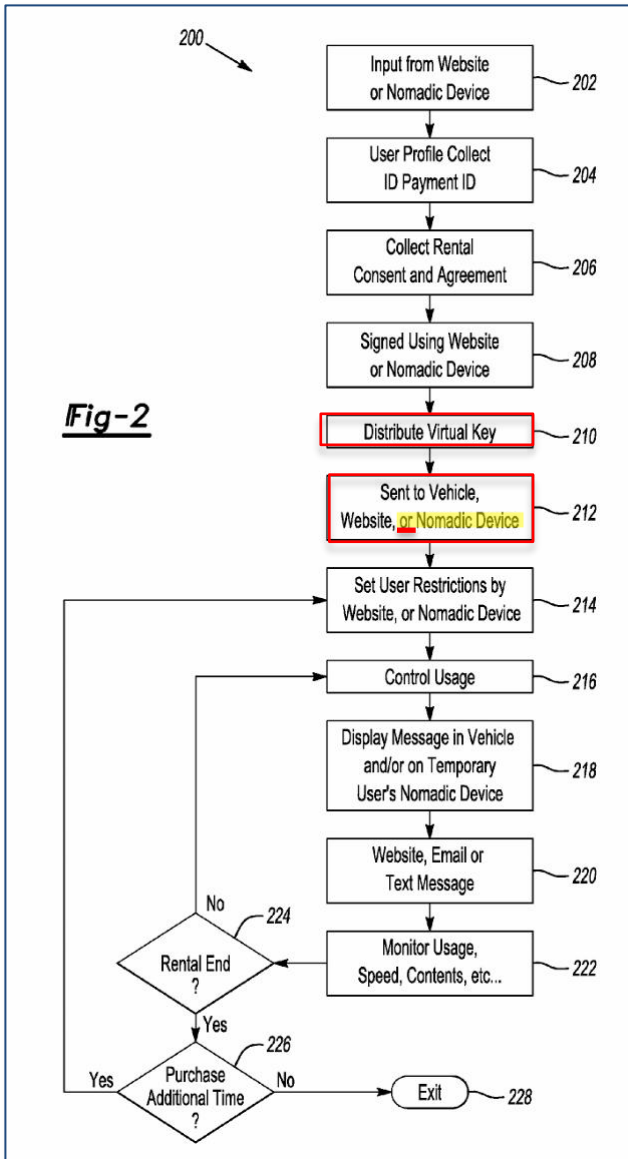


Fig-3A

Ground 1: Kleve Summary

- Virtual key is then sent to the renter

[0039] “At step 210, once the Temporary User selects the vehicle, pays the appropriate amount and signs a consent agreement, than [sic] the system may generate a virtual key to distribute to the Temporary User and VCS. The virtual key may be sent to, but not limited to, the website for the Temporary User to view, sent through an email, or to the Temporary User's nomadic device at step 212. The virtual key may also be sent to the vehicle configuring the VCS to enable the keyless drive system for the appropriate Temporary User during a given rental period.”



Ex. 1005 (Kleve) at ¶39, Fig. 2; Pet. 15, 24-25

Ground 1: Kleve Summary

- Virtual key is then sent to the renter

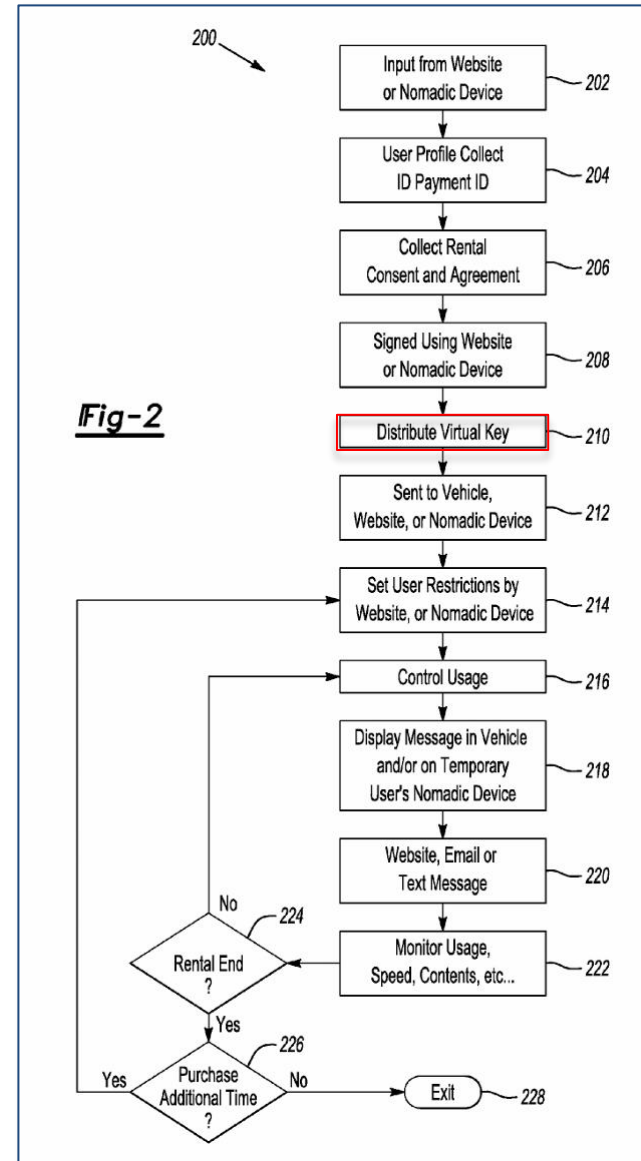
[0069] “Using a nomadic device, for example a smart phone, a Temporary User and vehicle Owner may set up user profiles, enter into an agreement and make a payment to initiate the vehicle rental process between the two parties at step 602 and 612. At step 604, the vehicle Owner may then generate a virtual key based on a password generated by the vehicle Owner that may include a matrix barcode or a code word that the Temporary User may enter/send to the vehicle when ready to begin the rental term. ... At step 616, the virtual key is generated and sent to the Temporary User.”

Ex. 1005 (Kleve) at ¶¶69; Pet. 25-26

Ground 1: Kleve Summary

- Rental period information is assigned to the virtual key and distributed:

[0039] “At step 210, once the Temporary User selects the vehicle, pays the appropriate amount and signs a consent agreement, than the system may generate a virtual key to distribute to the Temporary User and VCS. The virtual key may be sent to, but not limited to, the website for the Temporary User to view, sent through an email, or to the Temporary User's nomadic device at step 212. The virtual key may also be sent to the vehicle configuring the VCS to **enable the keyless drive system for the appropriate Temporary User during a given rental period.**”



Ex. 1005 (Kleve) at ¶39, Fig. 2; Pet. 15, 24-25

Ground 1: Kleve Summary

- Three different use cases for e-key after rental period starts:
- (1) E-key allows renter to unlock and turn on car without further verification needed:

[0048] “At step 322, ... [t]he virtual key may allow a Temporary User temporary granted access to the Owner's vehicle. The granted access allowed by the virtual key may permit entry of the vehicle; grant a keyless drive-away of a vehicle, and/or both.”

Ex. 1005 (Kleve) at ¶48; Pet. 15

- (2) Renter enters vehicle with e-key and uses credential for verification, **or** (3) Renter uses credential for verification at the exterior of car before entering:

[0049] “The system may be further extended to facilitate the virtual key with additional security by requiring remote credential verification at the vehicle. The remote credential verification at the vehicle may be done with additional hardware assembled on the exterior of the vehicle or in the vehicle cabin. The remote credential verification may be done by the VCS, using a server, or allowing the Owner to verify the Temporary User's request. For example, but not limited to, the Temporary User entering a credential verification password at the vehicle's touchscreen visual display while having the VCS, server, or owner compare and verify authorization.”

Ex. 1005 (Kleve) at ¶49; Pet. 23, 26

Ground 1: Kleve Summary

- Additional terms may be agreed-upon once inside the vehicle:

[0065] “An example for applying Temporary User credential verification at a vehicle may include, but not limited to, the use of additional hardware integrated with the VCS to allow collection and exchange of information to enable a keyless drive-away rental event. For example, the Temporary User may use their **credit card at a vehicle** with the use of hardware integrated with the VCS to collect payment credentials, identify the user, and/or **agree to rental terms**. Another exemplary embodiment of applying Temporary User credentials at a vehicle may be with the use of facial recognition done by having a camera integrated with the VCS.”

Ex. 1005 (Kleve) at ¶65; POR 47

[0047] “The agreement to rental terms and conditions between the parties may be done with the website using smart phones or a smart phone application, or any other type of nomadic device. Rental conditions may also be displayed on the vehicle's touchscreen visual display and **accepted or rejected through the touchscreen visual display.**”

Ex. 1005 (Kleve) at ¶47; Pet. 29

Ground 1: Kleve Summary

- Rental period:

[0038] “At step 206, the Owner may collect the monetary compensation in exchange for the use of his vehicle. The Owner and Temporary User may agree to terms and conditions for the rental period using the website or nomadic device.”

Ex. 1005 (Kleve) at ¶38; POR 5

[0084] “At step 812, if the owner decides he has no interest in accepting the Temporary User's offer, he may decline and wait for the vehicle rental authorization system to notify of any other offers. If the owner has decided to accept the offer he may begin the process of developing terms and conditions of the rental period.”

Ex. 1005 (Kleve) at ¶84; Reply 4

[0089] “If the owner has decided to accept the offer, he may begin the process of developing terms and conditions of the rental period. The owner may input additional terms and conditions based on the specific use and needs the Temporary User may have for renting the vehicle at step 918.”

Ex. 1005 (Kleve) at ¶89; Reply 4

[0047] The agreement to rental terms and conditions between the parties may be done with the website using smart phones or a smart phone application, or any other type of nomadic device.

Ex. 1005 (Kleve) at ¶47; Pet. 29

Ground 1: Kleve Summary

- The rental period can be terminated early:

[0053] “If the system detects that the **usage of the vehicle is extreme** by exceeding a predetermined threshold, the VCS may command controlling actions to put the vehicle in a remedial action at step 336. The remedial actions may include, but not limited to, reduce engine power, engine shut down, and **immobilization**.”

Ex. 1005 (Kleve) at ¶53; Pet. 26-27

- The rental period can be extended by agreement:

[0054] “If the Temporary User has not returned the vehicle at the time the rental period has expired, the system may notify the user if a rental term extension is desired at step 342. **If the extension term is desired**, the Temporary User may be prompted to accept additional rental charges at step 344. **The Temporary User may be charged for the additional rental time at step 346**. If the extension of time is not desired, and/or **not allowed by the Owner**, the system may transmit controlling action to warn and induce remedial actions at step 350.

Ex. 1005 (Kleve) at ¶54; Reply 11, 16

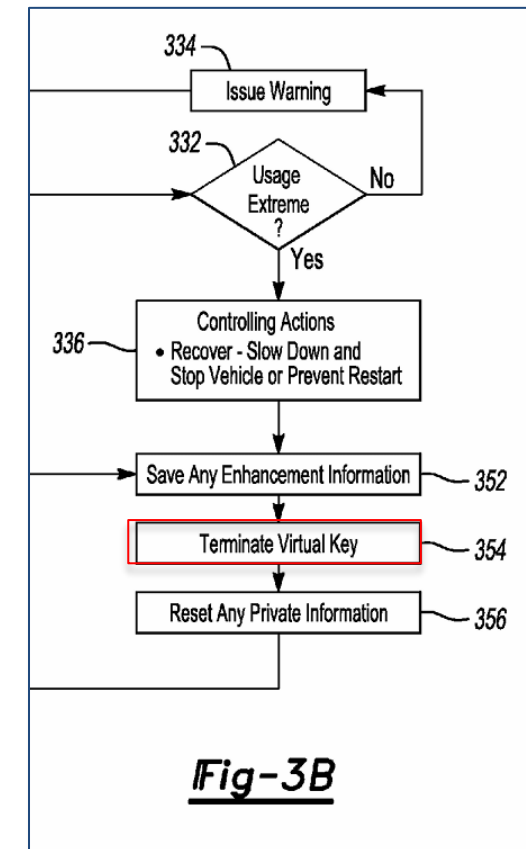


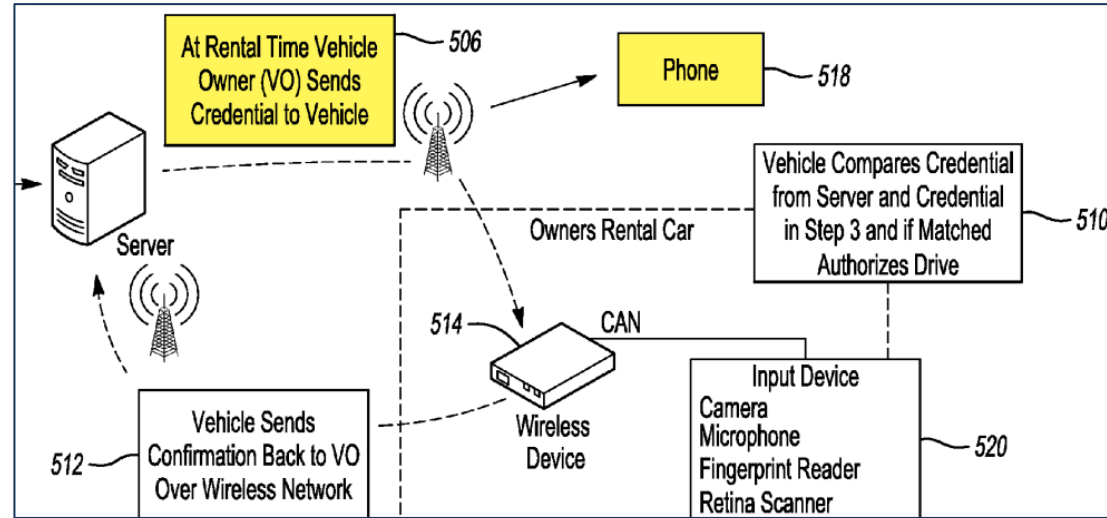
Fig-3B

G1: Kleve's "eKey" includes "privilege settings"

- PO:
 - POR: Kleve does not disclose distributing the "**privilege settings**" as coded data associated with the eKey
- PO is **incorrect:**
 - Kleve **expressly** discloses privilege settings such as *a rental period* associated with an eKey
 - A POSITA would consider it obvious to distribute the privilege settings as coded data associated with the eKey

G1: Kleve's "coded data" includes "privilege settings" / eKey is coded data

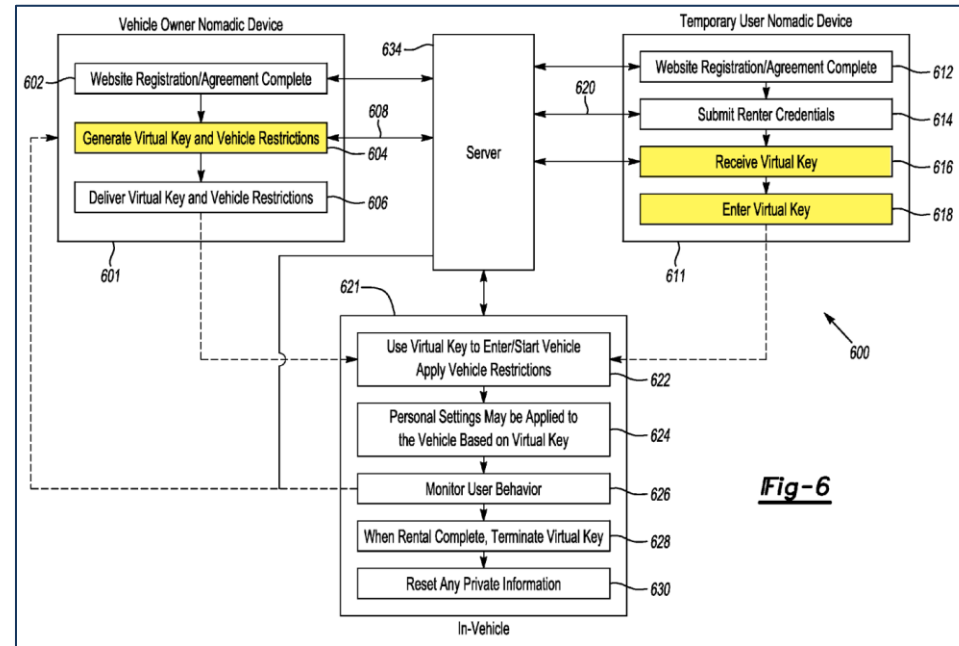
- Kleve's "virtual key" is sent as coded data:



[0063] "Additional Temporary User identification 504 may be sent to the vehicle Owner allowing for this information to be entered into the server and used as a virtual key, or in addition to the virtual key, allowing the Temporary User access to the Owner's vehicle while enabling a keyless drive away. The Temporary User identification and virtual key may be sent in an encrypted message to the VCS, Temporary User's nomadic device, and/or vehicle Owners nomadic device."

G1: Kleve's “coded data” includes “privilege settings” / eKey is coded data

- Kleve's “virtual key” is sent as coded data:

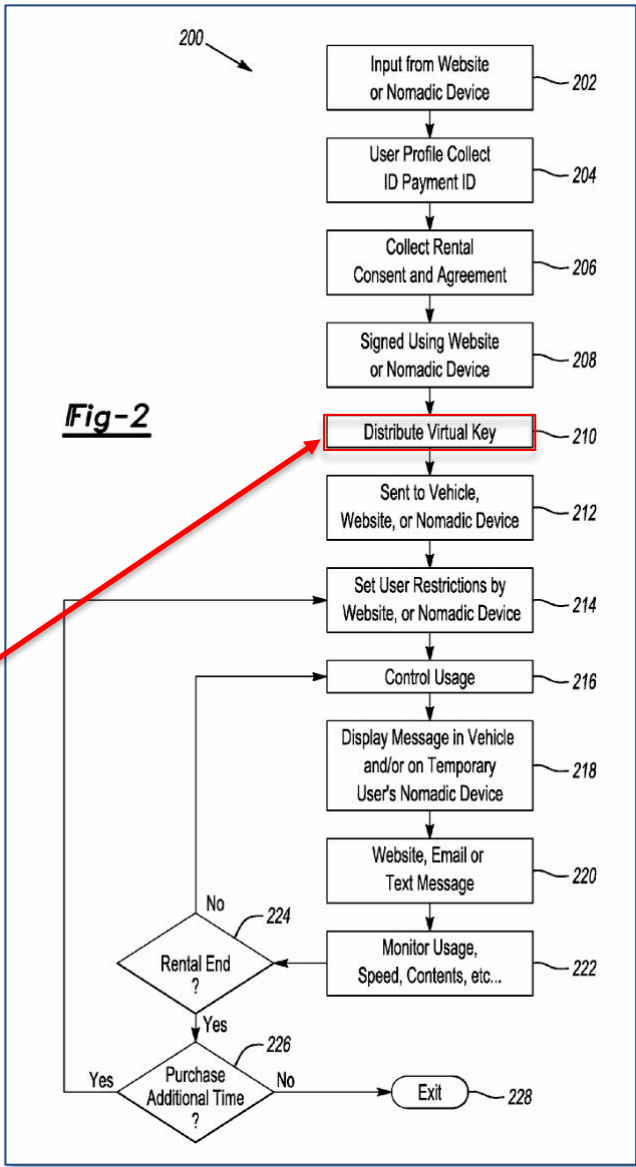


[0069] “At step 604, the vehicle Owner may then generate a virtual key based on a password generated by the vehicle Owner that may include a matrix barcode or a code word that the Temporary User may enter/send to the vehicle when ready to begin the rental term. ... At step 616, the virtual key is generated and sent to the Temporary User. The Owner may deliver a virtual key to the vehicle for recognizing the Temporary User having authorization to enable a keyless driveaway at step 606. ”

G1: Kleve’s “coded data” includes “privilege settings” / E-key includes privilege settings

- Kleve’s “virtual key” is “enable[d]” for the “rental period”:

[0039] “At **step 210**, once the Temporary User selects the vehicle, pays the appropriate amount and signs a consent agreement, than **the system may generate a virtual key to distribute to the Temporary User and VCS**. The virtual key may be sent to, but not limited to, the website for the Temporary User to view, sent through an email, or to the Temporary User's nomadic device at step 212. The virtual key may also be sent to the vehicle configuring the VCS to **enable the keyless drive system for the appropriate Temporary User during a given rental period**.”



Ex. 1005 (Kleve) at ¶39, Fig. 2; Pet. 15, 24-25

G1: Kleve's "coded data" includes "privilege settings" / E-key includes privilege settings

- Kleve's "virtual key" is "enable[d]" for the "rental period":

Kleve discloses that the virtual key, represented as encrypted data, includes privilege settings that limit types of use of the vehicle. EX1004, ¶¶138-140. For example, the vehicle's "Owner" "may set user restrictions ... based on ... parameters including, but not limited to, speed, global position coordinates, or load weight restrictions." EX1005, [0040]. The restrictions may be set in accordance with the types of use intended by the owner and temporary user. *Id.*, [0083] (owner may review rental request "based on what the Temporary User is looking to use the vehicle for (e.g., without limitation, for towing, hauling or errands)"), [0076] (VCS may monitor for "unauthorized objects or cargo ... and/or an unauthorized trailer tow").

Pet. 20-21

[0083] "At step 808, the vehicle owner may be able to review the temporary user's vehicle rental request. The owner may review the requested rental based on what the Temporary User is looking to use the vehicle for (e.g. without limitation, for towing, hauling, or errands), **when the requested use will be taking place**, and where. The owner may also review the Temporary Users profile and rental history, to see how they have ranked with past experiences using the vehicle rental authorization system at step 810."

Ex. 1005 (Kleve) at ¶83

G1: Kleve’s “coded data” includes “privilege settings” / E-key includes privilege settings

- Kleve’s “virtual key” is “enable[d]” for the “rental period”:

[0069] At step 604, the vehicle Owner may then generate a virtual key based on a password generated by the vehicle Owner that may include a matrix barcode or a code word that the Temporary User may enter/send to the vehicle when ready to begin the rental term. . . . At step 616, the virtual key is generated and sent to the Temporary User.

[0071] At step 618, the Temporary User may send the virtual key to the server requesting access to the vehicle, . . . if it is the scheduled time for the rental, the vehicle may compare the identity credentials just inputted at the vehicle and the one previously sent virtual key to the vehicle from the vehicle Owner to determine authorization.

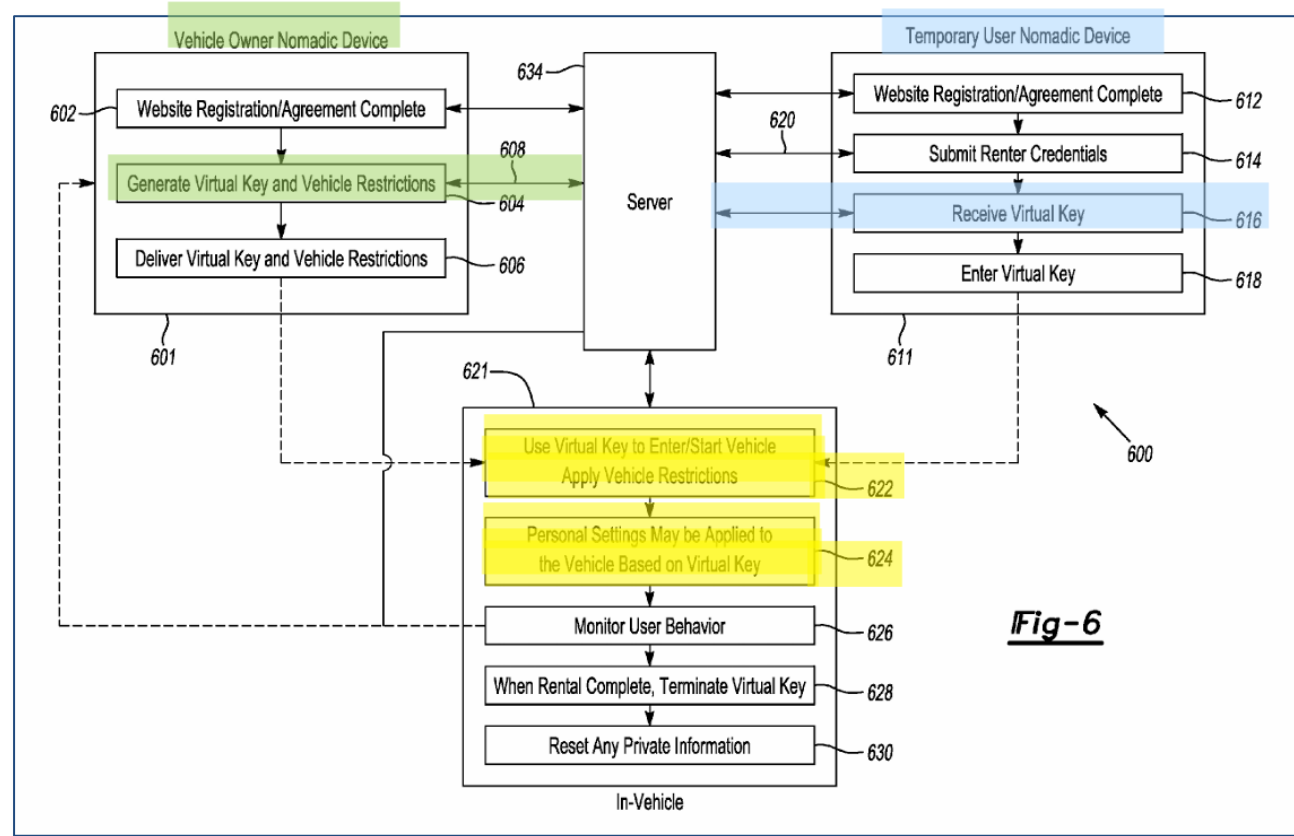


Fig-6

G1: Kleve's "coded data" includes "privilege settings" / E-key includes privilege settings

- Three different use cases for e-key after rental period starts:
- (1) E-key allows renter to unlock and turn on car without further verification needed:

[0048] "At step 322, ... [t]he virtual key may allow a Temporary User temporary granted access to the Owner's vehicle. The granted access allowed by the virtual key may permit entry of the vehicle; grant a keyless drive-away of a vehicle, and/or both."

Ex. 1005 (Kleve) at ¶48; Pet. 15

- (2) Renter enters vehicle with e-key and uses credential for verification, **or** (3) Renter uses credential for verification at the exterior of car before entering:

[0049] "The system may be further extended to facilitate the virtual key with additional security by requiring remote credential verification at the vehicle. The remote credential verification at the vehicle may be done with additional hardware assembled on the exterior of the vehicle or in the vehicle cabin. The remote credential verification may be done by the VCS, using a server, or allowing the Owner to verify the Temporary User's request. For example, but not limited to, the Temporary User entering a credential verification password at the vehicle's touchscreen visual display while having the VCS, server, or owner compare and verify authorization."

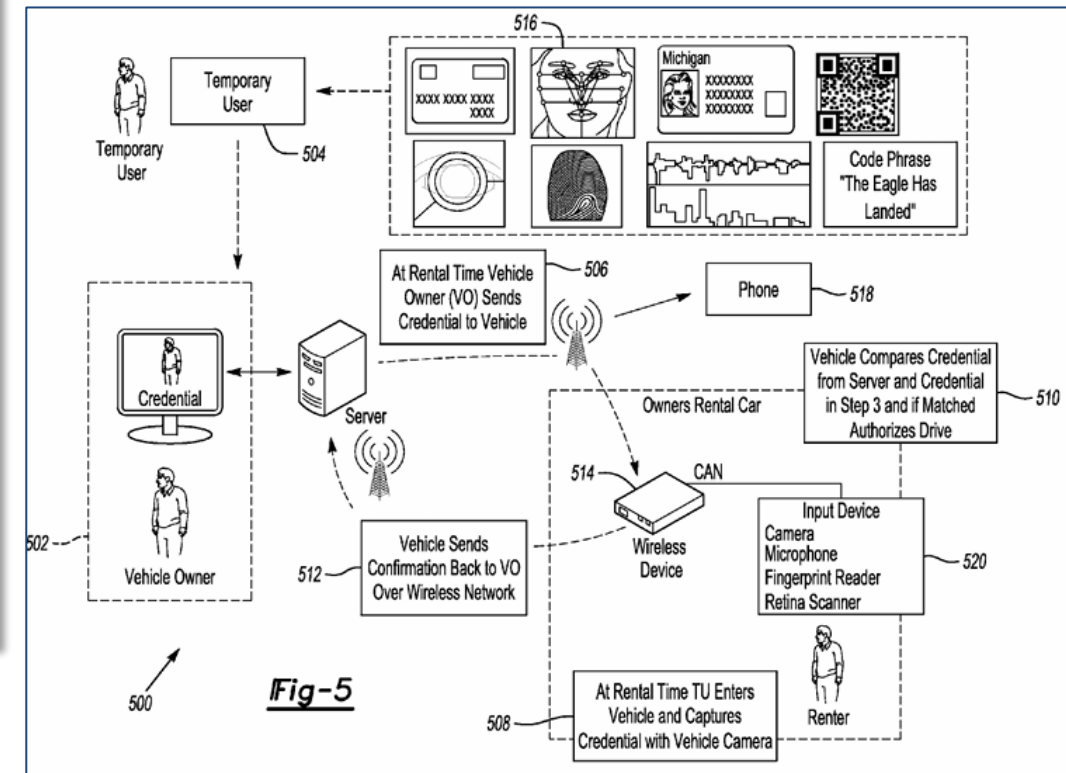
Ex. 1005 (Kleve) at ¶49; Pet. 23, 26

G1: Kleve's "coded data" includes "privilege settings" / E-key includes privilege settings

- Dr. Almeroth:

¶132: "For example, in one embodiment, Kleve discloses using a 'matrix barcode (ex. two-dimensional code) ... as the virtual key being recognized by the VCS.'" Kleve at ¶ [0044]. A matrix barcode may be an image, such as a QR code, as shown in Figure 5 of Kleve, annotated below. A 'smart phone may be used to communicate the matrix barcode information to the vehicle rental micro-business system directly.' *Id.* For example, the vehicle may have "input devices which may be connected to the VCS," such as "a camera" or "matrix barcode scanner." *Id.* at ¶ [0067]. These input devices use wireless communications because they can read coded data from a mobile device without a wired connection—for example, by capturing an image of a matrix barcode displayed on a mobile device.

Ex. 1004 (Almeroth Decl.) at ¶132; Pet. 20

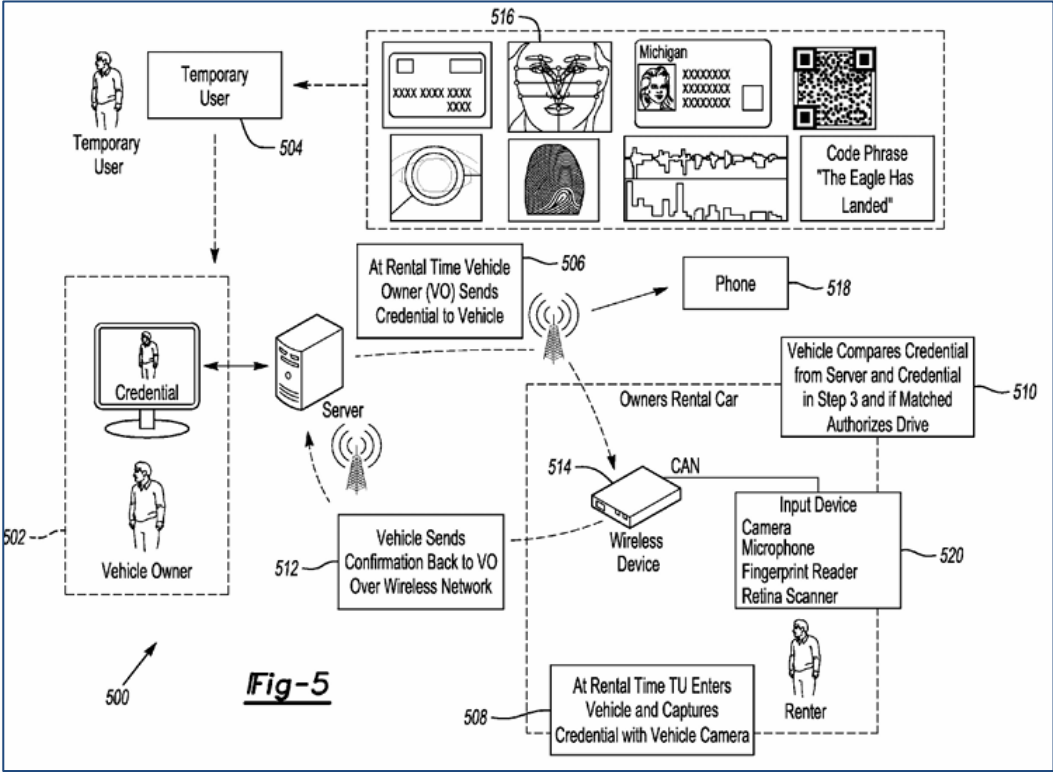


G1: Kleve’s “coded data” includes “privilege settings” / E-key includes privilege settings

- Dr. Almeroth:

¶133: “Kleve’s matrix barcode is associated to the eKey for use by the mobile device and enables functions of the virtual key for unlocking and use of the vehicle. For example, Kleve discloses that ‘Temporary User identification’ may be ‘used as a virtual key, or in addition to the virtual key, allowing the Temporary User access to the Owner’s vehicle while enabling a keyless drive-away.’ *Id.* at ¶ [0063]. The Temporary User’s information may include a ‘matrix barcode.’ *Id.* ‘Once the Temporary User has the matrix barcode scanned by the vehicle, the smart phone may be able to connect with the VCS and be used to enter and enable the vehicle drive away event.’ *Id.* at ¶ [0044]”

Ex. 1004 (Almeroth Decl.) at ¶133; Pet. 20

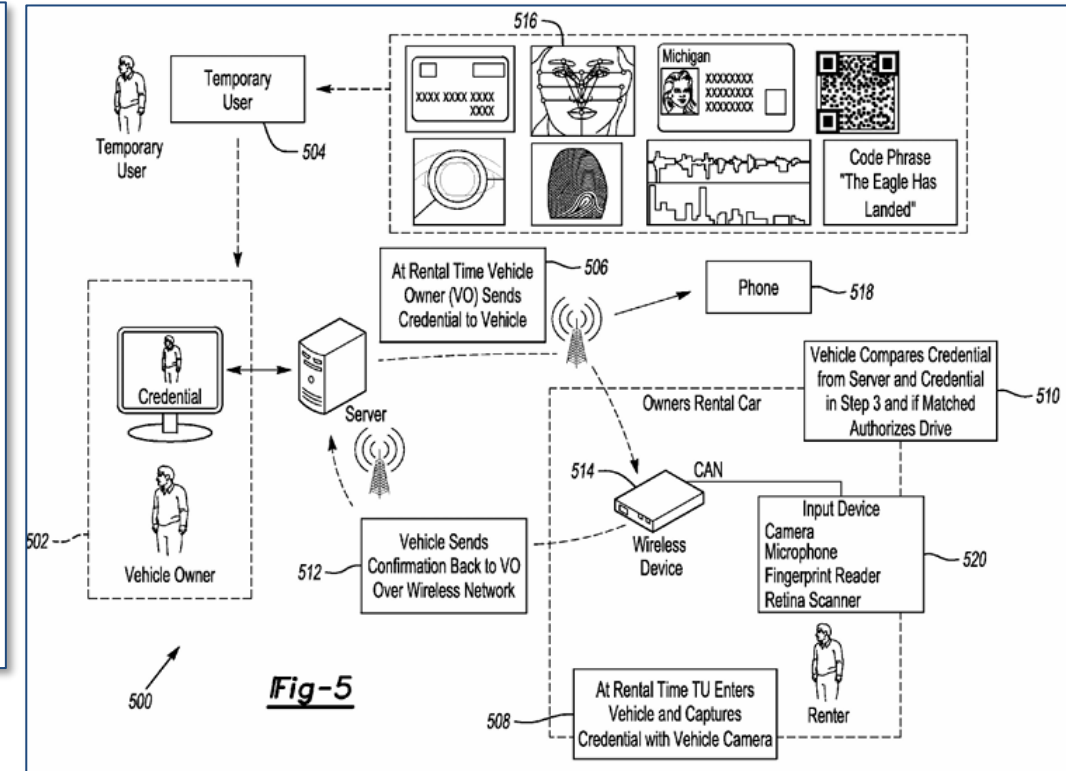


G1: Kleve's "coded data" includes "privilege settings" / E-key includes privilege settings

- Dr. Almeroth:

¶135: “Kleve teaches that ‘Temporary User identification and virtual key may be sent in an encrypted message to the VCS.’ Kleve at ¶ [0063]. An encrypted message is a type of coded data—specifically, data encoded according to an encryption scheme. Because Kleve uses wireless communication circuitry (e.g., the modem, Bluetooth transceiver, or wireless router that I discuss above for Limitations 1[b] and 1[c]) to communicate with a server and a user’s mobile device, a POSITA would have understood that the wireless communication circuitry would receive the encrypted message.”

Ex. 1004 (Almeroth Decl.) at ¶135; Pet. 19-20



G1: Kleve's "coded data" includes "privilege settings" / E-key includes privilege settings

- Dr. Almeroth testified that Kleve's virtual key includes "privilege settings":

¶139: "Kleve further discloses that the virtual key includes restrictions on the types of use of the vehicle by a Temporary User using the virtual key. For example, Kleve discloses that the 'Owner may set user restrictions,' and '[t]he restrictions may be based on, but not limited to, the owner's selection of parameters including, but not limited to, speed, global position coordinates, or load weight restrictions.' *Id.* at ¶ [0040]. The selection of restrictions may be based on the types of use agreed to between the Owner and the Temporary User when negotiating the terms of the rental. For example, the Temporary User may request to rent a vehicle for running errands, and not for towing and hauling cargo, and the virtual key may thus be configured to monitor for unauthorized cargo or an unauthorized trailer tow. *Id.* at ¶¶ [0083] ("The owner may review the requested rental based on what the Temporary User is looking to use the vehicle for (e.g. without limitation, for towing, hauling, or errands), when the requested use will be taking place, and where."), [0076] ("The monitoring done by the vehicle rental micro-business may include, but not limited to, unauthorized objects or cargo, unauthorized driving behavior, unauthorized driver, and/or an unauthorized trailer tow.").

Ex. 1004 (Almeroth Decl.) at ¶139; Pet. 20-21

G1: Kleve's "coded data" includes "privilege settings" / E-key includes privilege settings

- Dr. Almeroth testified that it would have been obvious to include the privilege settings in Kleve's "coded data":

¶140: "In my opinion, it also would have been obvious to a POSITA to include the restrictions on types of use of the vehicle as part of the coded data associated with a virtual key—for example, as part of the encrypted data described in Hatton. *See* Hatton at 7:33-56. As I explain above in the section titled "Motivation to Combine Kleve and Hatton and Reasonable Expectation of Success," a POSITA would have been motivated to include data identifying restrictions on a Temporary User's use of the vehicle as part of the encrypted data transmitted with the electronic key or as part of the electronic key so that the Temporary User cannot modify those restrictions at his or her mobile device and circumvent the restrictions."

