

**Toyota Motor Corp. and Kia Corp.
v.**

Emerging Automotive LLC

IPR2024-01167

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

Emerging Automotive LLC's Demonstratives

United States Patent and Trademark Office

'659 Patent, Claim 1[b]

1[b]

What is claimed is:

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.

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;

Ex. 1001 ('659 Patent), Claim 1

'659 Patent, Claim 1[c]

What is claimed is:

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.

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;

Ex. 1001 ('659 Patent), Claim 1

1[c]

'659 Patent, Claim 11[b]

11[b]

11. A system of a vehicle, the vehicle having an on-board computer for processing and communicating with the system for use of an electronic key (eKey), the system comprising:

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

communications circuitry of the vehicle interfaced with the on-board computer of the vehicle, 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 of the vehicle;

wherein the wireless communications circuitry of the vehicle is configured to receive coded data from the mobile device, the coded data is unique for said eKey, and the coded data includes privilege settings set for limiting types of use of the vehicle when using the vehicle via the eKey;

wherein the eKey is associated with a user account, the user account is accessible via a user interface of an application executed by the mobile device, the eKey when active enables said unlocking of the vehicle and said starting of the vehicle.

communications circuitry of the vehicle interfaced with the on-board computer of the vehicle, 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 of the vehicle;

Ex. 1001 ('659 Patent), Claim 11

'659 Patent, Claim 11[c]

11[c]

11. A system of a vehicle, the vehicle having an on-board computer for processing and communicating with the system for use of an electronic key (eKey), the system comprising:

memory associated with the on-board computer of the vehicle having program instructions for controlling unlocking and starting of the vehicle; and communications circuitry of the vehicle interfaced with the on-board computer of the vehicle, 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 of the vehicle;

wherein the wireless communications circuitry of the vehicle is configured to receive coded data from the mobile device, the coded data is unique for said eKey, and the coded data includes privilege settings set for limiting types of use of the vehicle when using the vehicle via the eKey;

wherein the eKey is associated with a user account, the user account is accessible via a user interface of an application executed by the mobile device, the eKey when active enables said unlocking of the vehicle and said starting of the vehicle.

wherein the wireless communications circuitry of the vehicle is configured to receive coded data from the mobile device, the coded data is unique for said eKey, and the coded data includes privilege settings set for limiting types of use of the vehicle when using the vehicle via the eKey;

Ex. 1001 ('659 Patent), Claim 11

'659 Patent, Claim 18[b]

18[b]

18. A vehicle having an on-board computer for processing and communicating an electronic key (eKey), the vehicle comprising:

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

communications circuitry of the vehicle interfaced with the on-board computer of the vehicle, 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 of the vehicle;

wherein the wireless communications circuitry of the vehicle is configured to receive coded data from the mobile device, the coded data is unique for said eKey to be used via the mobile device, and the coded data includes privilege settings for use of the vehicle when using the eKey with the vehicle;

wherein the eKey is associated with a user account, the user account is accessible via a user interface of an application executed by the mobile device, the eKey when active enables said unlocking of the vehicle and said starting of the vehicle.

communications circuitry of the vehicle interfaced with the on-board computer of the vehicle, 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 of the vehicle;

Ex. 1001 ('659 Patent), Claim 18

'659 Patent, Claim 18[c]

18[c]

18. A vehicle having an on-board computer for processing and communicating an electronic key (eKey), the vehicle comprising:

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

communications circuitry of the vehicle interfaced with the on-board computer of the vehicle, 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 of the vehicle;

wherein the wireless communications circuitry of the vehicle is configured to receive coded data from the mobile device, the coded data is unique for said eKey to be used via the mobile device, and the coded data includes privilege settings for use of the vehicle when using the eKey with the vehicle;

wherein the eKey is associated with a user account, the user account is accessible via a user interface of an application executed by the mobile device, the eKey when active enables said unlocking of the vehicle and said starting of the vehicle.

wherein the wireless communications circuitry of the vehicle is configured to receive coded data from the mobile device, the coded data is unique for said eKey to be used via the mobile device, and the coded data includes privilege settings for use of the vehicle when using the eKey with the vehicle;

Ex. 1001 ('659 Patent), Claim 18

Petition Failed to Show “Coded Data From the Mobile Device” that “Includes Privilege Settings” (Recited by All Independent Claims)

All grounds fail because both Kleve and Mikan lack any
“coded data from the mobile device ... the coded data includes privilege settings”

All independent claims recite receipt of:

1. coded data from the mobile device AND
2. the coded data includes privilege settings

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;

All Kleve-Based Grounds Fail to Disclose or Teach “Coded Data From the Mobile Device ... the Coded Data Includes Privilege Settings”

All Kleve-based grounds fail because:

1. Petitioners failed to show any disclosure or teaching of **coded data from the mobile device that includes privilege settings**
2. Petitioners’ relied-upon disclosures refer only to the virtual key sent to the vehicle from the server—not any “**coded data from the mobile device,**” as recited by all claims
3. Even under Petitioners’ theories to modify Kleve, Petitioners claim the vehicle already has restrictions—e.g., a rental period—BEFORE the Temporary User’s arrival, therefore **no reason for vehicle to again receive rental period from the mobile device**
4. Even under Petitioners’ theories to modify, Petitioners allege it is Kleve’s server that “simultaneously generates a virtual key and restrictions” which are both “delivered to the vehicle” from the server – **admitting there is no reason for the temporary user’s phone to ‘re-send’ to the vehicle the already “delivered” restrictions**

Kleve Does Not Disclose Including Any Rental Agreement Terms in Any Coded Data, Let Alone a Vehicle Receiving “Coded Data that Includes Privilege Settings”

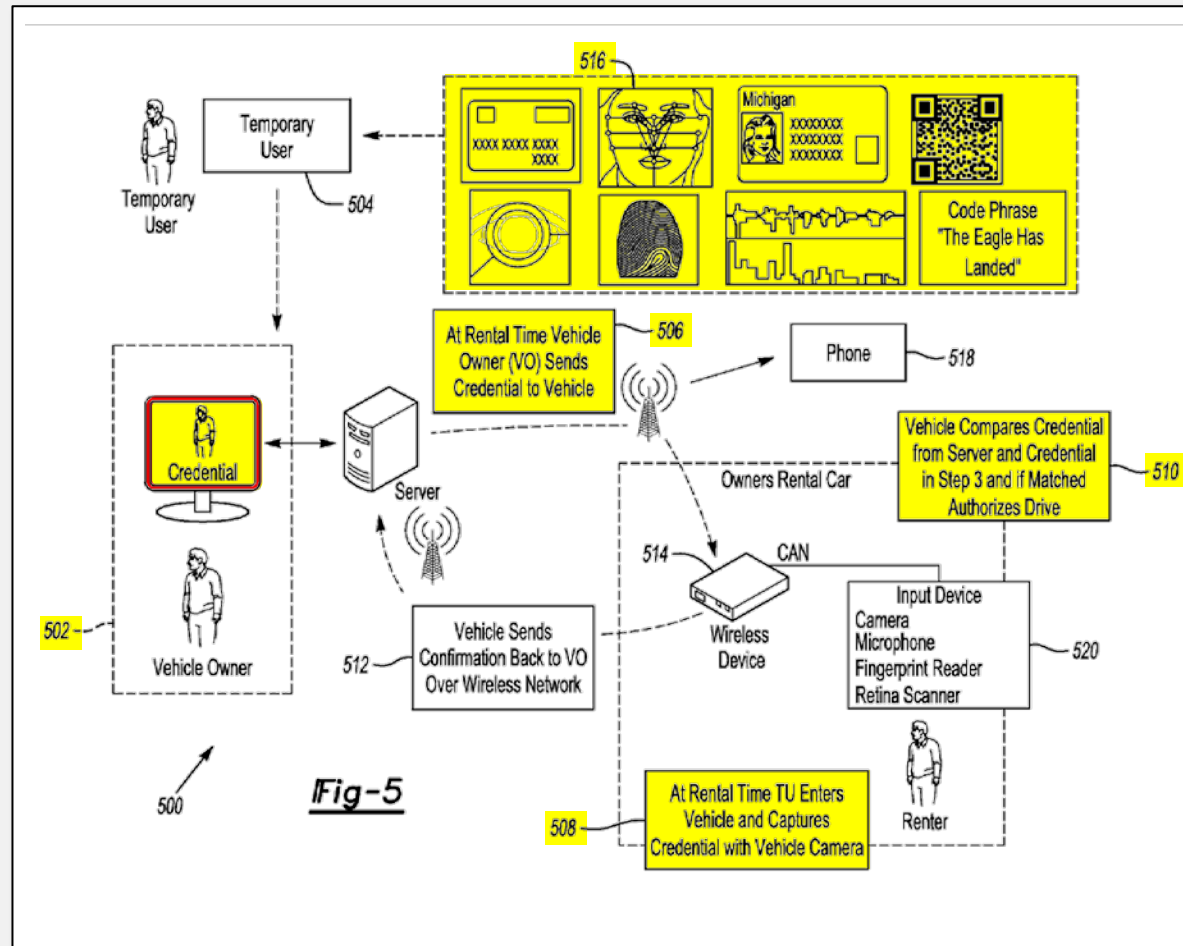
[0084] At step **812**, if the owner decides he has no interest in accepting the Temporary User’s offer, he may decline and wait for the vehicle rental authorization system to notify of any other offers. If the owner has decided to accept the offer he may begin the process of developing terms and conditions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

EX1005 (Kleve), ¶ 84

[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.