Ex. 1004 (Almeroth Decl.) at ¶140; Pet. 20-21

G1: Kleve's "coded data" includes "privilege settings" / E-key includes privilege settings

- ID:

"At this stage of the proceeding, we first are persuaded Petitioner demonstrates that Kleve's "virtual key" is coded data because it is wirelessly communicated from a server to a vehicle in an encrypted format. See Ex. 1005 ¶ 63."

ID at 37

"Second, we are persuaded that Petitioner adequately shows Kleve teaches, or at least suggests, an e-key that includes 'privilege settings that limit types of use of the vehicle' because we are persuaded that the distribution of Kleve's virtual e-key includes a rental period restriction. For purposes of institution, the rental period restriction appears to be a 'type of use of the vehicle' and delineates the start/stoppage of when the vehicle can be used. Specifically, we are persuaded by the Petition's reliance on Kleve's express disclosure that 'terms and conditions for the rental period' are agreed to before the virtual key is generated. See Pet. 15 (citing Ex. 1004 ¶ 138). We preliminarily agree with Petitioner that Kleve describes an e-key that is only operable during a rental period because Kleve discloses, 'The owner may review the requested rental based on what the Temporary User is looking to use the vehicle for (e.g., without limitation, for towing, hauling, or errands), when the requested use will be taking place, and where.'. Ex. 1004 ¶ 138; see Ex. 1005 ¶ 83."

ID at 37

G1: Kleve's "coded data" includes "privilege settings": Dr. Almeroth's testimony

- ***PO's Surreply Position:***

The Institution Decision credited Dr. Almeroth's testimony that "the virtual key in *Kleve* is always generated after the rental agreement." Paper 14, at 38.

during a given rental period." *Id.* ¶ 119. According to Dr. Almeroth, this "indicates that rental agreement restrictions were sent with the request so that the virtual key could be associated with said restrictions." *Id.* ¶ 152; *see also* Ex. 1005 ¶ 68 ("Once the rental period has expired the virtual key may be reset and cleared from the VCS.")). Dr. Almeroth further testifies that the virtual key in *Kleve* is always generated after the rental agreement.

Ex. 1004 ¶¶ 152, 156 ([Once] "the Temporary User selects the vehicle, pays the appropriate amount and signs a consent agreement," then "the system may generate a virtual key to distribute to the Temporary User and VCS.")).

Thus, after review of the arguments and evidence, we find that Petitioner has provided adequate explanation and supporting evidence that *Kleve* alone or in combination with *Hatton* teaches the challenged claim limitation.

On cross-examination, however, Dr. Almeroth admitted his testimony was wrong. Response, 47-48.

PO Surreply 7

G1: Kleve’s “coded data” includes “privilege settings”: Dr. Almeroth’s testimony

- **POR:**

period” included in the set up or distribution of a virtual key. *See* sections III.B.-D, *supra*.

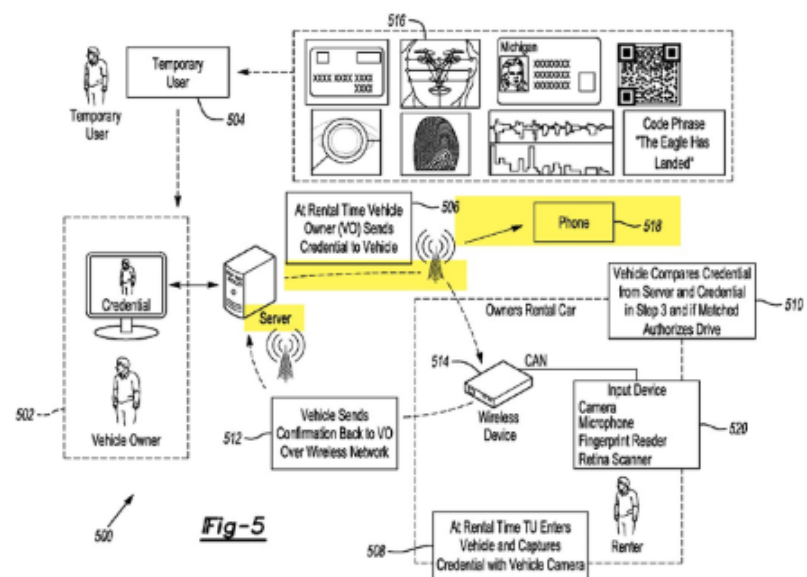
1. **Rental agreement terms are not included in the virtual key because a Temporary User uses the already-generated, already-distributed virtual key to access the vehicle and thereafter, “agree to rental terms.”**

Not only does *Kleve* never disclose rental agreement terms being included in either the generation or distribution of an electronic key, a POSITA would have understood from the disclosure of *Kleve* that they could not be. EX2021, ¶¶ 92-98. *Kleve* teaches that a Temporary User need not “agree to rental terms” until *after* the virtual key has been generated and distributed. EX1005, ¶ 65; EX2021, ¶ 93. Petitioners point to *Kleve*’s virtual key in the form of an encrypted message or matrix barcode as the alleged “coded data,” (Pet. 19-20), and *Kleve* teaches *after* this virtual key is distributed to the Temporary User, “the Temporary User may use their virtual key credential to access the vehicle” (EX1005, ¶ 67). However, *Kleve* explicitly discloses that the Temporary User may “agree to rental terms” *at the vehicle*—*after* the virtual key has been distributed to the Temporary User, and *after* the Temporary User has utilized the virtual key to access the Owner’s vehicle. EX1005, ¶¶ 65, 67.

There can be no dispute that by the time the virtual key is distributed to the Temporary User the virtual key has already been generated (EX2022, 58:8-59:10),

G1: Kleve’s “coded data” includes “privilege settings”: Dr. Almeroth’s testimony

- PO Surreply:**



Accordingly, this “encrypted message” is not “from the mobile device,” as required by all claims, and therefore whether or not combined with *Hatton* as proposed, *Kleve* fails for all claims. Pet., 19.

Petitioners further rely on *Kleve* as disclosing a “matrix barcode,” which they allege “as the virtual key,” and the alleged “coded data.” Pet., 20. However, *Kleve* does not teach that this “matrix barcode” includes the rental agreement or any of its alleged conditions. Response, 5-52. Instead, *Kleve* provides two different options for the server to obtain the rental agreement: (1) **before** the generation of a virtual key and (2) **after** the generation of a virtual key. EX1005, ¶¶ 62, 65.

Kleve teaches a rental agreement occurring after a user receives a virtual key. Here, the Temporary User, who has already used the virtual key to enter the vehicle, may “agree to rental terms” using the vehicle’s touchscreen. *Id.*, ¶¶ 65, 47, 67. Accordingly, the virtual key has already been generated and distributed, all before there is any rental agreement. *Id.*; Response, 44-45. Plainly, the alleged “privilege settings” of the rental agreement cannot be placed in any “virtual key” when the virtual key exists before any rental agreement, and Petitioners do not dispute this. Reply, 15 (characterizing *Kleve*’s disclosure as an “optional,” “alternative embodiment”).

There is no basis in fact for accepting Dr. Almeroth’s now discredited testimony that a key is “always generated after the rental agreement,” and likewise no basis for relying on this inaccurate statement to conclude that a request for a virtual key would include rental agreement terms. Paper 14, at 48.

- 2. **For any rental agreement made *before* a virtual key is generated, Petitioners claim the vehicle already has restrictions before the Temporary User’s arrival—*Kleve* does not teach to have the Temporary User send them to the vehicle and doing so would make no sense when the vehicle already has them.**

When a rental agreement is already in place, it would make no sense to provide the alleged “privilege setting” to the vehicle in coded data from the Temporary User’s mobile device, since Petitioners claim that the vehicle already

G1: Kleve's "coded data" includes "privilege settings": Dr. Almeroth's testimony

- Kleve Fig. 5 embodiment:

[0062] "FIG. 5 shows an illustrative example of an overview of how the vehicle rental micro-business may be structured with a keyless transaction between the Owner of the vehicle and the Temporary User. This example illustrates the process after the vehicle Owner and Temporary User have already setup a user profile within the database and have both agreed to the rental agreement. At step 502, the vehicle Owner may enter in vehicle authorization credentials based on information received by the Temporary User to set up a virtual key. The virtual key may be sent to the vehicle allowing Temporary User access to the Owner's vehicle."

Ex. 1005 (Kleve) at ¶¶62; Reply 4, 13-15

[0064] "The Temporary User's information for credential verification 516 may be collected and exchanged using several methods including . . ."

[0065] "An example for applying Temporary User credential verification at a vehicle may include, but not limited to, the use of additional hardware integrated with the VCS to allow collection and exchange of information to enable a keyless drive-away rental event. For example the Temporary User may use their credit card at a vehicle with the use of hardware integrated with the VCS to collect payment credentials, identify the user, and/or agree to rental terms."

Ex. 1005 (Kleve) at ¶¶64-65; Reply 13-15

G1: Kleve’s “coded data” includes “privilege settings”: Dr. Almeroth’s testimony

- Kleve Fig. 3 embodiment:

[0047] “... When the Temporary User and vehicle Owner agree to terms 316 the website may generate the exchange or propose a rental agreement 318. **The agreement between the Owner and Temporary User can be signed and payment made through the website at step 320.** The agreement to rental terms and conditions between the parties may be done with the website using smart phones or a smart phone application, or any other type of nomadic device. **Rental conditions may also be displayed on the vehicle's touchscreen visual display and accepted or rejected through the touchscreen visual display.**”

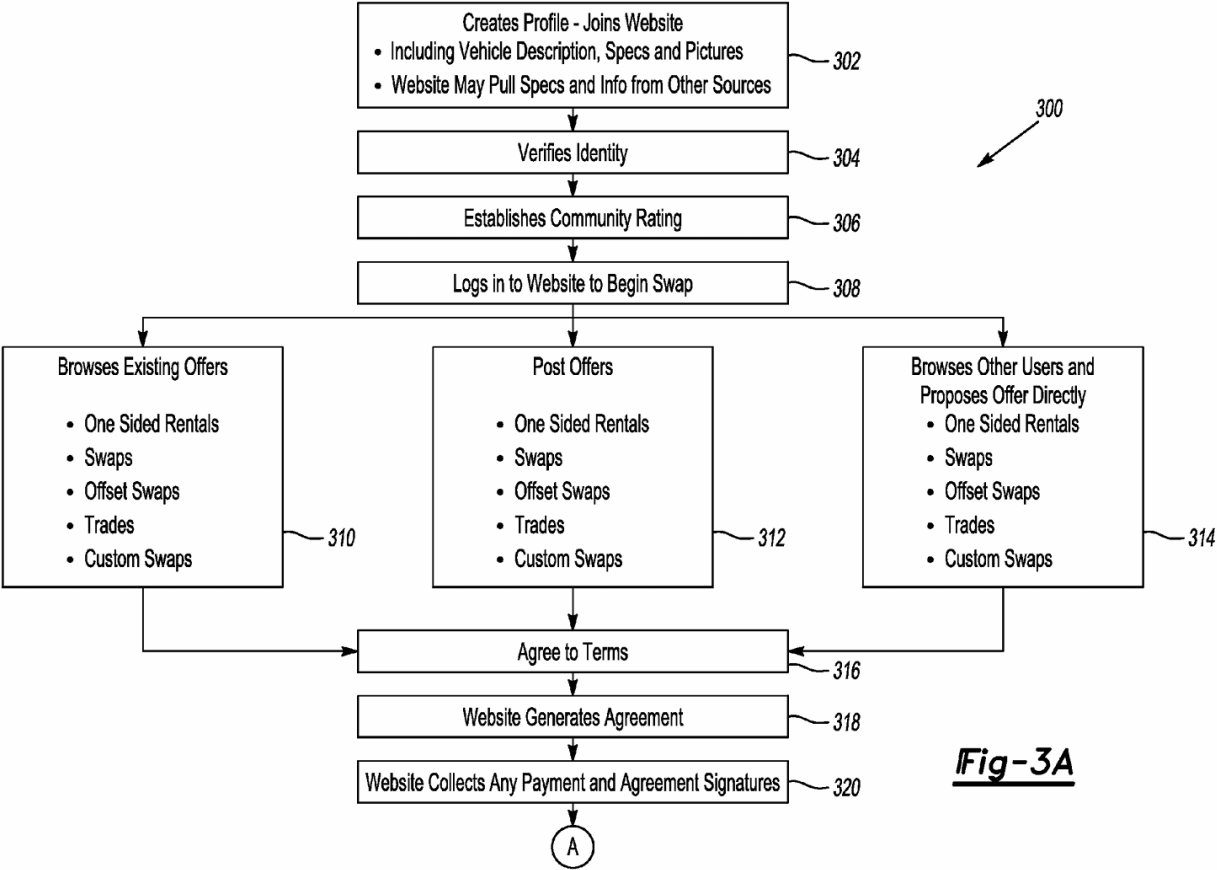


Fig-3A

G1: Kleve's "coded data" includes "privilege settings": Dr. Almeroth's testimony

- Kleve's Fig. 3 and Fig 5 embodiments:

[0062] "FIG. 5 shows an illustrative example of an overview of how the vehicle rental micro-business may be structured with a keyless transaction between the Owner of the vehicle and the Temporary User. This example illustrates the process after the vehicle Owner and Temporary User have already setup a user profile within the database and have both agreed to the rental agreement."

Ex. 1005 (Kleve) at ¶62; Reply 15

[0047] "... When the Temporary User and vehicle Owner agree to terms 316 the website may generate the exchange or propose a rental agreement 318. The agreement between the Owner and Temporary User can be signed and payment made through the website at step 320. The agreement to rental terms and conditions between the parties may be done with the website using smart phones or a smart phone application, or any other type of nomadic device. Rental conditions may also be displayed on the vehicle's touchscreen visual display and accepted or rejected through the touchscreen visual display."

Ex. 1005 (Kleve) at ¶47; Pet. 29

G1: Kleve's "coded data" includes "privilege settings": Settings Not Always Sent to the Vehicle

- ***PO's Surreply Position:*** Server **always** sends privilege settings to vehicle

I. Introduction

All claims require that a vehicle receives "coded data from the mobile device when using the eKey, the coded data enables functions of said eKey" and that "coded data includes privilege settings associated with the eKey for limiting types of use of the vehicle." Even after Reply, Petitioners cannot identify any disclosure of *Kleve* or *Mikan* that teaches or suggests including any "privilege settings" in any alleged coded data, let alone any coded data including privilege settings which is sent *from a mobile device*. For all grounds, Petitioners cannot explain why, if the vehicle already has the alleged "privilege settings," there would be any motivation to modify the references' disclosures for the vehicle to also "receive coded data from a mobile device ... the coded data includes privilege settings."

PO Surreply 1

G1: Kleve’s “coded data” includes “privilege settings”: Settings Not Always Sent to the Vehicle

- ***PO’s Surreply Position:*** Server **always** sends privilege settings to vehicle

⁸ does nothing to change the lack of disclosure fatal to all *Kleve*-based grounds. Reply, 2-3, 12-13, 16.¹

Nevertheless, even if all the Reply arguments were true—i.e., “following agreement, a virtual key is sent to the vehicle,” therefore “to restrict use of the virtual key to rental time, the rental period would need to be communicated to the vehicle with the virtual key”—this would still fail to teach or suggest including any privilege setting in any coded data sent to the vehicle *from the mobile device* of the

¹ Petitioners’ reliance on hindsight modifications based on purported “common sense” fails, as this attorney argument (or at best conclusory expert testimony) is not based on any prior art document. USPTO Memorandum, July 31, 2025, “Enforcement and Non-Waiver of 37 C.F.R. § 42.104(b)(4) and Permissible Uses of General Knowledge in Inter Partes Reviews” (“applicant admitted prior art (AAPA), expert testimony, common sense, and other evidence that is not ‘prior art consisting of patents or printed publications’ (collectively, ‘general knowledge’) may not be used to supply a missing claim limitation”); 35 U.S.C. § 312(a)(3) (Board shall deny any petition that fails to comply with Rule 104(b)(4)); *see Qualcomm Inc. v. Apple Inc.*, 24 F.4th 1367, 1373-77 (Fed. Cir. 2022) (vacating, remanding to determine whether AAPA improperly formed “basis” of petitioner’s patentability challenge).

⁹ Temporary User. Reply, 4. Doing so would be nonsensical, as neither *Kleve* nor Petitioners offer any reason why after “the restrictions are delivered to the vehicle,” they would be delivered again “afterwards, when Temporary User arrives at the vehicle.” *Id.*, 3.

A. Even if the “rental period” or any other alleged “privilege setting” were delivered to the vehicle with a virtual key, nothing in Reply shows any “privilege setting” included in coded data sent from the Temporary User’s mobile device.

Petitioners offer no evidence to support the Reply’s hollow attorney arguments, let alone any POSITA-supported evidence of what, Petitioners argue, “no POSITA would ever find desirable.” *Id.*, 16; *id.*, 2 (“nonsensical,” “makes no sense”), 8 (“there must be some mechanism”), 16 (“defies common sense”). Ultimately Petitioners provide only a litany of hindsight excuses to modify *Kleve*’s disclosure for “security,” “proper enforcement,” and “preventing a Temporary User from tampering with the electronic key or otherwise circumventing restrictions and limits on the use of the electronic key.” *Id.* 2-3, 8, 15-16. But none of that is based on any art of record.

Regardless, these arguments ignore the actual claim requirements, as the Reply provides no reason to include the rental period in any coded data sent from the Temporary User’s mobile device. To the contrary, there would be **no reason** for any data sent by the Temporary User’s mobile device to re-send to the vehicle

G1: Kleve's "coded data" includes "privilege settings": Settings Not Always Sent to the Vehicle

- ***Petitioner's Reply:***

1. **Kleve Teaches Assigning and Enforcing Restrictions Before the Rental Period**

Enforcing the rental period before the rental period begins is both common sense and made clear in Kleve. As the Board found, Kleve's virtual key is "only operable during a rental period." ID 37; EX1005, ¶139 ("The virtual key ... enable[s] the keyless drive system for the appropriate Temporary user *during a given rental period*"). Thus, the virtual key and its associated coded data includes (or it would have been obvious to include) at least the rental period so that access to vehicle is limited to "a given rental period." Pet. 15, 20; EX1004, ¶¶96, 111, 139-140.

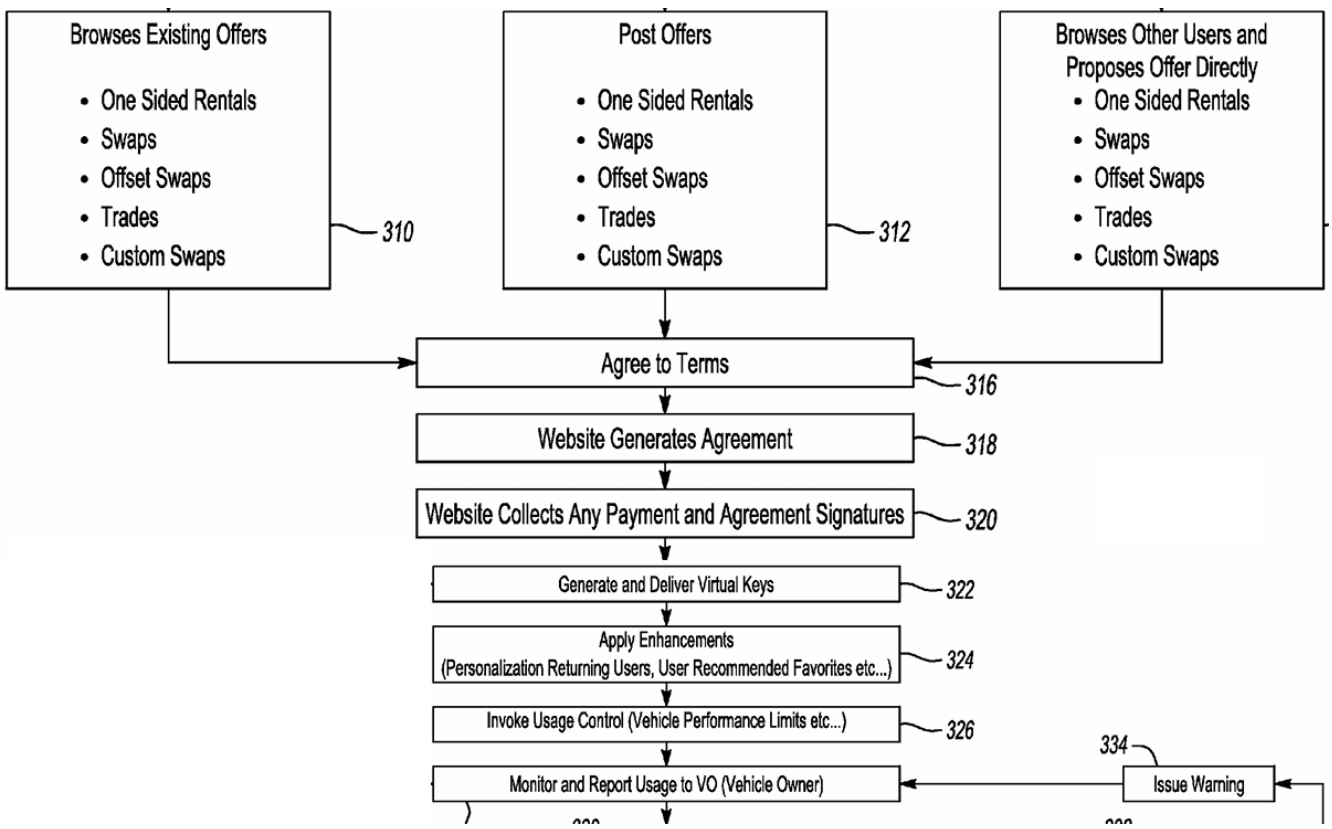
Kleve elsewhere teaches that restrictions are assigned *before* the rental period begins. For example, in Figure 6, Kleve teaches that after restrictions are agreed to, the server simultaneously "Generate[s] Virtual Key and Vehicle Restrictions." EX1005, Fig. 6. The virtual key is then "generated and sent to the Temporary User" at step 616, and the restrictions are delivered to the vehicle at step 606. *Id.*, ¶69. Afterwards, "when the Temporary User arrives at the vehicle *within the scheduled rental time*," the vehicle "Appl[ies] Restrictions." *Id.*, ¶70, Fig. 6.

Similarly, Kleve teaches that "the VCS may implement assigned vehicle control limitations during the use of the rental term," meaning restrictions are assigned *before* the rental term begins. EX1004, ¶51, Fig. 6 ("use virtual key" and "apply vehicle restrictions" occur simultaneously in step 622). A restriction that begins with the rental term, such as "speed," would have to be assigned before the

G1: Kleve’s “coded data” includes “privilege settings”: Settings Not Always Sent to the Vehicle

• **Kleve’s disclosure:**

[0048] “At step 322, after identification of the Temporary User with an accepted agreement and payments made, the Vehicle rental micro-business system may generate and deliver virtual keys to the Temporary User. The virtual key may allow a Temporary User temporary granted access to the Owner’s vehicle. The granted access allowed by the virtual key may permit entry of the vehicle; grant a keyless drive-away of the vehicle and/or both. The Temporary User may enter a virtual key outside or inside the vehicle, while credential authorization may be processed by the VCS, a server and/or by the Vehicle Owner.”



Ex. 1005 (Kleve) at ¶48, Fig. 3; Pet. 15,23, 25

G1: Kleve’s “coded data” includes “privilege settings”: Settings Not Always Sent to the Vehicle

- Kleve’s disclosure:**

[0069] “...At step 604, the vehicle Owner may then generate a virtual key based on a password generated by the vehicle Owner that may include a matrix barcode or a code word that the Temporary User may enter/send to the vehicle when ready to begin the rental term. Another exemplary embodiment of generating a virtual key may be done by using Temporary User's credentials including fingerprint recognition, photos of credit cards, photo of forms of ID, facial recognition, voice print recognition, phrase for speech recognition, temporary mobile web login IDs and password, or other type of unique Temporary User identification at step 614. **At step 616, the virtual key is generated and sent to the Temporary User.** The Owner may deliver a virtual key to the vehicle for recognizing the Temporary User having authorization to enable a keyless drive-away at step 606.”

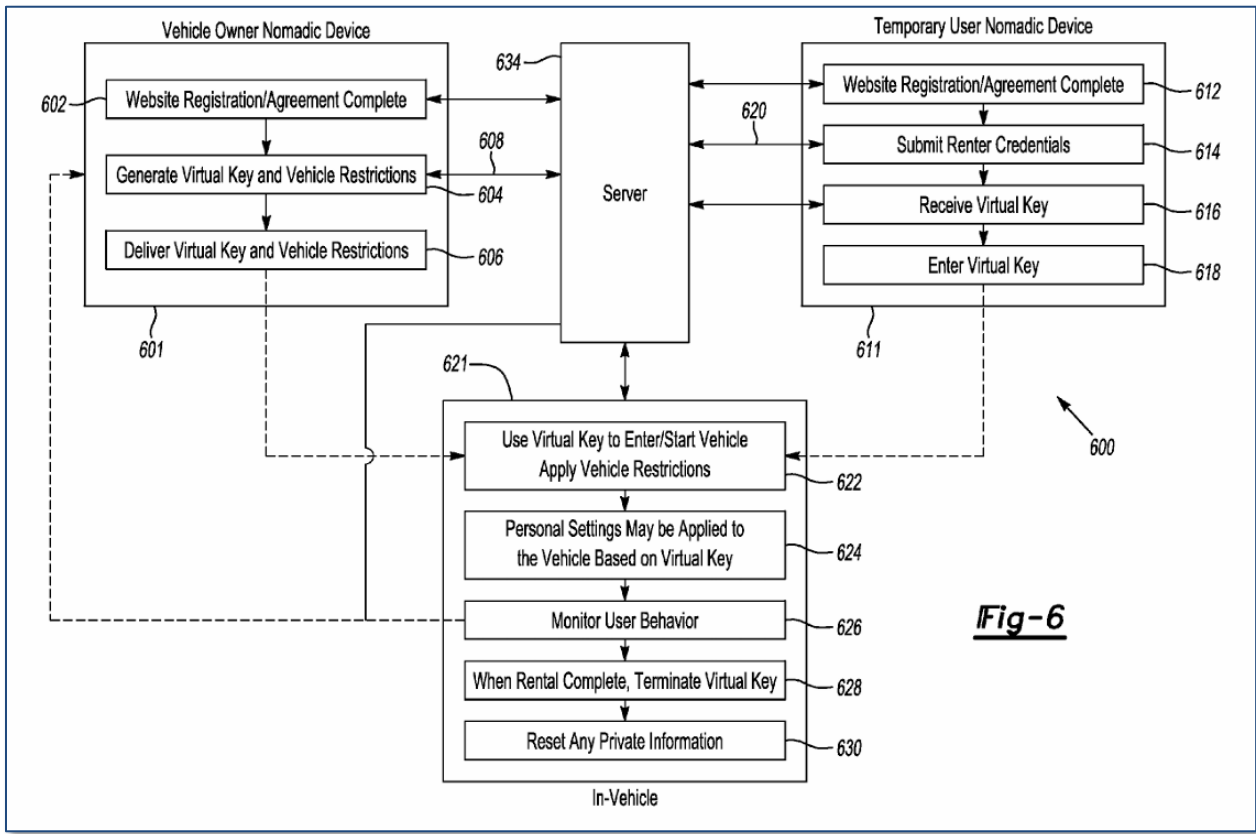


Fig-6

G1: Kleve’s “coded data” includes “privilege settings”: Server does not always send priv settings

• **Kleve’s disclosure:**

[0073] “At step 626, during the rental term the VCS may monitor the Temporary User's utilization of the vehicle including, but not limited to, renter verification, driving behavior, vehicle location, speed, fuel level, and other vehicle information requested by the vehicle owner. For example, the system may monitor that the actual authorized renter is the one driving the vehicle with the use of an interior viewing camera embedded with facial recognition software. The monitoring information is sent to the vehicle owner, and may have other additional parameters that may only be sent to the owner if they exceed or violate a restriction limit. These additional parameters may include, but not limited to speed limits, weight limits, or “No-Go Zones” which are prohibited areas where the owner does not want their vehicle to be used.”

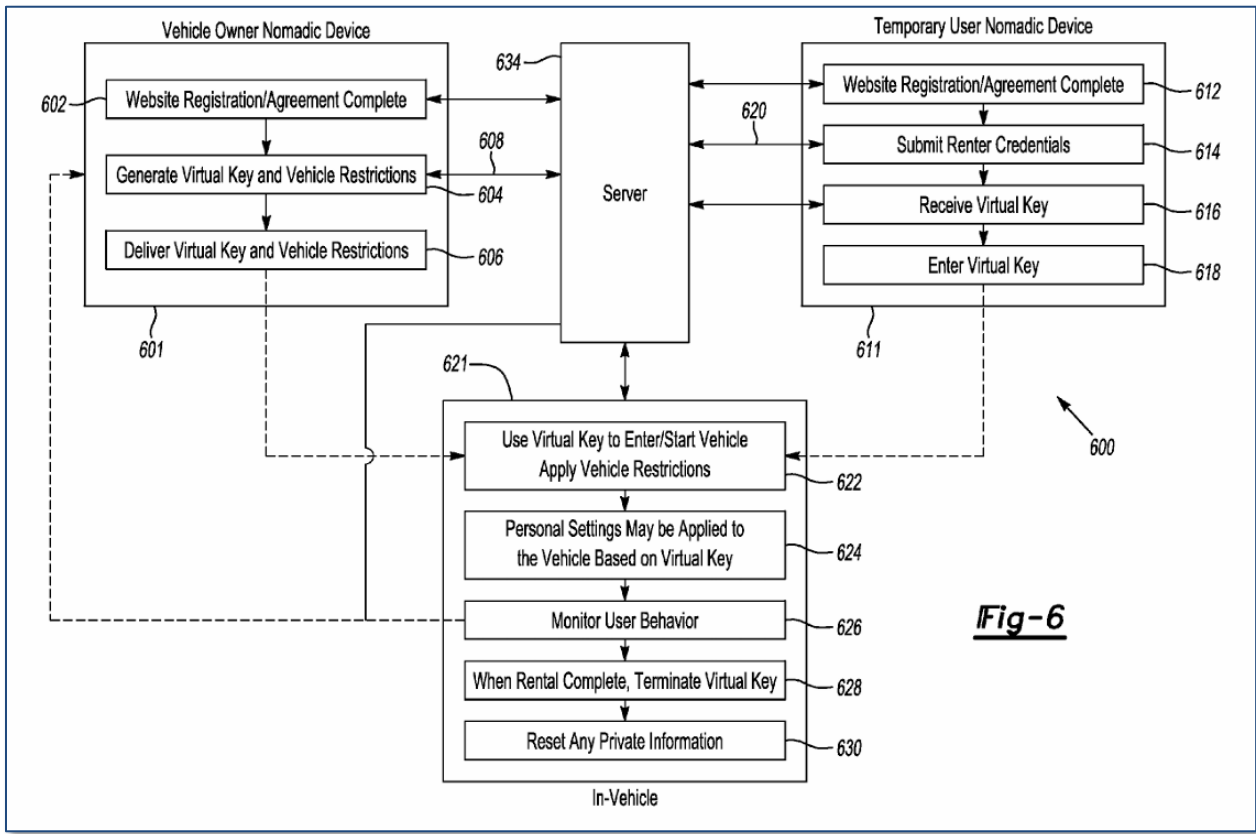
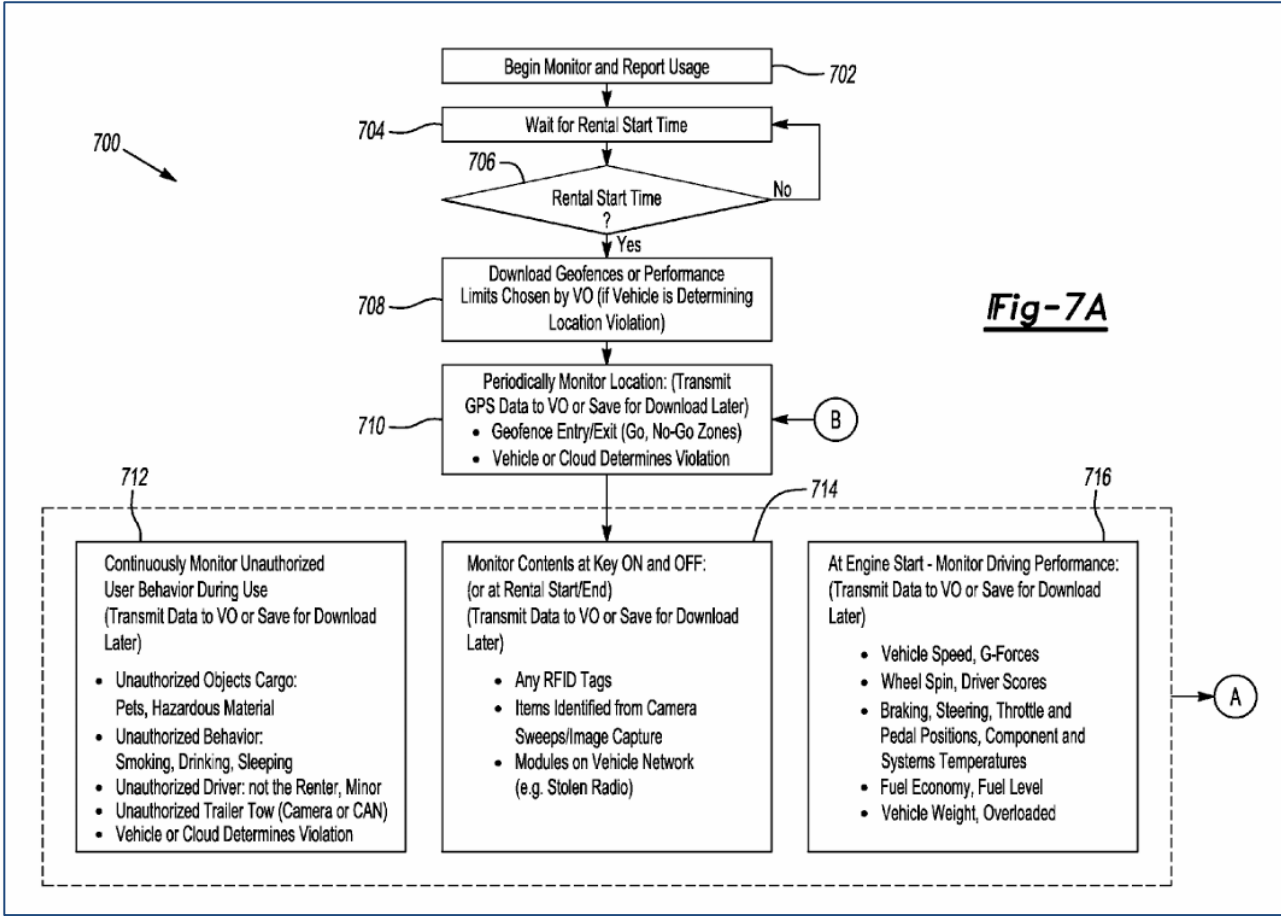


Fig-6

G1: Kleve’s “coded data” includes “privilege settings”: Server does not always send priv settings

• **Kleve’s disclosure:**

[0075] “In the illustrative embodiment as shown in FIG. 7 is an overview of a vehicle rental micro-business monitoring process integrated with a VCS. At step 702, the VCS may begin monitoring and report usage of the vehicle to the owner. The system may wait for the rental period to start at step 704. Once the Temporary User initiates the rental event, the system detects a rental time start at step 706. The system may begin to download performance limitations and restrictions assigned by the vehicle owner at the start of the rental period at step 708. The performance limitations and restrictions downloaded to the VCS may include, but not limited to: setting a top vehicle speed, limiting the cargo load, and alerting the vehicle owner if the driver enters an area deemed to be prohibited by the owner..”



G1: Kleve's "coded data" includes "privilege settings": Step 214 Is Not Mandatory

- PO:** Step 214 is the exclusive means for setting and enforcing restrictions

“Unlike the rental agreement terms, agreed to by both parties, Kleve’s system teaches that only a Vehicle Owner can “set user restrictions” that will be monitored, e.g. load weight restrictions, rental end time, “no-go zones” or any other restrictions regardless of the terms of the rental agreement. ... Kleve’s system allows only these Owner-set “user restrictions,” set at step 214, to be monitored and controlled by the vehicle’s “VCS” (vehicle computing system), ...

POR 5; see also POR 13-18

- PO is wrong:**

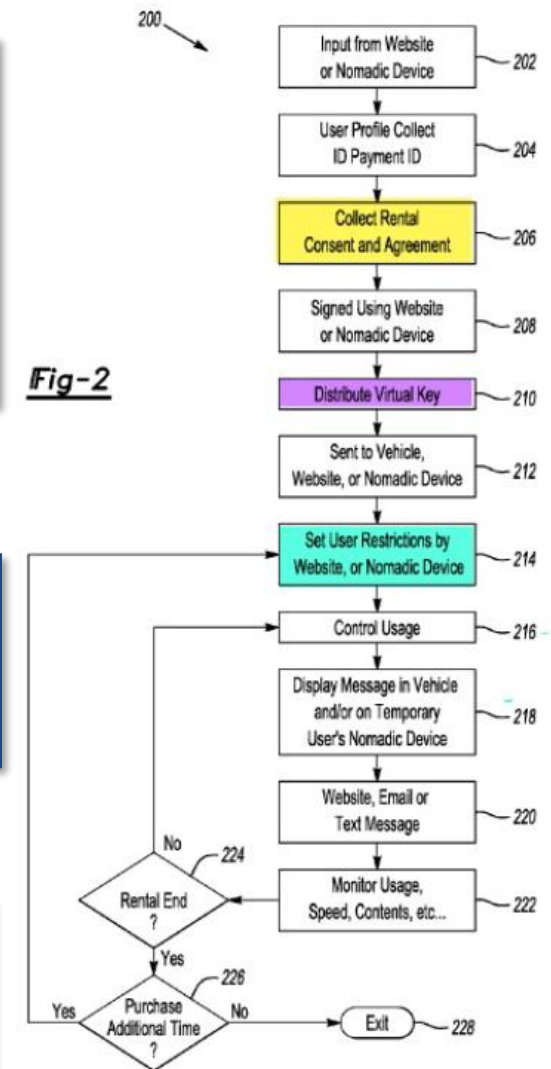
[0039] “At step 210, ... [t]he virtual key may also be sent to the vehicle configuring the VCS to enable the keyless drive system for the appropriate Temporary User during a given rental period.”

Ex. 1005 (Kleve) at ¶39; Pet. 15

- PO admits step 214 is “optional”:**

“Rather than include the parties’ rental agreement terms in the set up or distribution of a virtual key, Kleve’s system provides a separate, optional operation to allow only the Owner to “set user restrictions” at step 214.”