EX1005 (Kleve), ¶ 85

Kleve's Virtual Key is Nothing More Than a Credential, e.g., a User's Face, Fingerprint

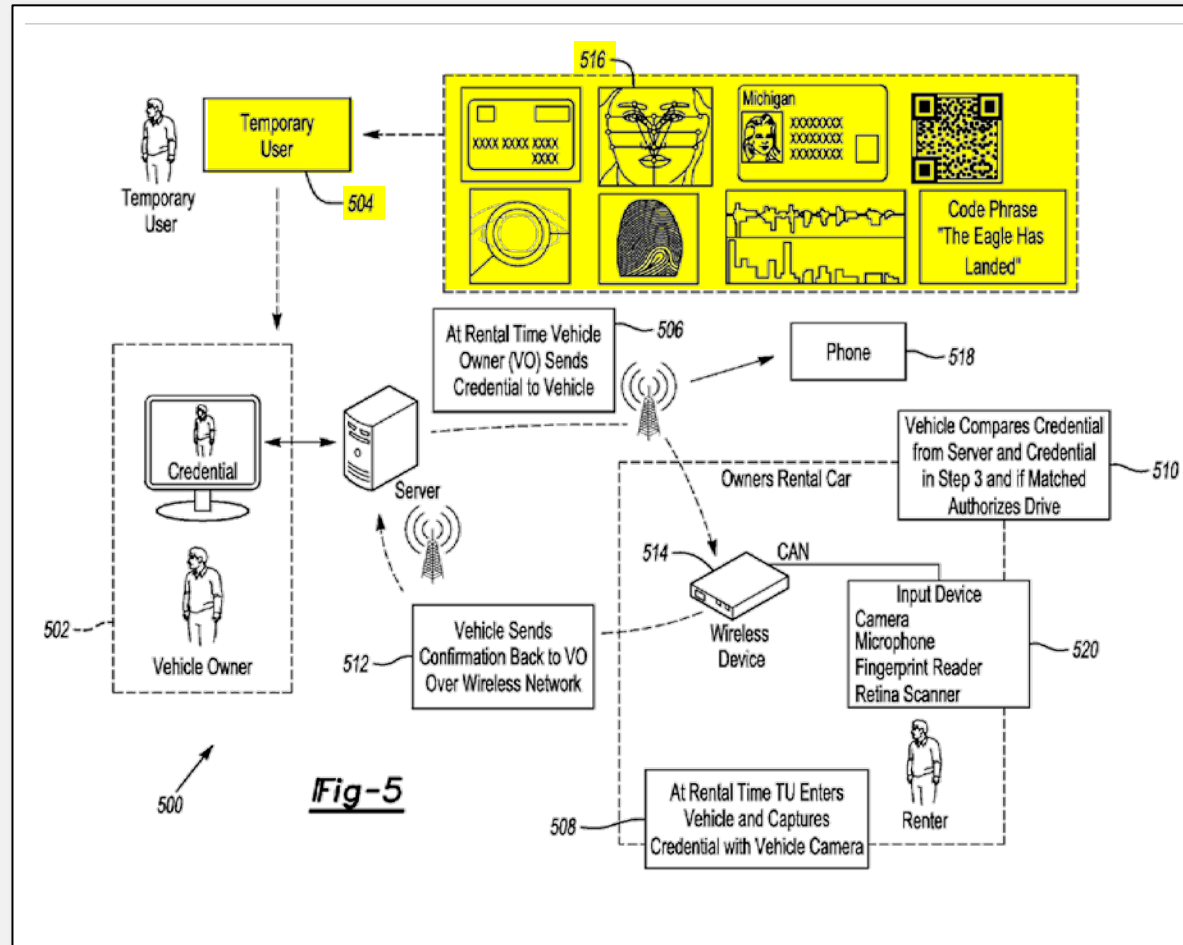


[0062] FIG. 5 shows an illustrative example of an overview of how the vehicle rental micro-business may be structured with a keyless transaction between the Owner of the vehicle and the Temporary User. This example illustrates the process after the vehicle Owner and Temporary User have already setup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

EX1005 (Kleve), ¶ 62

EX1005 (Kleve), Fig. 5

Kleve's Generation and Distribution of a Virtual Key is Devoid of Any Use Restriction

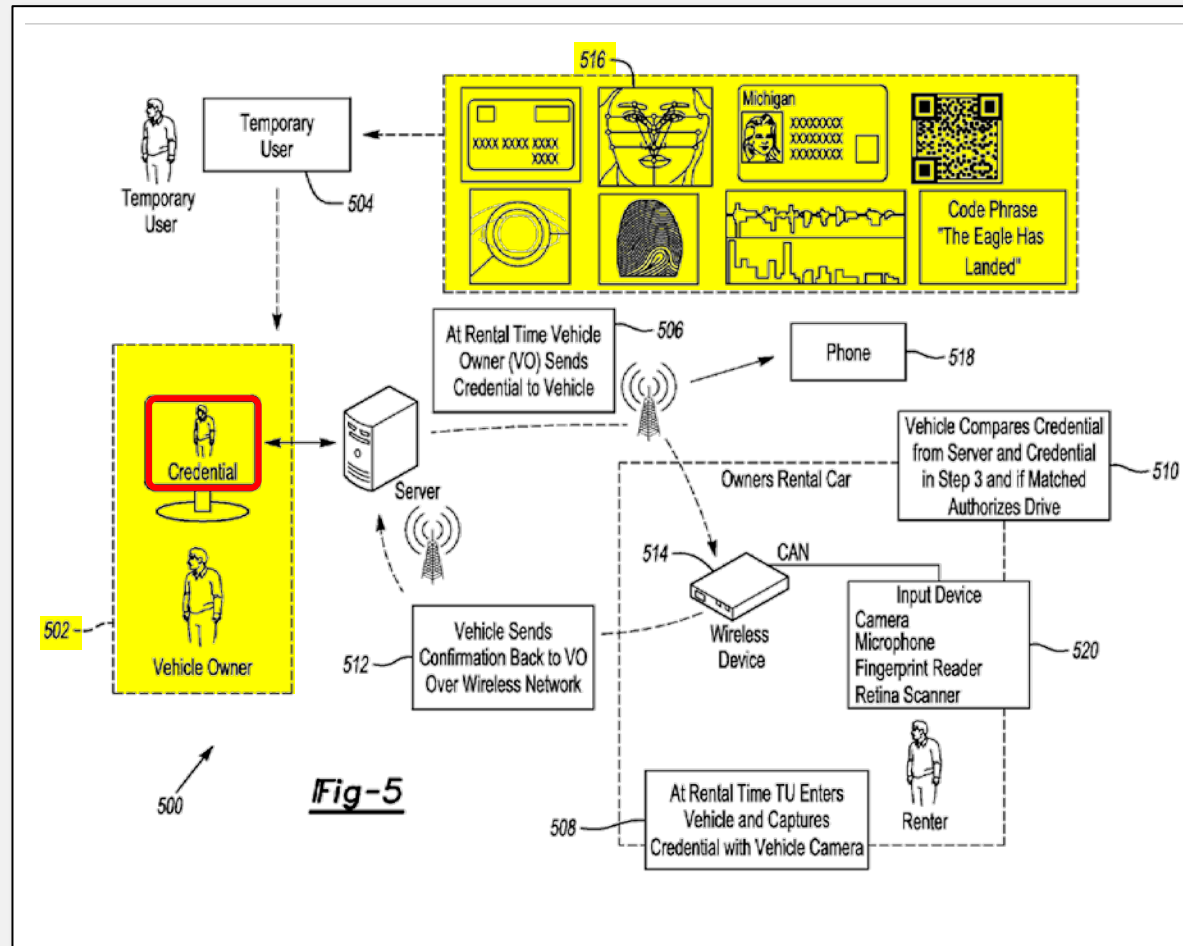


EX1005 (Kleve), Fig. 5

[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.

EX1005 (Kleve), ¶ 63

Kleve's Generation and Distribution of a Virtual Key is Devoid of Any Use Restriction