POR 13



G1: Kleve's "coded data" includes "privilege settings": Step 214 Is Not Mandatory

- **PO:** Owner can add use conditions "**regardless**" of the rental agreement:

"Unlike the rental agreement terms, agreed to by both parties, Kleve's system teaches that only a Vehicle Owner can "set user restrictions" that will be monitored, e.g. load weight restrictions, rental end time, "no-go zones" or any other restrictions regardless of the terms of the rental agreement."

"In Kleve, the Owner can enforce compliance with specific restrictions, whether or not such restrictions were also included as rental agreement terms."

POR 5

POR 9

[0041] "An exemplary example of control usage may be limiting the Temporary User from driving to restricted areas defined by the owner based on the rental terms and conditions. If the Temporary User enters a restricted area, he may be notified by the system and the vehicle may enter a remedial actions limiting vehicle speed."

[0051] "The Owner may have the options to set rental restrictions based on, but not limited to, speed, destination location, or load weight limitations. Controlling usage to enforce compliance with the rental agreement terms may be of more importance to a vehicle rental micro-business owner as this may be the only vehicle the Owner possesses."

Ex. 1005 (Kleve) at ¶¶ 41, 51; Reply 3-4

G1: Kleve's "coded data" includes "privilege settings": Step 214 Is Not Mandatory

- **PO:** If restrictions set during e-key setup, step 214 would be unnecessary

"Specifically, at step 214, shown in Figure 2 below, Kleve's system allows the Owner to select parameters that enforce the parties' agreed-upon terms and conditions and/or add specific restrictions for the usage of the rental vehicle, such as cargo load weight restrictions, rental end time, or global position coordinates corresponding to restricted areas. *Id.* It would not be necessary for Kleve to have such a solution to "enforce" any rental agreement terms if somehow those terms were already included as some "privilege setting" in Kleve's "set up," creation, or distribution of the virtual key, at step 210."

POR 15

- **POR:**

"Kleve's system provides a separate, optional operation to allow only the Owner to "set user restrictions" at step 214."

POR 13

- **Kleve:**

[0040] "At step 214, the Owner may have access to control usage of the vehicle being rented by the Temporary User. The Owner may set user restrictions by use of the website or nomadic device. The restrictions may be based on, but not limited to, the owner's selection of parameters including, but not limited to, speed, global position coordinates, or load weight restrictions.

Ex. 1005 (Kleve) at ¶40; Reply 7

- **PO is wrong:** Step 214 is "optional", and can still set restrictions after setup of key enables it for the rental period

G1: Kleve's "coded data" includes "privilege settings": Step 214 Is Not Mandatory

- **PO:** Kleve says all restrictions are "initially" set at start of rental period

"Instead, these restrictions are "***initially set*** by the Owner at the beginning of the rental term," which undisputably occurs after distribution of the virtual key credential, as discussed above. Id., ¶¶ 43 (emphases added), 40."

- **PO is wrong:**

POR 14

[0043]"At step 224, the system may notify the Temporary User that the agreed upon rental period may expire soon, and if the rental period has ended the system may prompt the Temporary User with a message asking if he would like to purchase additional rental time. The system may allow the Temporary User to purchase additional rental time or decline the offer with the use of the vehicle touchscreen display or a nomadic device at step 226. If the rental term has ended, and no additional time is purchased, the system may begin the vehicle rental exit process within the VCS at step 228. If the rental period is still within the agreed upon rental period, **the system may carry on to monitor** the vehicle allowing the Owner continued control of the vehicle with the use of **vehicle restriction limits initially set by the Owner at the beginning of the rental term.** At step 226, if the Temporary User decides that he may need to purchase additional rental time, the system may update the new rental period end time restriction and continue to monitor usage of the vehicle."

Ex. 1005 (Kleve) at ¶43; Reply 9

- Kleve does not suggest that ***all*** restrictions are initially set at rental term start

G1: Kleve’s “coded data” includes “privilege settings”: Step 214 Is Not Mandatory

- PO’s Surreply:** Restrictions always assigned at “start of the rental period”

During the rental term, therefore, the VCS implements restrictions. But Kleve dictates such restrictions are “assigned by the vehicle owner at the start of the rental period.” Id., ¶¶ 75, 43 (“initially set by the Owner at the beginning of the rental term.”).

Surreply 18

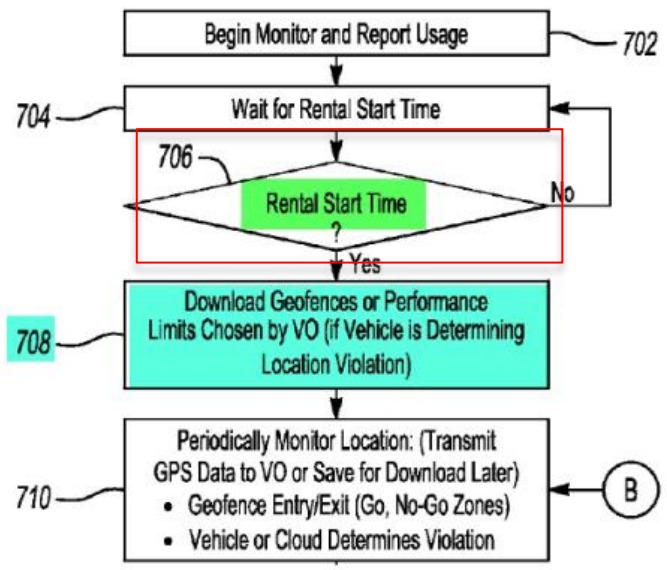
“Kleve reiterates that these restrictions cannot be set when the rental agreement is formed, . . . but are instead “restrictions assigned by the Vehicle Owner at the start of the rental period.” . . . The restrictions’ corresponding “performance limitations” for the VCS to monitor and control the vehicle’s usage are downloaded to the VCS at step 708, after “the Temporary User initiates the rental event,” at step 706.”

- PO is wrong:**

POR 16

[0075] “Once the Temporary User initiates the rental event, the system detects a rental time start at step 706. The system may begin to download performance limitations and restrictions assigned by the vehicle owner at the start of the rental period at step 708.”

Ex. 1005 (Kleve) at ¶75; Reply 14



Ex. 1005 (Kleve) at Fig. 7A; POR 18

G1: Kleve's "coded data" includes "privilege settings": Step 214 Is Not Mandatory

- ***PO's Surreply:*** Applying restrictions any earlier than step 214 would interfere with other renters

“Indeed, Kleve teaches the vehicle may not download any restrictions until the Temporary User has initiated the rental period, which makes sense, as the vehicle would not be able to apply any restrictions for an earlier renter.”

Surreply 23

G1: Kleve's "coded data" includes "privilege settings": Step 214 Is Not Mandatory

- **PO:** Kleve's virtual key is a credential that does not contain any restrictions

"The Temporary User identification or "credential" is ultimately distributed to be "used as a virtual key." ... Kleve's "virtual key credential" does not include any restrictions or other privilege about any agreed rental period, nor does this "credential" include any of the terms or conditions agreed to and accepted as the parties' rental agreement."

POR 11

- **PO is wrong:** Kleve:

[0063] "Additional Temporary User identification 504 may be sent to the vehicle Owner allowing for this information to be entered into the server and used as a virtual key, or **in addition to the virtual key**, allowing the Temporary User access to the Owner's vehicle while enabling a keyless drive-away."

Ex. 1005 (Kleve) at ¶63; Reply 4

[0049] "The system may be further extended to **facilitate the virtual key with additional security** by requiring remote credential verification at the vehicle. The remote credential verification at the vehicle may be done with additional hardware assembled on the exterior of the vehicle or **in the vehicle cabin**."

Ex. 1005 (Kleve) at ¶49; POR 24-25

- Key is for entering the vehicle, credential is for authenticating the renter

G1: Kleve's "coded data" includes "privilege settings": Step 214 Is Not Mandatory

- **PO:** Rental period is enforced by credentials, not by the privilege settings

"Moreover, by sending the authorization "credential" to the vehicle "at Rental Time," the Owner ensures "the scheduled rental period of time begins" (id., ¶ 66, Fig. 5) according to the agreed-upon rental period via sending the credential (id., ¶ 62, Fig. 5) and via receipt of the credential by the vehicle."

- **PO is wrong:** Kleve:

POR 36

[0048] "The granted access allowed by the virtual key may permit entry of the vehicle; grant a keyless drive-away of a vehicle, and/or both."

Ex. 1005 (Kleve) at ¶48; POR 48

[0049] "The system may be further extended to facilitate the virtual key with additional security by requiring remote credential verification at the vehicle. The remote credential verification at the vehicle may be done with additional hardware assembled on the exterior of the vehicle or in the vehicle cabin. The remote credential verification may be done by the VCS, using a server, or allowing the Owner to verify the Temporary User's request. For example, but not limited to, the Temporary User entering a credential verification password at the vehicle's touchscreen visual display while having the VCS, server, or owner compare and verify authorization."

Ex. 1005 (Kleve) at ¶49; POR 24

- Credential is optional, cannot enforce rental period

G1: Kleve's "coded data" includes "privilege settings": Step 214 Is Not Mandatory

- **PO:** If virtual key includes "rental period," credential is unnecessary

"In fact, were the agreed upon "rental period" somehow included in the virtual key credential set up or distribution as an alleged "privilege setting," it would not be necessary for the Vehicle Owner to also send the credential to the vehicle "at rental time.""

POR 12

- **PO is wrong:** Kleve:

[0049] "The system may be further extended to facilitate the virtual key with additional security by requiring remote credential verification at the vehicle."

Ex. 1005 (Kleve) at ¶49; POR 24

[0067] "Once the Temporary User enters the vehicle and captures the credentials with one of the methods mentioned above, the vehicle may verify that the Temporary User has approval to use the vehicle."

Ex. 1005 (Kleve) at ¶67; Reply 5

- Kleve expressly says the credential **facilitates** the key, it is complementary

G1: Kleve's renders obvious "coded data" including "privilege settings"

- Dr. Almeroth testified that it would have been obvious to include the privilege settings in Kleve's "coded data":

¶111: "A POSITA would have also understood that storing and transmitting electronic key information using encrypted data has an additional benefit: it prevents a Temporary User from tampering with the electronic key or otherwise circumventing restrictions and limits on the use of the electronic key (for example, by circumventing restrictions on use set by the Vehicle Owner, or by re-distributing the key to additional, unauthorized third parties). In order to make full use of these benefits, a POSITA would have been motivated to include data identifying restrictions on a Temporary User's use of the vehicle as part of the encrypted data transmitted with the electronic key or as part of the electronic key, so that the Temporary User cannot modify those restrictions at his or her mobile device."

Ex. 1004 (Almeroth Decl.) at ¶111; Pet. 13

- Well-known benefits:
 - Prevents tampering with the restrictions
 - Associates the restrictions to the v-key

G1: Kleve's renders obvious "coded data" including "privilege settings": PO's Incorrect Argument

- ***PO's argument against obviousness:*** No benefit over step 214

"But Kleve's solution already provides this benefit, and in a more secure way. ... Kleve teaches that the restrictions used to control and monitor vehicle usage are "initially set at the beginning of the rental term," after the virtual key has already been created and distributed, and in fact, are never transmitted to the Temporary User."

"Dr. Almeroth never offers any benefit that would be achieved by modifying Kleve to include restrictions in its virtual key and then encrypt those restrictions."

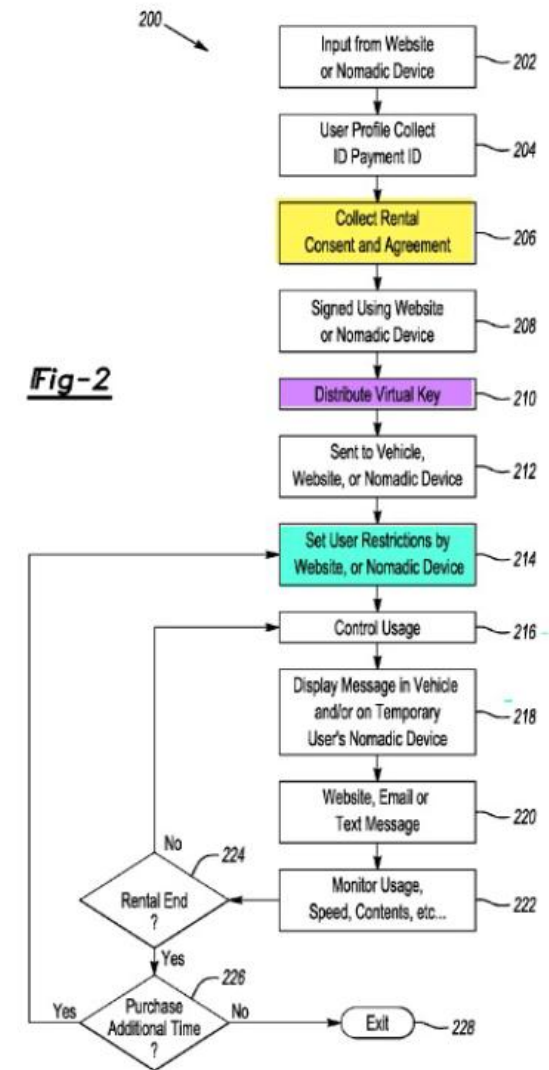
POR 51-52

- ***PO is wrong:*** Dr. Almeroth:

¶111: "In order to make full use of these benefits, a POSITA would have been motivated to include data identifying restrictions on a Temporary User's use of the vehicle as part of the encrypted data transmitted with the electronic key or as part of the electronic key, so that the Temporary User cannot modify those restrictions at his or her mobile device."

Ex. 1004 (Almeroth Decl.) at ¶111; Pet. 13

- No dispute that there is a benefit if the privilege settings are distributed with the v-key



Ground 3: Mikan renders obvious an e-key associated with “coded data” that includes “privilege settings” (All claims)

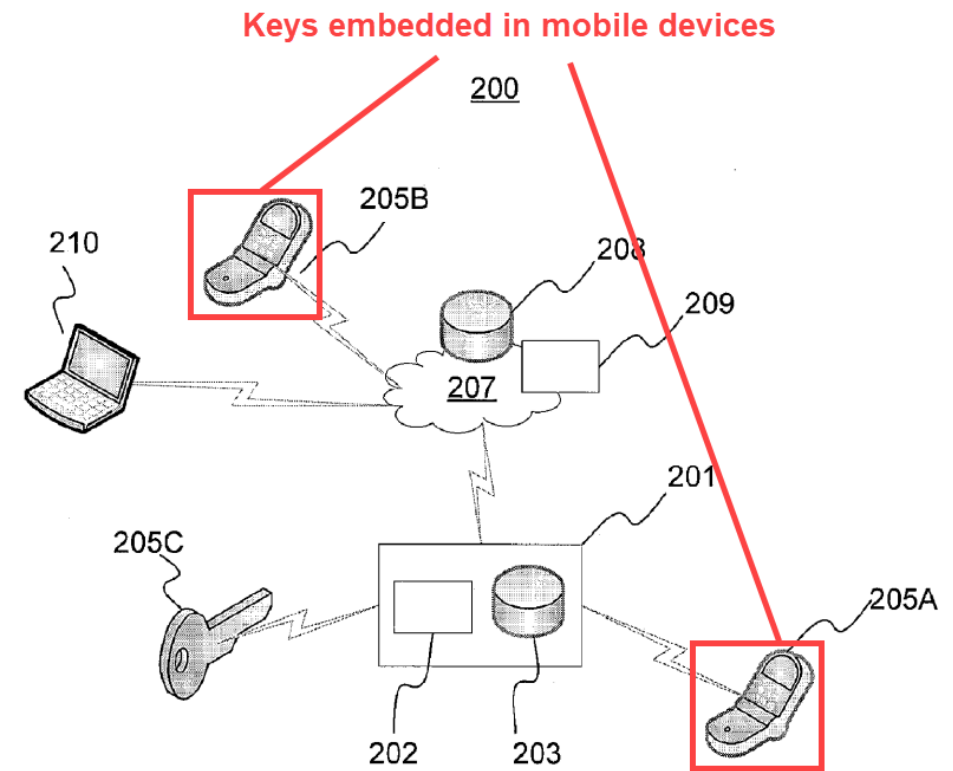
Ground 3: Mikan renders obvious “coded data” including “privilege settings”

- **Undisputed:**
 - Mikan discloses “vehicle operation policies” associated with an eKey
 - Mikan’s eKey is transmitted to and embedded in a mobile device
 - Mikan’s “vehicle operation policies” are used by the vehicle to restrict uses of the vehicle
- **PO:**
 - POR: Mikan **only** discloses that the privilege settings are sent directly from a **master database (server)** to a **local database** on the vehicle
- PO is **incorrect:**
 - PO attempts to artificially limit Mikan’s disclosure to exemplary embodiments
 - PO fails to address obviousness analysis providing motivation to distribute a vehicle operation policy as coded data to the mobile device along with its associated eKey

Ground 3: Mikan Summary

- Mikan uses eKeys embedded in a wireless device to control a vehicle.

[0050] “The system may include one or more keys 205A-C control unit 202 and local database 203, for example. Keys 205A-C may be electronic keys, traditional metal keys, or a combination of both. In one embodiment, keys 205A-C may be embedded in a wireless device such as a cellular telephone or Personal Digital Assistant (PDA), for example.”



Ex. 1007 (Mikan) at ¶50, Fig. 2; Pet. 40-41

Ground 3: Mikan Summary

- eKeys are managed by a security module on the mobile device, which securely stores information (*i.e.*, coded data) associated with the eKey

[0067] “Security module 406 may include security application 409 and vehicle access module 408. Vehicle access module 408 may receive secure identifier 407 from processor 401, and may communicate with vehicle 201 to send secure identifier 407 to vehicle 201. Vehicle access module 408 may communicate via any wireless protocol suitable for the transmission of data. For example, access module 408 may communicate via Bluetooth protocol, WiFi, RF-ID, cellular, and the like. Bluetooth protocol may be defined by the Institute of Electrical and Electronics Engineers (IEEE) specification 802.15.1. Security application 409 may include software relating to the management of secure identifiers 407. In one embodiment, security application 409 may provide a user with customizable features that may be presented by user interface module 402. Security application 409 may perform cryptographic functions related to the secure identifier, an authentication process, or cryptographic key generation, for example.”

Ground 3: Mikan Summary

- Mikan's eKeys communicate with the vehicle wirelessly using encrypted data

[0051] “In one embodiment, key 205A-C may communicate directly with control unit 202. For example, key 205A-C and control unit 202 may communicate directly via a radio frequency transmission.”

Ex. 1007 (Mikan) at ¶ 51; Pet. 43-44

[0070] “At 504, a user attempt to access or operate vehicle 201 with a key 205A-C is detected, which may initiate the authentication the detection of key 205A-C may include receiving secure identifier 407. Secure identifier 407 may be received, for example, at control unit 202. Where key 205A-C is an electronic key, such as a key embedded in wireless device 400 for example, key 205A-C may transmit secure identifier 407.”

Ex. 1007 (Mikan) at ¶ 70; Pet. 43-44

[0059] “Key set 310 may include a secure ID check 315 associated with a key 205A-C within the set. The secure ID check may be a serial number, electronic serial number (ESN), or other identifier of a key 205A-C. In one embodiment, secure ID check 315 may be a digital signature associated with a key 205A-C. For example, the digital signature may be the product of a public key encryption system.”

Ex. 1007 (Mikan) at ¶ 59; Pet. 43-44

Ground 3: Mikan Summary

- Mikan's eKeys also have an associated "vehicle operation policy" (*i.e.*, privilege settings) that is received and stored at a local database at the vehicle

[0060] "Local database 303 may include vehicle operation policy 311. Vehicle operation policy 311 may include vehicle operation feature ID 316 and a related access control rule 317. Vehicle operation feature ID 316 may be, for example, a data field identifying one vehicle operation feature. Vehicle 201 may support various vehicle operation features such as unlocking a door, opening a trunk, opening a glove box, engaging an ignition, directing the vehicle from a one geographic location to another geographic location and accelerating the vehicle, for example. Any aspect of the control, use, or functionality of vehicle 201 may be considered a vehicle operation feature. ... A vehicle operation feature may be associated with vehicle operation feature ID 316. Access control rule 317 may include a criterion relating to associated vehicle operation feature ID 316. For example, access control rule 317 may operate to enable, partially enable, or disable the related vehicle operation feature. Access control rule 317 may include advanced criteria relating to the manner and conditions under which the vehicle may be operated. For example, access control rule 317 may establish a maximum acceleration for the vehicle, a maximum distance traveled for the vehicle, a range of time within which the vehicle may be operated, a geographic range within which the vehicle may be operated and the like."

Ground 3: Mikan Summary

- Mikan's eKeys also have an associated "vehicle operation policy" (*i.e.*, privilege settings) that is received and stored at a local database at the vehicle

[0061] "Mapping 312 may link vehicle operation policy 311 and keys 205A-C. To illustrate this point, one embodiment may include two keys, first with greater access than the second. The first key, in this example illustration, may be related via mapping 312 to access control rule 317 that enables all vehicle operation features. The second key, in this illustration, may be a "valet key" with limited functionality. For example, the second key may be related to three access control rules 317: a first rule that disables access to the trunk and glove box, a second rule that limits the maximum speed to 35 miles per hour, and a third rule that limits the total allowed distance traveled to one mile."

Ground 3: Mikan Summary

- In one embodiment, the vehicle operation policy is synchronized from a master database to a local database

[0058] “Master database 300 may include any number of vehicle records 302. Each record may be associated with Vehicle ID 301. ... Vehicle ID 301 may relate to a physical vehicle that may be within wireless vehicle security system 200. In one embodiment, vehicle record 302 may include key set 310, policy set 313, and mapping 312. Key set 310 may include data representing a collection of keys 205A-C. Policy set 313 may include a collection of vehicle operation policies 311. Mapping 312 may include a collection of one or more relationships linking individual keys from key set 310 with individual vehicle operation policies from policy set 313.”

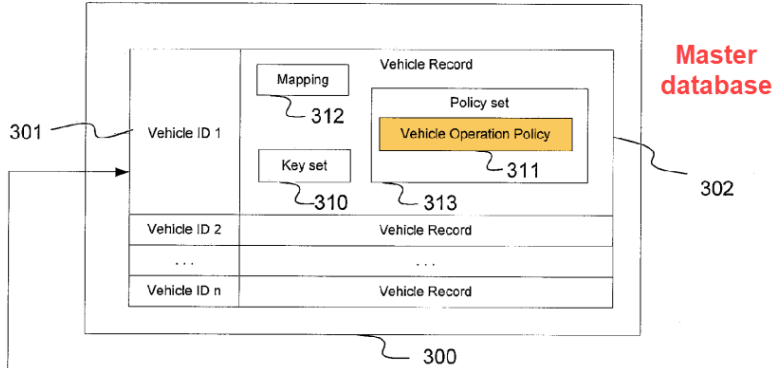


FIG. 3A

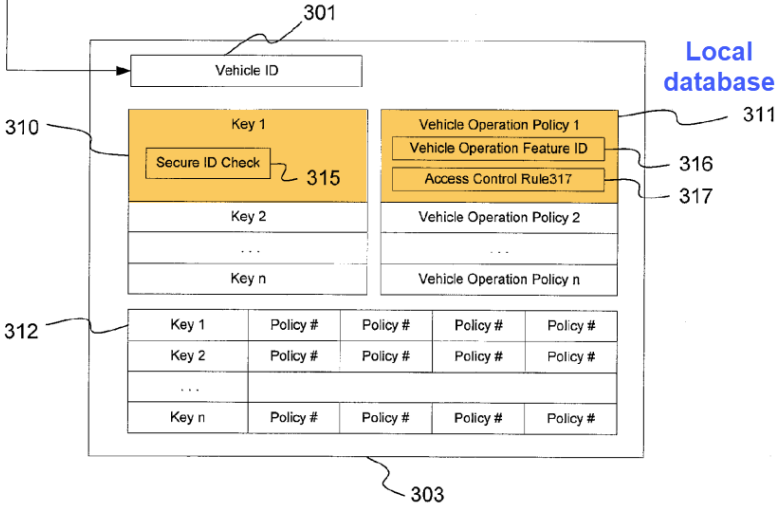


FIG. 3B

Ex. 1007 (Mikan) at ¶ 58, Figs. 3A-3B; POR 60

Ground 3: Mikan Summary

- In one embodiment, the vehicle operation policy is synchronized from a master database to a local database

[0069] “At 502 local database 203 may synchronize with master database 208. Control unit 202 or local database 203 may initiate the synchronization to pull updated data from master database 208. Alternatively, master application 209 or master database 208 may initiate the synchronization to push updated data to local database 203. The synchronization may be a partial or complete refresh of the data. For example, the updated data may represent only the changes in the master database made since the last synchronization in a partial refresh. In a complete refresh, the updated data may represent the entire contents of master database 208 that are relevant to vehicle 201.”

Ground 3: Mikan Summary

- Dr. Almeroth testified that it would have been obvious to send the vehicle operation policy as coded data with the eKey

¶221: “It would have been obvious to a POSITA to transmit the vehicle operation policy as additional coded data, either as part of or in addition to Mikan’s secure identifier. The purpose of the vehicle operation policy is to prevent certain users from taking certain actions when using the vehicle. If the vehicle operation policy is transmitted in unencrypted form, a user may be able to access the policy and modify it to enable unauthorized access to certain vehicle features. A POSITA would thus have been motivated to encrypt or otherwise encode the vehicle operation policy for transmission so that users cannot tamper with the vehicle operation policies and associated access control rules.”

Ground 3: Mikan Summary

- Sending the vehicle operation policy with the eKey allows it to be used even when the vehicle cannot communicate – a problem Mikan acknowledges

[0085] “In one embodiment, the synchronization data may be communicated via wireless network 207. Vehicle 201 may not always be in contact with wireless network 207, such as when vehicle 201 is parked underground and out of range of wireless network 207, for example. Where master database 208 pushes the synchronization to local database 203, master application 209 may establish communication with control unit 202 before initiating the synchronization. When communication cannot be established, master application 209 or master database 208 may queue the request for a later time.”

G3: Obvious to send Mikan's "privilege settings" as "coded data" with eKey

- PO:
 - POR: Mikan teaches away from including the privilege settings in coded data because it sends privilege settings from the master database directly to the local database
- PO is incorrect:
 - PO attempts to artificially limit Mikan's disclosure to exemplary embodiments, which are not a discouragement or teaching away from alternatives
 - PO does not rebut the Petition's obviousness analysis or Mikan's express acknowledgement of the problem when the vehicle cannot communicate with the server

G3: Obvious to send Mikan's "privilege settings" as "coded data" with eKey

- Mikan's eKeys communicate with the vehicle wirelessly using encrypted data

[0051] "In one embodiment, key 205A-C may communicate directly with control unit 202. For example, key 205A-C and control unit 202 may communicate directly via a radio frequency transmission."

Ex. 1007 (Mikan) at ¶ 51; Pet. 43-44

[0070] "At 504, a user attempt to access or operate vehicle 201 with a key 205A-C is detected, which may initiate the authentication the detection of key 205A-C may include receiving secure identifier 407. Secure identifier 407 may be received, for example, at control unit 202. Where key 205A-C is an electronic key, such as a key embedded in wireless device 400 for example, key 205A-C may transmit secure identifier 407."

Ex. 1007 (Mikan) at ¶ 70; Pet. 43-44

[0059] "Key set 310 may include a secure ID check 315 associated with a key 205A-C within the set. The secure ID check may be a serial number, electronic serial number (ESN), or other identifier of a key 205A-C. In one embodiment, secure ID check 315 may be a digital signature associated with a key 205A-C. For example, the digital signature may be the product of a public key encryption system."

Ex. 1007 (Mikan) at ¶ 59; Pet. 43-44

G3: Obvious to send Mikan's "privilege settings" as "coded data" with eKey

- Mikan's eKeys also have an associated "vehicle operation policy" (*i.e.*, privilege settings) that is received and stored at a local database at the vehicle

[0060] "Local database 303 may include vehicle operation policy 311. Vehicle operation policy 311 may include vehicle operation feature ID 316 and a related access control rule 317. Vehicle operation feature ID 316 may be, for example, a data field identifying one vehicle operation feature. Vehicle 201 may support various vehicle operation features such as unlocking a door, opening a trunk, opening a glove box, engaging an ignition, directing the vehicle from a one geographic location to another geographic location and accelerating the vehicle, for example. Any aspect of the control, use, or functionality of vehicle 201 may be considered a vehicle operation feature. ... A vehicle operation feature may be associated with vehicle operation feature ID 316. Access control rule 317 may include a criterion relating to associated vehicle operation feature ID 316. For example, access control rule 317 may operate to enable, partially enable, or disable the related vehicle operation feature. Access control rule 317 may include advanced criteria relating to the manner and conditions under which the vehicle may be operated. For example, access control rule 317 may establish a maximum acceleration for the vehicle, a maximum distance traveled for the vehicle, a range of time within which the vehicle may be operated, a geographic range within which the vehicle may be operated and the like."

G3: Obvious to send Mikan's "privilege settings" as "coded data" with eKey

- Dr. Almeroth testified that it would have been obvious to send the vehicle operation policy as coded data with the eKey

¶221: "It would have been obvious to a POSITA to transmit the vehicle operation policy as additional coded data, either as part of or in addition to Mikan's secure identifier. The purpose of the vehicle operation policy is to prevent certain users from taking certain actions when using the vehicle. If the vehicle operation policy is transmitted in unencrypted form, a user may be able to access the policy and modify it to enable unauthorized access to certain vehicle features. A POSITA would thus have been motivated to encrypt or otherwise encode the vehicle operation policy for transmission so that users cannot tamper with the vehicle operation policies and associated access control rules."

G3: Obvious to send Mikan's "privilege settings" as "coded data" with eKey

- **PO**: No reason to send the vehicle operation policy to the mobile device because it is synchronized directly between the master database (server) and local database (vehicle)
- ***PO is incorrect***: Synchronizing the master and local database is an optional step in an exemplary embodiment and not limiting

[0069] "At 502 local database 203 may synchronize with master database 208."

Ex. 1007 (Mikan) at ¶69; Reply 19-20

[0084] "At 612, local database 203 and master database 208 may synchronize."

Ex. 1007 (Mikan) at ¶84; Reply 19-20

[0068] "FIG. 5 depicts a flow diagram of example vehicle security process 500. Example process 500 is merely one embodiment and therefore describes features and functionality by way of example and illustration."

Ex. 1007 (Mikan) at ¶68; Reply 19-20

[0079] "FIG. 6 depicts a flow diagram of an example network security process 600. Example process 600 is merely an embodiment and describes features and functionality by way of example and illustration."

Ex. 1007 (Mikan) at ¶79; Reply 19-20

G3: Obvious to send Mikan's "privilege settings" as "coded data" with eKey

- PO: Mikan's mobile device only stores a secure identifier
- **PO is incorrect:** Mikan's disclosure is not so limiting

[0067] "Security module 406 may include security application 409 and vehicle access module 408. Vehicle access module 408 may receive secure identifier 407 from processor 401, and may communicate with vehicle 201 to send secure identifier 407 to vehicle 201. ... Security application 409 may include software relating to the management of secure identifiers 407. ... Security application 409 may perform cryptographic functions related to the secure identifier, an authentication process, or cryptographic key generation, for example."

Ex. 1007 (Mikan) at ¶67; Pet. 43-44

[0065] "In one embodiment, memory 404 may provide non-volatile storage of secure identifier 407 of wireless device 400. In another embodiment, memory 404 may provide volatile storage of secure identifier 407 retrieved, for example, via wireless communications module 403 or via user interface module 402 with a user/password prompt, biometric or other user authentication. In one embodiment, secure identifier 407 may authenticate wireless device 400 as a key 205A-B as discussed above in connection with FIG. 2."

Ex. 1007 (Mikan) at ¶54; Reply 20

G3: Obvious to send Mikan's "privilege settings" as "coded data" with eKey

- Sending the vehicle operation policy with the eKey allows it to be used even when the vehicle cannot communicate – a problem Mikan acknowledges

[0085] "In one embodiment, the synchronization data may be communicated via wireless network 207. Vehicle 201 may not always be in contact with wireless network 207, such as when vehicle 201 is parked underground and out of range of wireless network 207, for example. Where master database 208 pushes the synchronization to local database 203, master application 209 may establish communication with control unit 202 before initiating the synchronization. When communication cannot be established, master application 209 or master database 208 may queue the request for a later time."

G3: Obvious to send Mikan's "privilege settings" as "coded data" with eKey

- PO:
 - POR: No reason to store a "mapping" between keys and vehicle operation policies at the vehicle if the mobile device sends the vehicle operation policy. **POR 74-75**
- **PO is *Incorrect*:** Mikan's vehicle may have multiple keys and corresponding policies to keep track of.

[0050] "The system may include one or more keys 205A-C control unit 202 and local database 203, for example. Keys 205A-C may be electronic keys, traditional metal keys, or a combination of both. In one embodiment, keys 205A-C may be embedded in a wireless device such as a cellular telephone or Personal Digital Assistant (PDA), for example."

Dependent Claim 6: Kleve and Mikan render obvious “sharing of said eKey with a recipient user”

Ground 1/Claim 6: Kleve renders obvious “sharing of said eKey”

- PO: Kleve discourages allowing a renter to share an eKey with another user, and Kleve’s credential match would render meaningless any eKey sharing. *POR 80*
- PO is incorrect:
 - PO does not dispute that the same processes that enable sharing a v-key from an owner’s device to a renter’s device could be used to share the eKey between two authorized users (e.g., two members of a family that has rented the vehicle)
 - PO does not rebut Dr. Almeroth’s reasons why a POSITA would be motivated to modify Kleve to enable sharing between two authorized users
 - Sharing an eKey between two **authorized** users is consistent with Kleve’s goal of offering the owner control over the vehicle
 - Kleve’s credential check is optional and in only **some** embodiments, and thus does not negate the benefits of eKey sharing.

Ground 1/Claim 6: Kleve renders obvious “sharing of said eKey”

- No dispute that Kleve’s system could be used to share an eKey between two authorized renters

“Since Kleve’s vehicle rental system is already configured to use a smartphone application to generate, authenticate, and distribute keys, a POSITA would have been capable of implementing sharing between Temporary Users using the same or similar software already included in Kleve’s system to allow Owners to distribute virtual keys to temporary users.”

Ex. 1004 (Almeroth Dec) at ¶155; Pet. 25-26

Ground 1/Claim 6: Kleve renders obvious “sharing of said eKey”

- PO does not rebut Dr. Almeroth’s motivation to modify Kleve
- This does not undermine Kleve’s goal of maintaining owner control over the vehicle, because only **authorized** users may share the eKey in the proposed modification.

“In my opinion, it would have been obvious to a POSITA that the same smartphone application may also be used to allow Temporary Users to share their virtual keys with other authorized Temporary Users. For example, multiple members of a family or travel group may collectively rent a single vehicle, and different members may each need to be able to access the vehicle using their respective mobile devices. A POSITA would have understood that multiple Temporary Users could thus be authorized in connection with the same vehicle rental. A POSITA would thus have been motivated to enable each user to share the virtual key with other authorized users associated with the same rental request.”

Ex. 1004 (Almeroth Dec) at ¶155; Pet. 25-26

Ground 1/Claim 6: Kleve renders obvious “sharing of said eKey”

- Kleve’s credential check does not undermine the combination because it is not always required:
- (1) E-key allows renter to unlock and turn on car without further verification needed:

[0048] “At step 322, ... [t]he virtual key may allow a Temporary User temporary granted access to the Owner's vehicle. The granted access allowed by the virtual key may permit entry of the vehicle; grant a keyless drive-away of a vehicle, and/or both.”

Ex. 1005 (Kleve) at ¶48; Pet. 15

- (2) Renter enters vehicle with e-key and uses credential for verification, **or** (3) Renter uses credential for verification at the exterior of car before entering:

[0049] “The system may be further extended to facilitate the virtual key with additional security by requiring remote credential verification at the vehicle. The remote credential verification at the vehicle may be done with additional hardware assembled on the exterior of the vehicle or in the vehicle cabin. The remote credential verification may be done by the VCS, using a server, or allowing the Owner to verify the Temporary User's request. For example, but not limited to, the Temporary User entering a credential verification password at the vehicle's touchscreen visual display while having the VCS, server, or owner compare and verify authorization.”

Ex. 1005 (Kleve) at ¶49; Pet. 23, 26

Ground 5/Claim 6: Mikan renders obvious “sharing of said eKey”

- PO: Mikan only embeds a “secure ID” in the mobile device, not an eKey that can be shared; and Mikan’s key lacks the requisite privilege settings. *POR 80-81*
- PO is incorrect:
 - Mikan expressly teaches that electronic keys (not just secure IDs) are “embedded” in a wireless device.
 - PO ignores Sekiyama’s disclosure, which expressly teaches sharing eKeys between devices.
 - Claim 6 only requires sharing an eKey, not privilege settings, so PO’s second argument is irrelevant to the claim.

Ground 5/Claim 6: Mikan renders obvious “sharing of said eKey”

- Mikan discloses eKeys that are embedded in a wireless device.

[0050] “The system may include one or more keys 205A-C control unit 202 and local database 203, for example. Keys 205A-C may be electronic keys, traditional metal keys, or a combination of both. In one embodiment, keys 205A-C may be embedded in a wireless device such as a cellular telephone or Personal Digital Assistant (PDA), for example.”

Ex. 1007 (Mikan) at ¶50; Pet. 52, 65

Ground 5/Claim 6: Mikan renders obvious “sharing of said eKey”

- Sekiyama expressly discloses sharing eKeys between devices
- PO does not dispute motivation to combine

[0011] “The electronic key system shown in FIG. 1 is a keyless entry system using portable telephones, allowing for the unlocking of a door lock of a vehicle 40 using portable telephones 10, 30, which store key information, without possession of a dedicated key. As shown in FIG. 2, this electronic key system has a configuration that allows key information to be transmitted from portable telephone A (first terminal) 10, which functions as a master key, to portable telephone B (second terminal) 30, which functions as a duplicate electronic key.”

Ex. 1006 (Sekiyama) at ¶11; Pet. 65-66

Dependent Claims 12, 13, and 20: Kleve and Mikan Disclose or Render Obvious a “server” or “application” “associated with a vehicle manufacturer”

Grounds 1&4/Claims 12, 13, 20: Kleve/Xiao/Hatton disclose “server”/”application” associated with “vehicle manufacturer”

- PO: No reference discloses a server or mobile application “associated with a manufacturer of the vehicle”. *POR 81*
- PO is **incorrect:**
 - Kleve is a Ford reference and its systems would clearly be associated with a vehicle manufacturer
 - Hatton and Xiao also expressly disclose mobile applications and servers associated with a vehicle manufacturer and render these limitations obvious in combination with Kleve or Mikan
 - PO does not address these arguments raised in the Petition

Grounds 1&4/Claims 12, 13, 20: Kleve/Xiao/Hatton disclose “server”/“application” associated with “vehicle manufacturer”

- Kleve/Xiao/Hatton render obvious a server/application associated with the car manufacturer:

“Kleve is a Ford patent; thus, a POSITA reviewing Kleve would have understood that the disclosed system is a system developed by or for Ford. Kleve even identifies a specific Ford system that may be used as the VCS—specifically, “the SYNC system manufactured by THE FORD MOTOR COMPANY.” Kleve at ¶ [0021].”

Ex. 1004 (Almeroth Dec) at ¶176; Pet. 30-31

“[S]ystem 100 may be associated with an automobile company that provides the disclosed wireless automobile key service.”

Ex. 1010 (Xiao) at 11:15-31, 16:6-18; Pet. 31, 59

“The mobile device 210 may receive the security codes from the vehicle key and allow a software application 212 to be configured to perform one or more vehicle controls using the mobile device. The vehicle key application 212 may be an application that was developed and/or associated with the vehicle manufacturer.”

Ex. 1008 (Hatton) at 12:46-51; Pet. 32-33

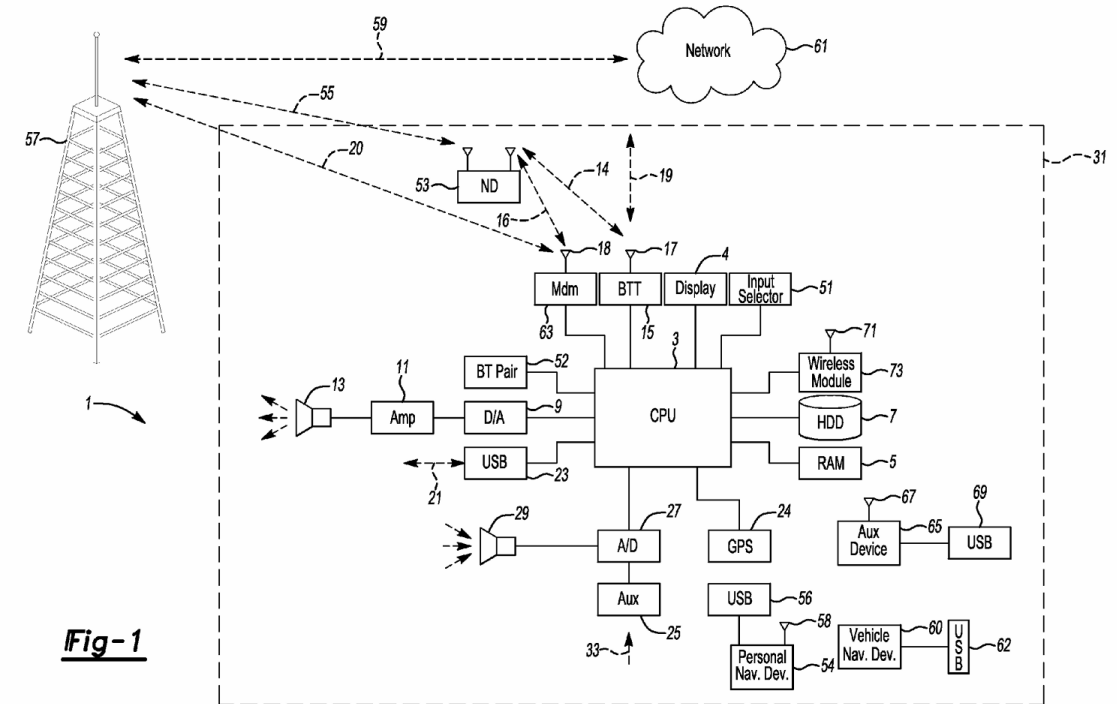
Kleve (EX1005)

Appendix: Kleve

- EX1005, Abstract, Fig. 1

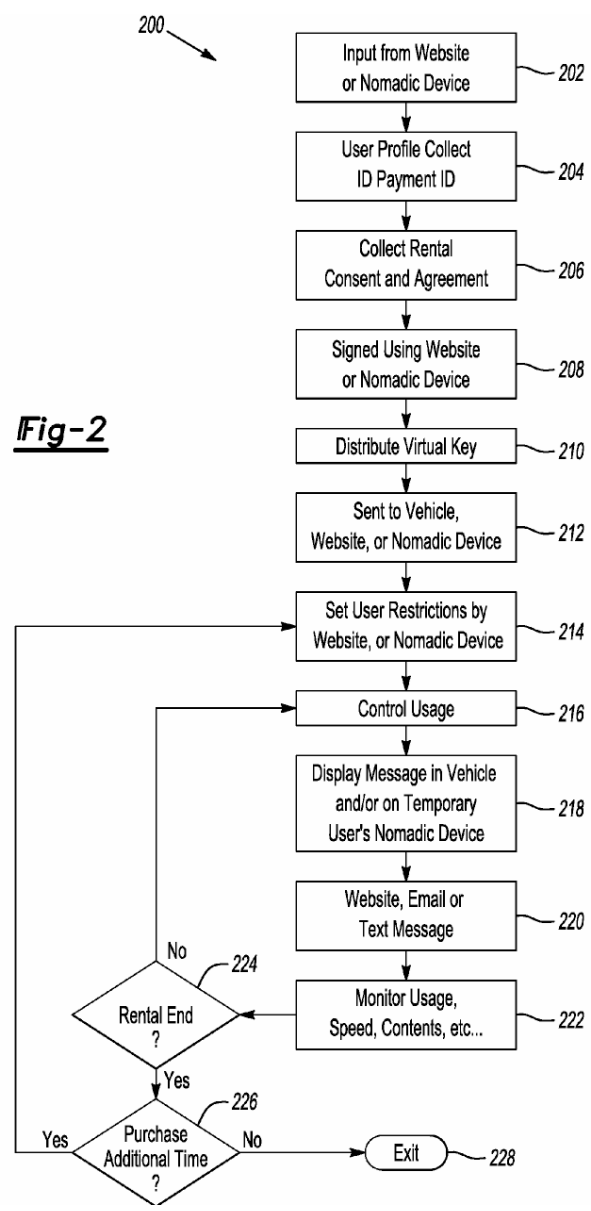
(57) **ABSTRACT**

A vehicle computing system includes a processor programmed and configured to establish communication with a wireless device brought into proximity of a vehicle. The processor may use the wireless device to receive an identifier from a vehicle rental administrative system. The identifier is configured with the processor to activate a vehicle during a prescribed rental period. The processor may receive user input to activate the vehicle for a rental period. The processor may compare the user input to the received identifier and enable a keyless drive-away of the vehicle if the user input corresponds to the identifier.



Appendix: Kleve

- EX1005, Fig. 2



Appendix: Kleve

- EX1005, Fig. 3A

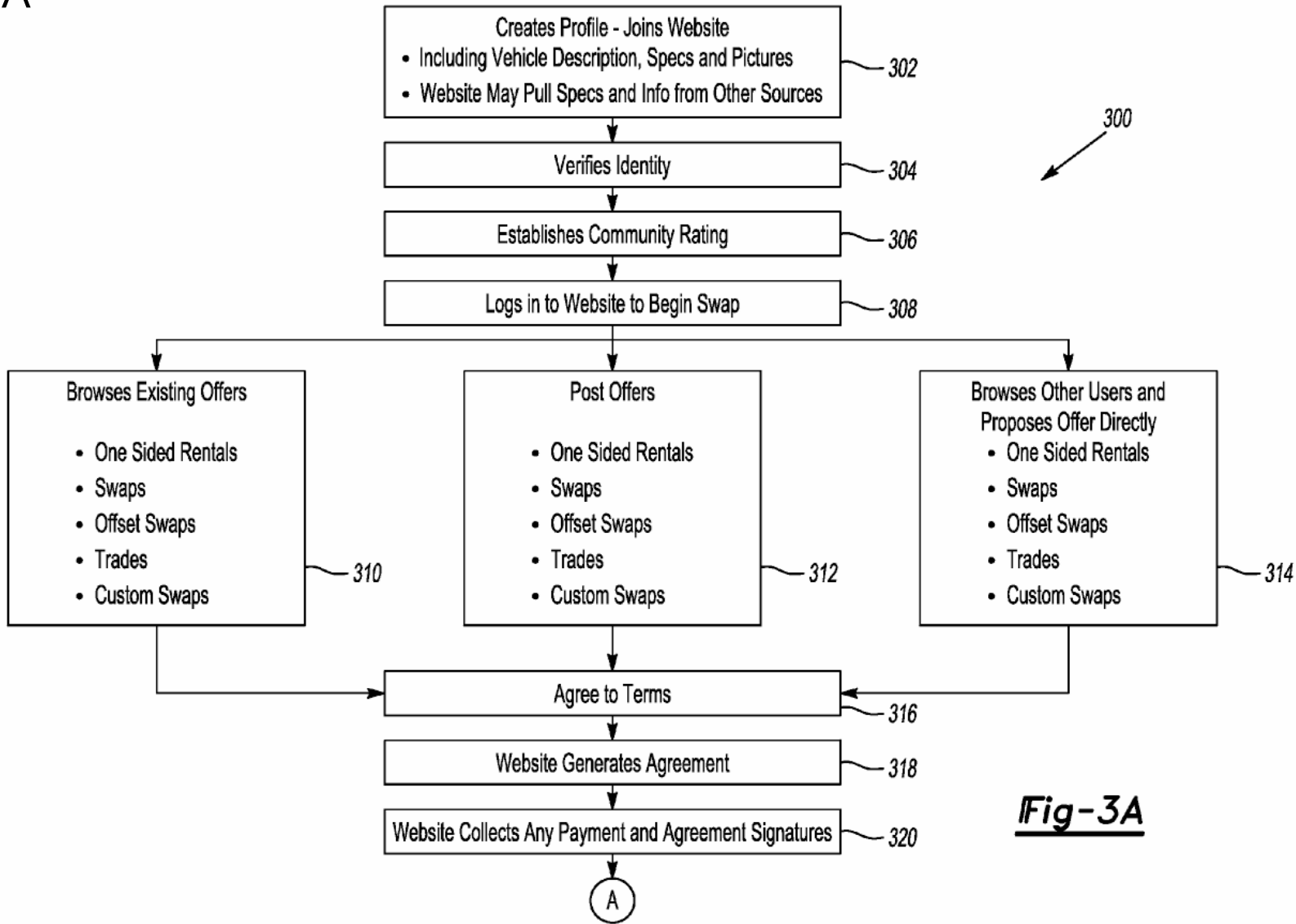


Fig-3A

Appendix: Kleve

- EX1005, Fig. 3B

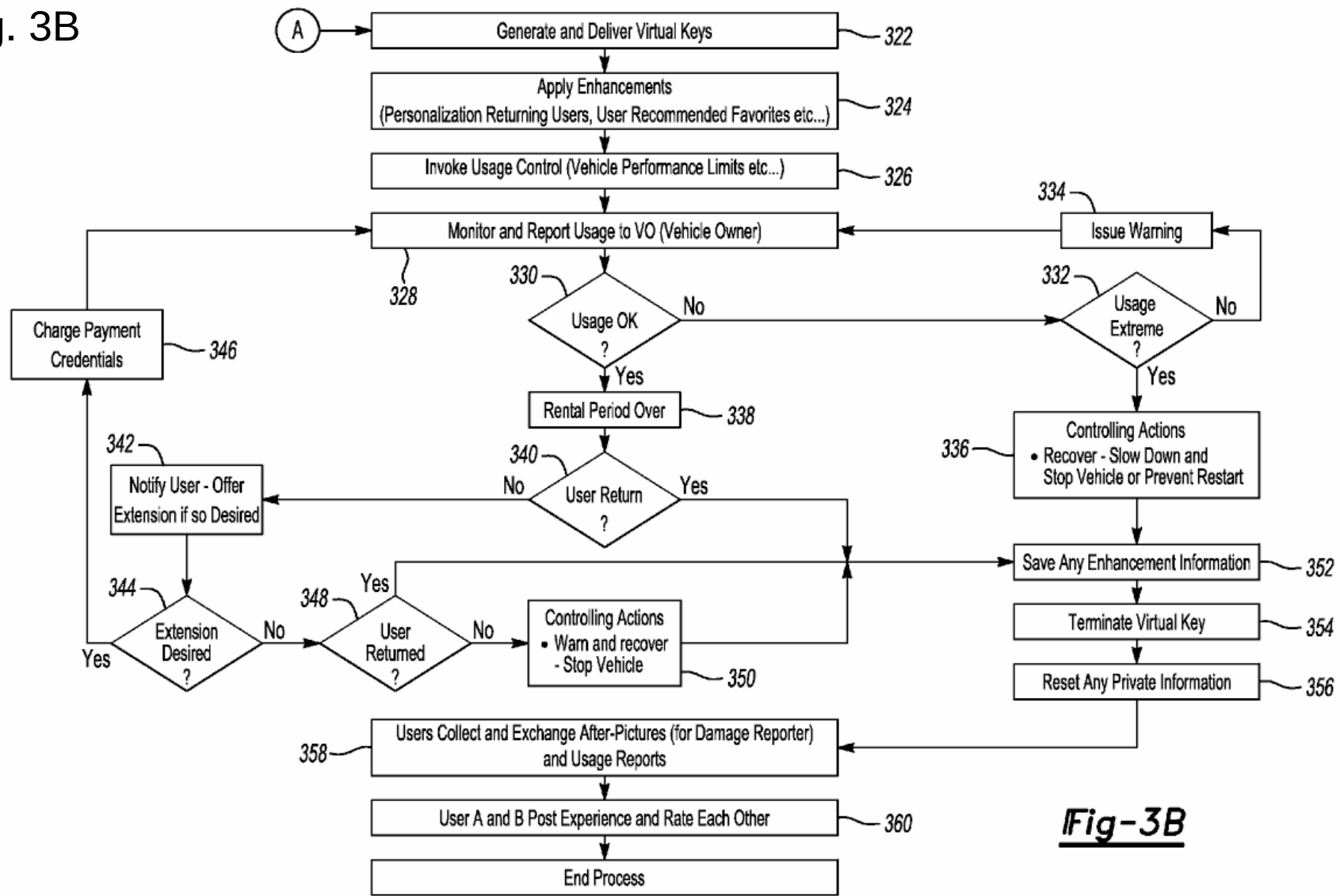
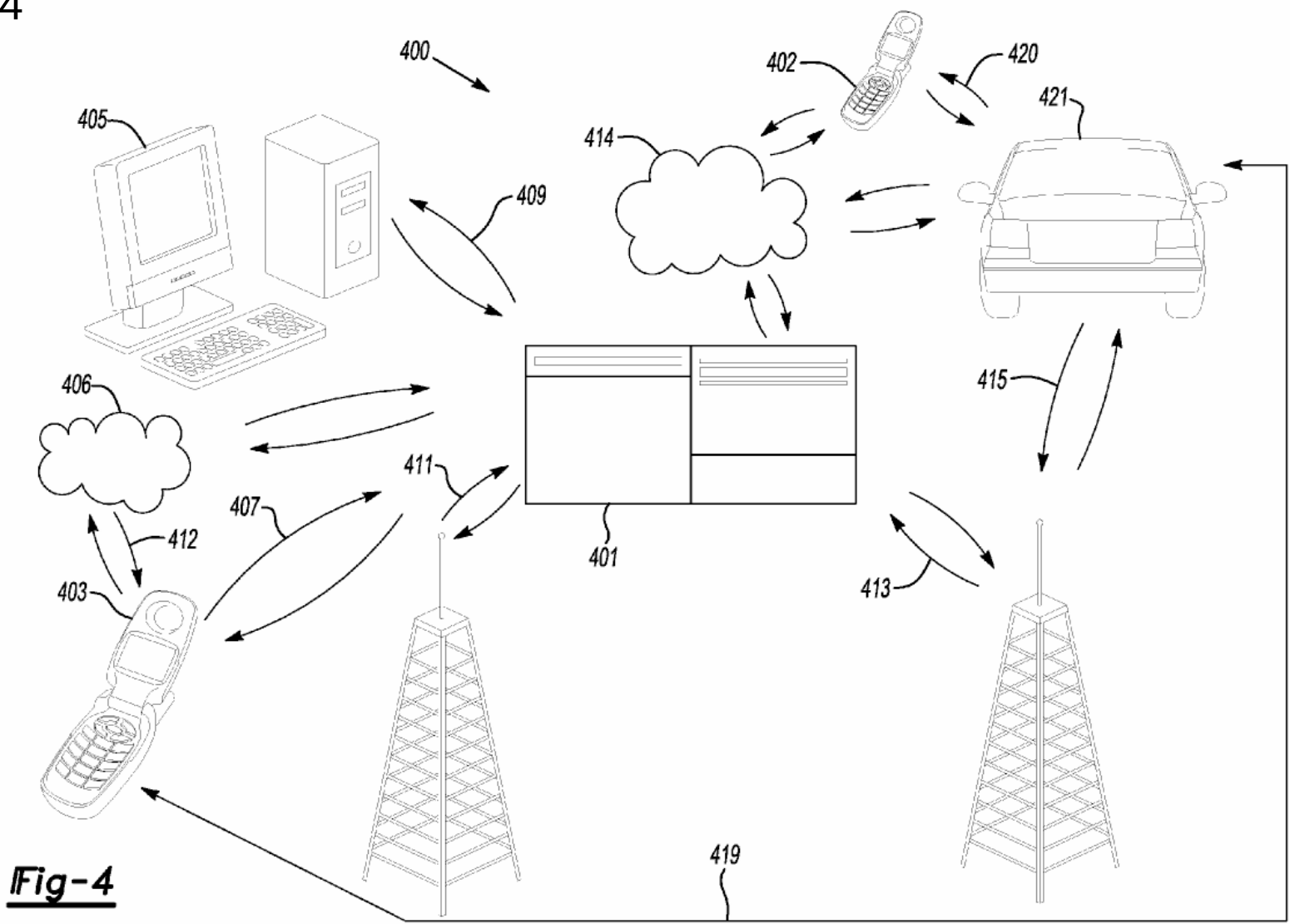


Fig-3B

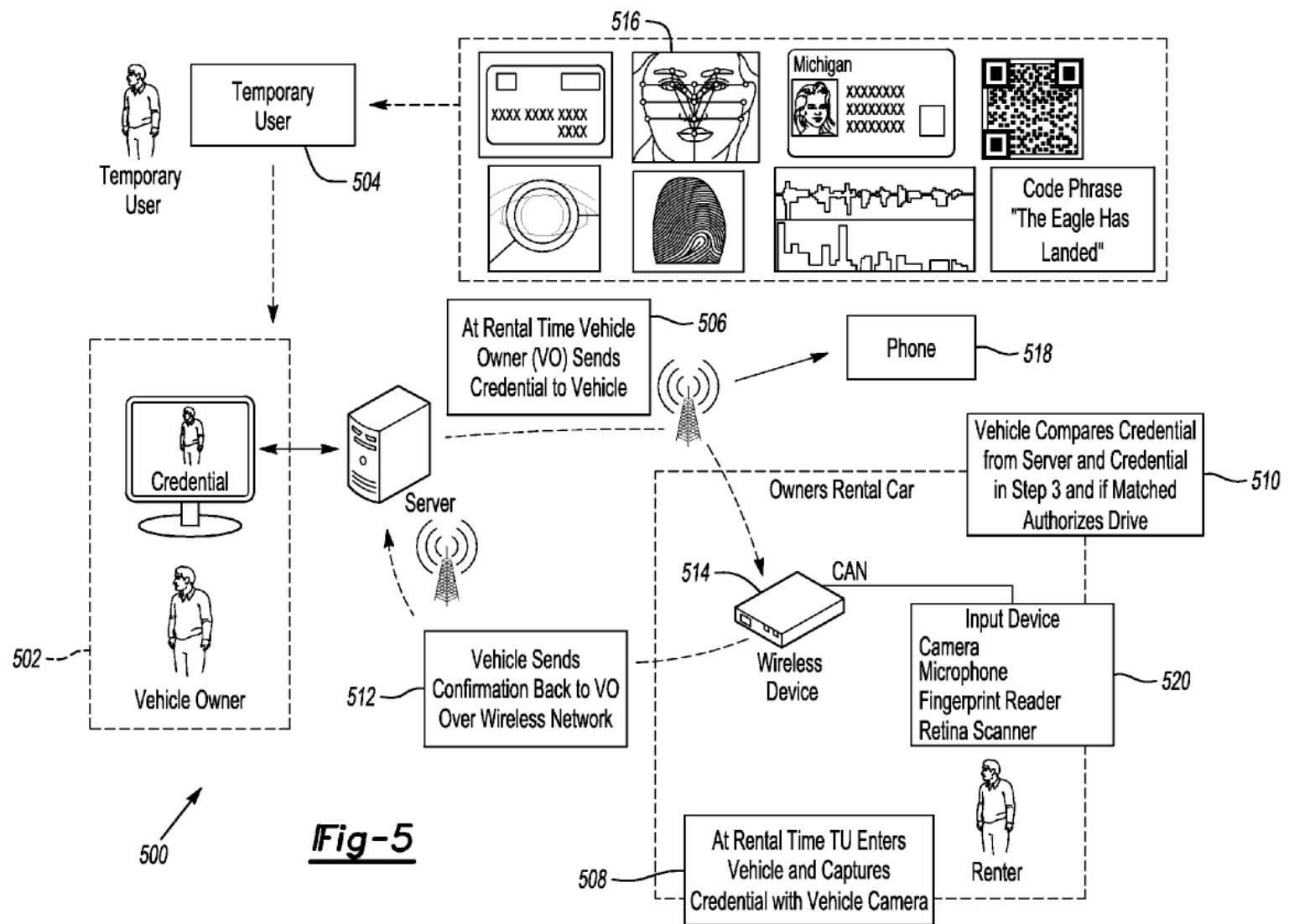
Appendix: Kleve

- EX1005, Fig. 4



Appendix: Kleve

- EX1005, Fig. 5



Appendix: Kleve

- EX1005, Fig. 6

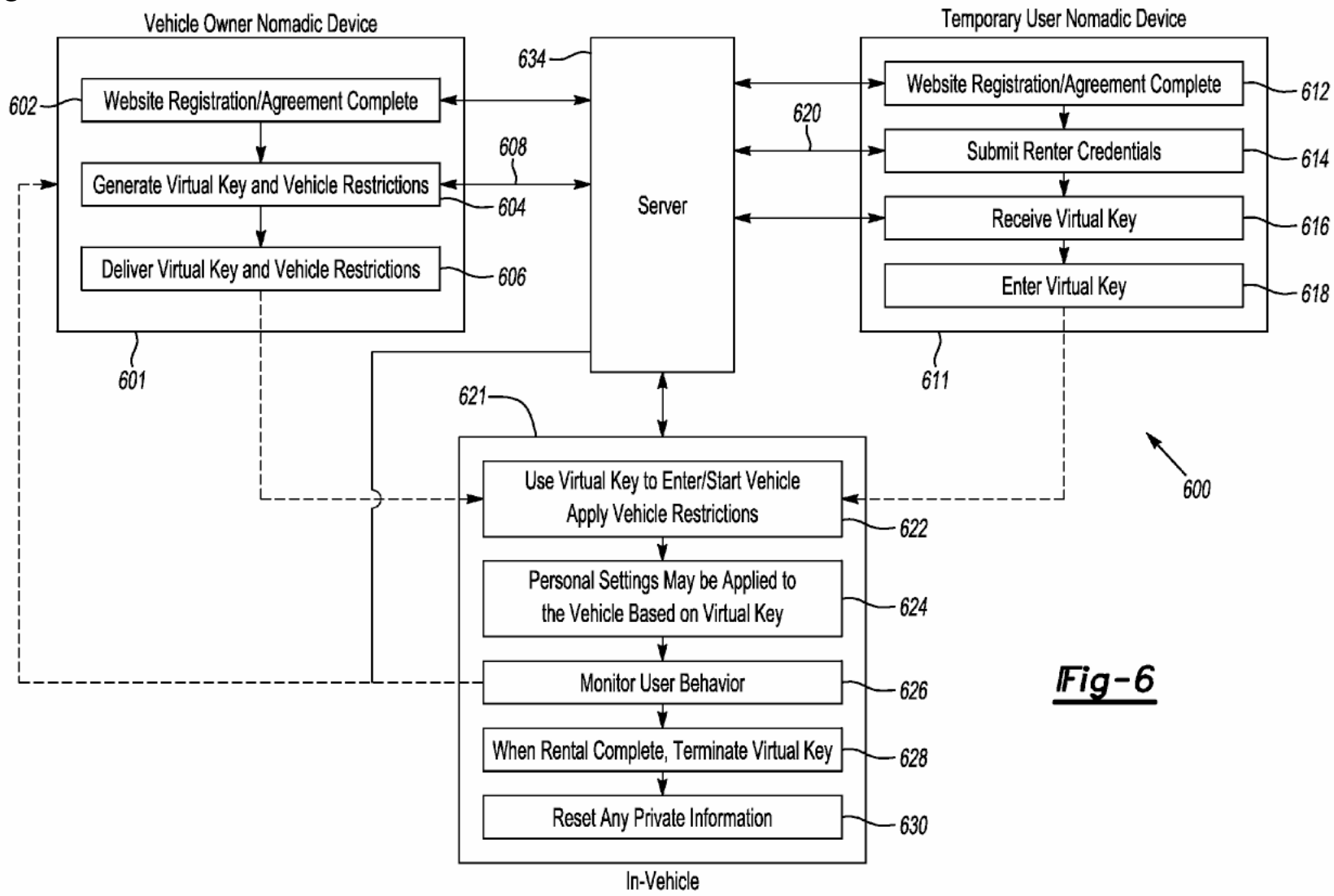
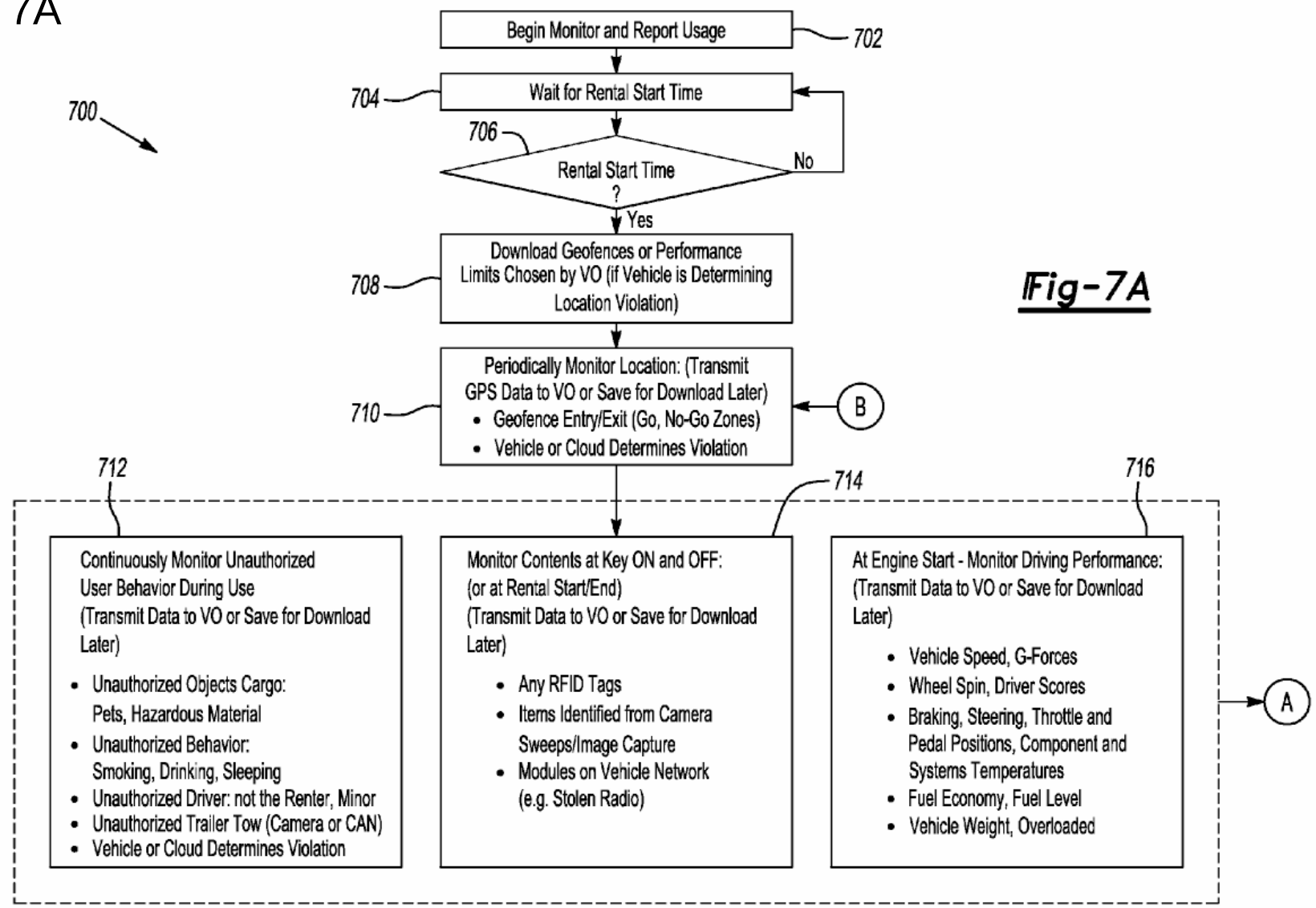


Fig-6

Appendix: Kleve

- EX1005, Fig. 7A



Appendix: Kleve

- EX1005, Fig. 7B

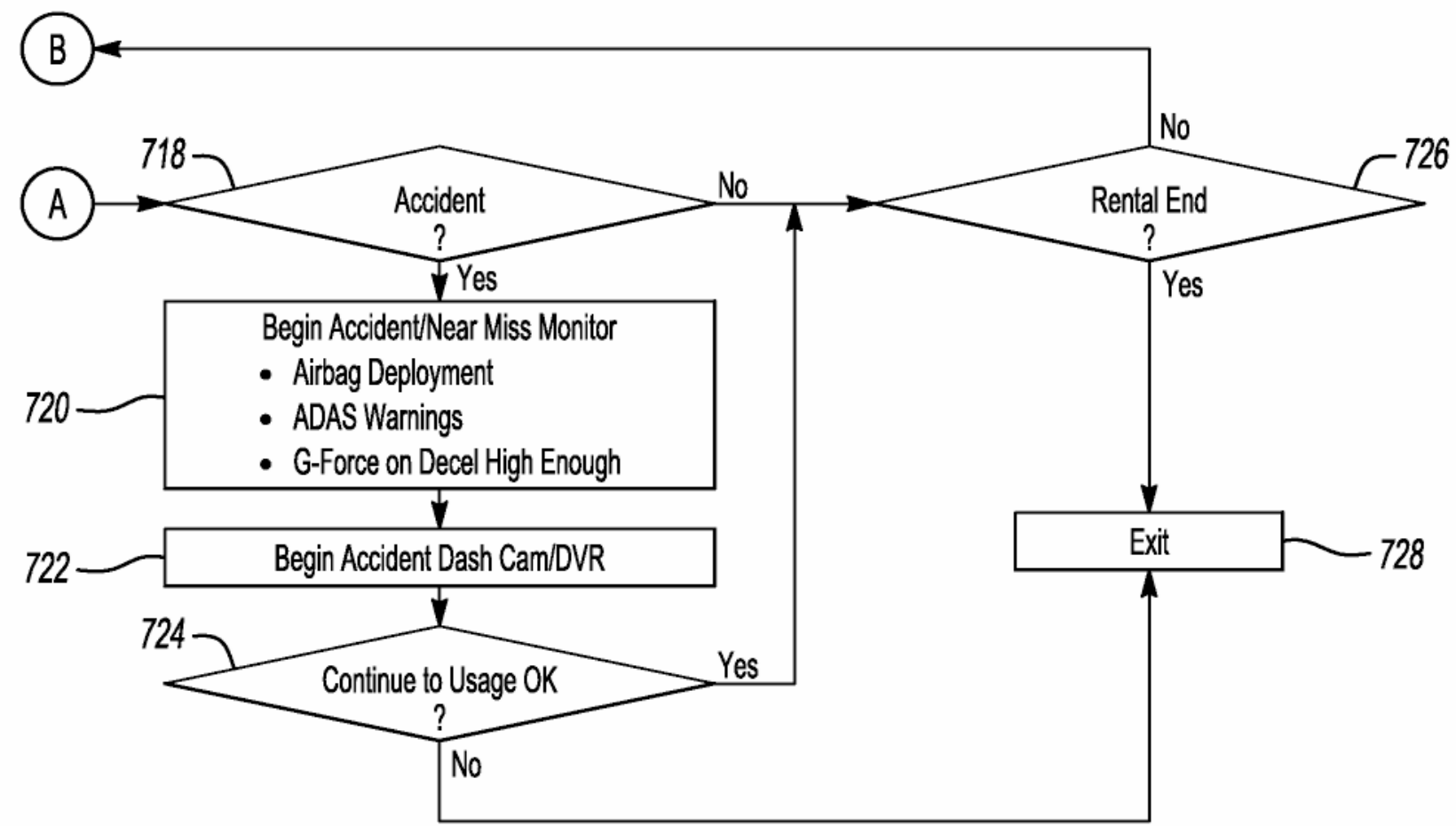


Fig-7B

Appendix: Kleve

- EX1005, Fig. 8

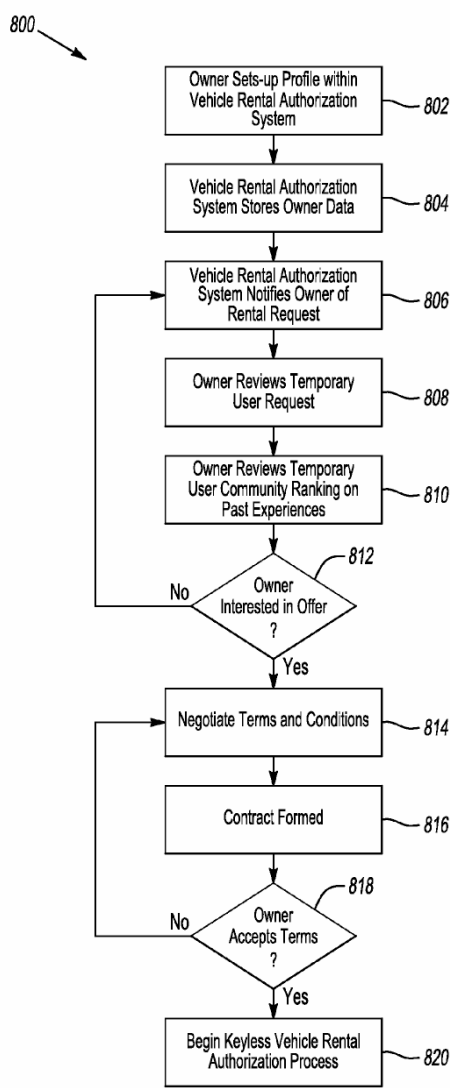


Fig-8

- EX1005, Fig. 9

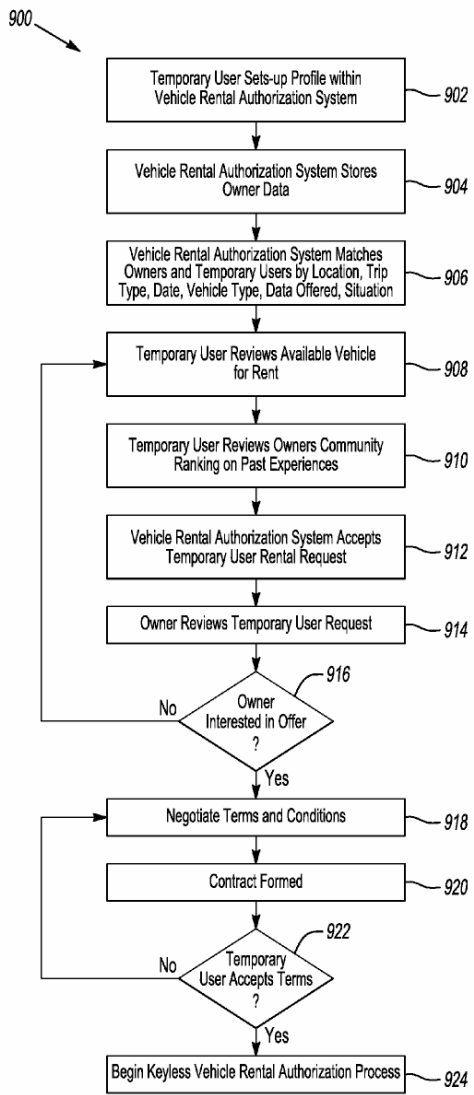


Fig-9

Appendix: Kleve

• EX1005, ¶¶1-19

CREDENTIAL CHECK AND AUTHORIZATION SOLUTION FOR PERSONAL VEHICLE RENTAL

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application is related to Ser. No. _____ MOBILE AUTOMOTIVE WIRELESS COMMUNICATION SYSTEM ENABLED MICROBUSINESSES filed concurrently with Ser. No. _____ HARDWARE AND CONTROLS FOR PERSONAL VEHICLE RENTAL.

TECHNICAL FIELD

[0002] The embodiments described herein generally relate to a method and system for authorizing a vehicle rental micro-business.

BACKGROUND

[0003] RelayRides.com allows car owners to list their car online in a few minutes to potential Temporary Users. Once registered, the car owner is notified of any reservation requests, however the owner is still in charge of who can drive their car. The car owner will meet the Temporary User to hand them their car keys, and once the Temporary User is complete with the car at the end of the trip, the car and keys are returned to the car owner.

[0004] Ridejoy.com allows a car owner to list available seats in their car online to potential passengers. The owner, who already is planning a road trip, may sell their extra seats to other users. Owners earn money on trips they were planning on taking anyway and the passenger who rented the available seat gets to their destination for less than they would have had to pay riding a bus.

[0005] As stated in US2011/0213629, an online site allows owners of assets and borrowers of assets to arrange sharing transactions with respect to the assets. Assets listed on the online site may include any kind of land, sea or airborne vehicle, tools, equipment or other devices subject to being moved. Online confirmation is provided to the owners and the borrowers that the arranged sharing transactions have been covered by insurance provided by the online site. Completion of the arranged sharing transactions is managed using information from electronic devices associated with the assets.

[0006] As stated in U.S. Pat. No. 6,975,997, a system for sharing a fleet of vehicles among a plurality of users, where in preferred embodiments of the shared vehicles are electrically powered. The sharing system comprises a control computer that assigns vehicles in response to requests by users, and monitors system performance of the rented vehicle. The computer subsystem through which users request vehicles for trips, and a vehicle subsystem within each vehicle that is in communication with the control computer allowing the control computer to monitor the location and status of each vehicle in the vehicle sharing fleet.

SUMMARY

[0007] In a first illustrative embodiment, a processor operably programmed and configured to establish communication with a wireless device brought into proximity of a vehicle. The processor may use the wireless device to receive an identifier from a vehicle rental administrative system. The identifier is configured with the processor to activate a vehicle during a prescribed rental period. The processor may receive

user input to activate the vehicle for a rental period. The processor may compare the user input to the received identifier; and enable a keyless drive-away of the vehicle if the user input corresponds to the identifier.