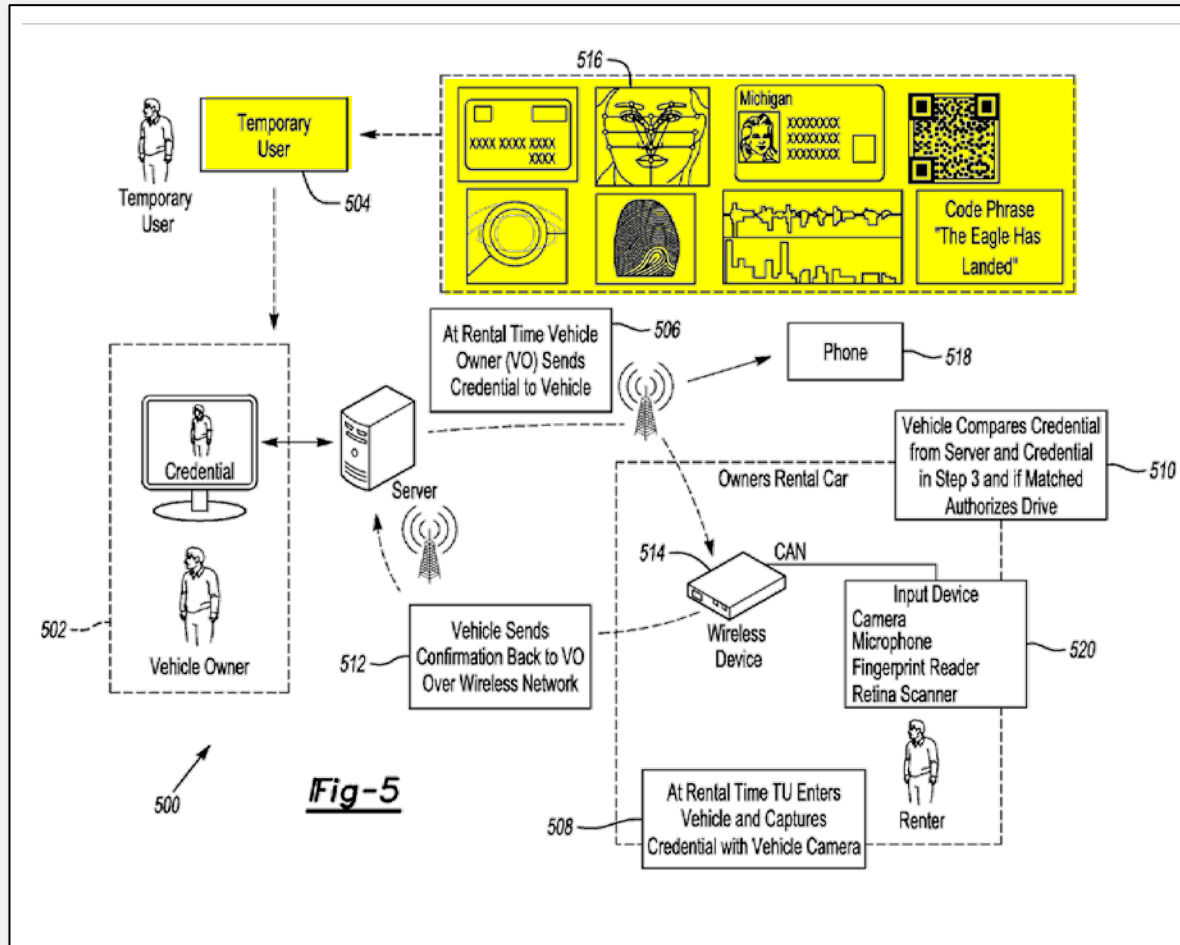


EX1005 (Kleve), Fig. 5

[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.

EX1005 (Kleve), ¶ 62

Temporary User's Unique Identification is Entered into Server and Used as a Virtual Key

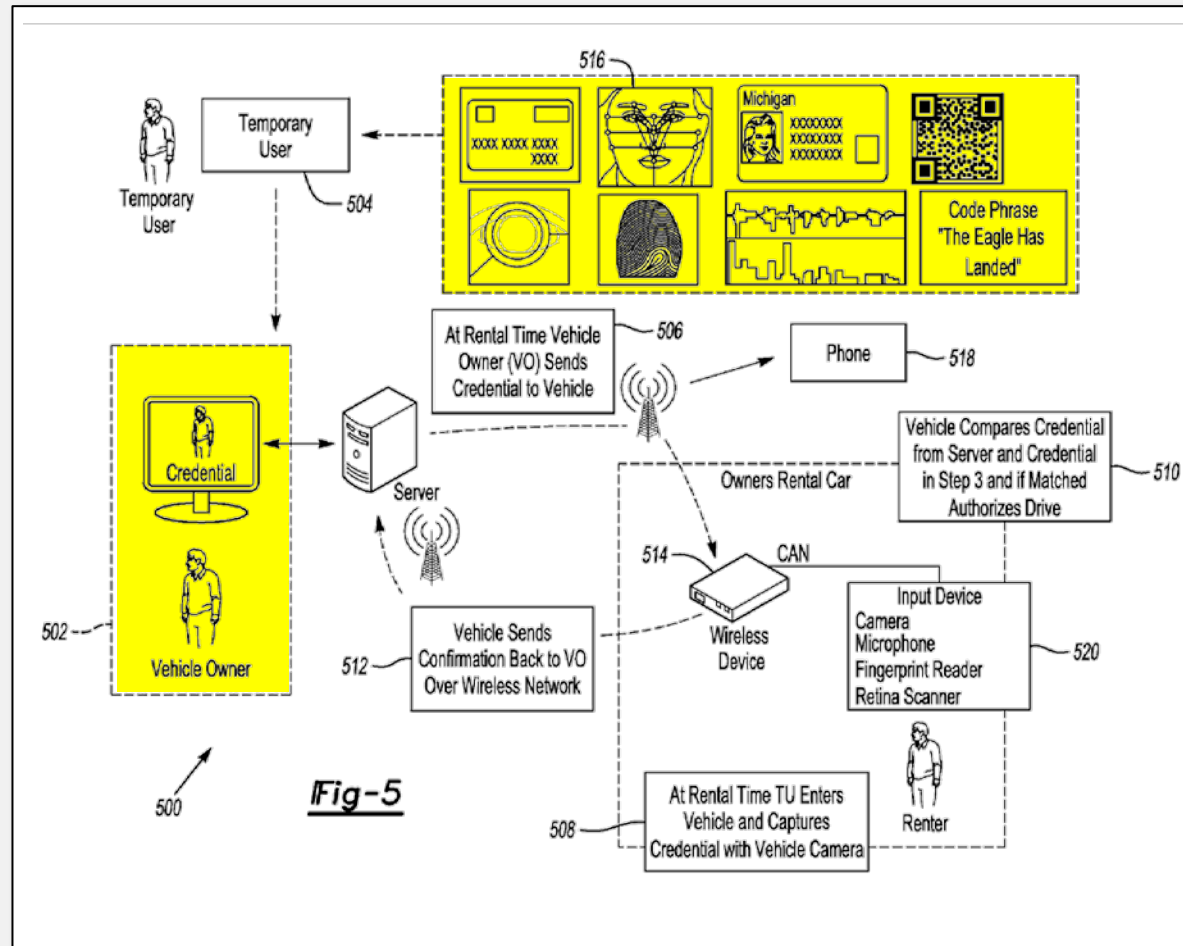


EX1005 (Kleve), Fig. 5

[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.

EX1005 (Kleve), ¶ 63

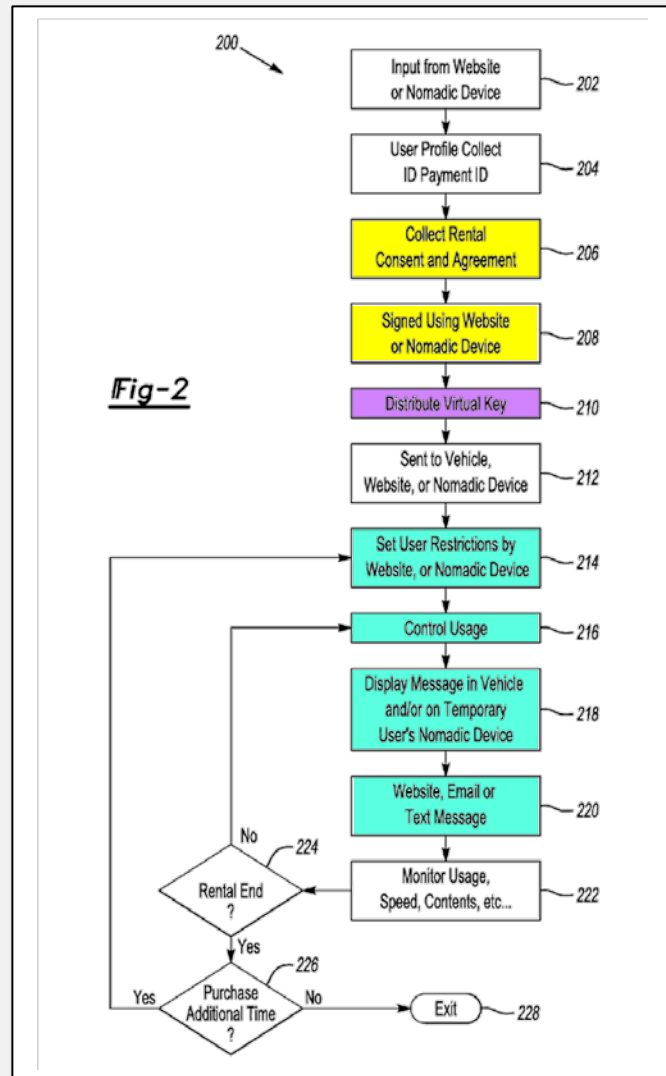
No Privilege Setting Included in Either Generation or Distribution of Virtual Key



[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 recogni-

Virtual Key Sent to Vehicle Enables Driving During Rental Period— But Vehicle Does Not Receive any Privilege Setting from Mobile Device



EX1005 (Kleve), Fig. 2

[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.

EX1005 (Kleve), ¶ 39

Petitioners Ask the Board to Interpret Kleve Differently Depending on the Claims Presented

'659 Petitioners' Reply: User's virtual key includes 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, ¶39 ("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.

'188 Proceeding Server check to see if user's key within rental period

5 I walked through that. I may walk through that one more time. But
6 setting that aside, this is express disclosure of the E-key being enabled
7 during the rental period. No one disputes that that rental period is a
8 condition on use. This is, I didn't go through this in the, in the opening, but
9 this is also shown paragraph 71 where the user goes up to the car, he sends a
10 request to the server requesting access. If it is in the scheduled time for
11 rental, he's given access. This is in connection. I think this, this is in
12 connection with figure six.
13 This goes to your point, Judge Galligan, that there is a server lookup
14 that it, Patent Owner's counselor kept saying repeatedly that it's the
15 condition is not included in the E-key. That's not our position. Kleve is
16 not -- it's not a model of clarity on this point, but it very -- it does very
17 clearly state that there is a server check to see if that rental period, if that key
18 is within that rental period, this is in connection with figure six.



Virtual Key “Sent to the Vehicle ... to Enable the Keyless Drive System ... During a Given Rental Period” Does Not Show Vehicle’s Receipt of “Coded Data From the Mobile Device ... the Coded Data Includes Privilege Settings”

[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.

EX1005 (Kleve) ¶ 39

’188 Proceeding *Server check to see if user’s key within rental period*

5 I walked through that. I may walk through that one more time. But
6 setting that aside, this is express disclosure of the E-key being enabled
7 during the rental period. No one disputes that that rental period is a
8 condition on use. This is, I didn't go through this in the, in the opening, but
9 this is also shown paragraph 71 where the user goes up to the car, he sends a
10 request to the server requesting access. If it is in the scheduled time for
11 rental, he's given access. This is in connection. I think this, this is in
12 connection with figure six.