[0008] In a second illustrative embodiment, a vehicle rental method implemented in one or more vehicle processors for enabling a keyless vehicle drive-away during a scheduled rental period. The exemplary method performed by the processor includes establishing communication with a wireless device brought within proximity of a vehicle, and receiving a user identifier from a vehicle rental administrative system through the wireless device. The processor may use the identifier to activate the vehicle during a scheduled rental period. The processor may receive user input to activate the vehicle during the scheduled rental period. Once the user input is entered, the processor may compare the user input to the identifier and enable a keyless-drive away if the user input corresponds to the identifier.

[0009] In a third illustrative embodiment a computer readable storage medium for storing instructions that, when executed by a processor is configured to enable a vehicle rental transaction. The processor may establish communication with a wireless device brought within proximity of a vehicle. The processor is able to receive a user identifier from a vehicle rental administrative system using the wireless device. The identifier may be used to activate the vehicle during a prescribed rental period. The processor may receive user input corresponding to an attempt to activate the vehicle during the rental period and compare the user input to the received identifier. If the user input corresponds to the identifier the processor may enable a keyless drive-away.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] FIG. 1 is an exemplary block topology of a vehicle infotainment system implementing a user-interactive vehicle information display system;

[0011] FIG. 2 is a flow-chart illustrating an example method of a vehicle rental micro-business;

[0012] FIG. 3A is a flow-chart illustrating an example method of a vehicle rental micro-business having vehicle monitoring and control features;

[0013] FIG. 3B is a continuation of the flowchart of FIG. 3A illustrating an example method of a vehicle rental micro-business having vehicle monitoring and control features at A;

[0014] FIG. 4 shows an illustrative example of a communication system through which a nomadic device can communicate with a vehicle according to one of the various embodiments;

[0015] FIG. 5 illustrates a vehicle drive-away authorization and monitoring process for a temporary user according to one of the various embodiments;

[0016] FIG. 6 is a flow-chart illustrating an example method of the authorization process between a vehicle owner and temporary user;

[0017] FIGS. 7A & 7B show an illustrative example of monitoring a vehicle rental micro-business;

[0018] FIG. 8 is a flow-chart illustrating an example method of a vehicle owner interface with a vehicle rental authorization system; and

[0019] FIG. 9 is a flow-chart illustrating an example method of a temporary user interface with a vehicle rental authorization system.

Appendix: Kleve

• EX1005, ¶¶20-31

DETAILED DESCRIPTION

[0020] Detailed embodiments of the present invention are disclosed herein; however, it is to be understood that the disclosed embodiments are merely exemplary of the invention that may be embodied in various and alternative forms. The figures are not necessarily to scale; some features may be exaggerated or minimized to show details of particular components. Therefore, specific structural and functional details disclosed herein are not to be interpreted as limiting, but merely as a representative basis for teaching one skilled in the art to variously employ the present invention.

[0021] FIG. 1 illustrates an example block topology for a vehicle based computing system 1 (VCS) for a vehicle 31. An example of such a vehicle-based computing system 1 is the SYNC system manufactured by THE FORD MOTOR COMPANY. A vehicle enabled with a vehicle-based computing system may contain a visual front end interface 4 located in the vehicle. The user may also be able to interact with the interface if it is provided, for example, with a touch sensitive screen. In another illustrative embodiment, the interaction occurs through, button presses, spoken dialog system with automatic speech recognition and speech synthesis.

[0022] In the illustrative embodiment 1 shown in FIG. 1, a processor 3 controls at least some portion of the operation of the vehicle-based computing system. Provided within the vehicle, the processor allows onboard processing of commands and routines. Further, the processor is connected to both non-persistent 5 and persistent storage 7. In this illustrative embodiment, the non-persistent storage is random access memory (RAM) and the persistent storage is a hard disk drive (HDD) or flash memory.

[0023] The processor is also provided with a number of different inputs allowing the user to interface with the processor. In this illustrative embodiment, a microphone 29, an auxiliary input 25 (for input 33), a USB input 23, a GPS input 24, touchscreen visual display 4 and a BLUETOOTH input 15 are all provided. An input selector 51 is also provided, to allow a user to swap between various inputs. Input to both the microphone and the auxiliary connector is converted from analog to digital by a converter 27 before being passed to the processor. Although not shown, numerous of the vehicle components and auxiliary components in communication with the VCS may use a vehicle network (such as, but not limited to, a CAN bus) to pass data to and from the VCS (or components thereof).

[0024] Outputs to the system can include, but are not limited to, a touchscreen visual display 4 and a speaker 13 or stereo system output. The speaker is connected to an amplifier 11 and receives its signal from the processor 3 through a digital-to-analog converter 9. Output can also be made to a remote BLUETOOTH device such as PND 54 or a USB device such as vehicle navigation device 60 along the bi-directional data streams shown at 19 and 21 respectively.

[0025] In one illustrative embodiment, the system 1 uses the BLUETOOTH transceiver 15 to communicate 17 with a user's nomadic device 53 (e.g., cell phone, smart phone, PDA, or any other device having wireless remote network connectivity). The nomadic device can then be used to communicate 59 with a network 61 outside the vehicle 31 through, for example, communication 55 with a cellular tower 57. In some embodiments, tower 57 may be a WiFi access point.

[0026] Exemplary communication between the nomadic device and the BLUETOOTH transceiver is represented by signal 14.

[0027] Pairing a nomadic device 53 and the BLUETOOTH transceiver 15 can be instructed through a button 52 or similar input. Accordingly, the CPU is instructed that the onboard BLUETOOTH transceiver will be paired with a BLUETOOTH transceiver in a nomadic device.

[0028] Data may be communicated between CPU 3 and network 61 utilizing, for example, a data-plan, data over voice, or DTMF tones associated with nomadic device 53. Alternatively, it may be desirable to include an onboard modem 63 having antenna 18 in order to communicate 16 data between CPU 3 and network 61 over the voice band. The nomadic device 53 can then be used to communicate 59 with a network 61 outside the vehicle 31 through, for example, communication 55 with a cellular tower 57. In some embodiments, the modem 63 may establish communication 20 with the tower 57 for communicating with network 61. As a non-limiting example, modem 63 may be a USB cellular modem and communication 20 may be cellular communication.

[0029] In one illustrative embodiment, the processor is provided with an operating system including an API to communicate with modem application software. The modem application software may access an embedded module or firmware on the BLUETOOTH transceiver to complete wireless communication with a remote BLUETOOTH transceiver (such as that found in a nomadic device). Bluetooth is a subset of the IEEE 802 PAN (personal area network) protocols. IEEE 802 LAN (local area network) protocols include WiFi and have considerable cross-functionality with IEEE 802 PAN. Both are suitable for wireless communication within a vehicle. Another communication means that can be used in this realm is free-space optical communication (such as IrDA) and non-standardized consumer IR protocols.

[0030] In another embodiment, nomadic device 53 includes a modem for voice band or broadband data communication. In the data-over-voice embodiment, a technique known as frequency division multiplexing may be implemented when the owner of the nomadic device can talk over the device while data is being transferred. At other times, when the owner is not using the device, the data transfer can use the whole bandwidth (300 Hz to 3.4 kHz in one example). While frequency division multiplexing may be common for analog cellular communication between the vehicle and the internet, and is still used, it has been largely replaced by hybrids of Code Domain Multiple Access (CDMA), Time Domain Multiple Access (TDMA), Space-Domain Multiple Access (SDMA) for digital cellular communication. These are all ITU IMT-2000 (3G) compliant standards and offer data rates up to 2 mbs for stationary or walking users and 385 kbs for users in a moving vehicle. 3G standards are now being replaced by IMT-Advanced (4G) which offers 100 mbs for users in a vehicle and 1 gbs for stationary users. If the user has a data-plan associated with the nomadic device, it is possible that the data-plan allows for broad-band transmission and the system could use a much wider bandwidth (speeding up data transfer). In still another embodiment, nomadic device 53 is replaced with a cellular communication device (not shown) that is installed to vehicle 31. In yet another embodiment, the ND 53 may be a wireless local area network (LAN) device capable of communication over, for example (and without limitation), an 802.11g network (i.e., WiFi) or a WiMax network.

[0031] In one embodiment, incoming data can be passed through the nomadic device via a data-over-voice or data-plan, through the onboard BLUETOOTH transceiver and into

Appendix: Kleve

• EX1005, ¶¶31-41

the vehicle's internal processor 3. In the case of certain temporary data, for example, the data can be stored on the HDD or other storage media 7 until such time as the data is no longer needed.

[0032] Additional sources that may interface with the vehicle include a personal navigation device 54, having, for example, a USB connection 56 and/or an antenna 58, a vehicle navigation device 60 having a USB 62 or other connection, an onboard GPS device 24, or remote navigation system (not shown) having connectivity to network 61. USB is one of a class of serial networking protocols. IEEE 1394 (FireWire™ (Apple), i.LINK™ (Sony), and Lynx™ (Texas Instruments)), EIA (Electronics Industry Association) serial protocols, IEEE 1284 (Centronics Port), S/PDIF (Sony/Philips Digital Interconnect Format) and USB-IF (USB Implementers Forum) form the backbone of the device-device serial standards. Most of the protocols can be implemented for either electrical or optical communication.

[0033] Further, the CPU could be in communication with a variety of other auxiliary devices 65. These devices can be connected through a wireless 67 or wired 69 connection. Auxiliary device 65 may include, but are not limited to, personal media players, wireless health devices, portable computers, and the like.

[0034] Also, or alternatively, the CPU could be connected to a vehicle based wireless router 73, using for example a WiFi (IEEE 803.11) 71 transceiver. This could allow the CPU to connect to remote networks in range of the local router 73.

[0035] In addition to having exemplary processes executed by a vehicle computing system located in a vehicle, in certain embodiments, the exemplary processes may be executed by a

computing system in communication with a vehicle computing system. Such a system may include, but is not limited to, a wireless device (e.g., and without limitation, a cellular telephone) or a remote computing system (e.g., and without limitation, a server) connected through the wireless device. Collectively, such systems may be referred to as vehicle associated computing systems (VACS). In certain embodiments particular components of the VACS may perform particular portions of a process depending on the particular implementation of the system. By way of example and not limitation, if a process has a step of sending or receiving information with a paired wireless device, then it is likely that the wireless device is not performing the process, since the wireless device would not "send and receive" information with itself. One of ordinary skill in the art will understand when it is inappropriate to apply a particular VACS to a given solution. In all solutions, it is contemplated that at least the vehicle computing system (VCS) located within the vehicle itself is capable of performing the exemplary processes.

[0036] In the illustrative embodiment as shown in FIG. 2 is an overview of the several steps that may contribute to the process of a vehicle rental micro-business integrated with a VCS. The process of a vehicle rental micro-business integrated with a computing system may be applied, but not limited to, automobiles, boats, machinery, and equipment rentals. The vehicle rental micro-business 200 may include a website, smart phone application or other nomadic device that an Owner and Temporary User may use to manage their assets and/or user profile. The following elements within a vehicle rental micro-business 200 may include a process for collecting identification and payment from Temporary User 204, collecting rental consent and agreement 206, distributing a virtual key to the Temporary User and VCS 210, giving

the Owner a selection of vehicle parameters to monitor usage of the vehicle including vehicle speed, load capacity, etc. . . . 222, control temporary user's usage 216, and other features that may assist the Owner and Temporary User with the virtual rental experience.

[0037] At step 202, the Owner and Temporary User may set up a user profile using a website or a nomadic device communicating with the site that is stored in a database. The Owner may set up a user profile by inputting information into the website or nomadic device including, but not limited to the make, model and year of the vehicle available for rent. The Temporary User may also fill out a user profile using the website or nomadic device to include, but not limited to, photos of credit cards, photo of forms of ID, facial recognition, voice print recognition, matrix barcode (ex. two-dimensional code), code word or phrase for speech recognition, temporary mobile web login IDs and password, or other types of unique Temporary User identification to validate and pay for the rental service at step 204.

[0038] At step 206, the Owner may collect the monetary compensation in exchange for the use of his vehicle. The Owner and Temporary User may agree to terms and conditions for the rental period using the website or nomadic device. The Owner may create a standard rental agreement form, or may develop a custom form based on the type of use the Temporary User is requesting to use the vehicle for. For example, if the Temporary User wants to use the Owner's vehicle to move furniture, the Owner can tailor the rental agreement to include what can and cannot be transported. The Temporary User and Owner can sign the consent and agreement using the website or the nomadic device at step 208.

[0039] At step 210, once the Temporary User selects the vehicle, pays the appropriate amount and signs a consent agreement, then the system may generate a virtual key to distribute to the Temporary User and VCS. The virtual key may be sent to, but not limited to, the website for the Temporary User to view, sent through an email, or to the Temporary User's nomadic device at step 212. The virtual key may also be sent to the vehicle configuring the VCS to enable the keyless drive system for the appropriate Temporary User during a given rental period.

[0040] At step 214, the Owner may have access to control usage of the vehicle being rented by the Temporary User. The Owner may set user restrictions by use of the website or nomadic device. The restrictions may be based on, but not limited to, the owner's selection of parameters including, but not limited to, speed, global position coordinates, or load weight restrictions. At step 216, the control parameters use restrictions may be monitored and if a restriction exceeds a limit the Temporary User and Owner may be notified. The monitoring information may be sent to the Owner through the website, with an email notification, or on the Owner's nomadic device at step 220. Email notification, text messages or an in-vehicle display message may be sent to notify the Temporary User if a restriction limit has been exceeded at step 218.

[0041] At step 222, control use may limit the Temporary User from exceeding the restrictions the Owner has set by several remedial actions that may reduce or stall vehicle performance. The remedial actions may include, but not limited to, reduce engine power, engine shut down, and immobilization. The reduce engine power remedial action may reduce engine power, limiting vehicle speed. An exemplary example of control usage may be limiting the Temporary User from

Appendix: Kleve

- EX1005, ¶¶41-48

driving to restricted areas defined by the Owner based on the rental terms and conditions. If the Temporary User enters a restricted area, he may be notified by the system and the vehicle may enter a remedial actions limiting vehicle speed.

[0042] Another exemplary example of monitoring vehicle parameters may be the use of the rental vehicle to haul cargo; if the Temporary User exceeds the max cargo weight limitation set as a numerical value by the Owner, the engine may enter a remedial action preventing the Temporary User from starting or stalling the vehicle. Additional vehicle variables being monitored by the Owner may include, but not limited to, vehicle diagnostics, in-vehicle cabin activity, and driver performance. Vehicle diagnostics may include, but not limited to, tire pressure, fuel level, trailer towing, and additional vehicle performance variables monitored by the VCS. In-vehicle cabin activity variables may include, but not limited to, unauthorized pet detection, a smoke detector, interior-viewing video camera, authorized driver verification, and audio control activity. Driver performance variables may include, but not limit to, braking, steering, throttle and accelerator pedal positions.

[0043] At step 224, the system may notify the Temporary User that the agreed upon rental period may expire soon, and if the rental period has ended the system may prompt the Temporary User with a message asking if he would like to purchase additional rental time. The system may allow the Temporary User to purchase additional rental time or decline the offer with the use of the vehicle touchscreen display or a nomadic device at step 226. If the rental term has ended, and no additional time is purchased, the system may begin the

vehicle rental exit process within the VCS at step 228. If the rental period is still within the agreed upon rental period, the system may carry on to monitor the vehicle allowing the Owner continued control of the vehicle with the use of vehicle restriction limits initially set by the Owner at the beginning of the rental term. At step 226, if the Temporary User decides that he may need to purchase additional rental time, the system may update the new rental period end time restriction and continue to monitor usage of the vehicle.

[0044] Another exemplary example of the vehicle rental micro-business system may include other enhancements including, but not limited to, matrix barcode (ex. two-dimensional code) used as the virtual key being recognized by the VCS. The smart phone may be used to communicate the matrix barcode information to the vehicle rental micro-business system directly. The system may be able to communicate information from the smart phone to the vehicle notifying the VCS of a virtual key. Once the Temporary User has the matrix barcode scanned by the vehicle, the smart phone may be able to connect with the VCS and be used to enter and enable the vehicle drive away event.

[0045] While the virtual key disclosed herein may be implemented in the manner as set forth above, it is recognized that the virtual key feature may be implemented as a key ignition device as set forth in U.S. Publication No. 2009/0198445 (the '445 publication) to Miller et al. which is hereby incorporated by reference in its entirety. For example, the key ignition device generally provides a driver status signal indicative of whether the driver is a primary driver (e.g. owner, parent, employer, etc.) or a secondary driver (e.g. temporary user, teenager, employee, etc.). A controller as disclosed in the '445 publication receives the driver status signal and controls various vehicle features and/or functionality based on the identity of the driver as provided on the

driver status signal. In this case, multiple ignition key devices may be provided. For example, a first ignition key device may be provided to transmit a first driver status signal indicating that the driver is the Owner of the vehicle. In addition, a second ignition key device may be provided to transmit a second driver status signal indicating that the driver is the Temporary User. In the event the vehicle detects that the driver is the Owner of the vehicle based on the first driver status signal, the vehicle may grant vehicle functionality to the Owner. In the event the vehicle detects that the driver is the Temporary User based on the second driver status signal, vehicle functionality may be restricted or limited in view of the teachings as set forth herein.

[0046] FIG. 3 is a flow-chart illustrating an example method of a vehicle rental micro-business having vehicle monitoring and control features. For example, and without limitation, the vehicle rental micro-business method may be used to include other services including, but not limited to having Temporary User's offer trades, offset swaps, and one sided rentals. At step 302, a vehicle Owner and Temporary User creates a user profile submitted through a website. The vehicle owner joins the website and may submit vehicle information including, but not limited to, vehicle description, specifications, and pictures at step 302. The website may be able to pull in addition vehicle specification and information from other sources. The vehicle Owner may include additional information, including but not limited to, setting up a deposit account, for example a paypal account. The vehicle Owner may then update and verify their information and identification within the website at step 304.

[0047] After a Temporary User setups their user identity within the website, the Temporary User may begin to use the vehicle rental services. The Temporary User may establish a community rating 306 based on past experiences and services with other vehicle owners that use the site. The Temporary User can log-in to the website to begin browsing the database of available vehicles to rent at step 308. Once the Temporary User is logged-in they may browse existing rental offers available, which may include, but not limited to, one sided rentals, swaps, offset swaps, trades, and custom swaps at step 310. At step 312, the Temporary User may also post offers of offset swaps, one sided rentals, and trades. The Temporary User may also browse other users and proposes an offer directly at step 314. When the Temporary User and vehicle Owner agree to terms 316 the website may generate the exchange or propose a rental agreement 318. The agreement between the Owner and Temporary User can be signed and payment made through the website at step 320. The agreement to rental terms and conditions between the parties may be done with the website using smart phones or a smart phone application, or any other type of nomadic device. Rental conditions may also be displayed on the vehicle's touchscreen visual display and accepted or rejected through the touchscreen visual display. Acceptance may be sent back to the Owner over the wireless network. A Temporary User may also access the Owner's web page to view and accept rental terms and conditions online at step 320.

[0048] At step 322, after identification of the Temporary User with an accepted agreement and payments made, the vehicle rental micro-business system may generate and deliver virtual keys to the Temporary User. The virtual key may allow a Temporary User temporary granted access to the Owner's vehicle. The granted access allowed by the virtual key may permit entry of the vehicle; grant a keyless drive-

Appendix: Kleve

• EX1005, ¶¶48-57

away of a vehicle, and/or both. The Temporary User may enter a virtual key outside or inside the vehicle, while credential authorization may be processed by the VCS, a server and/or by the vehicle Owner.

[0049] The system may be further extended to facilitate the virtual key with additional security by requiring remote credential verification at the vehicle. The remote credential verification at the vehicle may be done with additional hardware assembled on the exterior of the vehicle or in the vehicle cabin. The remote credential verification may be done by the VCS, using a server, or allowing the Owner to verify the Temporary User's request. For example, but not limited to, the Temporary User entering a credential verification password at the vehicle's touchscreen visual display while having the VCS, server, or owner compare and verify authorization. Once the Temporary User has completed the rental period and returned the vehicle to the appropriate drop off, the virtual key may terminate allowing the system to reset any private information stored on the vehicle-based computing system.

[0050] At 324, the Temporary User may have vehicle preset settings applied when renting a vehicle. These enhancements may include, but not limited to providing the Temporary User with stored frequent destinations sent to the VCS, radio presets, seat and mirror position, and ambient lighting preferences. The personalization of returning user's may also include a "bread crumb" feature allowing users to mark their usage to leave future users recommendations including which restaurant to eat at, or which routes to avoid.

[0051] At 326, the VCS may implement assigned vehicle control limitations during the use of the rental term by mitigating vehicle performance while preventing the Temporary User to exceed a limitation set by the Owner. The Owner may have the options to set rental restrictions based on, but not limited to, speed, destination location, or load weight limitations. Controlling usage to enforce compliance with the rental agreement terms may be of more importance to a vehicle rental micro-business owner as this may be the only vehicle the Owner possesses. These restrictions can be input using the vehicle rental website, a smart phone application or the Owner's nomadic device interacting with the VCS.

[0052] At 328, the control usage of the vehicle by the Temporary User may be monitored by the vehicle owner. The vehicle may be able to monitor and record its location, speed, and driving behavior while transmitting this information to the vehicle owner. Another exemplary example of the monitoring feature may be the use of RFID tags or CAN network monitoring of particular components of the vehicle that may be tampered with or removed. The use of RFID tags and/or the CAN network may allow the user to get additional vehicle information during the vehicle rental period or at the end of the rental period.

[0053] At 330, the VCS may monitor that a restriction threshold has been violated indicating that the Temporary User may be abusing the vehicle. At step 332, the Temporary User operating the vehicle under excessive conditions may cause the system to send an issue warning to the vehicle display information center. At step 334, the system may send a message to issue a warning to the Temporary User notifying of unauthorized usage of the vehicle at the display information center, instrument cluster, and/or other driver display device. If the system detects that the usage of the vehicle is extreme by exceeding a predetermined threshold, the VCS may command controlling actions to put the vehicle in a remedial action at step 336. The remedial actions may

include, but not limited to, reduce engine power, engine shut down, and immobilization. The VCS may monitor and detect the Temporary User exceeding a restriction limit and may notify the Owner while implementing remedial actions that may include preventing the vehicle from being started. The display message to alert the Temporary User of a restriction violation may be sent to the vehicle display information console and/or to the temporary user's nomadic device.

[0054] At 330, the VCS may continue to monitor the vehicle for the entire rental period. If the rental period is soon to expire the system may notify Temporary User at step 338. If the Temporary User has not returned the vehicle at the time the rental period has expired, the system may notify the user if a rental term extension is desired at step 342. If the extension term is desired, the Temporary User may be prompted to accept additional rental charges at step 344. The Temporary User may be charged for the additional rental time at step 346. If the extension of time is not desired, and/or not allowed by the Owner, the system may transmit controlling action to warn and induce remedial actions at step 350. If the extension of time is not desired, and the Temporary User is within the allocated time and distance to return the vehicle to the required parking location at step 348. If the Temporary User has returned to the required parking spot, the system may begin to prepare for return to the vehicle Owner. During the preparation to return vehicle to Owner and end the rental period, the system may save any enhancements information based on the Temporary User's settings at step 352.

[0055] At step 354, once the Temporary User has completed the rental period and returned the vehicle to the appropriate drop off, the virtual key may terminate. Once the virtual key has terminated, the system may reset any private information stored on the vehicle-based computing system by the Temporary User at step 356. The Temporary User may collect pictures to report status of the vehicle to the Owner after the rental period has ended at step 358. The system may include a standardized report form that requires certain information the Temporary User must fill out when returning the vehicle, including pictures. After the rental experience, the Owner and Temporary User may rate their experience on the website to notify others of their satisfaction each person had during the transaction at step 360.

[0056] FIG. 4 shows an illustrative example of a communication system through which a wireless communication device can communicate with a vehicle 421 to enable a vehicle rental micro-business. In this illustrative embodiment, a nomadic device (e.g., without limitation, a cellular phone, a personal cellular telephone) 403 is used to send a communication through a cellular network 407. This communication is relayed through a network 411 (e.g., without limitation, the cellular network, the internet, etc.) to a centralized system 401. In another embodiment, the nomadic device 403 may send a communication through network 412 which may include, but is not limited to, WiFi or WiMax. This communication is relayed through a network 406 (e.g., without limitation, cloud computing, the internet,) to a centralized system 401.

[0057] In this illustrative embodiment, the centralized system is a server system that includes processing capability for incoming nomadic device signals designated to interact with a remote vehicle 421. For example, the server(s) 401 may include an automated call server and/or web host. Further, the server(s) 401 may route an incoming signal from a nomadic device (ND) 403 to the appropriate remote vehicle to enable

Appendix: Kleve

- EX1005, ¶¶57-67

a Temporary User keyless access and drive away capabilities of the Owner's vehicle. Data sent in this fashion may be sent using data-over-voice, a data-plan, or in any other suitable format.

[0058] Data can also be sent to the vehicle 421 through the server(s) 401 using a personal computer 405. In this case, the data is likely, although not necessarily, sent over the internet 409. Once the server(s) 401 receive the incoming data request from the remote source 403, 405, the message is processed and/or relayed to a vehicle 421 and the Temporary User's nomadic device 402. The vehicle may be identified by a header associated with one or more incoming data packets, or may be identifiable based on a database lookup, for example.

[0059] In one embodiment, a message is relayed to the remote source 403, 405 as well. For example, as will be described in further detail below, when an authorized temporary user remotely transmits a request from a Temporary User's nomadic device 402 (e.g., via a button or key press) to receive authorization to operate and drive away the vehicle 421, the server(s) 401 may respond by transmitting an authorization code to both the Temporary User's nomadic device 402 and to the vehicle control system for input by the authorized Temporary User at the vehicle 421. An authorized temporary user may be any individual recognized by the vehicle 421 as an authorized user based on a matrix barcode, a fingerprint scan, an authorized code typed in a touchscreen, voice recognition, and the like. It should be understood that these examples are non-limiting and other means of authorization for the vehicle rental micro-business may be used.

[0060] The relay to the vehicle 421 is sent out from the server(s) 401 through a network (e.g., without limitation, a cellular network 113, the internet, etc.) and passed through a cellular network 415 to the vehicle 421. In another embodiment, the relay may be passed through network 414 (e.g., WiFi or WiMax) and to the vehicle 421. A remote communication module in the vehicle 421 receives the signal sent from the server(s) 401 and processes it or relays it to an appropriate processing system within the vehicle 421.

[0061] In at least one illustrative embodiment, the vehicle 421 is also outfitted with a communication transceiver, such as, but not limited to, a BLUETOOTH transceiver. This transceiver may allow communication with the nomadic device 403 using a direct signal 419. This transceiver may also allow communication with the Temporary User's nomadic device 402 to the vehicle 421 using a wireless connection 420 including, but not limited to, a smart phone that may connect to the vehicle through SYNC or other Bluetooth pairing device. It should be understood that the communication between nomadic device 403, temporary user nomadic device 402, server 401, and vehicle 421 may be performed in a number of ways and FIG. 4 is presented for illustrative purposes. FIG. 4 illustrates various alternatives for communicating data. For example, and without limitation, data communication may be partially or entirely cellular or WiFi, or a combination of cellular and WiFi.

[0062] FIG. 5 shows an illustrative example of an overview of how the vehicle rental micro-business may be structured with a keyless transaction between the Owner of the vehicle and the Temporary User. This example illustrates the process after the vehicle Owner and Temporary User have already setup a user profile within the database and have both agreed to the rental agreement. At step 502, the vehicle Owner may enter in vehicle authorization credentials based on information received by the Temporary User to set up a virtual key.

The virtual key may be sent to the vehicle allowing Temporary User access to the Owner's vehicle.

[0063] Additional Temporary User identification 504 may be sent to the vehicle Owner allowing for this information to be entered into the server and used as a virtual key, or in addition to the virtual key, allowing the Temporary User access to the Owner's vehicle while enabling a keyless drive-away. The Temporary User identification and virtual key may be sent in an encrypted message to the VCS, Temporary User's nomadic device, and/or vehicle Owners nomadic device. The Temporary User's information for vehicle authorization credential verification 516 may include, but not limited to fingerprint recognition of user, photos of credit cards, photo of forms of ID, facial recognition, voice print recognition, matrix barcode (ex. two-dimensional code), code word or code phrase for speech recognition, temporary mobile web login IDs and password, or other types of unique Temporary User identification.

[0064] The Temporary User's information for credential verification 516 may be collected and exchanged using several methods including, but not limited to, a website, at a vehicle, or through a nomadic device. A website may be developed to have the Temporary User submit information including, but not limited to, forms of ID, driver license, facial pictures, fingerprints, code phase and/or credit card information. A vehicle may also be equipped to collect and exchange the Temporary User credential verification with the use of additional hardware mounted on the outside or inside of the vehicle. The Temporary User may also use their nomadic device to exchange or collect information for the enablement of a keyless drive-away system.

[0065] An example for applying Temporary User credential verification at a vehicle may include, but not limited to, the use of additional hardware integrated with the VCS to allow collection and exchange of information to enable a keyless drive-away rental event. For example, the Temporary User may use their credit card at a vehicle with the use of hardware integrated with the VCS to collect payment credentials, identify the user, and/or agree to rental terms. Another exemplary embodiment of applying Temporary User credentials at a vehicle may be with the use of facial recognition done by having a camera integrated with the VCS.

[0066] The Temporary User's information for credential verification may be sent to both the vehicle computer system and the Temporary User's nomadic device 518 including, but not limited to, a smart phone. When the scheduled rental period of time begins the vehicle Owner may send the credentials to the vehicle with the use of a server 506 and the vehicle may be able to receive the information using a wireless device 514. The wireless device 514 may include, but not limited to, an embedded cellular modem, embedded WiFi device, Near Field Communication connected phone, brought-in cellular device like a USB modem, MiFi, smart phone that may be connect to the vehicle through SYNC or other Bluetooth pairing device, or a PC (ex. IPAD) that may be connected to the vehicle through SYNC or other Bluetooth pairing device. Additional hardware input device 520 for credential verification may include but not limited to a camera, microphone, matrix barcode scanner, fingerprint reader, or retina scanner integrated with the vehicle control system.

[0067] At step 508, the Temporary User may use their virtual key credential to access the vehicle. The virtual key credential can be collected via email, phone message or other established method or in a novel way presented here; or this

Appendix: Kleve

• EX1005, ¶¶67-76

can be collected by the vehicle itself through various input devices which may be connected to the VCS using a camera, matrix barcode scanner, optical scanner, fingerprint scanner or microphone. Once the Temporary User enters the vehicle and captures the credentials with one of the methods mentioned above, the vehicle may verify that the Temporary User has approval to use the vehicle.

[0068] At step 510, the vehicle may verify the Temporary User's virtual key by communicating with the server to compare the credential and verify Temporary User's access. The vehicle using the wireless device to transmit confirmation back to the vehicle Owner 512 through a telecommunications network notifying that the Temporary User entered the vehicle and has commenced the vehicle rental agreement. Once the rental period has expired the virtual key may be reset and cleared from the VCS.

[0069] FIG. 6 is an exemplary embodiment of the vehicle rental micro-business distributing and controlling virtual keys using a nomadic device with a vehicle. The vehicle rental micro-business administrative system may consist of a computer system configured to host one or more websites for interaction with a vehicle Owner and Temporary User. In the illustration 600, a server 634 is used to communicate between a vehicle Owner nomadic device 601, a Temporary User nomadic device 611, and a vehicle computing system 621. Using a nomadic device, for example a smart phone, a Temporary User and vehicle Owner may set up user profiles, enter into an agreement and make a payment to initiate the vehicle rental process between the two parties at step 602 and 612. At

step 604, the vehicle Owner may then generate a virtual key based on a password generated by the vehicle Owner that may include a matrix barcode or a code word that the Temporary User may enter/send to the vehicle when ready to begin the rental term. Another exemplary embodiment of generating a virtual key may be done by using Temporary User's credentials including fingerprint recognition, photos of credit cards, photo of forms of ID, facial recognition, voice print recognition, phrase for speech recognition, temporary mobile web login IDs and password, or other type of unique Temporary User identification at step 614. At step 616, the virtual key is generated and sent to the Temporary User. The Owner may deliver a virtual key to the vehicle for recognizing the Temporary User having authorization to enable a keyless drive-away at step 606.

[0070] At step 622, when the Temporary User arrives at the vehicle within the scheduled rental time, he or she may enter the virtual key using several methods. One method may include having the Temporary User scan their finger with the use of a fingerprint scanner integrated with the VCS to validate authorization to access the vehicle. The Temporary User's virtual key may be authorized several ways including, but not limited to, at the vehicle, communicated back to the vehicle rental authorization server using a telecommunications network, or by having the vehicle Owner verify access using their nomadic device.

[0071] At step 618, the Temporary User may send the virtual key to the server requesting access to the vehicle, or use a vehicle input device, like camera, microphone, fingerprint scanner or retinal scanner integrated with the VCS to capture his identity and/or payment credentials to enable a keyless drive-away. If it is the scheduled time for the rental, the vehicle may compare the identity credentials just inputted at the vehicle and the one previously sent virtual key to the vehicle from the vehicle Owner to determine authorization. If

the comparison is successful, the vehicle may enable drive-away access to that Temporary User for the scheduled time period of the rental agreement. For the duration of the rental term, the Temporary User may again input the same identifying credentials to unlock and drive.

[0072] At step 624, the Temporary User's nomadic device may be paired with the VCS and may send personal settings to the vehicle including, but not limited to, radio station presets, navigation routes, and/or preferred climate control settings. Another exemplary example of setting personal preferences may include, but not limited to, facial recognition to recognize the driver using a camera mounted in the vehicle cabin on the dash. Once the camera recognizes the Temporary User, the VCS may request additional user settings and preferences including seat adjustment, and climate control temperatures.

[0073] At step 626, during the rental term the VCS may monitor the Temporary User's utilization of the vehicle including, but not limited to, renter verification, driving behavior, vehicle location, speed, fuel level, and other vehicle information requested by the vehicle owner. For example, the system may monitor that the actual authorized renter is the one driving the vehicle with the use of an interior viewing camera embedded with facial recognition software. The monitoring information is sent to the vehicle owner, and may have other additional parameters that may only be sent to the owner if they exceed or violate a restriction limit. These additional parameters may include, but not limited to speed limits, weight limits, or "No-Go Zones" which are prohibited areas where the owner does not want their vehicle to be used.

[0074] At the end of the rental term, the vehicle may warn the customer of the time expired either on the vehicle touch-screen visual display or over a remote device while preparing to take a predetermined action—probably a series of increasing actions from warning and tracking to slowdown or shut-down of the vehicle. At step 628, once the schedule rental is complete the virtual key may be terminated, allowing the vehicle to be secured for either the Owners entry or the next temporary user scheduled to use the vehicle. Any personal settings or private information entered onto or within the VCS by the Temporary User may be reset after the schedule rental period has been complete at step 630.

[0075] In the illustrative embodiment as shown in FIG. 7 is an overview of a vehicle rental micro-business monitoring process integrated with a VCS. At step 702, the VCS may begin monitoring and report usage of the vehicle to the owner. The system may wait for the rental period to start at step 704. Once the Temporary User initiates the rental event, the system detects a rental time start at step 706. The system may begin to download performance limitations and restrictions assigned by the vehicle owner at the start of the rental period at step 708. The performance limitations and restrictions downloaded to the VCS may include, but not limited to: setting a top vehicle speed, limiting the cargo load, and alerting the vehicle owner if the driver enters an area deemed to be prohibited by the owner.

[0076] At step 710, the monitoring of the vehicle's location may be done to reassure the vehicle owner that their asset is being driven in an approved manner and area. The GPS data may be transmitted to the server and monitored using the vehicle owner's nomadic device. The continuous monitoring of the Temporary User's behavior during the rental period may be transmitted to the server, sent to a nomadic device, or stored for a later download at step 712. The monitoring done by the vehicle rental micro-business may include, but not

Appendix: Kleve

• EX1005, ¶¶76-86

limited to, unauthorized objects or cargo, unauthorized driving behavior, unauthorized driver, and/or an unauthorized trailer tow. The methods to accomplish the monitoring of the mentioned examples above may include, but not limited to, using a camera system, biometric recognition, and the VCS monitoring sensors and subsystems throughout the vehicle.

[0077] At step 714, monitoring may start and end when the ignition key is turned on and off. In an exemplary example when the vehicle ignition is off, the monitoring may allow the VCS to wake up periodically to check certain performance limits and components identified using RFIDs. The components using an RFID may be parts that could be high left items, or easily removed from the vehicle including, but not limited to, radios, navigation systems, catalytic converters, and wheels. When the vehicle ignition is on, the monitoring is continuous using RFIDs placed on certain vehicle components while transmitting data to the vehicle owner. The vehicle owner may have a further sense of security knowing high theft items are intact with intermittent and continuous monitoring features no matter if the ignition is on or off.

[0078] At step 716, once the vehicle ignition is on, the monitoring of driver behavior is done by the VCS. This information is transmitted to either the server, directly to the vehicle owner's nomadic device, or saved on a storage device for later download. The vehicle owner may review the monitored data at a given time throughout the rental period. The monitoring of driver behavior events includes, but not limited to, vehicle speed, acceleration force, wheel speed, breaking, steering, vehicle weight, throttle and pedal position. The vehicle owner may understand based on the data if the Temporary User is using the vehicle under extreme circumstances or if they are driving responsibly. An example of using the vehicle under an extreme circumstance may include driving the vehicle at excessive vehicle speeds.

[0079] At step 718, the vehicle owner may also be notified if the system has a detected driver behavior event. The vehicle owner may be sent information that the Temporary User has been in an accident or near miss based on airbag deployment, accelerometer data, and/or anti-lock brake information. If the Temporary User is involved in an accident, the system may store and save previous recorded data leading up to the accident at step 720. For example, if the airbag is deployed the VCS may save three minutes of all monitored data leading up to the airbag deployment including, but not limited to, a dashboard camera, accelerator pedal position, speed, and brake pedal position at step 722. The monitoring system may continue to check to see if continued usage of the vehicle is acceptable based on the accident data/near miss data to determine if the vehicle is safe for continued operation at step 724. At 726, if the vehicle is in an acceptable condition for continued usage and rental time has not expired, the system may continue to monitor the vehicle rental usage. If the vehicle cannot be used, the VCS may begin the vehicle rental exit mode process at step 728.

[0080] At step 718, if the VCS monitoring detects no accident, and the rental period has not expired, the system may continue to monitor the vehicle rental usage. If the rental period has ended, the monitoring and control system of the vehicle rental micro-business may begin to start its Temporary User vehicle rental exit mode process at step 728. The exit mode process may include the monitoring system to store additional variables and data to report to the vehicle Owner including, but not limited to, vehicle location, fuel level, and additional vehicle diagnostic information. The exit mode process

may also include, but not limited to, terminating the virtual key while allowing the system to reset any private information stored on the vehicle-based computing system. The system may include a standardized report form that requires certain information the Temporary User must fill out when returning the vehicle.