13 This goes to your point, Judge Galligan, that there is a server lookup
14 that it, Patent Owner’s counselor kept saying repeatedly that it's the
15 condition is not included in the E-key. That's not our position. Kleve is
16 not -- it's not a model of clarity on this point, but it very -- it does very
17 clearly state that there is a server check to see if that rental period, if that key
18 is within that rental period, this is in connection with figure six.

Virtual Key “Sent to the Vehicle ... to Enable the Keyless Drive System ... During a Given Rental Period” Does Not Show Vehicle’s Receipt of “Coded Data From the Mobile Device ... the Coded Data Includes Privilege Settings”

[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.

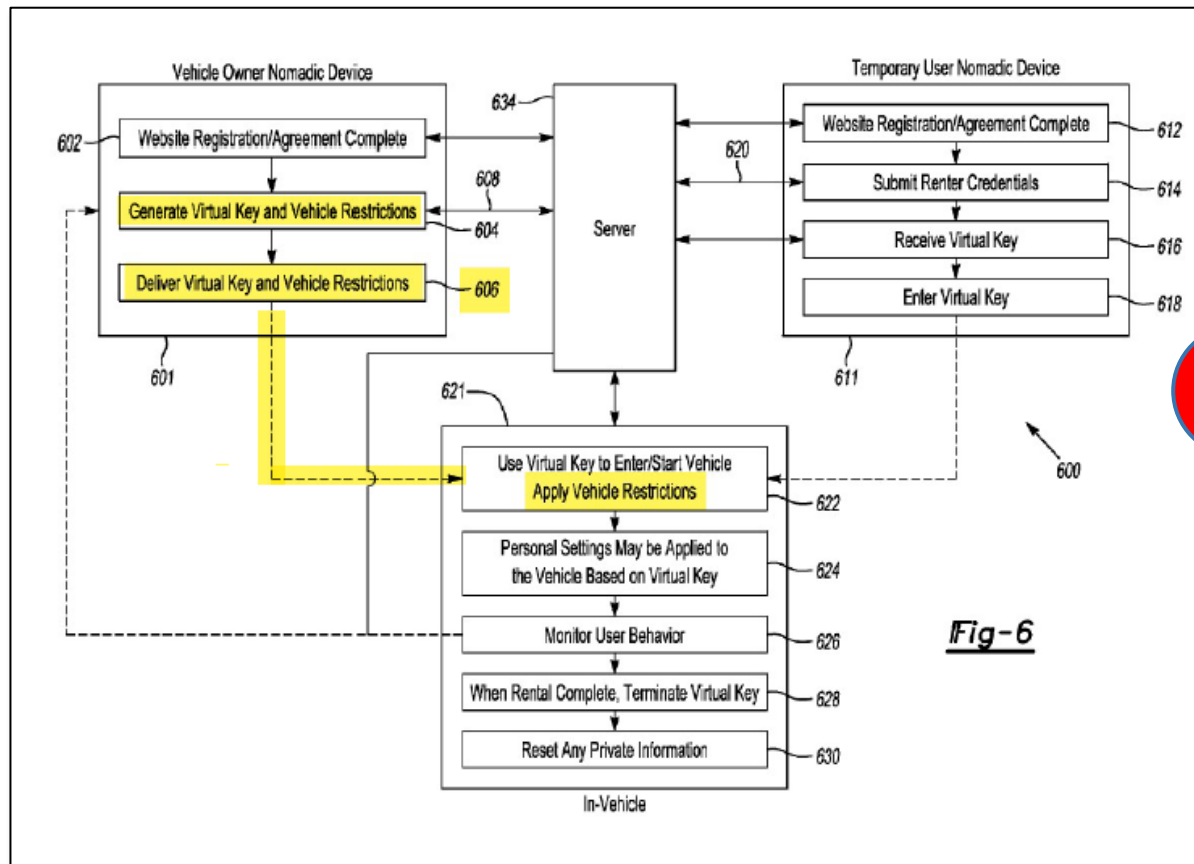
EX1005 (Kleve) ¶ 44

'188 Proceeding *Server check to see if user's key within rental period*

5 I walked through that. I may walk through that one more time. But
6 setting that aside, this is express disclosure of the E-key being enabled
7 during the rental period. No one disputes that that rental period is a
8 condition on use. This is, I didn't go through this in the, in the opening, but
9 this is also shown paragraph 71 where the user goes up to the car, he sends a
10 request to the server requesting access. If it is in the scheduled time for
11 rental, he's given access. This is in connection. I think this, this is in
12 connection with figure six.

13 This goes to your point, Judge Galligan, that there is a server lookup
14 that it, Patent Owner's counselor kept saying repeatedly that it's the
15 condition is not included in the E-key. That's not our position. Kleve is
16 not -- it's not a model of clarity on this point, but it very -- it does very
17 clearly state that there is a server check to see if that rental period, if that key
18 is within that rental period, this is in connection with figure six.

Virtual Key “Sent to the Vehicle ... to Enable the Keyless Drive System ... During a Given Rental Period” Kleve Teaches Only That Vehicle Receives Restrictions, But Not From Temporary User



EX1005 (Kleve) , Fig. 6

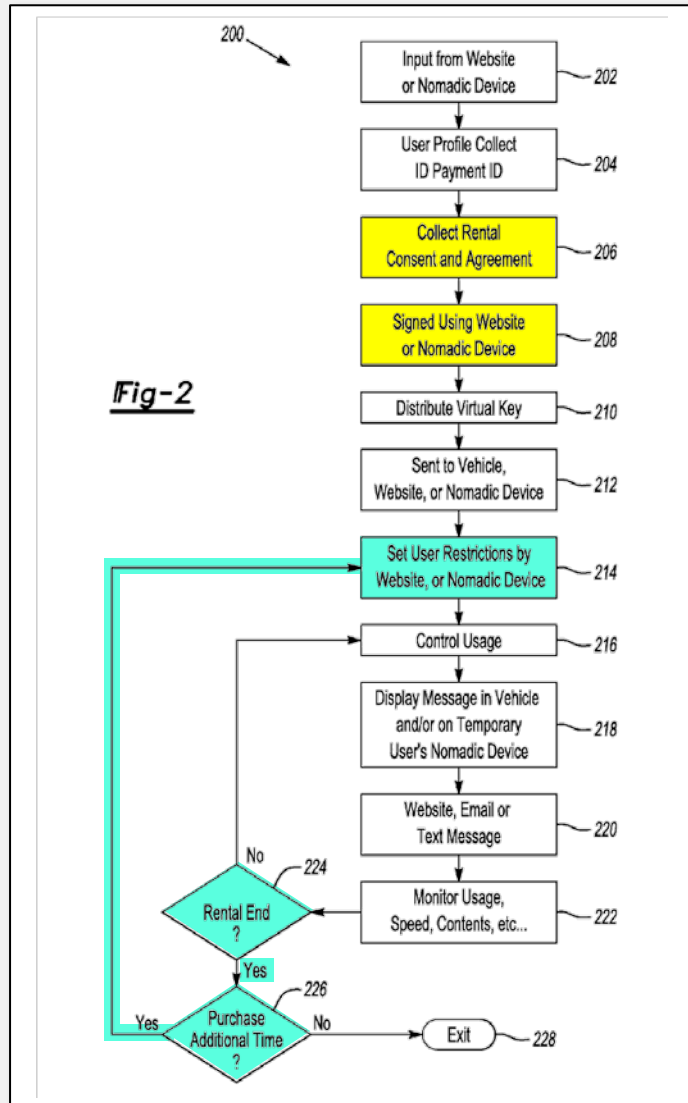
Petitioners' Reply
U.S. Patent No. 11,738,659

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, ¶39 ("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.

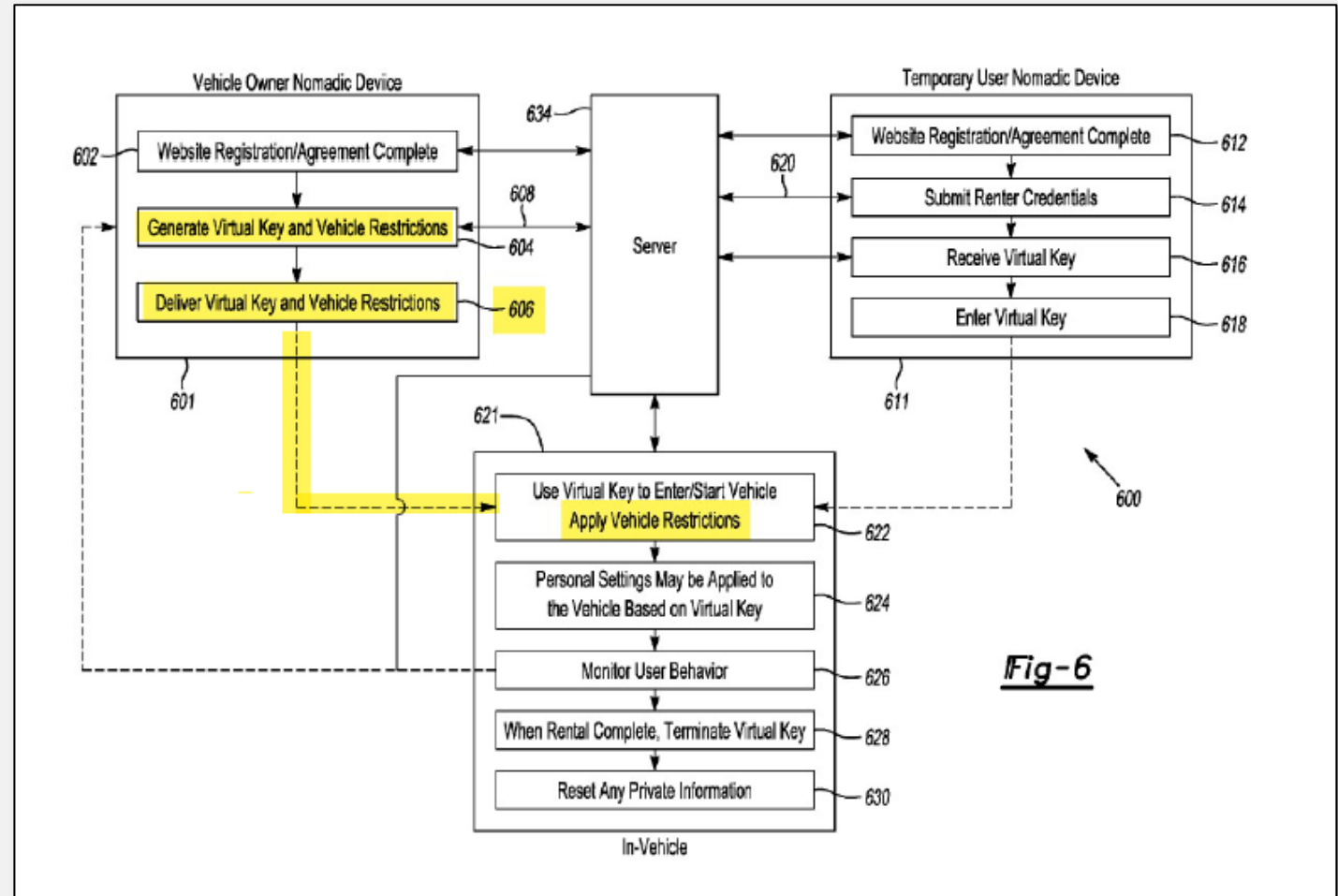
Kleve elsewhere teaches that restrictions are assigned *before* the rental period begins. For example, in Figure 6, Kleve teaches that after restrictions are agreed to, the server simultaneously "Generate[s] Virtual Key and Vehicle Restrictions." EX1005, Fig. 6. The virtual key is then "generated and 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.