[0081] In the illustrative embodiment shown in FIG. 8 is a flow-chart illustrating an example method of a vehicle owner interface with a vehicle rental authorization system. The owner may begin by setting up a user profile within the vehicle rental authorization system at step 802. The owner may interact with the vehicle rental authorization system through a website. The website may be formatted to allow the owner to input profile information using a personal computer, smart phone or other nomadic device. The user profile may include owner's personal information including details about the vehicle he intends to list as a rental within the vehicle rental authorization system. Information may include, but not limited to, owners name, home address, email address, and vehicle specifications including pictures. The vehicle rental authorization system may have one or more databases with a list of vehicle owners and rental vehicles available.

[0082] At step 804, the vehicle rental authorization system stores the owner's data. The data may be organized by the vehicle rental authorization system to allow potential Temporary Users to view vehicle information. Once a Temporary User has selected the owner's vehicle to rent, the vehicle rental authorization system may notify the owner of a rental request at step 806.

[0083] At step 808, the vehicle owner may be able to review the temporary user's vehicle rental request. The owner may review the requested rental based on what the Temporary User is looking to use the vehicle for (e.g. without limitation, for towing, hauling, or errands), when the requested use will be taking place, and where. The owner may also review the Temporary Users profile and rental history, to see how they have ranked with past experiences using the vehicle rental authorization system at step 810.

[0084] At step 812, if the owner decides he has no interest in accepting the Temporary User's offer, he may decline and wait for the vehicle rental authorization system to notify of any other offers. If the owner has decided to accept the offer he may begin the process of developing terms and conditions of the rental period. At step 814, the owner may negotiate additional terms and conditions based on the specific use and needs the Temporary User may use the vehicle for. These additional terms and conditions may include, but not limited to, cargo load weight restrictions, tow load restrictions, or the amount of miles that can be driven during the rental period. The negotiation of the terms and conditions may be done using the vehicle authorization rental system.

[0085] At step 818, once the contract is formed, the Owner and Temporary User may use the vehicle authorization rental system to accept the terms and conditions. The vehicle authorization rental system may begin the keyless vehicle rental authorization process at step 820. The owner may complete the entire vehicle rental process using the vehicle rental authorization system without meeting the Temporary User.

[0086] In the illustrative embodiment shown in FIG. 9 is a flow-chart illustrating an example method of a Temporary User's interface with a vehicle rental authorization system. The Temporary User may begin by setting up a user profile that is saved in a database within the vehicle rental authorization system at step 902. The Temporary User may interact

Appendix: Kleve

- EX1005, ¶¶86-91

with the vehicle rental authorization system through a website. The website may be formatted to allow the Temporary User to input profile information using a personal computer, smart phone or other nomadic device. The user profile may include Temporary User's personal information including details about the vehicle he intends to rent within the vehicle rental authorization system. Information may include, but not limited to, Temporary User's name, home address, email address, driving record, and a driver's licenses.

[0087] At step 904, the vehicle rental authorization system stores the Temporary User's data in a database. The data may be organized by the vehicle rental authorization system to allow vehicle owner's to review this information before renting their valuable asset to the Temporary User. The vehicle rental authorization system may allow the Temporary User to be matched with a vehicle based on location, trip type, date, vehicle type requested, scheduled number of hours needed, a certain day of the week, and vehicle condition at step 906. For example, the Temporary User may have a pickup truck request for this weekend because they need to move furniture. Based on the selection offered by the vehicle rental authorization system, the Temporary User may review the generated output list of vehicles and select the vehicle to rent at step 908. The Temporary User may decide which vehicle to rent not only on vehicle needs and performance, but also looking at what the vehicle owner's community rating is based on past rental experiences at step 910

[0088] At step 912, the vehicle rental authorization system may accept the Temporary User's selection of which vehicle he would like to rent. The system may output a notification to the owner of the requested vehicle rental by a Temporary User. The owner may review the Temporary User's request based on several factors including, but not limited to, the use, trip type, and date the Temporary User is requesting to rent the vehicle at step 914. The owner may also review the Temporary User community ranking to determine if he should rent to the interested Temporary User.

[0089] At step 916, if the owner decides he has no interest in accepting the Temporary User's offer, therefore declining, the Temporary User may go back and select another potential vehicle to rent. If the owner has decided to accept the offer, he may begin the process of developing terms and conditions of the rental period. The owner may input additional terms and conditions based on the specific use and needs the Temporary User may have for renting the vehicle at step 918. These additional terms and conditions may include, but not limited to, cargo load weight restrictions, tow load restrictions, or the amount of miles that can be driven during the rental period. The negotiation of the terms and conditions may be done using the vehicle authorization rental system. After negotiation of terms and conditions, the authorization rental system may output rental terms for the parties to review.

[0090] At step 920, once the contract (e.g. without limitation, a rental contract) is formed, the owner and Temporary User may use the vehicle authorization rental system to accept the terms and conditions. The Temporary User may review the contract and accept the term using the vehicle authorization rental system at step 922. Once the contract is accepted, the vehicle authorization rental system may begin the keyless vehicle rental authorization process at step 924. The Temporary User may complete the entire vehicle rental process using the vehicle rental authorization system without physically meeting the owner.

[0091] While exemplary embodiments are described above, it is not intended that these embodiments describe all possible forms of the invention. Rather, the words used in the specification are words of description rather than limitation, and it is understood that various changes may be made without departing from the spirit and scope of the invention. Additionally, the features of various implementing embodiments may be combined to form further embodiments of the invention.

Mikan (EX1007)

Appendix: Mikan

- EX1007, Fig. 1

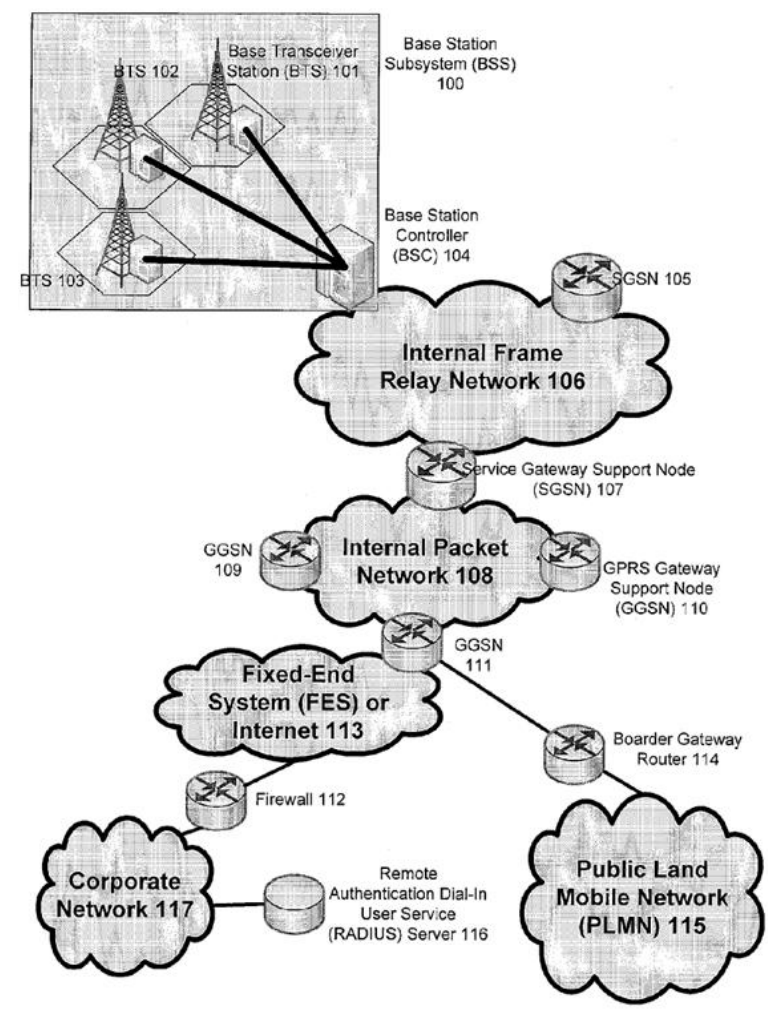


FIG. 1A

Appendix: Mikan

- EX1007, Fig. 1B

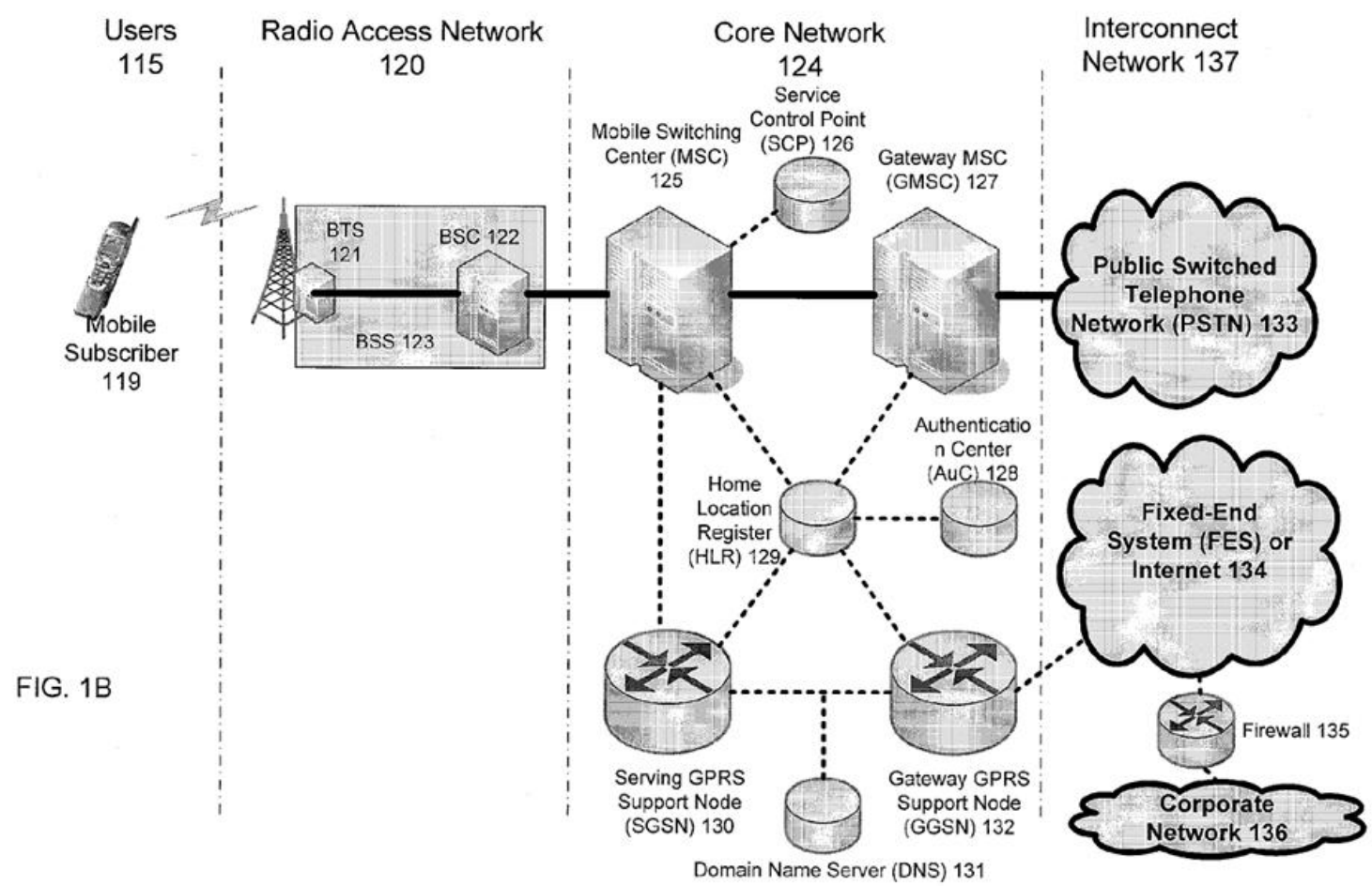
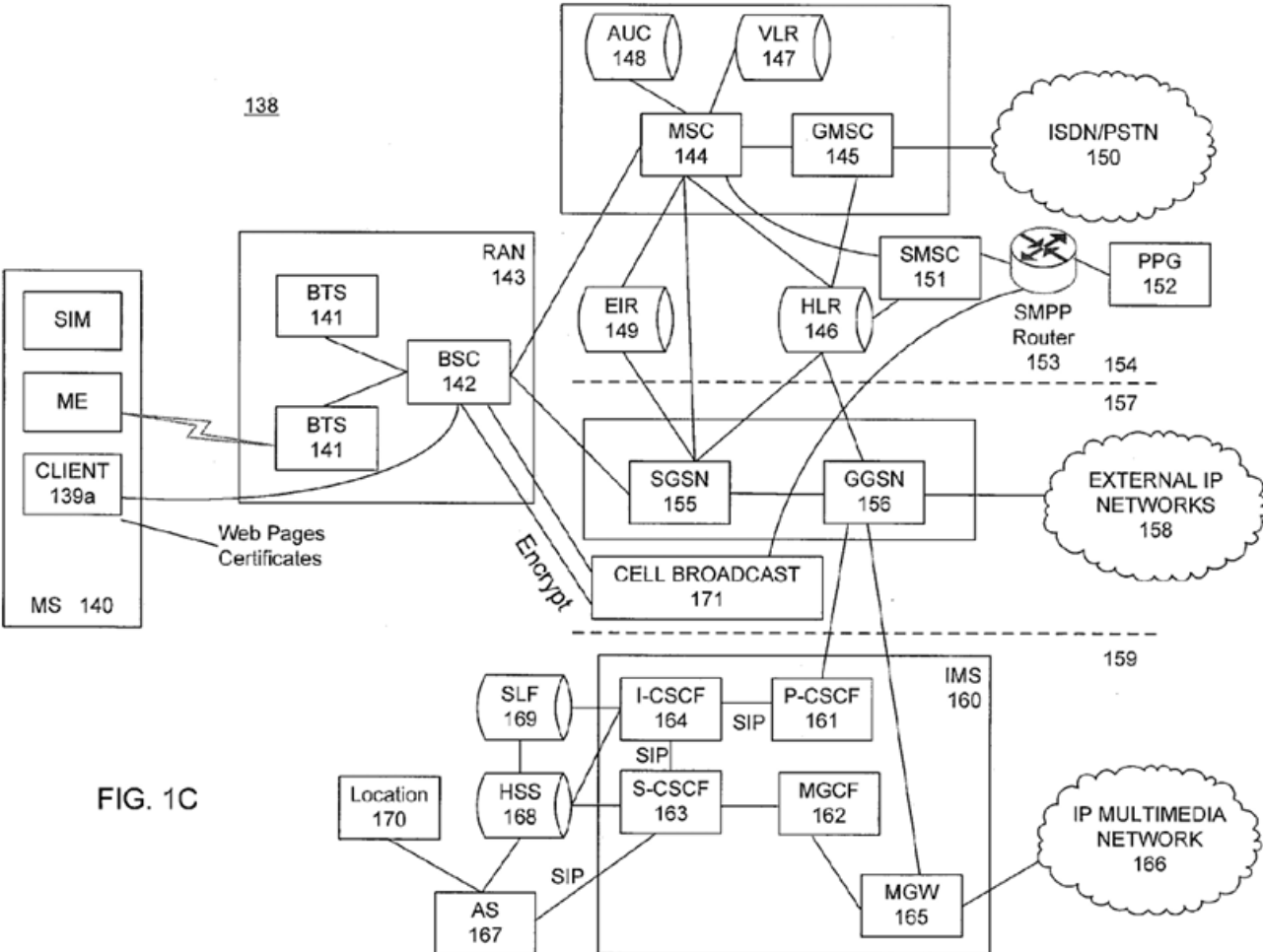


FIG. 1B

Appendix: Mikan

- EX1007, Fig. 1C



Appendix: Mikan

- EX1007, Fig. 2

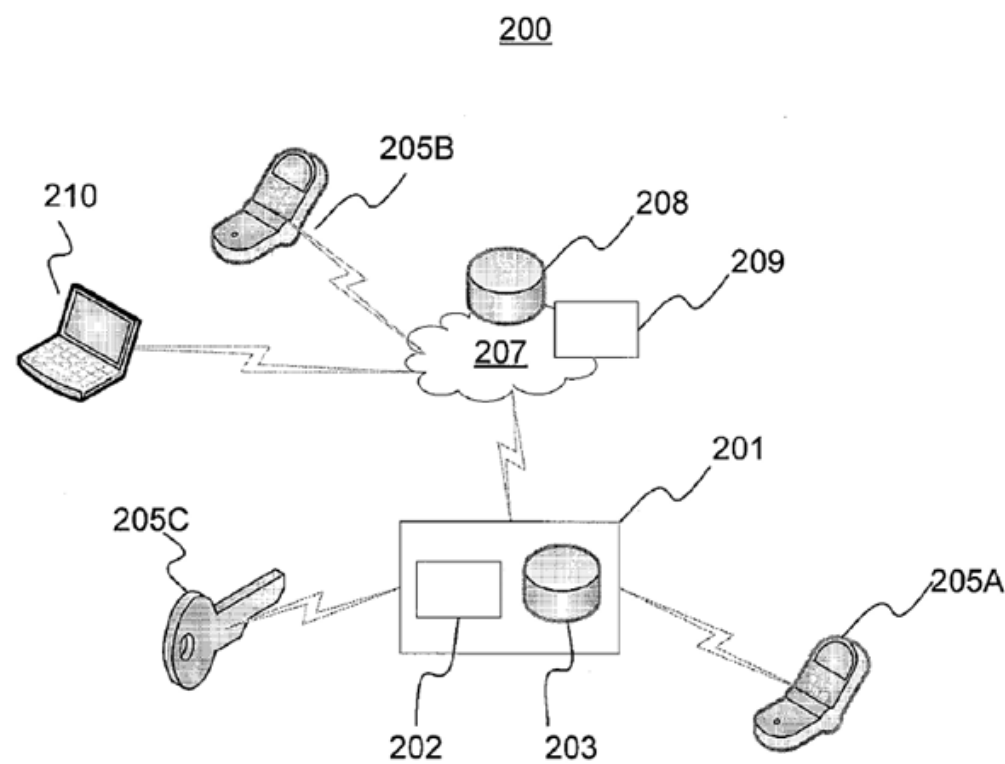
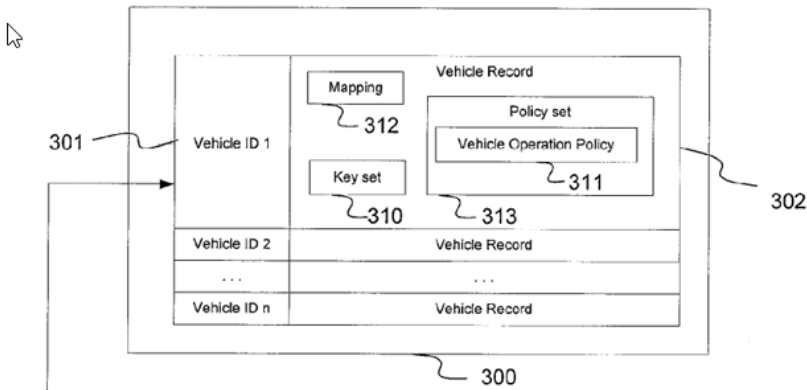
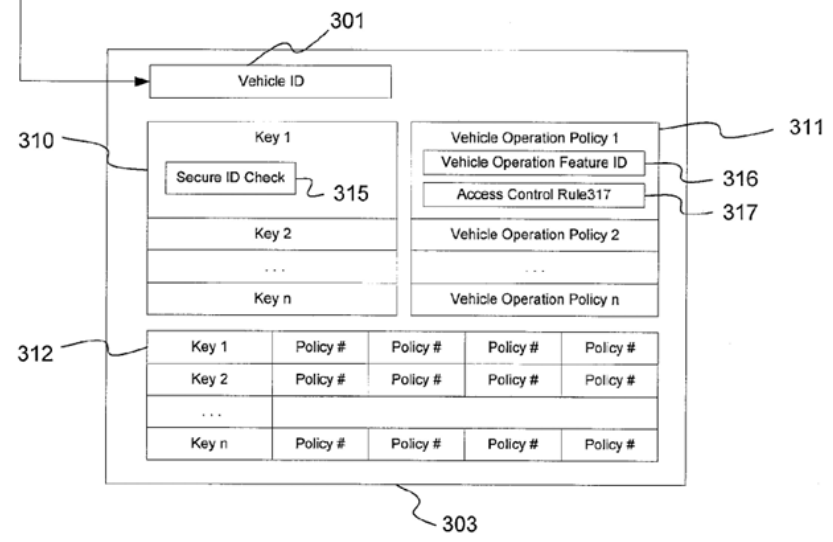


FIG. 2

Appendix: Mikan

- EX1007, Fig. 3A-3B



Appendix: Mikan

- EX1007, Fig. 4

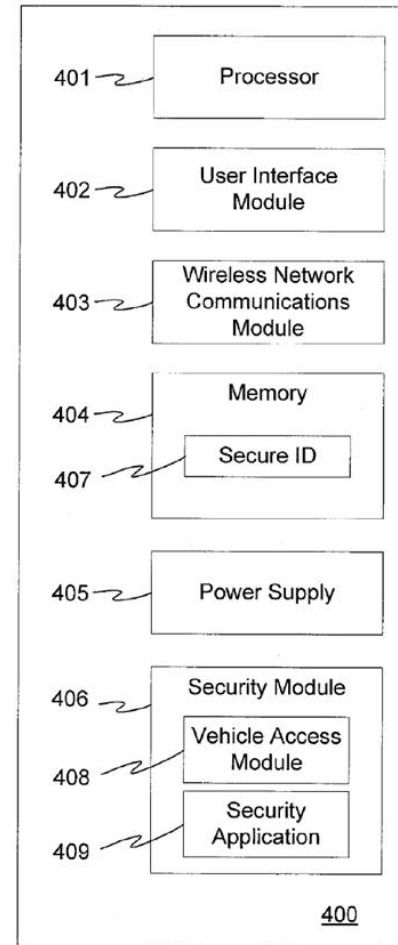


FIG. 4

- EX1007, Fig. 5

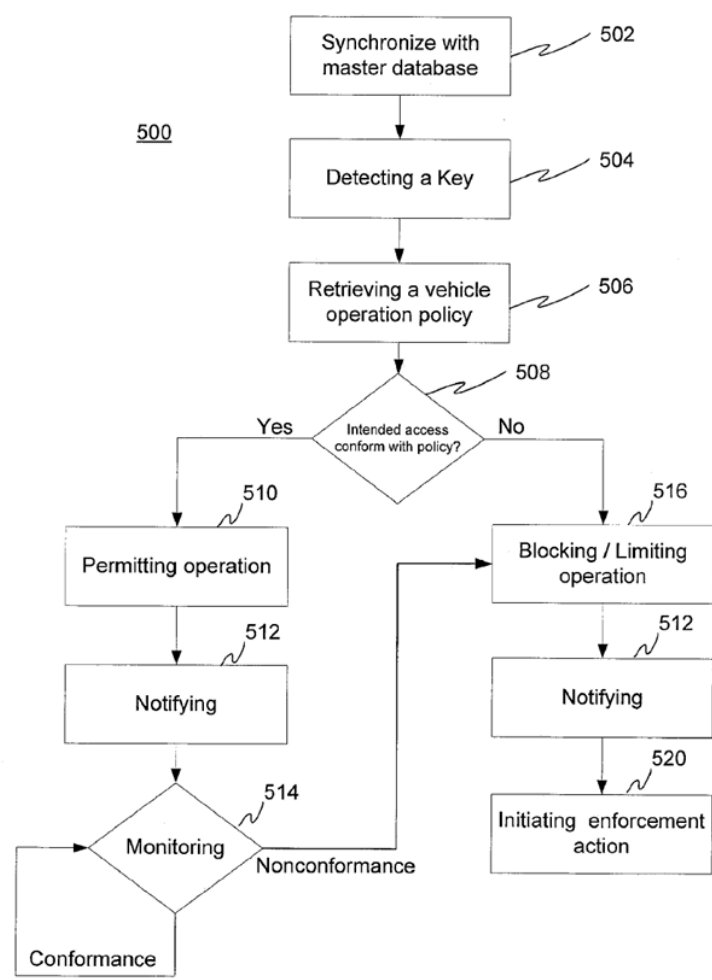


FIG. 5

Appendix: Mikan

- EX1007, Fig. 6

600

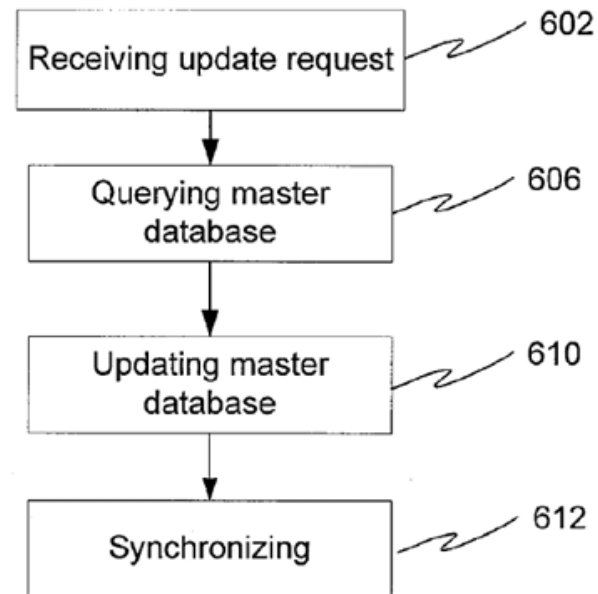


FIG. 6

Appendix: Mikan

- EX1007, ¶¶1-17

WIRELESS DEVICE AS PROGRAMMABLE VEHICLE KEY

BACKGROUND

[0001] Automobiles and other vehicles are often secured from unauthorized access and operation via lock and key. Once locked, the vehicle's doors and ignition system remain inoperable until the proper key is used. Keys traditionally have been made of metal blanks with grooves and teeth shaped to engage the lock. Electronic keys may provide similar functionality as their metal key counterparts. In addition, an electronic key may not require the operator of the vehicle to physically place the key within the lock. For example, the electronic key may operate via a proximity sensor within the car. When the electronic key is within range of the proximity sensor, the vehicle may shift from an inoperable, "locked" mode to an operable mode.

[0002] In addition to metal and electronic keys that grant full access to open and operate a vehicle, some vehicle manufacturers provide a "valet key" that grants limited access to the vehicle. The valet key is typically a metal key that allows the holder to unlock the driver's side door and operate the ignition lock. The valet key typically does not provide access to the vehicle's trunk, glove box, or other secure areas of the vehicle. With respect to the operation of the vehicle, however, the valet key does not limit the range or manner in which the holder operates the vehicle. The holder of a valet key may operate the vehicle at any speed or over any distance, which may not be acceptable for the vehicle's owner.

[0003] Thus, when a vehicle owner wishes to allow another person (e.g., child, valet, friend, etc.) to operate the owner's vehicle, conventional metal and electronic keys typically provide the owner with only two options. The first option is to provide the person with a "regular" key that provides the person with full access to all of the vehicle's features. The second option is to provide the person with a valet key that restricts the person's access to certain vehicle compartments. In either case, the owner has no way to restrict the person's ability to operate the vehicle.

[0004] Wireless devices, such as cellular telephones, are increasingly ubiquitous. They are increasingly able to process applications and perform digital functions beyond placing and receiving telephone calls. Their network connectivity gives them functionality typically not found in other handheld devices.

SUMMARY

[0005] In view of the foregoing drawbacks and shortcomings, a method and device for providing secure operation of a vehicle is presented. The method includes detecting a key for accessing a vehicle, retrieving a vehicle operation policy associated with the key, and permitting operation of the vehicle consistent with the vehicle operation policy. The key may be embedded within a wireless device such as a cellular telephone. The vehicle operation policy may include an access control rule that may indicate to enable, partially enable, or disable a vehicle operation feature. Where the intended operation of the vehicle is not consistent with the access control rule, the operation may not be permitted and an enforcement action may be taken, such as disabling a feature of the vehicle for example.

Inside in a vehicle and the first database may communicate with the second database via a wireless network. The records may include an access control rule.

[0007] A wireless device for providing secure operation of a vehicle is also presented. The wireless device may include a user interface module, a wireless communications module, a memory, a processor, and a vehicle access module. The wireless communications module may communicate an request to update an access control rule via the wireless network. The vehicle access module may communicate a secure identifier to access the vehicle.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] FIG. 1A depicts an overview of a network environment in which aspects of an embodiment may be implemented;

[0009] FIG. 1B depicts a GPRS network architecture in which aspects of an embodiment may be implemented;

[0010] FIG. 1C depicts an alternate block diagram of an example GSM/GPRS/IP multimedia network architecture in which aspects of an embodiment may be implemented;

[0011] FIG. 2 depicts a block diagram of an example wireless vehicle security system;

[0012] FIGS. 3A-B depicts a block diagram of an example master database and local database, respectively;

[0013] FIG. 4 depicts a block diagram of an example wireless device equipped for use as an electronic key;

[0014] FIG. 5 depicts a flow diagram of an example vehicle security process; and

[0015] FIG. 6 depicts a flow diagram of an example network security process.

DETAILED DESCRIPTION

Example Network and Operating Environments

[0016] The following description sets forth some example telephony radio networks and non-limiting operating environments in which a wireless vehicle security system according to an embodiment may be used. The below-described operating environments should be considered non-exhaustive, however, and thus the below-described network architecture merely shows an example network architecture in which aspects of various embodiments may be incorporated. One can appreciate, however, that aspects of an embodiment may be incorporated into now existing or future alternative architectures for communication networks.

[0017] The global system for mobile communication ("GSM") is one of the most widely-used wireless access systems in today's fast growing communication systems. GSM provides circuit-switched data services to subscribers, such as mobile telephone or computer users, for example. General Packet Radio Service ("GPRS"), which is an extension to GSM technology, introduces packet switching to GSM networks. GPRS uses a packet-based wireless communication technology to transfer high and low speed data and signaling in an efficient manner. GPRS optimizes the use of network and radio resources, thus enabling the cost effective and efficient use of GSM network resources for packet mode applications. For purposes of explanation, various embodiments are described herein in connection with GSM. The references to GSM are not exclusive, however, as it should be appreciated that embodiments may be implemented in connection with any type of wireless access system such as, for example, CDMA or the like.

Appendix: Mikan

• EX1007, ¶¶18-25

[0018] As may be appreciated, the example GSM/GPRS environment and services described herein can also be extended to 3G services, such as Universal Mobile Telephone System (“UMTS”), Frequency Division Duplexing (“FDD”) and Time Division Duplexing (“TDD”), High Speed Packet Data Access (“HSPDA”), cdma2000 1× Evolution Data Optimized (“EVDO”), Code Division Multiple Access-2000 (“cdma2000 3×”), Time Division Synchronous Code Division Multiple Access (“TD-SCDMA”), Wideband Code Division Multiple Access (“WCDMA”), Enhanced Data GSM Environment (“EDGE”), International Mobile Telecommunications-2000 (“IMT-2000”), Digital Enhanced Cordless Telecommunications (“DECT”), etc., as well as to other network services that shall become available in time. In this regard, the techniques of the various embodiments discussed below may be applied independently of the method of data transport, and does not depend on any particular network architecture, or underlying protocols.

[0019] FIG. 1A depicts an overall block diagram of an example packet-based mobile cellular network environment, such as a GPRS network, in which aspects of an embodiment may be practiced. In such an environment, there may be any number of subsystems that implement the functionality of the environment such as, for example, a plurality of Base Station Subsystems (“BSS”) 100 (only one is shown in FIG. 1A), each of which comprises a Base Station Controller (“BSC”) 104 serving a plurality of Base Transceiver Stations (“BTS”) such as, for example, BTSs 101, 102 and 103. BTSs 101, 102, 103, etc., are the access points where users of packet-based mobile devices become connected to the wireless network. In one embodiment, the packet traffic originating from user devices is transported over the air interface to BTS 103, and

from BTS 103 to BSC 104. Base station subsystems, such as BSS 100, may be a part of internal frame relay network 106 that may include Service GPRS Support Nodes (“SGSN”) such as SGSN 105 and 107. Each SGSN 105, 107, etc. may be in turn connected to internal packet network 108 through which SGSN 105, 107, etc. can route data packets to and from a plurality of gateway GPRS support nodes (GGSN) 222, 111, 110, etc. As illustrated, SGSN 107 and GGSNs 222, 111 and 110 are part of internal packet network 108. Gateway GPRS serving nodes 222, 111 and 110 may provide an interface to external Internet Protocol (“IP”) networks such as Public Land Mobile Network (“PLMN”) 115, corporate intranets 117, Fixed-End System (“FES”), the public Internet 113 or the like. As illustrated, subscriber corporate network 117 may be connected to GGSN 111 via firewall 112; and PLMN 115 may be connected to GGSN 111 via boarder gateway router 114. Remote Authentication Dial-In User Service (“RADIUS”) server 116 may be used for caller authentication when a user of a mobile cellular device calls corporate network 117, for example.

[0020] Generally, there can be four different cell sizes in a GSM network—macro, micro, pico and umbrella cells. The coverage area of each cell is different in different environments. Macro cells may be regarded as cells where the base station antenna is installed in a mast or a building above average roof top level. Micro cells are cells whose antenna height is under average roof top level; they are typically used in urban areas. Pico cells are small cells having a diameter is a few dozen meters; they are mainly used indoors. On the other hand, umbrella cells are used to cover shadowed regions of smaller cells and fill in gaps in coverage between those cells.

[0021] FIG. 1B illustrates the architecture of a typical GPRS network as segmented into four groups: users 115, radio access network 120, core network 124 and interconnect network 137. Users 115 comprise a plurality of end users. Radio access network 120 comprises a plurality of base station subsystems such as BSSs 123, which include BTSs 121 and BSCs 122. Core network 124 comprises a host of various network elements. As illustrated here, core network 124 may comprise Mobile Switching Center (“MSC”) 125, Service Control Point (“SCP”) 126, gateway MSC 127, SGSN 130, Home Location Register (“HLR”) 129, Authentication Center (“AuC”) 128, Domain Name Server (“DNS”) 131 and GGSN 132. Interconnect network 137 also comprises a host of various networks and other network elements. As illustrated in FIG. 1B, interconnect network 137 comprises Public Switched Telephone Network (“PSTN”) 133, Fixed-End System (“FES”) or Internet 134, firewall 135 and Corporate Network 136.

[0022] A mobile switching center 125 may be connected to a large number of base station controllers. At MSC 125, for example, depending on the type of traffic, the traffic may be separated such that voice may be sent to Public Switched Telephone Network (“PSTN”) 133 through Gateway MSC (“GSMSC”) 127, and/or data may be sent to SGSN 130, which then sends the data traffic to GGSN 132 for further forwarding.

[0023] When MSC 125 receives call traffic, for example, from BSC 122, it may send a query to a database hosted by SCP 126. The SCP 126 processes the request and issues a response to MSC 125 so that it may continue call processing as appropriate.

[0024] HLR 129 is a centralized database for users to register to the GPRS network. HLR 129 stores static information about the subscribers such as the International Mobile Subscriber Identity (“IMSI”), subscribed services, and a key for authenticating the subscriber. HLR 129 also stores dynamic subscriber information such as the current location of the mobile subscriber. Associated with HLR 129 may be AuC 128. AuC 128 is a database that contains the algorithms for authenticating subscribers and includes the associated keys for encryption to safeguard the user input for authentication.

[0025] In the following, depending on context, the term “mobile subscriber” may refer to either the end user or to the actual portable device used by an end user of the mobile cellular service. When a mobile subscriber turns on his or her mobile device, the mobile device goes through an attach process by which the mobile device attaches to an SGSN of the GPRS network. Referring now to FIG. 1B, when mobile subscriber 119 initiates the attach process by turning on the network capabilities of the mobile device, an attach request is sent by mobile subscriber 119 to SGSN 130. The SGSN 130 queries another SGSN, to which mobile subscriber 119 was attached before, for the identity of mobile subscriber 119. Upon receiving the identity of mobile subscriber 119 from the other SGSN, SGSN 130 requests more information from mobile subscriber 119. This information is used to authenticate mobile subscriber 119 to SGSN 130 by HLR 129. Once verified, SGSN 130 sends a location update to HLR 129 indicating the change of location to a new SGSN, in this case SGSN 130. HLR 129 notifies the old SGSN, to which mobile subscriber 119 was attached, to cancel the location process for mobile subscriber 119. HLR 129 then notifies SGSN 130 that the location update has been performed. At this time,

Appendix: Mikan

• EX1007, ¶¶25-35

SGSN 130 sends an Attach Accept message to mobile subscriber 119, which in turn sends an Attach Complete message to SGSN 130.

[0026] After attaching itself with the network, mobile subscriber 119 then goes through the authentication process. In the authentication process, SGSN 130 sends the authentication information to HLR 129, which sends information back to SGSN 130 based on the user profile that was part of the user's initial setup. SGSN 130 then sends a request for authentication and ciphering to mobile subscriber 119. Mobile subscriber 119 uses an algorithm to send the user identification (ID) and password to SGSN 130. SGSN 130 uses the same algorithm and compares the result. If a match occurs, SGSN 130 authenticates mobile subscriber 119.

[0027] Next, mobile subscriber 119 establishes a user session with the destination network, corporate network 136, by going through a Packet Data Protocol ("PDP") activation process. Briefly, in the process, mobile subscriber 119 requests access to the Access Point Name ("APN"), for example, UPS.com (e.g., which can be corporate network 279) and SGSN 130 receives the activation request from mobile subscriber 119. SGSN 130 then initiates a Domain Name Service ("DNS") query to learn which GGSN node has access to the UPS.com APN. The DNS query is sent to the DNS server within the core network 124, such as DNS 131, which is provisioned to map to one or more GGSN nodes in the core network 124. Based on the APN, the mapped GGSN 132 can access the requested corporate network 279. The SGSN 130 then sends to GGSN 132 a Create Packet Data Protocol ("PDP") Context Request message that contains necessary information. The GGSN 132 sends a Create PDP Context Response message to SGSN 130, which then sends an Activate PDP Context Accept message to mobile subscriber 119.

[0028] Once activated, data packets of the call made by mobile subscriber 119 can then go through radio access network 120, core network 124, and interconnect network 137, in particular fixed-end system or Internet 134 and firewall 135, to reach corporate network 136.

[0029] Thus, network elements that may implicate the functionality of the service delivery based on real-time performance requirement(s) in accordance with an embodiment may include but are not limited to Gateway GPRS Support Node tables, Fixed End System router tables, firewall systems, VPN tunnels and any number of other network elements as required by the particular digital network.

[0030] FIG. 1C shows another example block diagram view of a GSM/GPRS/IP multimedia network architecture 138 in which the apparatus and methods for transferring multimedia content between receiving devices of the below-discussed embodiments may be incorporated. As illustrated, architecture 138 of FIG. 1C includes GSM core network 154, GPRS network 157 and IP multimedia network 159. GSM core network 154 includes Mobile Station (MS) 140, at least one Base Transceiver Station (BTS) 141 and Base Station Controller (BSC) 142. MS 140 is physical equipment or Mobile Equipment (ME), such as a mobile phone or a laptop computer that is used by mobile subscribers, with a Subscriber identity Module (SIM). The SIM includes an International Mobile Subscriber Identity (IMSI), which is a unique identifier of a subscriber. BTS 141 is physical equipment, such as a radio tower, that enables a radio interface to communicate with the MS. Each BTS may serve more than one MS. BSC 142 manages radio resources, including the BTS.