Virtual Key “Sent to the Vehicle ... to Enable the Keyless Drive System ... During a Given Rental Period”

Kleve Teaches Only That Vehicle Receives Restrictions, But Not From Temporary User



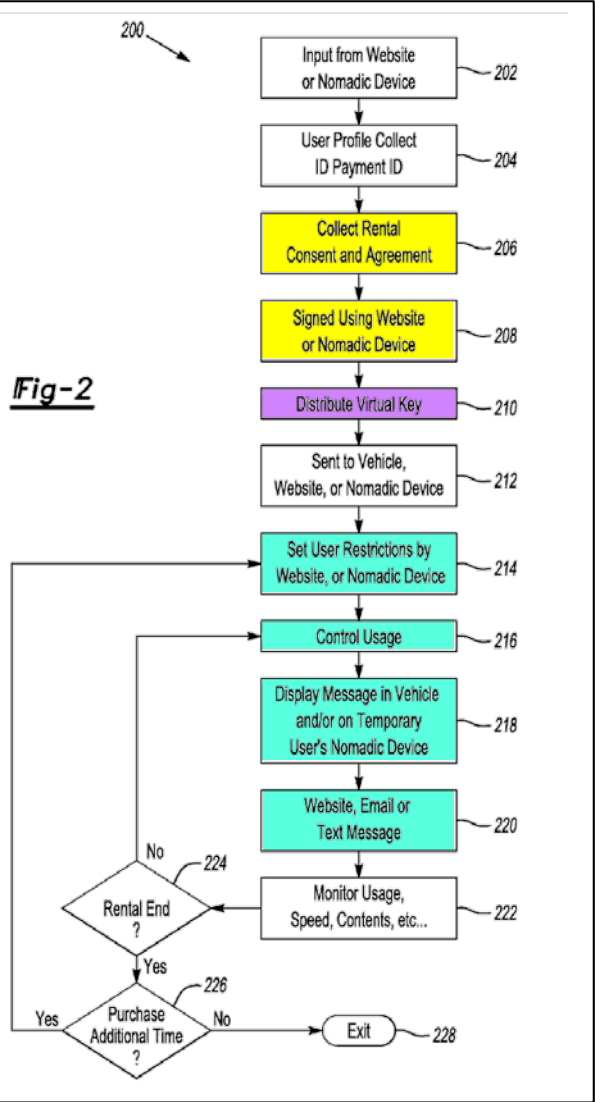
EX1005 (Kleve), Fig. 2



EX1005 (Kleve), Fig. 6

Virtual Key “Sent to the Vehicle ... to Enable the Keyless Drive System ... During a Given Rental Period”
Kleve Teaches Only That Vehicle Receives Restrictions, But Not From Temporary User

Fig-2

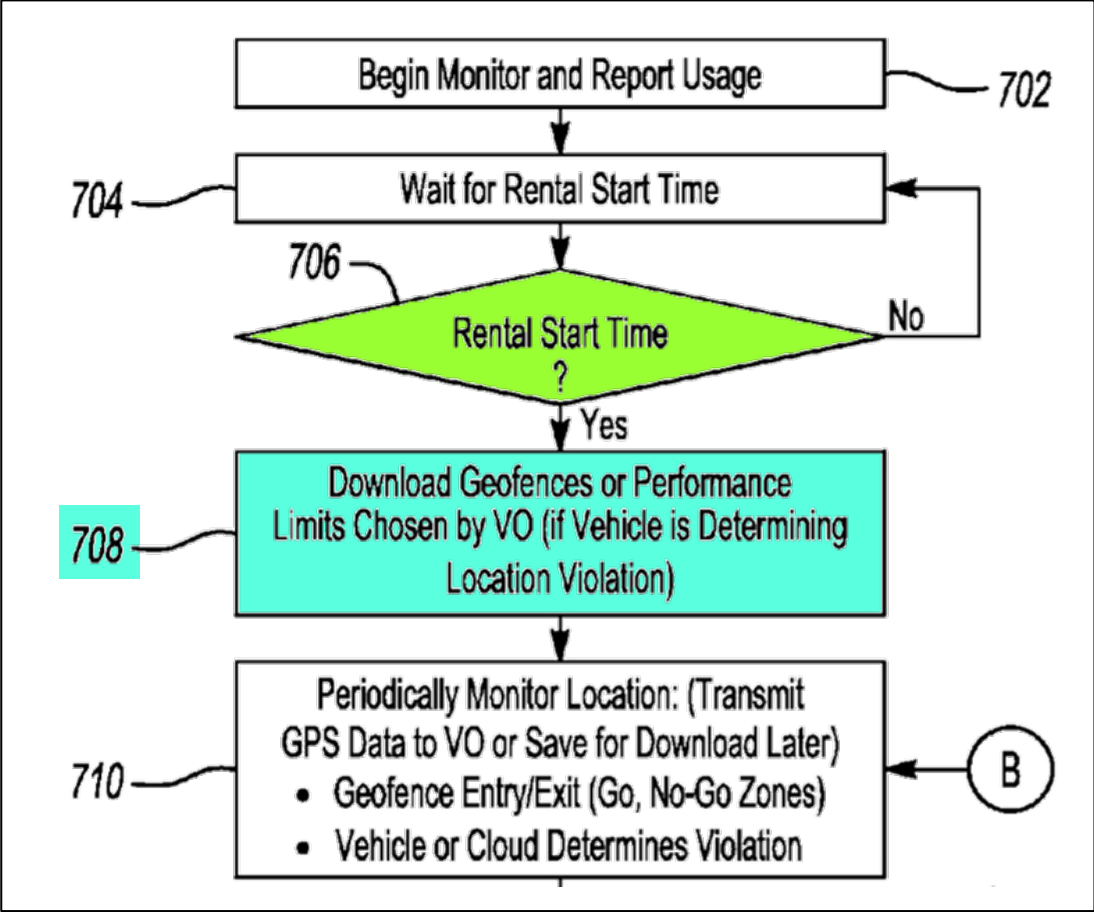


[0040] At step 214, the Owner may have access to control usage of the vehicle being rented by the Temporary User. The Owner may set user restrictions by use of the website or nomadic device. The restrictions may be based on, but not limited to, the owner’s selection of parameters including, but not limited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

EX1005 (Kleve), ¶ 40

EX1005 (Kleve), Fig. 2

Virtual Key “Sent to the Vehicle ... to Enable the Keyless Drive System ... During a Given Rental Period”
Kleve Teaches Only That Vehicle Receives Restrictions, But Not From Temporary User



EX1005 (Kleve), Fig. 7A

[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.

EX1005 (Kleve), ¶ 40

[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.

EX1005 (Kleve), ¶ 51
Patent Owner Sur-Reply at pp. 1-22 | 24

Virtual Key “Sent to the Vehicle ... to Enable the Keyless Drive System ... During a Given Rental Period” Kleve Teaches Only That Vehicle Receives Restrictions, But Not From Temporary User

[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.

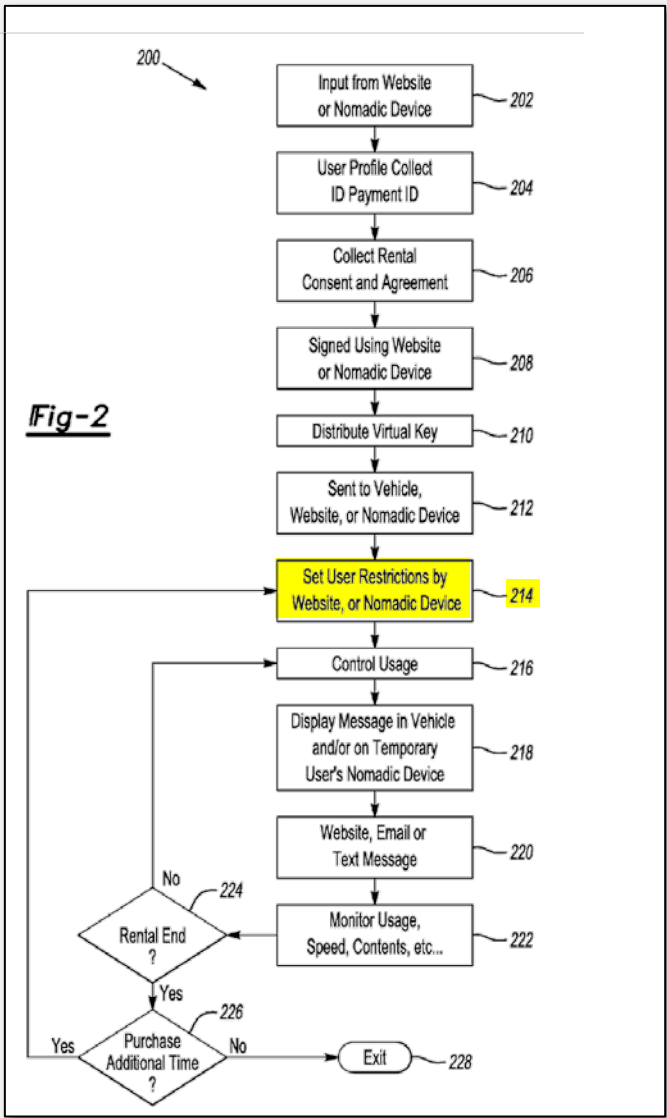
EX1005 (Kleve), ¶ 43

[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.

EX1005 (Kleve), ¶ 75

Virtual Key “Sent to the Vehicle ... to Enable the Keyless Drive System ... During a Given Rental Period”

Kleve Teaches Only That Vehicle Receives Restrictions, But Not From Temporary User



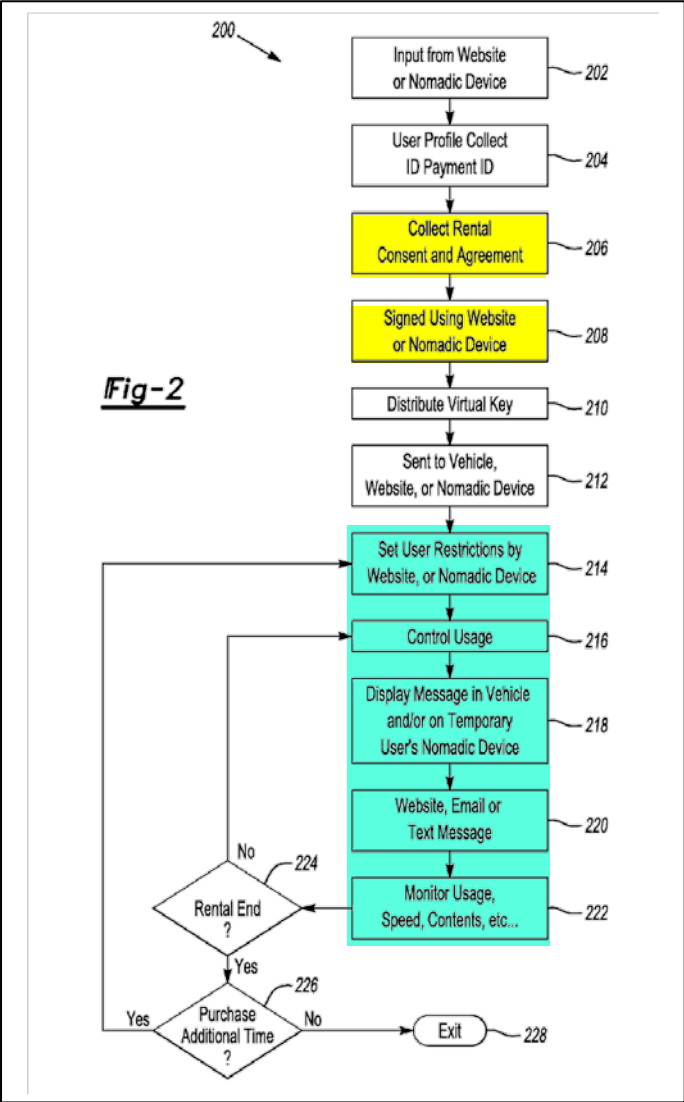
[0040] At step 214, the Owner may have access to control usage of the vehicle being rented by the Temporary User. The Owner may set user restrictions by use of the website or nomadic device. The restrictions may be based on, but not limited to, the owner's selection of parameters including, but not limited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

[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.

[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 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

EX1005 (Kleve), Fig. 2, ¶¶ 40, 51, 43, 75

Virtual Key “Sent to the Vehicle ... to Enable the Keyless Drive System ... During a Given Rental Period”
Kleve Teaches Only That Vehicle Receives Restrictions, But Not From Temporary User



EX1005 (Kleve), Fig. 2

[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.

EX1005 (Kleve), ¶ 51

Virtual Key “Sent to the Vehicle ... to Enable the Keyless Drive System ... During a Given Rental Period” Kleve Teaches Only That Vehicle Receives Restrictions, But Not From Temporary User

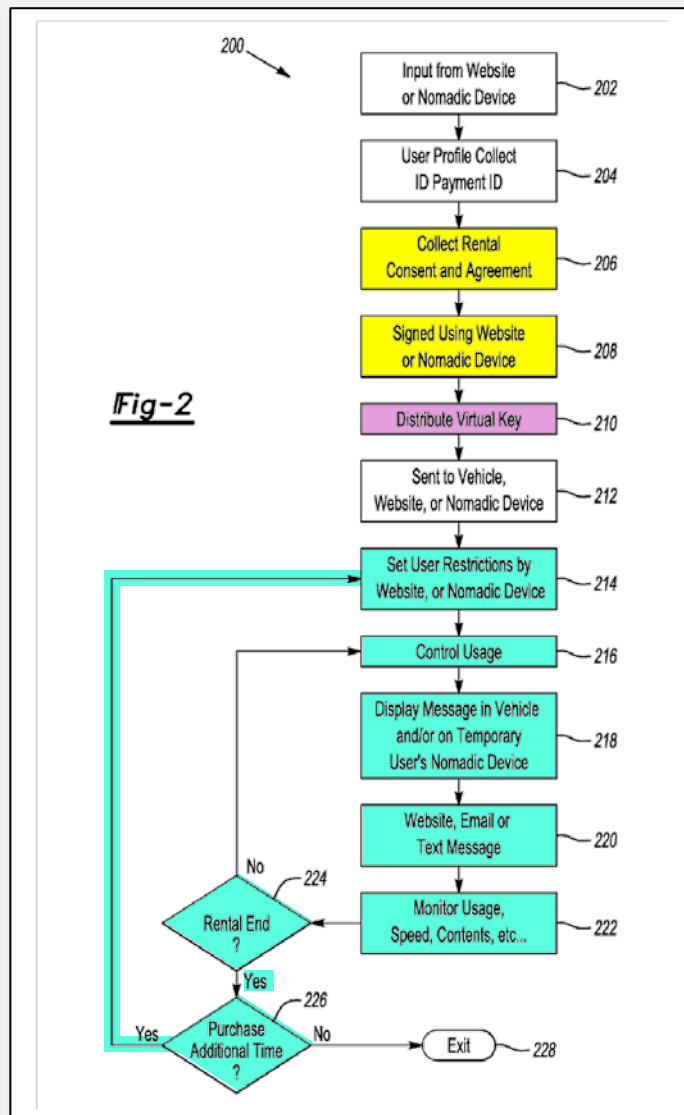
[0039] At step 210, once the Temporary User selects the vehicle, pays the appropriate amount and signs a consent agreement, then the system may generate a virtual key to distribute to the Temporary User and VCS. The virtual key may be sent to, but not limited to, the website for the Temporary User to 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.

EX1005 (Kleve), ¶ 39

[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.

EX1005 (Kleve), ¶ 9

Termination of Rental Period is Tied to “User Restrictions” Set by Owner, Independent of Virtual Key



[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.

EX1005 (Kleve), ¶ 54

Termination of Rental Period is Tied to “User Restrictions” Set by Owner, Independent of Virtual Key