The BSC may be connected to several BTSs. The BSC and BTS components, in combination, are generally referred to as a base station (BSS) or radio access network (RAN) 143.

[0031] GSM core network 154 also includes Mobile Switching Center (MSC) 144, Gateway Mobile Switching Center (GMSC) 145, Home Location Register (HLR) 146, Visitor Location Register (VLR) 147, Authentication Center (AuC) 149 and Equipment Identity Register (EIR) 148. MSC 144 performs a switching function for the network. The MSC also performs other functions, such as registration, authentication, location updating, handovers and call routing. GMSC 145 provides a gateway between the GSM network and other networks, such as an Integrated Services Digital Network (ISDN) or Public Switched Telephone Networks (PSTNs) 150. In other words, GMSC 145 provides interworking functionality with external networks.

[0032] HLR 146 is a database that contains administrative information regarding each subscriber registered in a corresponding GSM network. HLR 146 also contains the current location of each MS. VLR 147 is a database that contains selected administrative information from HLR 146. The VLR contains information necessary for call control and provision of subscribed services for each MS currently located in a geographical area controlled by the VLR. HLR 146 and VLR 147, together with MSC 144, provide the call routing and roaming capabilities of GSM. AuC 148 provides the parameters needed for authentication and encryption functions. Such parameters allow verification of a subscriber's identity. EIR 149 stores security-sensitive information about the mobile equipment.

[0033] Short Message Service Center (SMSC) 151 allows one-to-one Short Message Service (SMS) messages to be sent to/from MS 140. Push Proxy Gateway (PPG) 152 is used to "push" (i.e., send without a synchronous request) content to MS 102. PPG 152 acts as a proxy between wired and wireless networks to facilitate pushing of data to MS 140. Short Message Peer to Peer (SMPP) protocol router 153 is provided to convert SMS-based SMPP messages to cell broadcast messages. SMPP is a protocol for exchanging SMS messages between SMS peer entities such as short message service centers. It is often used to allow third parties, e.g., content suppliers such as news organizations, to submit bulk messages.

[0034] To gain access to GSM services, such as speech, data, and short message service (SMS), the MS first registers with the network to indicate its current location by performing a location update and IMSI attach procedure. MS 140 sends a location update including its current location information to the MSC/VLR, via BTS 141 and BSC 142. The location information is then sent to the MS's HLR. The HLR is updated with the location information received from the MSC/VLR. The location update also is performed when the MS moves to a new location area. Typically, the location update is periodically performed to update the database as location updating events occur.

[0035] GPRS network 157 is logically implemented on the GSM core network architecture by introducing two packet-switching network nodes, a serving GPRS support node (SGSN) 155 and a cell broadcast and a Gateway GPRS support node (GGSN) 156. SGSN 155 is at the same hierarchical level as MSC 144 in the GSM network. The SGSN controls the connection between the GPRS network and MS 140. The SGSN also keeps track of individual MS's locations and security functions and access controls.

Appendix: Mikan

• EX1007, ¶¶36-49

[0036] Cell Broadcast Center (CBC) **171** communicates cell broadcast messages that are typically delivered to multiple users in a specified area. Cell Broadcast is one-to-many geographically focused service. It enables messages to be communicated to multiple mobile phone customers who are located within a given part of its network coverage area at the time the message is broadcast.

[0037] GGSN **156** provides a gateway between the GPRS network and a public packet network (PDN) or other IP networks **158**. That is, the GGSN provides interworking functionality with external networks, and sets up a logical link to the MS through the SGSN. When packet-switched data leaves the GPRS network, it is transferred to external TCP-IP network **158**, such as an X.25 network or the Internet. In order to access GPRS services, the MS first attaches itself to the GPRS network by performing an attach procedure. The MS then activates a packet data protocol (PDP) context, thus activating a packet communication session between the MS, the SGSN, and the GGSN.

[0038] In a GSM/GPRS network, GPRS services and GSM services can be used in parallel. The MS can operate in one three classes: class A, class B, and class C. A class A MS can attach to the network for both GPRS services and GSM services simultaneously. A class A MS also supports simultaneous operation of GPRS services and GSM services. For example, class A mobiles can receive GSM voice/data/SMS calls and GPRS data calls at the same time.

[0039] A class B MS can attach to the network for both GPRS services and GSM services simultaneously. However, a class B MS does not support simultaneous operation of the GPRS services and GSM services. That is, a class B MS can only use one of the two services at a given time.

[0040] A class C MS can attach for only one of the GPRS services and GSM services at a time. Simultaneous attachment and operation of GPRS services and GSM services is not possible with a class C MS.

[0041] GPRS network **157** can be designed to operate in three network operation modes (NOM1, NOM2 and NOM3). A network operation mode of a GPRS network is indicated by a parameter in system information messages transmitted within a cell. The system information messages dictates a MS where to listen for paging messages and how signal towards the network. The network operation mode represents the capabilities of the GPRS network. In a NOM1 network, a MS can receive pages from a circuit switched domain (voice call) when engaged in a data call. The MS can suspend the data call or take both simultaneously, depending on the ability of the MS. In a NOM2 network, a MS may not received pages from a circuit switched domain when engaged in a data call, since the MS is receiving data and is not listening to a paging channel. In a NOM3 network, a MS can monitor pages for a circuit switched network while received data and vice versa.

[0042] IP multimedia network **159** was introduced with 3GPP Release 5, and includes IP multimedia subsystem (IMS) **160** to provide rich multimedia services to end users. A representative set of the network entities within IMS **160** are a call/session control function (CSCF), media gateway control function (MGCF) **162**, media gateway (MGW) **165**, and a master subscriber database, referred to as a home subscriber server (HSS) **168**. HSS **168** may be common to GSM network **154**, GPRS network **157** as well as IP multimedia network **159**.

[0043] IP multimedia system **160** is built around the call/session control function, of which there are three types: inter-

rogating CSCF (I-CSCF) **164**, proxy CSCF (P-CSCF) **161** and serving CSCF (S-CSCF) **163**. P-CSCF **161** is the MS's first point of contact with IMS **160**. P-CSCF **161** forwards session initiation protocol (SIP) messages received from the MS to an SIP server in a home network (and vice versa) of the MS. P-CSCF **161** may also modify an outgoing request according to a set of rules defined by the network operator (for example, address analysis and potential modification).

[0044] I-CSCF **164** forms an entrance to a home network and hides the inner topology of the home network from other networks and provides flexibility for selecting an S-CSCF. I-CSCF **164** may contact subscriber location function (SLF) **169** to determine which HSS **168** to use for the particular subscriber, if multiple HSSs **168** are present. S-CSCF **163** performs the session control services for MS **140**. This includes routing originating sessions to external networks and routing terminating sessions to visited networks. S-CSCF **163** also decides whether application server (AS) **167** is required to receive information on an incoming SIP session request to ensure appropriate service handling. This decision is based on information received from HSS **168** (or other sources, such as application server **167**). AS **167** also communicates to location server **170** (e.g., a Gateway Mobile Location Center (GMLC)) that provides a position (e.g., latitude/longitude coordinates) of MS **140**.

[0045] HSS **168** contains a subscriber profile and keeps track of which core network node is currently handling the subscriber. It also supports subscriber authentication and authorization functions (AAA). In networks with more than one HSS **168**, a subscriber location function provides information on HSS **168** that contains the profile of a given subscriber.

[0046] The MGCF **162** provides interworking functionality between SIP session control signaling from IMS **160** and ISUP/BICC call control signaling from the external GSN networks (not shown). It also controls media gateway (MGW) **165** that provides user-plane interworking functionality (e.g., converting between AMR- and PCM-coded voice). MGW **165** also communicates with other IP multimedia networks **166**.

[0047] Push to Talk over Cellular (PoC) capable mobile phones register with the wireless network when the phones are in a predefined area (e.g., job site, etc.). When the mobile phones leave the area, they register with the network in their new location as being outside the predefined area. This registration, however, may not indicate the actual physical location of the mobile phones outside the pre-defined area.

[0048] While the various embodiments have been described in connection with the preferred embodiments of the various figures, it is to be understood that other similar embodiments may be used or modifications and additions may be made to the described embodiment for performing the same function of the various embodiments without deviating therefrom. Therefore, the embodiments should not be limited to any single embodiment, but rather should be construed in breadth and scope in accordance with the appended claims.

Example Embodiments

[0049] FIG. 2 illustrates a block diagram of an example wireless vehicle security system **200**. Wireless vehicle security system **200** may secure access and operation of vehicle **201**. Vehicle **201** may be a car, truck, boat, motorcycle or other mechanism for transporting people or things. Vehicle **201** may support various vehicle operation features such as

Appendix: Mikan

• EX1007, ¶¶49-59

unlocking a door, opening a trunk, opening a glove box, engaging an ignition, directing the vehicle from a one geographic location to a another geographic location, and accelerating the vehicle, for example. Any aspect of the control, use, or functionality of vehicle 201 may be considered a vehicle operation feature.

[0050] The system may include one or more keys 205A-C control unit 202 and local database 203, for example. Keys 205A-C may be electronic keys, traditional metal keys, or a combination of both. In one embodiment, keys 205A-C may be embedded in a wireless device such as a cellular telephone or Personal Digital Assistant (PDA), for example.

[0051] Control unit 202 may be any combination of hardware and/or software that is in operative communication with vehicle 201 and keys 205A-C. For example, the control unit may be an onboard computer. In one embodiment, key 205A-C may communicate directly with control unit 202. For example, key 205A-C and control unit 202 may communicate directly via a radio frequency transmission. In another embodiment, vehicle 201 may communicate to control unit 202 when key 205A-C is inserted into a key slot of vehicle 201. Control unit 202 may be in operative communication with local database 203. In one embodiment, control unit 202 and local database 203 may be resident within vehicle 201. Local database 203 may be any software system or device suitable for storing and retrieving data records. In one embodiment, local database 203 may be a Structured Query Language (SQL)-compliant database, for example. In another embodiment, local database 203 may be implemented as a relational database, hierarchical database, or the like. Local database 203 may include any number of records, where each record represents a vehicle operation policy. The vehicle operation policy may relate to vehicle operation features and keys 205A-C.

[0052] Control unit 202 may be in communication with wireless network 207. Wireless network 207 may be any system suitable for wirelessly sending and receiving data. Wireless network 207 may be a GSM network, a GPRS network, an EDGE network, Wideband Integrated Dispatch Enhanced Network (WiDEN), Wideband Code Division Multiple Access (W-CDMA) network, Wireless Local Area Network (WLAN), or a 802.11a/b/g/n network, for example. In one embodiment, wireless network 207 may host master database 208 and application 209. Wireless network 207 may interconnect with other networks, such as corporate extranets, private networks, the Internet, or the public switched telephone network (PSTN), for example.

[0053] Control unit 202 may interface with vehicle 201. Control unit 202 may control vehicle functions and may sense operation of vehicle 201. For example, control unit 202 may signal to lock and unlock the vehicle doors. For example, control unit 202 may sense vehicle speed and the status of the ignition. Control unit 202 may interface to a Global Positioning System (GPS) unit to sense the position of vehicle 201. In one embodiment, any aspect of the vehicle operation that may be controlled by an electrical signal may be controlled by control unit 202, and aspect of the vehicle operation that may be sensed and converted to an electronic signal may be sensed by control unit 202.

[0054] Master database 208 may be any software system or device suitable for storing and retrieving data records. For example, master database 208 may be a Structured Query Language (SQL)-compliant database. Master database 208 may include any number of records representing a vehicle

operation policy, and master database 208 may include any number of vehicle operation policies relating to more than one vehicle. Master database 208 may communicate with local database 203. In one embodiment, local database 203 may mirror some of the data in master database 208 such that records within each database are consistent. For example, local database 203 may regularly poll master database 208 to maintain consistent data. In one embodiment, each of local database 203 and master database 208 may communicate an update to the other after a record change.

[0055] Master application 209 may be any interface, software, or device suitable for managing communication to and from master database 208. For example, master application 209 may be software resident on a server platform, may be integrated into master database 208, may stand alone, etc. In one embodiment, master application 209 may include a hypertext transfer protocol (HTTP) server.

[0056] Key 205B and computer 210 may be in communication with wireless network 207. In one embodiment, key 205B and computer 210 may communicate with application 209, with master database 208, or, via wireless network 207, with control unit 202 and/or local database 203. Both computer 210 and key 205B may provide a user interface with wireless vehicle security system 200 to enable a user to manage and monitor system 200. For example, where key 205B is part of a mobile telephone, the user of the mobile telephone may use the mobile telephone to send updates to master database 208 via master application 209.

[0057] FIGS. 3A-B illustrate a block diagram of an example structure for master database 300 and local database 303, respectively. It will be appreciated that FIGS. 3A-B depict just one possible embodiment; master database 300 and local database 303 may be structured in accordance with other database schema. An embodiment of the master database 208 is depicted in FIG. 3 as master database 300. Similarly, an embodiment of the local database 203 is depicted in FIG. 3 as local database 303.

[0058] Master database 300 may include any number of vehicle records 302. Each record may be associated with Vehicle ID 301. Vehicle ID 301 may be an identifier that uniquely defines a vehicle record 302. For example, vehicle ID 301 may be a vehicle identification number (VIN), serial number, an alphanumeric string, or the like. Vehicle ID 301 may relate to a physical vehicle that may be within wireless vehicle security system 200. In one embodiment, vehicle record 302 may include key set 310, policy set 313, and mapping 312. Key set 310 may include data representing a collection of keys 205A-C. Policy set 313 may include a collection of vehicle operation policies 311. Mapping 312 may include a collection of one or more relationships linking individual keys from key set 310 with individual vehicle operation policies from policy set 313. In one embodiment, there may be a one-to-one relationship between vehicle ID 301 and vehicle record 302. Mapping 312 may include a one-to-many relationship between an individual key of key set 310 and vehicle operation policies 311. It will be appreciated that other schema may be used to practice master database 300.

[0059] Local database 303 may include vehicle ID 301, key set 310, one or more vehicle operation policies, and mapping 312. Vehicle ID 301 in local database 303 may map directly to that in master database 300. In one embodiment, vehicle ID 301 in local database 303 may be a singular record that associates particular vehicle ID 301 with physical vehicle

Appendix: Mikan

• EX1007, ¶¶59-66

201. Key set **310** may include a secure ID check **315** associated with a key **205A-C** within the set. The secure ID check may be a serial number, electronic serial number (ESN), or other identifier of a key **205A-C**. In one embodiment, secure ID check **315** may be a digital signature associated with a key **205A-C**. For example, the digital signature may be the product of a public key encryption system. In another embodiment, the secure ID check may be a component of a challenge and response system such as the challenge-handshake authentication protocol (CHAP), for example.

[0060] Local database **303** may include vehicle operation policy **311**. Vehicle operation policy **311** may include vehicle operation feature ID **316** and a related access control rule **317**. Vehicle operation feature ID **316** may be, for example, a data field identifying one vehicle operation feature. Vehicle **201** may support various vehicle operation features such as unlocking a door, opening a trunk, opening a glove box, engaging an ignition, directing the vehicle from a one geographic location to another geographic location and accelerating the vehicle, for example. Any aspect of the control, use, or functionality of vehicle **201** may be considered a vehicle operation feature. It will be appreciated that one or more vehicle subsystems that control one or more of such vehicle operation features may be in operative communication with, for example, wireless vehicle security system **200** (not shown in FIGS. 3A-B). A vehicle operation feature may be associated with vehicle operation feature ID **316**. Access control rule **317** may include a criterion relating to associated vehicle operation feature ID **316**. For example, access control rule **317** may operate to enable, partially enable, or disable the related vehicle operation feature. Access control rule **317** may include advanced criteria relating to the manner and condi-

tions under which the vehicle may be operated. For example, access control rule **317** may establish a maximum acceleration for the vehicle, a maximum distance traveled for the vehicle, a range of time within which the vehicle may be operated, a geographic range within which the vehicle may be operated and the like. For illustration, access control rule **317** may indicate that the vehicle's ignition may not be engaged between 12 a.m. and 5 a.m., or it may indicate that the vehicle may not be operated above 65 miles per hour. For example, access control rule **317** may relate to the number of people in the car. Weight sensors within the seat may be used to determine the number of people in the car, for example. For example, access control rule **317** may relate to the distance between vehicle **201** and key **205A-C**. For illustration, wireless network **207** may send the position of a key embedded within a cellular phone, and using an GPS, control unit **202** may determine the distance between the cellular phone and vehicle **201**.

[0061] Mapping **312** may link vehicle operation policy **311** and keys **205A-C**. To illustrate this point, one embodiment may include two keys, first with greater access than the second. The first key, in this example illustration, may be related via mapping **312** to access control rule **317** that enables all vehicle operation features. The second key, in this illustration, may be a "valet key" with limited functionality. For example, the second key may be related to three access control rules **317**: a first rule that disables access to the trunk and glove box, a second rule that limits the maximum speed to 35 miles per hour, and a third rule that limits the total allowed distance traveled to one mile.

[0062] FIG. 4 illustrates a block diagram of an example wireless device **400** equipped for use as a key **205A-C** within

wireless vehicle security system **200**. Wireless device **400** may include processor **401**, user interface module **402**, wireless communications module **403**, memory **404**, power supply **405**, and security module **406**, for example. In addition, the functions performed by any or all of the components and modules illustrated in FIG. 4 may be performed by any number of physical components. Thus, it is possible that in some embodiments the functionality of more than one component and/or module illustrated in FIG. 4 may be performed by any number or types of hardware and/or software.

[0063] User interface module **402** may include a display for illustrating textual and graphical information to a user and a collection of keys, buttons, or voice controls for receiving input from the user. For example, the buttons or keys may relate to fixed, pre-defined functions (hard keys), or they may have dynamically defined or context controlled functions (soft keys). User interface module **402** may be enabled receive user requests from the user, such as an update request and an access request, for example. The update request may include access control rule **317** from the user. User interface module **402** may be enabled to receive access control rule **317** from the user, and it may be enabled to display access control rule **317** to the user. In an embodiment, the access request access may relate to a vehicle operation feature. In addition, and in an embodiment, the user interface module **402** may include a hard key related to unlocking a vehicle door.

[0064] Wireless communications module **403** may be a subsystem suitable to provide communications between wireless device **400** and wireless network **207**. Wireless communications module **403** may include a modulator, a transmitter, a receiver and an antenna, for example. In one embodiment, wireless communications module **403** may enable communication over a GSM or GPRS network for example. Wireless communications module **403** may communicate the update request via wireless network **207**. Wireless communications module **403** may support telephony and data services.

[0065] Memory **404** may be a subsystem suitable for storing and retrieving data. Memory **404** may be random access memory (RAM) or read only memory (ROM), or the like. In one embodiment, memory **404** may provide non-volatile storage of secure identifier **407** of wireless device **400**. In another embodiment, memory **404** may provide volatile storage of secure identifier **407** retrieved, for example, via wireless communications module **403** or via user interface module **402** with a user/password prompt, biometric or other user authentication. In one embodiment, secure identifier **407** may authenticate wireless device **400** as a key **205A-B** as discussed above in connection with FIG. 2. Secure identifier **407** may be a serial number, electronic serial number (ESN), or other identifier of wireless device **400**. In one embodiment, secure identifier **407** may be a digital signature associated with wireless device **400**. The digital signature may, for example, be the product of a public key encryption system. In another embodiment, secure identifier **407** may be a component of a challenge and response system, such as the challenge-handshake authentication protocol (CHAP).

[0066] Processor **401** may be a microprocessor packaged in one or more integrated circuits with support circuitry. Processor **401** may be structured as a reduced instruction set computer (RISC), an advanced RISC machine (ARM) and/or as a gate-level logic circuit, for example. Processor **401** may include an array processor and/or a digital signal processor (DSP), for example. Processor **401** may be in communication with user interface module **402**, wireless communications

Appendix: Mikan

• EX1007, ¶¶66-76

module **403**, memory **404**, power supply **405**, and security module **400**. In one embodiment, processor **401** may operate responsive to user input, such as a user request, for example. Thus, and responsive to a user request, processor **401** may retrieve secure identifier **407** from memory **404**, and may perform one or more operations on secure identifier **407**. Processor **401** may also operate responsive to instructions from security application **409**.

[0067] Security module **406** may include security application **409** and vehicle access module **408**. Vehicle access module **408** may receive secure identifier **407** from processor **401**, and may communicate with vehicle **201** to send secure identifier **407** to vehicle **201**. Vehicle access module **408** may communicate via any wireless protocol suitable for the transmission of data. For example, access module **408** may communicate via Bluetooth protocol, WiFi, RF-ID, cellular, and the like. Bluetooth protocol may be defined by the Institute of Electrical and Electronics Engineers (IEEE) specification 802.15.1. Security application **409** may include software relating to the management of secure identifiers **407**. In one embodiment, security application **409** may provide a user with customizable features that may be presented by user interface module **402**. Security application **409** may perform cryptographic functions related to the secure identifier, an authentication process, or cryptographic key generation, for example.

[0068] FIG. 5 depicts a flow diagram of example vehicle security process **500**. Example process **500** is merely one embodiment and therefore describes features and functionality by way of example and illustration. Reference will also be made to FIGS. 2, 3A-B, and 4 where appropriate.

[0069] At **502** local database **203** may synchronize with master database **208**. Control unit **202** or local database **203** may initiate the synchronization to pull updated data from master database **208**. Alternatively, master application **209** or master database **208** may initiate the synchronization to push updated data to local database **203**. The synchronization may be a partial or complete refresh of the data. For example, the updated data may represent only the changes in the master database made since the last synchronization in a partial refresh. In a complete refresh, the updated data may represent the entire contents of master database **208** that are relevant to vehicle **201**. To balance design concerns of data integrity and bandwidth usage, periodic complete refreshes may be supplemented by intermediate partial refreshes.

[0070] At **504**, a user attempt to access or operate vehicle **201** with a key **205A-C** is detected, which may initiate the authentication. The detection of key **205A-C** may include receiving secure identifier **407**. Secure identifier **407** may be received, for example, at control unit **202**. Where key **205A-C** is an electronic key, such as a key embedded in wireless device **400** for example, key **205A-C** may transmit secure identifier **407**. Where key **205A-C** is a metal key for insertion into a physical lock, the physical lock may authenticate the key—by the patterns of grooves and teeth, for example—and signal a secure identifier within vehicle **201** to control unit **202**.

[0071] Control unit **202** may authenticate key **205A-C** via secure ID check **315**. For example, where the secure ID is a serial number the secure ID check may be a copy of the serial number. For security, the control unit and key **205A-C** may determine the secure ID from a common hopping code or

rolling code, where the secure ID changes after each use. The authentication may include verifying a digital signature and timestamp, for example.

[0072] At **506** vehicle operation policy **311** may be retrieved by, for example, querying local database **203**. In one embodiment, the query may be based on authenticated key **205A-C**. The records queried reflect the vehicle operation policy **311** that may be in effect with relation to the key **205A-C** being used. More than one vehicle operation policy **311** record may be returned as a result of the query. In one embodiment, control unit **202** may perform the query and may temporarily store or cache the records for the duration of the users operation of the vehicle **201**.

[0073] Vehicle **201** may receive a user request, such as an access request for example. The access request may include unlocking a door, opening a trunk, opening a glove box, engaging an ignition, directing the vehicle from a first geographic location to a second geographic location, and accelerating the vehicle, for example. To illustrate, the user may approach the vehicle **201**, signal the secure ID **407** and an access request to unlock a vehicle door. To illustrate, the user may be operating the vehicle and press the accelerator of the vehicle, signaling an access request to accelerate the vehicle.

[0074] At **508**, control unit **202** may process the access request and compare the access request with retrieved vehicle operation policy **311**. Where the access request is consistent with retrieved vehicle operation policy **311**, control unit **202** may permit the operation of the vehicle at **510**. Where the access request is inconsistent with the with the retrieved vehicle operation policy **311**, then at **516** control unit **202** may block and/or limit the operation of the vehicle.

[0075] At **512**, the control unit **202** may notify a user or a system by signaling an indication of whether an access request conformed with the retrieved vehicle operation policy **311**. In one embodiment, the notification need not occur, particularly if the access did conform with the retrieved vehicle operation policy **311**. Notification may occur whether or not the access request was permitted or blocked. The nature and extent of the notification may depend on the significance of the access request or related vehicle operation policy **311**. The notification may be an electronic message, an audible alarm and/or a visual alarm, for example. The electronic message may be any digital communication such as e-mail, a database query or update, a text message via Short Message Service (SMS), and/or appending a text string to a log file, for example. The electronic message may be sent via wireless network **207** to wireless device **400**, computer **210**, or other device reachable by network **207**. The audible alarm may be within vehicle **201**, at wireless device **400**. The visual alarm may be within vehicle **201**, such as a dash board indicator light for example, at a wireless device **400**, or displayed on the screen of a computer. The notification may be directed or redirected to the police or other security officers.

[0076] At **514**, the control unit **202** may monitor the status of a particular vehicle operation feature and confirming its conformance with vehicle operation policy **311** associated with the key **205A-C** that is currently in use. Once control unit **202** has permitted a vehicle operation feature, monitoring ensures that the feature stays in conformance with policy **311**. For example, where vehicle operation policy **311** includes setting a maximum speed for the operation of vehicle **201**, monitoring continuously checks the speed of vehicle **201** and compares it to the maximum imposed by vehicle operation

Appendix: Mikan

• EX1007, ¶¶76-85

policy 311. If vehicle 201's speed exceeds that defined by policy 311, notification and/or enforcement action may be taken.

[0077] At 516, the control unit 202 may block and/or limit operation of vehicle 201 may occur when an access request does not conform with vehicle operation policy 311 or may occur when a vehicle operation feature being monitored no longer conforms with vehicle operation policy 311. In such a situation, and in one embodiment, control unit 202 may disallow the operation. For example, where key 205A-C signals an access request to vehicle 201 to unlock a door and the access request is not allowed by vehicle operation policy 311 retrieved for that specific key 205A-C, blocking operation may include maintaining the locked condition of the doors, or if the doors were previously unlocked, blocking may include locking the doors.

[0078] In addition to limiting or blocking, control unit 202 may, at 520, initiate an enforcement action when an access request does not conform with vehicle operation policy 311 or when a vehicle operation feature being monitored no longer conforms with vehicle operation policy 311. An enforcement action may include sending an electronic message, sounding an audible alarm, illuminating a visual alarm, gradually lowering a maximum speed of the vehicle, disabling an audio system of the vehicle, and the like. In one embodiment, where the enforcement action is directed to bringing the vehicle to a stop, control unit 202 may direct vehicle 201 to gradually lower the maximum speed while indicating to the driver that vehicle 201 soon will be inoperable. In another embodiment, where vehicle 201 may be in operation late in the evening outside of a defined time range, the enforcement action may disable the audio system and/or other comfort features of the vehicle.

[0079] FIG. 6 depicts a flow diagram of an example network security process 600. Example process 600 is merely an embodiment and describes features and functionality by way of example and illustration. In one embodiment, network security process 600 may be implemented by a combination of wireless network 207, master database 208 and master application 209. Network security process 600 may, for example, handle messages and logic related to the overall management of wireless vehicle security system 200.

[0080] In one embodiment, at 602 master application 209 may receive an update request. The update request may have originated at a computing device such as a wireless telephone, a computer 210, a wireless handheld device, a server, control unit 202, key 205B, or any other device capable of formulating and sending a message via wireless network 207. The update request may include, but is not limited to, a vehicle identifier, a secure key identifier, and an access control rule, for example. The update request may be formatted in any acceptable computer readable format such as an HTTP message, an SMS message, a protocol related to a downloadable web application (Java and/or ActiveX, for example), a SQL formatted query, and the like.

[0081] At 606, master database 208 may be queried. This may include a request for information from master database 208 via a database query. In one embodiment, the query may include a vehicle identifier to filter only records relating to a particular vehicle. The query may be generated via master application 209, computer 210, or other device that may be in operative communication with wireless network 207. The query may retrieve and return query results, which may include information such as, for example, a vehicle record,

key set 310, vehicle operation policy 311, mapping 312 and the like. In one embodiment, the query results may support a display application at computer 210 for providing a user with a current view of the keys 205A-C and policies related to a vehicle. In one embodiment, the query may return results to an application that may process the results. Master application 209 processing an update request may query 606 master database 208 to locate the records related to the update request. Master application 209 may extract the vehicle identifier from the update request and populate a field of the query with the vehicle identifier.

[0082] Master application 209 may consider the query results in processing an update request. For example, master application 209 may compare the secure identifier of the update request with the key set retrieved via the query to authenticate the update request. Master application 209 may compare the access control rule of the update request with that contained in vehicle operation policy 311 retrieved via the query. On this basis, master application 209 may reject the update request, defer the update request, or continue to process the update request.

[0083] At 610, master database 208 may be updated with data to supersede or supplement one or more existing records. Master application 209 may update master database 208 responsive to a properly authenticated update request. The updating may include editing or overwriting one or more records, deleting one or more records, or adding one or more records, for example. Where master application 209 receives an access control rule in the update request, updating may include making the records in master database 208 reflect the received access control rule.

[0084] At 612, local database 203 and master database 208 may synchronize. This may include sending or receiving data that, when processed by either local database 203 and/or master database 208, make the records in each consistent with each other. In one embodiment, consistency may be achieved by making the data of local database 203 mirror that of corresponding vehicle record 302. Master database 208 may push data to local database 203, or local database 203 may pull data from master database 208 or some combination thereof. In one embodiment, master database 208 may push data to synchronize after every update request. Master database 208 may maintain an accounting of the changes made to vehicle record 302 since the last synchronization and include that data when synchronizing with local database 203. In one embodiment, local database 203 may request a complete refresh, where the entire record is synchronized. This approach may be desirable when some or all data of local database 203 has become corrupted or lost.

[0085] In one embodiment, the synchronization data may be communicated via wireless network 207. Vehicle 201 may not always be in contact with wireless network 207, such as when vehicle 201 is parked underground and out of range of wireless network 207, for example. Where master database 208 pushes the synchronization to local database 203, master application 209 may establish communication with control unit 202 before initiating the synchronization. When communication cannot be established, master application 209 or master database 208 may queue the request for a later time.

Appendix: Mikan

• EX1007, ¶¶76-85

policy 311. If vehicle 201's speed exceeds that defined by policy 311, notification and/or enforcement action may be taken.

[0077] At 516, the control unit 202 may block and/or limit operation of vehicle 201 may occur when an access request does not conform with vehicle operation policy 311 or may occur when a vehicle operation feature being monitored no longer conforms with vehicle operation policy 311. In such a situation, and in one embodiment, control unit 202 may disallow the operation. For example, where key 205A-C signals an access request to vehicle 201 to unlock a door and the access request is not allowed by vehicle operation policy 311 retrieved for that specific key 205A-C, blocking operation may include maintaining the locked condition of the doors, or if the doors were previously unlocked, blocking may include locking the doors.

[0078] In addition to limiting or blocking, control unit 202 may, at 520, initiate an enforcement action when an access request does not conform with vehicle operation policy 311 or when a vehicle operation feature being monitored no longer conforms with vehicle operation policy 311. An enforcement action may include sending an electronic message, sounding an audible alarm, illuminating a visual alarm, gradually lowering a maximum speed of the vehicle, disabling an audio system of the vehicle, and the like. In one embodiment, where the enforcement action is directed to bringing the vehicle to a stop, control unit 202 may direct vehicle 201 to gradually lower the maximum speed while indicating to the driver that vehicle 201 soon will be inoperable. In another embodiment, where vehicle 201 may be in operation late in the evening outside of a defined time range, the enforcement action may disable the audio system and/or other comfort features of the vehicle.

[0079] FIG. 6 depicts a flow diagram of an example network security process 600. Example process 600 is merely an embodiment and describes features and functionality by way of example and illustration. In one embodiment, network security process 600 may be implemented by a combination of wireless network 207, master database 208 and master application 209. Network security process 600 may, for example, handle messages and logic related to the overall management of wireless vehicle security system 200.

[0080] In one embodiment, at 602 master application 209 may receive an update request. The update request may have originated at a computing device such as a wireless telephone, a computer 210, a wireless handheld device, a server, control unit 202, key 205B, or any other device capable of formulating and sending a message via wireless network 207. The update request may include, but is not limited to, a vehicle identifier, a secure key identifier, and an access control rule, for example. The update request may be formatted in any acceptable computer readable format such as an HTTP message, an SMS message, a protocol related to a downloadable web application (Java and/or ActiveX, for example), a SQL formatted query, and the like.

[0081] At 606, master database 208 may be queried. This may include a request for information from master database 208 via a database query. In one embodiment, the query may include a vehicle identifier to filter only records relating to a particular vehicle. The query may be generated via master application 209, computer 210, or other device that may be in operative communication with wireless network 207. The query may retrieve and return query results, which may include information such as, for example, a vehicle record,

key set 310, vehicle operation policy 311, mapping 312 and the like. In one embodiment, the query results may support a display application at computer 210 for providing a user with a current view of the keys 205A-C and policies related to a vehicle. In one embodiment, the query may return results to an application that may process the results. Master application 209 processing an update request may query 606 master database 208 to locate the records related to the update request. Master application 209 may extract the vehicle identifier from the update request and populate a field of the query with the vehicle identifier.

[0082] Master application 209 may consider the query results in processing an update request. For example, master application 209 may compare the secure identifier of the update request with the key set retrieved via the query to authenticate the update request. Master application 209 may compare the access control rule of the update request with that contained in vehicle operation policy 311 retrieved via the query. On this basis, master application 209 may reject the update request, defer the update request, or continue to process the update request.

[0083] At 610, master database 208 may be updated with data to supersede or supplement one or more existing records. Master application 209 may update master database 208 responsive to a properly authenticated update request. The updating may include editing or overwriting one or more records, deleting one or more records, or adding one or more records, for example. Where master application 209 receives an access control rule in the update request, updating may include making the records in master database 208 reflect the received access control rule.

[0084] At 612, local database 203 and master database 208 may synchronize. This may include sending or receiving data that, when processed by either local database 203 and/or master database 208, make the records in each consistent with each other. In one embodiment, consistency may be achieved by making the data of local database 203 mirror that of corresponding vehicle record 302. Master database 208 may push data to local database 203, or local database 203 may pull data from master database 208 or some combination thereof. In one embodiment, master database 208 may push data to synchronize after every update request. Master database 208 may maintain an accounting of the changes made to vehicle record 302 since the last synchronization and include that data when synchronizing with local database 203. In one embodiment, local database 203 may request a complete refresh, where the entire record is synchronized. This approach may be desirable when some or all data of local database 203 has become corrupted or lost.

[0085] In one embodiment, the synchronization data may be communicated via wireless network 207. Vehicle 201 may not always be in contact with wireless network 207, such as when vehicle 201 is parked underground and out of range of wireless network 207, for example. Where master database 208 pushes the synchronization to local database 203, master application 209 may establish communication with control unit 202 before initiating the synchronization. When communication cannot be established, master application 209 or master database 208 may queue the request for a later time.

Institution Decision

Appendix: Institution Decision

- ID, 1-2

Trials@uspto.gov
571-272-7822

Paper 14
Entered: January 27, 2025

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

KIA CORP. and TOYOTA MOTOR CORP.,
Petitioners,

v.

EMERGING AUTOMOTIVE LLC,
Patent Owner.

IPR2024-01167
Patent 11,738,659 B2

Before GEORGIANNA W. BRADEN, BARBARA A. PARVIS, and
FRANCES L. IPPOLITO, *Administrative Patent Judges*.

BRADEN, *Administrative Patent Judge*.

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

Kia Corp. and Toyota Motor Corp. (collectively “Petitioner”) filed a Petition (Paper 3, “Pet.”) requesting *inter partes* review of claims 1–21 of U.S. Patent No. 11,738,659 B2 (Ex. 1001, “the ’659 patent”). Emerging Automotive LLC (“Patent Owner”) filed a Preliminary Response (Paper 7, “Prelim. Resp.”).

With our authorization, Petitioner filed a Reply to Patent Owner’s Preliminary Response (Paper 8, “Prelim. Reply”) and Patent Owner filed a Sur-reply to Petitioner’s Reply (Paper 9, “Prelim. Sur-reply”) to address whether we should deny institution under 35 U.S.C. §§ 314(a), 325(d), and *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020) (precedential) (“*Fintiv*”). For reasons provided below, we decide not to invoke this discretion to deny institution.

Under 35 U.S.C. § 314(a) and 37 C.F.R. § 42.4(a), we have authority to determine whether to institute review. Based on the current record and for the reasons explained below, Petitioner has shown that there is a reasonable likelihood that it would prevail with respect to at least one of the challenged claims. Therefore, pursuant to § 314, we institute an *inter partes* review of claims 1–21 in the ’659 patent on all challenges included in the Petition.

A. *Real Parties in Interest*

Petitioner identifies Toyota Motor Corp., Toyota Motor North America, Inc., and Toyota Motor Sales, U.S.A., Inc., Kia Corp., and Kia America Inc., as the real parties-in-interest. Pet. 71. Patent Owner identifies Emerging Automotive LLC as the real party-in-interest. Paper 5 (Patent Owner’s Mandatory Disclosures), 2.

Appendix: Institution Decision

- ID, 32-33

C. Claims 1 and 3—21 Allegedly Rendered Obvious by Kleve and Hatton

Petitioner contends that Kleve in combination with Hatton teaches every limitation of claims 1 and 3–21. Pet. 9–36. Patent Owner disagrees. Prelim. Resp. 9–26. Patent Owner specifically challenges whether Petitioner has shown that the combined teachings of Kleve with Hatton teach (a) an “alleged” “memory” has “program instructions for instructing/controlling unlocking and starting of the vehicle,” or (b) a “coded data” that “includes privilege settings,” as required by the challenged independent claims. *Id.* at 14, 21. Patent Owner further challenges whether Petitioner has demonstrated a reason to combine Kleve with Hatton. *Id.* at 23

1. Analysis of Independent Claim 1

a) Limitation [1a]

Claim 1 recites the steps:

[1a] memory associated with the on-board computer of the vehicle having program instructions for instructing unlocking and starting of the vehicle;

Ex. 1001, 52:16–18.

For this limitation, Petitioner contends that “Kleve discloses memory associated with the VCS processor.” Pet. 16 (citing Ex. 1005, Fig. 1). According to Petitioner, Kleve’s memory includes random access memory (RAM) and a hard disk drive (HDD) or flash memory. *Id.* (citing Ex. 1005 ¶ 22). Petitioner asserts that this memory is used to store data. *Id.* (citing Ex. 1005 ¶ 31). According to Petitioner, “Kleve’s processor executes instructions stored at a ‘storage medium [*i.e.*, memory]’ that ‘enable a vehicle rental transaction’ by ‘activat[ing] [*i.e.*, starting] the vehicle during a

prescribed rental period’ and, ‘enabl[ing] a keyless driveaway.’” *Id.* (citing Ex. 1005 ¶¶ 9, 71).