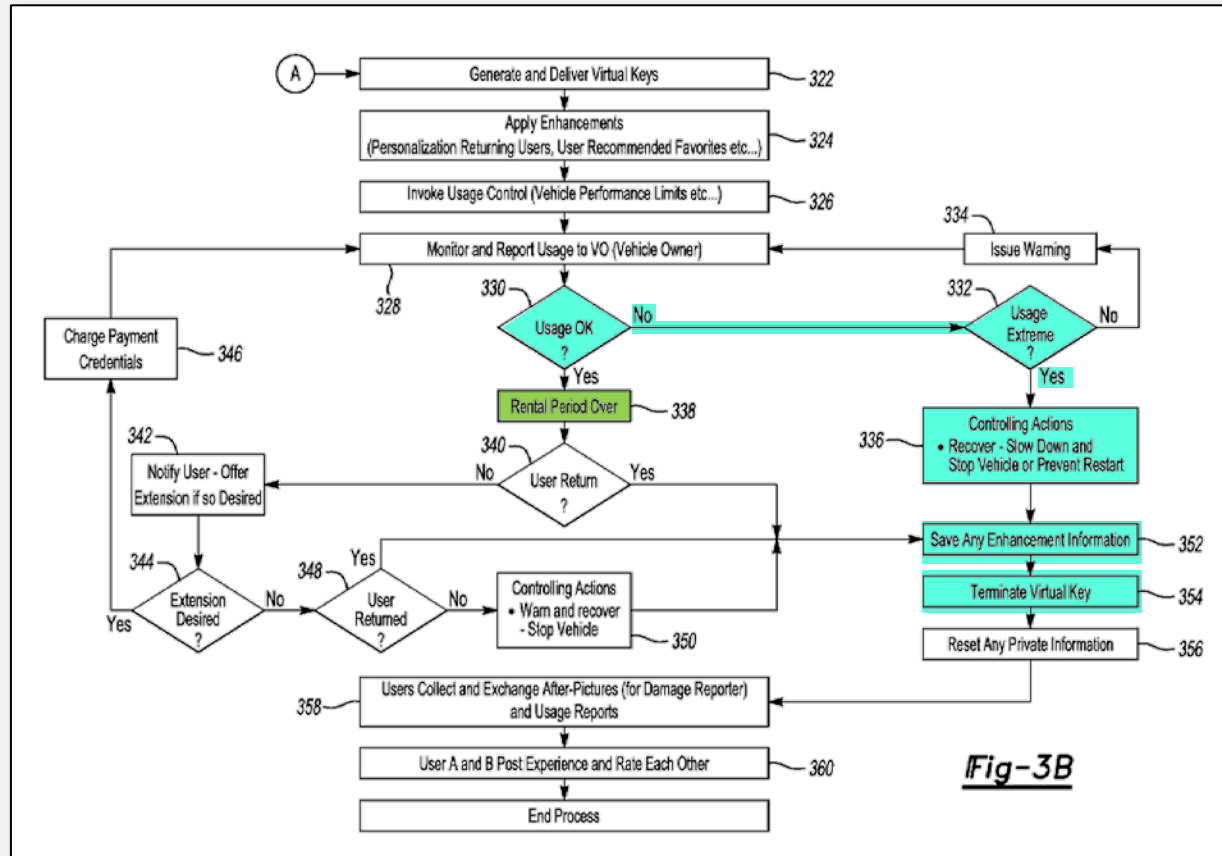


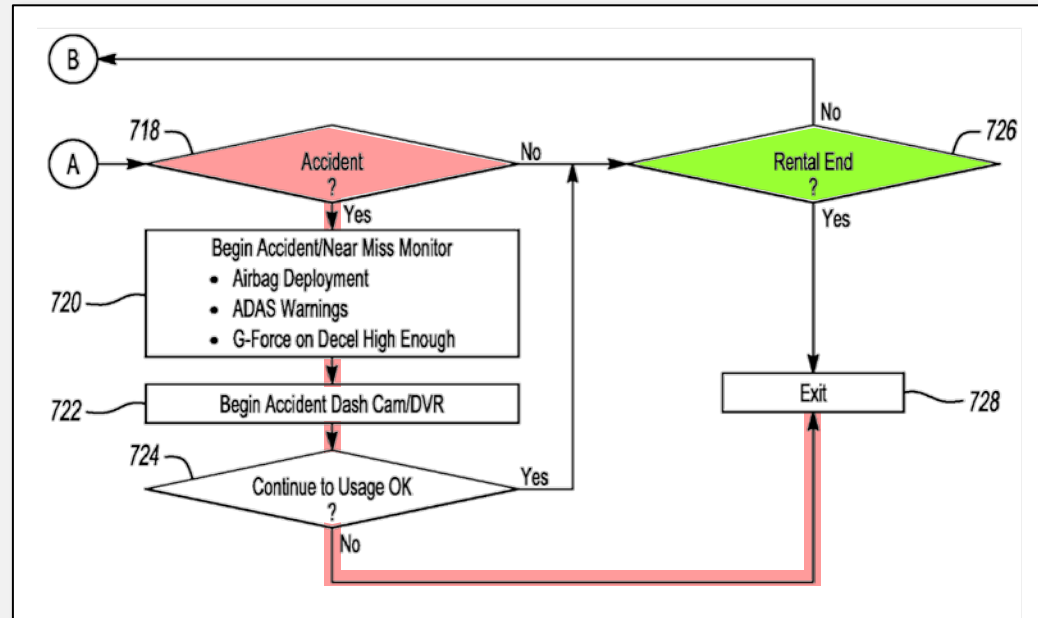
Fig-3B

EX1005 (Kleve), Fig. 3B

[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.

EX1005 (Kleve), ¶ 53

Termination of Rental Period is Tied to “User Restrictions” Set by Owner, Independent of Virtual Key

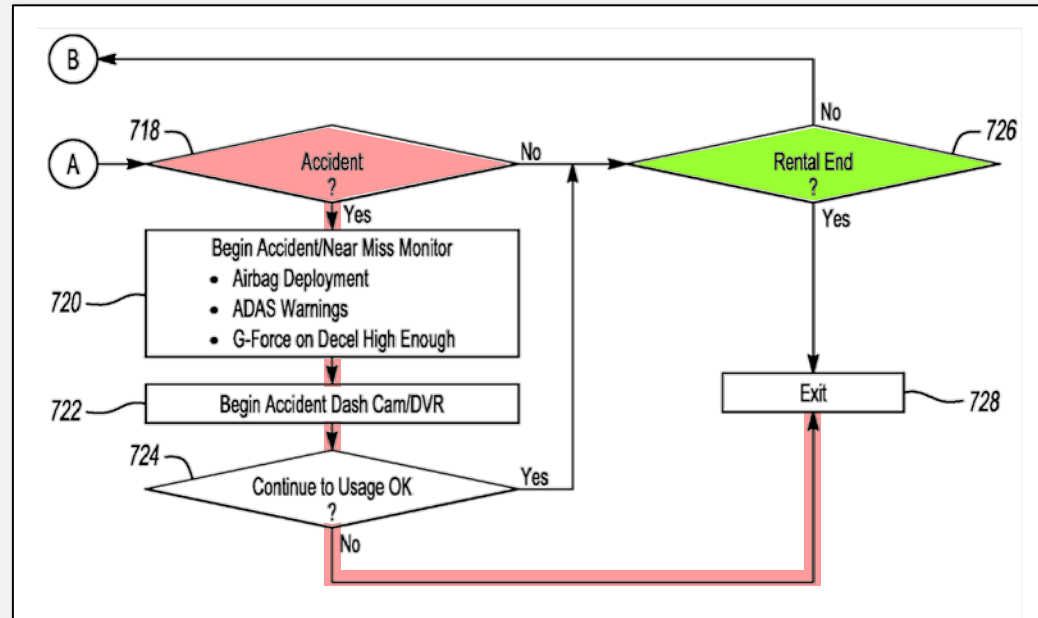


EX1005 (Kleve), Fig. 7B

[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.

EX1005 (Kleve), ¶ 79

Termination of Rental Period is Tied to “User Restrictions” Set by Owner, Independent of Virtual Key

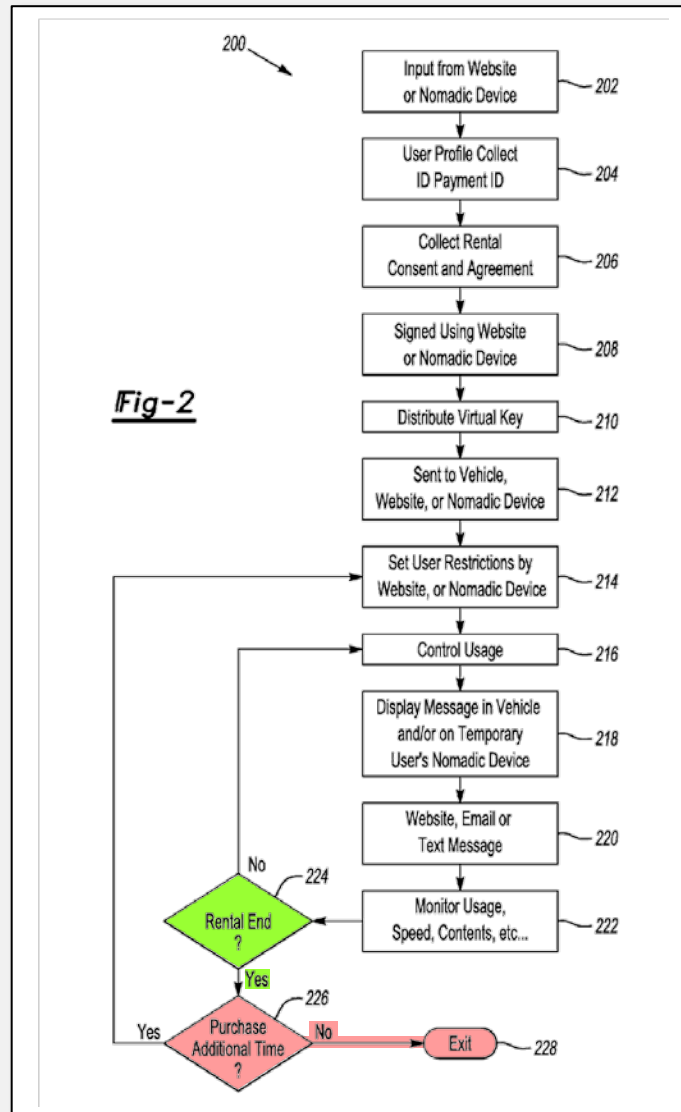


EX1005 (Kleve), Fig. 7B

[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.