Patent Owner disagrees with Petitioner’s reading of Kleve and contends there is no teaching of a memory having program instructions for instructing unlocking and starting of the vehicle. Prelim. Resp. 22; Ex. 2001 ¶ 64. According to Patent Owner, Petitioners rely on a particular memory in Kleve (*i.e.*, the HDD and RAM), as well as Kleve’s processor that enables a rental transaction by activating the vehicle to enable keyless drive away. Prelim. Resp. 22 (citing Pet. 16). Patent Owner argues that Petitioner does “not identify any alleged instructions as being in the previously-identified memory.” *Id.*

Patent Owner relies on Dr. Malek’s testimony to support its position. Specifically, Dr. Malek testifies that a person of ordinary skill in the art would have understood “that merely ‘activating’ a vehicle is not ‘instructions for unlocking and starting the vehicle’ or ‘instructions for controlling unlocking and starting of the vehicle.’” Ex. 2001 ¶ 64. Dr. Malek further testifies that “POSITA would understand ‘activating’ a vehicle to mean making the vehicle operative [(*e.g.*,) such as setting a flag to indicate that a particular rental agreement is in effect].” *Id.* Instead, according to Patent Owner, Kleve’s vehicle is active “during a prescribed rental period” but it is “not ‘started’ during the entire rental period or continuously being started.” Prelim. Resp. 22 (citing Ex. 1005, code (57)). Patent Owner asserts that a person of ordinary skill in the art would not have understood instructions “to ‘activate’ a vehicle to be instructions for starting and unlocking of the vehicle.” *Id.* Patent Owner further argues that Petitioner fails to identify any instruction in the identified alleged memory that unlocks and drives Kleve’s vehicle. *Id.*

Appendix: Institution Decision

- ID, 34-35

IPR2024-01167
Patent 11,738,659 B2

At this stage of the proceeding, based on the teachings of Kleve, we are persuaded that a person of ordinary skill in the art at the critical time would have understood that Kleve’s memory (including random access memory (RAM) and a hard disk drive (HDD) or flash memory) would have included program instructions for instructing unlocking and starting of a vehicle. Additionally, we credit the testimony of Dr. Almeroth, whose testimony is consistent with Kleve’s disclosure. *See* Ex. 1004 ¶¶ 120–123.

Kleve states that one of its embodiments includes a computer readable storage medium for storing instructions that, when executed by a processor is configured to enable a vehicle rental transaction. *See* Ex. 1005 ¶ 9. Then Kleve states that after e-key comparison and authorization, “the vehicle may enable driveaway access to that Temporary User for the scheduled time period of the rental agreement” and for “the duration of the rental term, the Temporary User may again input the same identifying credentials to unlock and drive.” *Id.* ¶ 71. Unlike Patent Owner supposition, we do not understand this to mean that the vehicle would be “started” with the engine running continuously during the entirety of the rental period. Rather, we understand this to mean that the vehicle itself has program instructions stored in memory so that the Temporary User can (1) “start” the engine running at any time during the rental period and (2) unlock and drive the vehicle any time during the rental period. *See* Ex. 1004 ¶¶ 122–123.

Thus, after review of the arguments and evidence, we find that Petitioner has provided adequate explanation and supporting evidence that Kleve in view of Hatton teaches or suggests the challenged claim limitation.

b) *Limitation [1e]*

Claim 1 recites the step:

[1d] wherein the wireless communications circuitry of the vehicle is configured to receive coded data from the mobile device when using the eKey, the coded data enables functions of said eKey for said unlocking and use of the vehicle, the coded data is associated to the eKey for use by the mobile device,

[1e] and the coded data includes privilege settings associated with the eKey for limiting types of use of the vehicle when using the eKey with the vehicle;

Ex. 1001, 52:27–36.

For this limitation, Petitioner first contends Kleve discloses or renders this limitation obvious because Kleve teaches “a virtual key is wirelessly communicated to the vehicle using encrypted data,” with the encrypted data being the recited “coded data.” Pet. 19 (citing Ex. 1004 ¶¶ 131–137; Ex. 1005 ¶ 63). Petitioner next contends that “the virtual key, represented as encrypted data, includes privilege settings that limit types of use of the vehicle.” *Id.* at 20 (citing Ex. 1004 ¶¶ 138–140). Petitioner provides the example of where “the vehicle’s ‘Owner’ ‘may set user restrictions . . . based on . . . parameters including, but not limited to, speed, global position coordinates, or load weight restrictions.’” *Id.* at 20–21 (citing Ex. 1005 ¶ 40). According to Petitioner, such restrictions can “be set in accordance with the types of use intended by the owner and temporary user.” *Id.* (citing Ex. 1005 ¶¶ 76, 83). Therefore, Petitioner concludes that a person of ordinary skill of art at the critical time would have found it obvious to include the use restrictions within the encrypted data associated with the virtual key in order to prevent tampering by a temporary user.

Appendix: Institution Decision

- ID, 36-37

Patent Owner disagrees with Petitioner’s reading of Kleve and contends there is no teaching of “the coded data includes privilege settings associated with the eKey for limiting types of use of the vehicle.” Prelim. Resp. 14. According to Patent Owner, “Petitioners did not show—and could not have shown—that Kleve’s ‘restrictions’ are included in Kleve’s ‘virtual key.’” *Id.* at 15 (citing Pet. 20–21; Ex. 1003 ¶¶ 55–62). Patent Owner argues that for Petitioner relies on Kleve’s “virtual key” as the “coded data” and on Kleve’s “restrictions” as the alleged “privilege settings,” but none the paragraphs in Kleve discussing the “restrictions” disclose the use of a “virtual key” and none of the paragraphs discussing the “virtual key” include any “restrictions.” *Id.* (citing Pet. 19–21 (relying on Ex. 1005 ¶¶ 40, 76, 83); Ex. 2001 ¶ 56). According to Patent Owner, Kleve’s “virtual key” is provided before rental time, and “Kleve is clear any ‘restrictions’ are not applied provided until the rental period has begun.” *Id.* (citing Ex. 1005 ¶¶ 75 (after “the system detects a rental time start . . . [t]he system may begin to download. . . restrictions.”), 40 (Owner may set restrictions for “vehicle being rented.”), Fig. 7).

Patent Owner then asserts that Petitioner’s reliance on Hatton to suggest that modifying Kleve’s virtual key via encryption is misplaced because Petition does not rely on Hatton to suggest modifying the virtual key to include any “privilege settings.” *Id.* at 16 (citing Pet. 12–14, 20–30). Nor would it have been obvious, according to Patent Owner, to include any privilege settings in the virtual key. *Id.* at 17. Patent Owner relies on the testimony of Dr. Malek to support its position. *Id.* Dr. Malek testifies that “[a] POSITA would understand that Kleve teaches to ‘set user restrictions’ after the virtual key is distributed and after the step in which the virtual key is ‘sent to vehicle, website or nomadic device.’” Ex. 1005, Fig. 2, ¶¶ 39–

40). Therefore, Patent Owner concludes, that no “restrictions”—set after the virtual key was made and distributed—could be included in the key. Prelim. Resp. 17–20 (citing Ex. 1005 ¶ 57).

At this stage of the proceeding, we first are persuaded Petitioner demonstrates that Kleve’s “virtual key” is coded data because it is wirelessly communicated from a server to a vehicle in an encrypted format. *See* Ex. 1005 ¶ 63.

Second, we are persuaded that Petitioner adequately shows Kleve teaches, or at least suggests, an e-key that includes “privilege settings that limit types of use of the vehicle” because we are persuaded that the distribution of Kleve’s virtual e-key includes a rental period restriction. For purposes of institution, the rental period restriction appears to be a “type of use of the vehicle” and delineates the start/stoppage of when the vehicle can be used. Specifically, we are persuaded by the Petition’s reliance on Kleve’s express disclosure that “terms and conditions for the rental period” are agreed to before the virtual key is generated. *See* Pet. 15 (citing Ex. 1004 ¶ 138). We preliminarily agree with Petitioner that Kleve describes an e-key that is only operable during a rental period because Kleve discloses, “The owner may review the requested rental based on what the Temporary User is looking to use the vehicle for (e.g., without limitation, for towing, hauling, or errands), when the requested use will be taking place, and where.” *Ex. 1004 ¶ 138; see Ex. 1005 ¶ 83.*

We note Patent Owner’s citations to Kleve’s Figure 7 that indicates “geofences or performance limits” are added after the rental start time. *See* Prelim. Resp. 16. For purposes of institution, however, based on the disclosure of Kleve we are persuaded the rental period would be included as

Appendix: Institution Decision

- ID, 38-39

⁸ a restriction when the virtual key is created at step 206 of Figure 2 prior to the distribution of the virtual key at 210. *See* Ex. 1005 ¶¶ 38–39.

At this stage of the proceeding, we credit the testimony of Dr. Almeroth, who opines that Kleve discloses that certain restrictions are sent with the request to generate a virtual key. Ex. 1004 ¶¶ 119–123. Specifically, Dr. Almeroth testifies that Kleve discloses that the virtual key “enable[s] the keyless drive system for the appropriate Temporary User during a given rental period.” *Id.* ¶ 119. According to Dr. Almeroth, this “indicates that rental agreement restrictions were sent with the request so that the virtual key could be associated with said restrictions.” *Id.* ¶ 152; *see also* Ex. 1005 ¶ 68 (“Once the rental period has expired the virtual key may be reset and cleared from the VCS.”)). Dr. Almeroth further testifies that the virtual key in Kleve is always generated after the rental agreement. Ex. 1004 ¶¶ 152, 156 ([Once] “the Temporary User selects the vehicle, pays the appropriate amount and signs a consent agreement,” then “the system may generate a virtual key to distribute to the Temporary User and VCS.”)).

Thus, after review of the arguments and evidence, we find that Petitioner has provided adequate explanation and supporting evidence that Kleve alone or in combination with Hatton teaches the challenged claim limitation.

c) Limitations [1b] – [1d] and [1f]

Claim 1 recites additional steps at limitations [1b] through [1d] and limitation [1f]. Ex. 1001, 52:18–33.

Petitioner provides arguments and evidence regarding each of these claim limitations. Pet. 17–20, 21–22. Patent Owner has not provided separate arguments regarding Kleve alone or in combination with Sekiyama in regards to these challenged claims. *See generally* Prelim. Resp.

Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

We have reviewed the Petition’s analysis of the other claimed subject matter not discussed in the previous sections and determine that the analysis is sufficient at this stage. Based on our review of the arguments and evidence submitted for limitations [1b] through [1d] and limitation [1f] and the reasons presented previously, we are persuaded for purposes of institution only that Petitioner has sufficiently shown sufficiently that Kleve alone or in combination with Hatton teaches or suggests these limitations as recited in independent claim 1.

d) Rationale to Combine

Petitioner contends a person of ordinary skill in the art at the critical time would have been motivated to combine Kleve’s system with Hatton’s teaching of an e-key system for vehicles. Pet. 12 (citing Ex. 1004 ¶¶ 109–115). According to Petitioner, “[t]here were well-known benefits of using encrypted data for wireless communications” including being able to ensure that only authorized receivers can view messages that are sent over radio waves. *Id.* (citing Ex. 1004 ¶ 110). Petitioner argues that “[f]or electronic key systems, encrypted communications would be particularly effective to prevent unauthorized access to the vehicle” while “[a]ssociating encrypted data with specific electronic keys would further facilitate an owner’s monitoring and control of vehicle use by individual users.” *Id.* at 12–13. According to Petitioner, a person of ordinary skill in the art would have “been motivated to bind the virtual key to the receiving user’s mobile device (*e.g.*, by associating the virtual key with an identifier unique to the mobile device) to prevent unauthorized distribution to third parties.” *Id.* at 13 (citing Ex. 1004 ¶ 111).

Appendix: Institution Decision

- ID, 40-41

Petitioner explains that a person of ordinary skill in the art would have been “particularly motivated to look to Hatton’s teachings to improve Kleve because both Kleve and Hatton are Ford references directed to similar electronic key systems for use in a vehicle.” *Id.* (citing Ex. 1004 ¶ 113). Petitioner cites as an example the fact that “both Kleve and Hatton describe an identical architecture for a computing system within a vehicle (the ‘VCS’ in both references) and a ‘vehicle rental’ business using that system.” *Id.* at 13–14 (citing Ex. 1005 ¶¶ 21–36, Fig. 1; Ex. 1008, 2:54–5:53, Fig. 1).

Petitioner further argues that a person of ordinary skill in the art would have had a reasonable expectation of success in applying Hatton to Kleve because “Kleve already uses its wireless communications circuitry for encrypted communications (*e.g.*, with a server)” and “[c]onfiguring the wireless communications circuitry to additionally receive encrypted messages associated with a virtual key and including use restriction information directly from a mobile device would have been a straightforward and routine application of well-known techniques in wireless communications and encryption.” *Id.* at 14 (citing Ex. 1004 ¶ 114; Ex. 1005 ¶ 63). Petition then concludes that “it would have been obvious to a POSITA to use one of several standard, well-known encryption techniques (such as public/private key encryption) to implement the encryption schemes described by Kleve and Hatton, and a POSITA would have been capable of implementing such encryption techniques within those systems.” *Id.*

Patent Owner disagrees with Petitioner because it contends that Hatton is directed to encryption for authentication and not encryption for confidentiality. Prelim. Resp. 23 (citing Ex. 2001 ¶¶ 67–68). According to Patent Owner, these are distinct conception so a person of ordinary skill in the art at the critical time would not have been motivated to modify Kleve in

view of Hatton in order to add encryption for authentication purposes. *Id.* at 23–24 (citing Ex. 2001 ¶ 68).

Patent Owner then contends that Petitioner fails to explain how Kleve could be modified as proposed because “Hatton does not disclose generating any encrypted data at a mobile device.” *Id.* at 24–25 (citing Ex. 2001 ¶ 69). Patent Owner explains that because Hatton’s encrypted data is assigned to a vehicle at the manufacturing process, it would not have been obvious in view of Hatton to generate encrypted data to include restrictions for use in a rental vehicle because the encrypted data would have already been generated. *Id.* at 25 (citing Ex. 1008, 8:24–36, 14:7–18). Patent Owner argues that “[u]nder Petitioners’ theory, encrypted data would need to be generated each time ‘restrictions’ were created or modified, but Hatton does not have a mechanism for doing this.” *Id.*

After review of the arguments and evidence, we are persuaded at this stage of the proceeding by Petitioner’s position. Specifically, we are persuaded that (1) both Kleve and Hatton are directed to use of electronic key systems for vehicles (*see* Ex. 1005 ¶¶ 7–9, 39, 63; Ex. 1008, 1:48–52, 1:61–2:2, 5:25–34) and (2) encrypted communications would have been understood to effective in preventing unauthorized access to the vehicle, something that is taught explicitly by Hatton (*see* Ex. 1008, 9:50–63). Given these disclosures by Kleve and Hatton, we are persuaded by Petitioner that a person of ordinary skill in the art would have had a reasonable expectation of success in combining these teachings and arriving at the challenged claims. Accordingly, for purposes of institution, we find that a person of ordinary skill in the art at the critical time would have reason to combine the teachings of Kleve with that of Hatton.

Appendix: Institution Decision

- ID, 42-43

2. *Analysis of Independent Claims 11, 18 and Dependent Claims 3–10, 12–17, 19–21*

Petitioner provides arguments and evidence regarding independent claims 11 and 18, as well as dependent claims 3–10, 12–17, and 19–21 in view of Kleve in combination with Hatton. Pet. 22–36. Patent Owner has not provided separate arguments regarding Kleve in combination with Hatton in regards to these challenged claims. *See generally* Prelim. Resp. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

We have reviewed the Petition’s analysis of the other claimed subject matter not discussed in the previous sections and determine that the analysis is sufficient at this stage. Based on our review of the arguments and evidence submitted for independent claims 11 and 18, as well as dependent claims 3–10, 12–17, and 19–21 and the reasons presented previously, we are persuaded for purposes of institution only that Petitioner has shown sufficiently that Kleve in combination with Hatton teaches or suggests the limitations as recited in independent claims 11 and 18, as well as dependent claims 3–10, 12–17, and 19–21.

3. *Summary regarding Challenged Based on Kleve in combination with Hatton*

Based on the current record, Petitioner has established a reasonable likelihood that it will prevail in demonstrating that claims 1 and 3–21 would have been obvious over Kleve in combination with Hatton.

D. *Claim 2 Allegedly Rendered Obvious by Kleve and Hatton in combination with Sekiyama*

Claim 2 recites

The sub-system of the vehicle of claim 1, wherein said privileges function as restrictions that enable access to specific vehicle

areas that include one or more of vehicle door operation, or trunk operation.

Ex. 1001, 52:40–43.

Petitioner provides arguments and evidence regarding dependent claim 2 in view of Kleve in combination with Hatton and with Sekiyama. Pet. 36–39. Patent Owner has not provided separate arguments regarding Kleve in combination with Hatton and with Sekiyama in regards to this challenged claim, except to state that “Sekiyama does not cure any of the deficiencies of the proposed Kleve / Hatton combination.” Prelim. Resp. 26 Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

We have reviewed the Petition’s analysis and determine that the analysis is sufficient at this stage. Based on our review of the arguments and evidence submitted for dependent claim 2, we are persuaded for purposes of institution only that Petitioner has shown sufficiently that Kleve in combination with Hatton and with Sekiyama teaches or suggests the limitations as recited in dependent claim 2.

E. *Claims 1, 3, 5–7, 9, 11–16, and 18–20 Allegedly Anticipated by or Rendered Obvious in View of Mikan*

Petitioner contends that the disclosure and teachings of Mikan either anticipate or would have rendered the subject matter of claims 1–3, 5, and 8–10 obvious. Pet. 39–49. Patent Owner disagrees. Prelim. Resp. 26–36. Patent Owner specifically challenges whether Petitioner has shown that Mikan discloses or teaches “coded date” that includes privilege settings and is “from a mobile device” as recited in limitations [1d] and [1e] of independent claims 1, 11, and 11. Accordingly, for purposes of institution, we will only provide analysis for limitations [1d] and [1e].

POR

- POR, 1-2

I. Introduction

The Board's Institution Decision preliminarily credited Dr. Almeroth's testimony that the primary references, *Kleve* (grounds 1-2) and *Mikan* (grounds 3-6), disclose circuitry of a vehicle that is configured to "*receive coded data from a mobile device ... the coded data includes privilege settings*." As demonstrated here, however, each ground of the Petition fails because Dr. Almeroth's testimony for this claim requirement is incorrect and contrary to the express disclosures of the references.

For the "coded data" requirement, Petitioners rely on *Kleve*'s "virtual key," which is merely a credential, such as a user's face, fingerprint, or other identifying information. Petitioners contend that when this virtual key is encrypted as a message or matrix barcode, it discloses the claimed "coded data." However, *Kleve*'s "virtual key," in whatever form and whether or not encrypted, is independent of any alleged "privilege settings." For the claimed "privilege settings," Petitioners rely on *Kleve*'s restrictions, e.g., a rental period agreed to in the rental agreement. But *Kleve*'s "virtual key credential" does not include *any* restrictions at all. Indeed, *Kleve*'s system does not, and cannot, incorporate restrictions, including any rental agreement terms, in the creation or distribution of its virtual key. Thus, *Kleve* does

not teach or suggest any alleged "privilege settings" in any alleged coded data, let alone any "coded data" received from a mobile device.

In *Kleve*'s system, a rental agreement is negotiated and agreed to by both the Vehicle Owner and the renter. However, *Kleve*'s functionality "to enforce compliance with rental agreement terms" does not trust *a renter* to put alleged "privilege settings" on a virtual key. Unsurprisingly, *Kleve* makes clear that its solution is intentionally designed to put its "controlling usage" mechanism *solely* in the hands of the individual who is most interested in protecting the vehicle—the *Vehicle Owner*. EX1005, ¶¶ 51, 40, Fig. 7A. Were *Kleve*'s system modified to control vehicle usage according to a vehicle renter's demands, as Dr. Almeroth proposes, *Kleve*'s express purpose—giving the Vehicle Owner total control of their own vehicle—would be vitiated altogether.

Similarly, the Petition's reliance on *Mikan* fails. Petitioners rely on *Mikan*'s "secure ID" as the alleged "coded data" and *Mikan*'s "vehicle operation policies" as the alleged "privilege settings." But *Mikan* makes clear that the "secure ID"—sent to the vehicle from the wireless device—is used merely for authentication. The wireless device's "secure ID 407" includes no vehicle operation policies or any other privilege settings whatsoever. Instead, the vehicle operation policies are stored in and "retrieved" from the vehicle's local database—never from the alleged

- POR, 3-4

mobile device when using the eKey. When the user in *Mikan* seeks to use a wireless device as an electronic key to access the vehicle, the vehicle already has any vehicle operation policy locally stored on the vehicle and therefore never receives, nor has any need to “receive coded data *from a mobile device ... the coded data includes privilege settings*.” Indeed, *Mikan*’s express disclosure of a mapping function links the vehicle-stored vehicle operation policies to the vehicle-stored key set; the whole purpose of which is that the vehicle does not receive operation policies from the mobile device. Were any privilege settings included in coded data received by the vehicle from the wireless device, it would be unnecessary for the vehicle to perform this mapping operation between these two locally stored sets of records.

Unlike Patent Owner’s Preliminary Response, which did not delve into the details of either *Kleve* or *Mikan*, Patent Owner does so here, demonstrating below that each of the premises on which Dr. Almeroth and Petitioners base their anticipation and obviousness conclusions are directly refuted by the references themselves. All grounds fail.

II. The ’659 patent

The ’659 patent describes providing vehicle access to individuals, including an owner or “guest driver,” e.g., a friend, service person, or valet. EX1001, 10:28-39. This access can be provided by an electronic key, or eKey, which allows use of

the vehicle. *Id.*, 10:40-42. An eKey may be used by an owner or others, such as a guest. *Id.*, 40-51. Usage of an eKey, such as usage by a guest, may be associated with privilege settings, e.g., speed limits, geographic restrictions, amount of time, etc. *Id.* As an example, “the vehicle can be loaned to a child of driving age ... and the child can be provided with restricted use of the vehicle.” *Id.*, 14:51-53. The ’659 patent describes creating profiles for users that have privileges set by an administrator. *Id.*, 17:5-13. For example, accounts for a driver may be created with “defined roles,” which can “include a set of privileges,” such as speed limit or geographic privileges. *Id.*, 38:52-62. In this way, logins of user profiles can be controlled. For example, “[a]dministrators can decide which settings are locked for specific logins or roles, which are open for the login user to toggle and which settings are to be enforced.” *Id.*, 17:18-26. Thus “use of the vehicle can be restricted to predefined rules.” *Id.*, 22:24-28.

Each independent claim (1, 11, 18) of the ’659 patent requires “communications circuitry of a vehicle”; “the communications circuitry includes wireless communication circuitry” that is “configured to receive coded data from [a] mobile device”; and “the coded data includes privilege settings.” EX1001, claims 1, 11, 18.

Appendix: POR

- POR, 5-6

- 87
- III. *Kleve* (EX1005) discloses distinct operations for (1) forming a rental agreement, (2) setting up and distributing a virtual key, and finally, (3) setting user restrictions—available to only a Vehicle Owner and only at the beginning of the rental term, after the virtual key has been sent to the vehicle.

Kleve discloses a system to “check” a “credential” and use that “credential” as the “authorization” or “virtual key” for use of a “personal vehicle rental.” EX1005, face page, ¶ 36. *Kleve* discloses that parties negotiate and form a rental contract, allowing the parties to exchange identifying information that is used as a credential virtual key. *Id.*, ¶ 38. *Kleve* specifies an operation in which the Vehicle Owner—and only the Vehicle Owner—“may have the options [sic] to set rental restrictions” to “control[] usage to enforce compliance with the rental agreement terms.” EX1005, ¶¶ 51, 40. However, by using “restriction limits initially set by the Owner at the beginning of the rental term,” *Kleve*’s solution for controlling vehicle usage is not available until after any generation and distribution of the virtual key. *Id.*, ¶ 43, Fig. 2; EX2021, ¶ 45.

Unlike the rental agreement terms, agreed to by both parties, *Kleve*’s system teaches that only a Vehicle Owner can “set user restrictions” that will be monitored, e.g. load weight restrictions, rental end time, “no-go zones” or any other restrictions regardless of the terms of the rental agreement. EX1005, ¶¶ 40, 43, 51, 75; EX2021, ¶¶ 47-48. *Kleve*’s system allows only these Owner-set “user restrictions,” set at step

214, to be monitored and controlled by the vehicle’s “VCS” (vehicle computing system), e.g., premature termination of the rental period if the usage of the vehicle is “extreme” or updating a new rental period end time restriction if additional time is paid for and authorized by the Owner. EX1005, ¶¶ 41, 43, 51; EX2021, ¶¶ 49-52.

- A. *Kleve*’s “terms and conditions for the rental period” reflect the agreed-to terms of a rental contract and are independent of any “virtual key.”

Kleve provides a system whereby the Vehicle Owner and Temporary User can negotiate and execute a rental agreement. EX1005, ¶¶ 38, 84, 89, Fig. 2, steps 206, 208. As shown further below in Section III.C., this rental agreement procedure is distinct from, and not coextensive with, *Kleve*’s operation to “distribute virtual key” and thereafter “set user restrictions.” *Id.*, ¶¶ 38, 40, 51, Fig. 2; EX2021, ¶¶ 47-52.

Appendix: POR

- POR, 7-8



Fig-2

EX1005, Fig. 2 (annot.).

To use *Kleve's* personal vehicle rental system, a Vehicle Owner inputs personal information into a website, including details about the vehicle for rent. *Id.*, ¶¶ 81, 38. A Temporary User also uses this website to input “personal information” (*id.*, ¶ 86), including a “unique Temporary User identification,” such as “photos of credit cards, photo of forms of ID, facial recognition, voice print recognition, matrix barcode [], code word or phrase for speech recognition, temporary mobile web login

IDs and password, or other types of unique Temporary User identification” (i.e., “credentials”) (*id.*, ¶ 37).

The parties can use the website to negotiate “terms and conditions based on the specific use and needs the Temporary User may use the vehicle for,” and ultimately accept terms and sign the agreement. *Id.*, ¶¶ 46, 84-85, 89-90, 38, Figs. 8-9. As part of this rental agreement, the parties can agree to specific conditions for the vehicle rental, e.g., “cargo load weight restrictions, tow load restrictions, or [mileage restrictions].” *Id.*, ¶¶ 89, 84. The website may thereafter generate a rental agreement and collect payment and signatures. *Id.*, ¶¶ 47, 90, 85, 38, Fig. 3A.

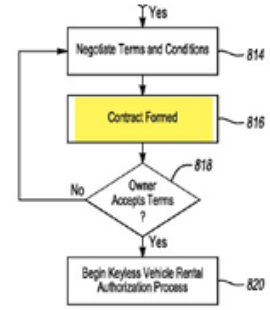


Fig-8

Id., Fig. 8 (annot.). Here, *Kleve* teaches nothing more than two parties forming an agreement. *Kleve* does not teach that the parties’ agreed-upon conditions are ever included in the set up or eventual distribution of a virtual key or provided to the

Appendix: POR

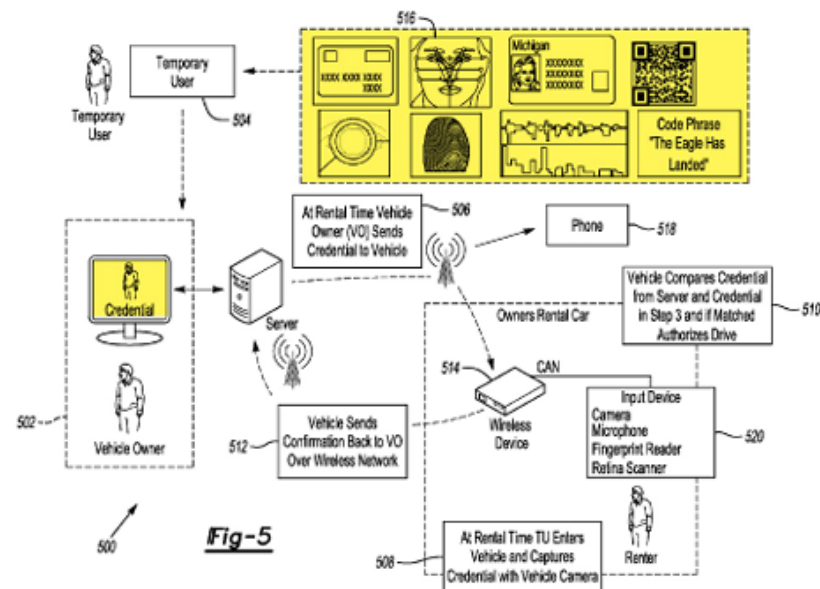
- POR, 9-10

vehicle. EX2021, ¶¶ 47-50. Instead, as detailed in Section III.C, below, *Kleve*'s system provides an Owner the option to separately set any restrictions the Owner chooses—whether or not identified the rental agreement—at the beginning of the rental term, *which is independent of, and after the distribution of, the virtual key*. *Id.*; EX1005, ¶¶ 40-41, 43, 51, 75. In *Kleve*, the Owner can enforce compliance with specific restrictions, whether or not such restrictions were also included as rental agreement terms. *Id.*, ¶¶ 40-41, 43, 51, 75.

B. Neither the “set up” of a virtual key nor the distribution of a virtual key includes the rental agreement terms or any other restrictions.

Kleve describes that a Vehicle Owner may “set up a virtual key” to allow a Temporary User to use their virtual key credential to access the Owner's vehicle. *Id.*, ¶¶ 62, 67.

To set up a virtual key, the *Temporary User* sends “information for credential verification” to “the Vehicle Owner allowing for this information to be entered into the server and used as a virtual key[.]” *Id.*, ¶ 63, Fig. 5, 516 (emphasis added). “At step 502, the Vehicle Owner may enter in vehicle authorization credentials based on information received by the Temporary User to set up a virtual key.” *Id.*, ¶ 62, Fig. 5 (emphasis added).



Id., Fig. 5 (annot.). This “credential” is the information collected from the Temporary User, such as “fingerprint recognition,” “photos of credit cards, photo of forms of ID, facial recognition, voice print recognition, matrix barcode [], code word or code phrase for speech recognition,” or “other types of unique Temporary User identification.” *Id.*, ¶¶ 63-64.

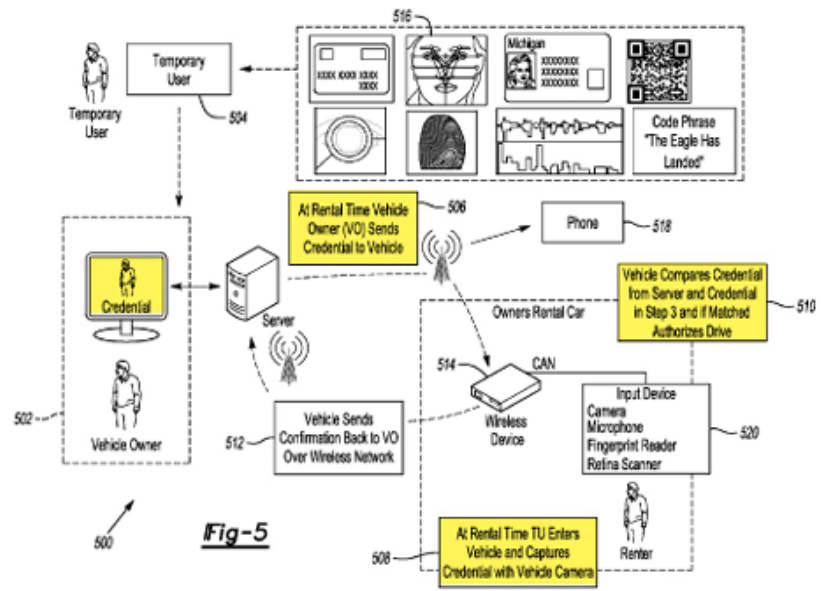
The Temporary User identification or “credential” is ultimately distributed to be “used as a virtual key.” *Id.*, ¶ 63; *see also id.*, ¶ 44 (matrix barcode as the virtual key); *id.*, ¶ 67 (“the virtual key credential”). *Kleve*'s “virtual key credential”

Appendix: POR

- POR, 11-12

does not include any restriction or other privilege about any agreed rental period, nor does this “credential” include *any* of the terms or conditions agreed to and accepted as the parties’ rental agreement. *Id.*, ¶¶ 62-64, 44, 67; EX2021, ¶ 46.

Instead, “to set up a virtual key,” the Vehicle Owner enters only the vehicle authorization credential or “unique Temporary User identification” (EX1005, Fig. 5: 504, 516), which was received from the Temporary User (*id.*, ¶ 62, Fig. 5). Moreover, to authorize access, the vehicle compares this credential, sent by the Owner, with the credential entered by the Temporary User. *Id.*, Fig. 5, steps 506, 508, 510. The Vehicle Owner sends this same “credential” received from the Temporary User to the vehicle. The Temporary User provides this same credential to the vehicle, e.g., captured via camera, microphone, etc. *Id.*, Fig. 5. And, as illustrated in Figure 5 below, the vehicle compares *the credential* from the Owner and *the credential* from the Temporary User to authorize the Temporary User. *Id.*, Fig. 5, step 510.



Id., Fig. 5 (annot.).

Kleve does not disclose or suggest that the Owner enter a “rental time period” to “set up a virtual key,” nor does *Kleve* suggest that this “rental time” is included in the transmission of the virtual key credential to the vehicle. *Id.*; see also *id.*, ¶¶ 62, 66; EX2021, ¶ 62. In fact, were the agreed upon “rental period” included in the virtual key credential as an alleged “privilege setting,” it would not be necessary for the Vehicle Owner to send the credential to the vehicle “at rental time.” EX1005, Fig. 5, ¶ 66. *Kleve* instructs: “[a]t rental time Vehicle Owner (VO) sends credential

- POR, 13

to vehicle.” *Id.*, Fig. 5 (emphasis added); *see also id.*, ¶ 66 (“[w]hen the scheduled rental period of time begins[,] the Vehicle Owner may send the credentials to the vehicle with the use of a server.”) (emphasis added).

Further, *Kleve* discloses “at rental time, TU [the Temporary User] enters [the] vehicle and captures [this] credential.” *Id.*, Fig. 5 (emphasis added); *id.*, ¶ 67. As *Kleve* illustrates, the vehicle compares the “credential,” not any “rental time” information, and based solely on this “matched” credential the vehicle “authorizes [the] drive.” *Id.*, Fig. 5, step 510. Because the vehicle’s match of the two entries of credentials “authorizes [the] drive,” the Temporary User cannot use the virtual key to drive away a Vehicle Owner’s vehicle until after, “at rental time[,] vehicle Owner (VO) sends [the] credential to [the] vehicle.” *Id.*, Fig. 5, ¶ 66.

C. To monitor and control vehicle usage, a Vehicle Owner may independently “set user restrictions”—an operation distinct from the rental agreement and “set up” and distribution of a virtual key credential.

Rather than include the parties’ rental agreement terms in the set up or distribution of a virtual key, *Kleve* provides a separate, optional operation to allow only the Owner to “set user restrictions” at step 214. *Id.*, ¶ 51, Fig. 2; *id.*, ¶ 40; EX2021, ¶¶ 47-50. *Kleve* makes clear that restrictions are set at the beginning of the rental term, *separately* from the virtual key. *Id.*; EX1005, ¶¶ 43, 40, 75, Fig. 2.

Dr. Almeroth's Deposition Testimony (EX2022)

Appendix: Almeroth Deposition Testimony

- EX2022, Page 26

Kevin C. Almeroth, Ph.D.

April 1, 2025

1 recall. I don't recall that it matters to the claim
2 whether it's automatically generated or not, so it's
3 probably not a question I've looked at.

4 Sitting here right now, it seems like it
5 could be automatically generated or it could not,
6 depending on kind of how the system would be
7 implemented.

8 Q. So with respect to "always generated," are
9 you referring there to, again, that it's a
10 prerequisite as we just discussed, that the rental
11 agreement having been formed by the parties is a
12 prerequisite to the virtual key being generated?

13 MR. LU: Objection. Form.

14 THE WITNESS: I think what I'm saying is
15 basically what's described in the declaration, which
16 is basically a person of skill in the art reading
17 Kleve would understand that there is an embodiment
18 where the virtual key is generated after the rental
19 agreement, and always generated after the rental
20 agreement at least in that embodiment.

21 BY MS. ENTZMINGER:

22 Q. Well, it doesn't say "in that embodiment."
23 It says "always generated after the rental
24 agreement."

25 MR. LU: Objection. Form.

Appendix: Almeroth Deposition Testimony

- EX2022, Page 27

Kevin C. Almeroth, Ph.D.

April 1, 2025

1 BY MS. ENTZMINGER:

2 Q. So are you now clarifying that it's only
3 when embodiment where it's generated always after
4 the rental agreement?

5 A. I wouldn't characterize it as a
6 clarification. I don't think Kleve is limited in
7 all of its embodiments, where that a person of skill
8 in the art reading Kleve would understand that in
9 every embodiment, the only way the eKey could be
10 generated is after the rental agreement.

11 Certainly I think it would make sense to a
12 person of skill in the art that that's typically
13 what would happen.

14 Q. Well, this says "always." So always
15 refers to all of the embodiments in Kleve, correct?

16 A. I don't see where it says that.

17 Q. Your sentence says, "Kleve discloses that
18 the virtual key is always generated after the rental
19 agreement."

20 A. I think you read that sentence correctly.

21 Q. Okay. So "always generated after the
22 rental agreement" encompasses all embodiments of
23 Kleve, correct?

24 MR. LU: Objection. Form. Asked and
25 answered.

Appendix: Almeroth Deposition Testimony

- EX2022, Page 28

Kevin C. Almeroth, Ph.D.

April 1, 2025

1 THE WITNESS: No. Not necessarily.
2 BY MS. ENTZMINGER:
3 Q. So you use typically and always. So
4 always does not refer to all of the embodiments of
5 Kleve, is that fair?
6 A. I think a person of skill in the art could
7 read Kleve and understand that there are probably
8 multiple ways in which the flow of actions among the
9 parties could occur. And I think thinking about a
10 real world scenario, in most cases you have an
11 agreement before you would generate an eKey, but
12 maybe, maybe not. I don't -- I don't know that the
13 real world is necessarily cut and dry.
14 So reading -- a person reading Kleve would
15 understand it's describing embodiments where it's
16 always the case. That might be a pretty common
17 scenario, but I don't know that it would necessarily
18 be a hard and fast rule in every embodiment or in
19 the understanding a person of skill in the art would
20 have.
21 Q. Well, this sentence in paragraph 120 of
22 your declaration is describing Kleve's disclosure.
23 It's not describing the, quote, "real world." This
24 says, "Kleve discloses that the virtual key is
25 always generated after the rental agreement."