EX1005 (Kleve), ¶ 80

Termination of Rental Period is Tied to “User Restrictions” Set by Owner, Independent of Virtual Key

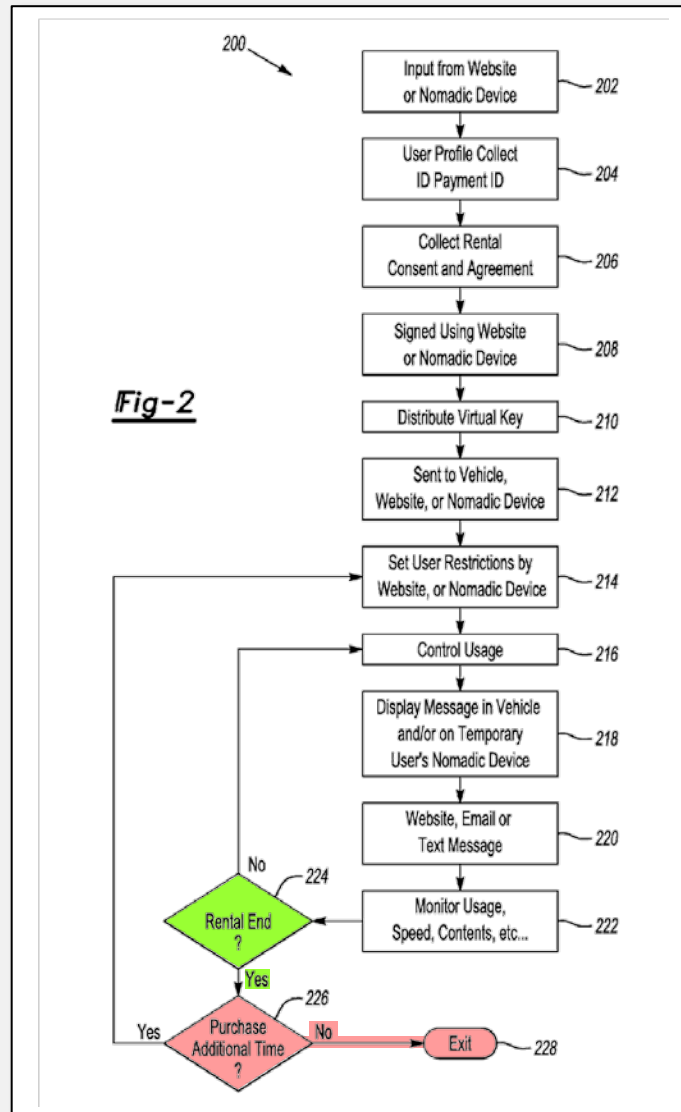


EX1005 (Kleve), Fig. 2

[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.

EX1005 (Kleve), ¶ 43

Termination of Rental Period is Tied to “User Restrictions” Set by Owner, Independent of Virtual Key



EX1005 (Kleve), Fig. 2

[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.

EX1005 (Kleve), ¶ 80

Termination of Rental Period is Tied to “User Restrictions” Set by Owner, Independent of Virtual Key

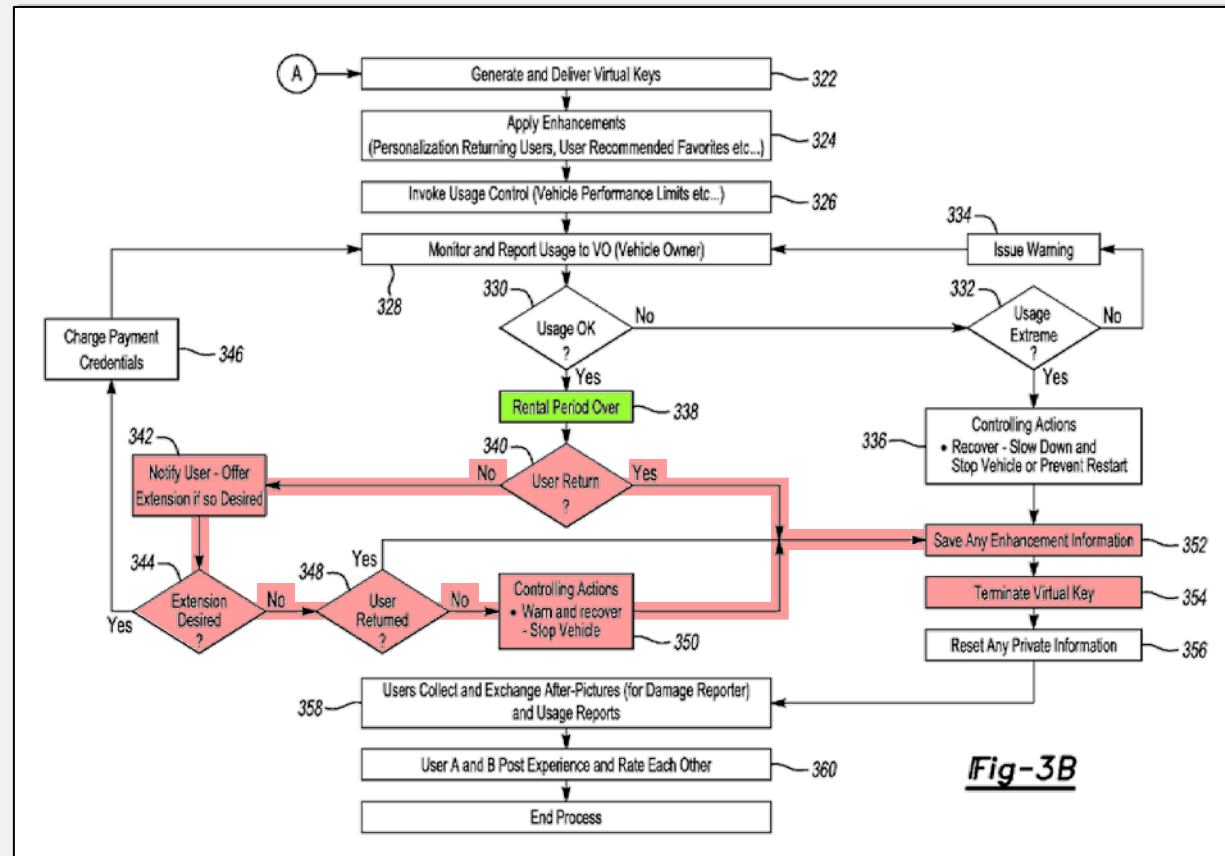


Fig-3B

EX1005 (Kleve), Fig 3B

[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.

EX1005 (Kleve), ¶ 54

Virtual Key Not Always Generated After Rental Agreement

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

EX2022 (Dr. Almeroth Deposition – Objection omitted), 27:5-10

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

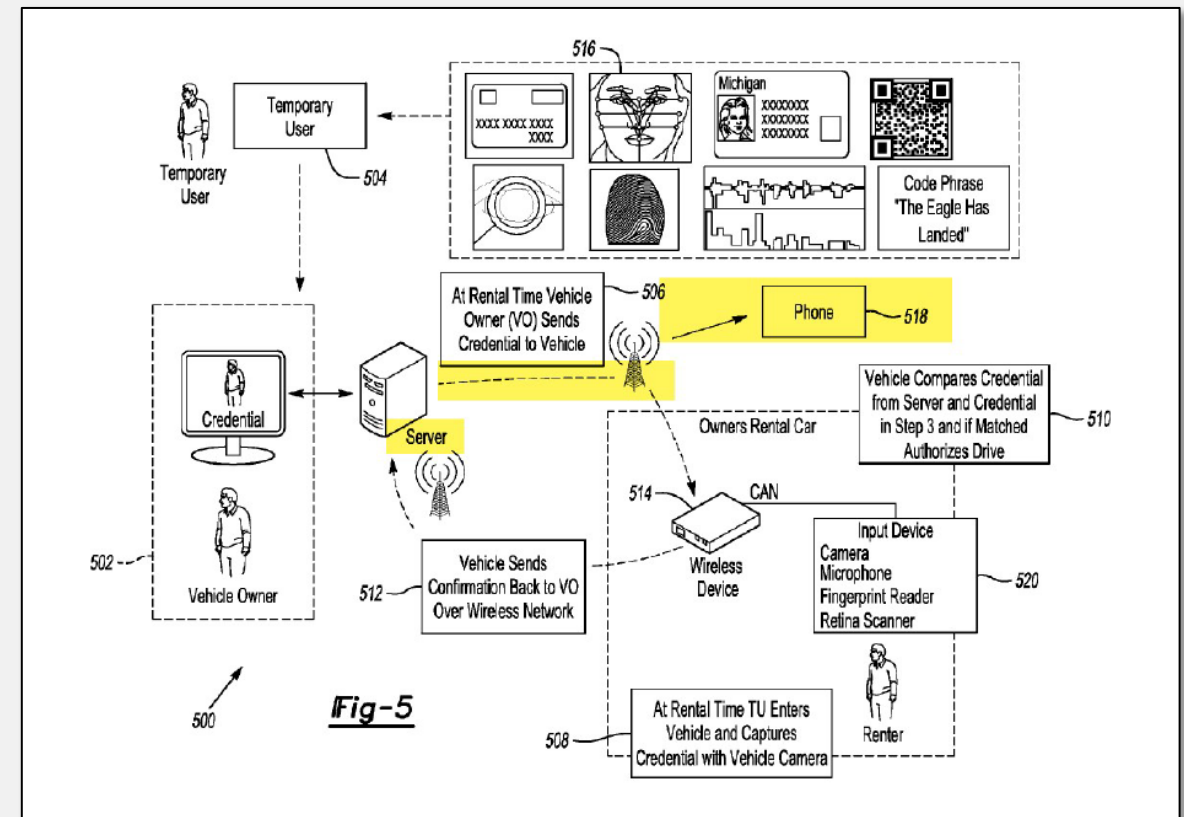
A. No. Not necessarily.

EX2022 (Dr. Almeroth Deposition – Objection omitted), 27:21-28:8

Virtual Key “Sent to the Vehicle ... to Enable the Keyless Drive System ... During a Given Rental Period”
Kleve Teaches Only That Vehicle Receives Restrictions, But Not the Temporary User

Kleve confirms unilateral direction of its “encrypted message” from the server to the vehicle, User’s phone 518

[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.



That Kleve's Virtual Key "Enables Keyless Drive System ... During a Given Rental Period" Fails to Show Vehicle Receipt of "Coded Data From the Mobile Device ... the Coded Data Includes Privilege Settings"

- **The Petition:** only the virtual key that "the server simultaneously generates" with "vehicle restrictions" is delivered to the vehicle
- Figure 6 fails to connect any "rental period" or other "vehicle restriction" to the virtual key sent to the Temporary User, nor anything received from Temporary User's mobile device

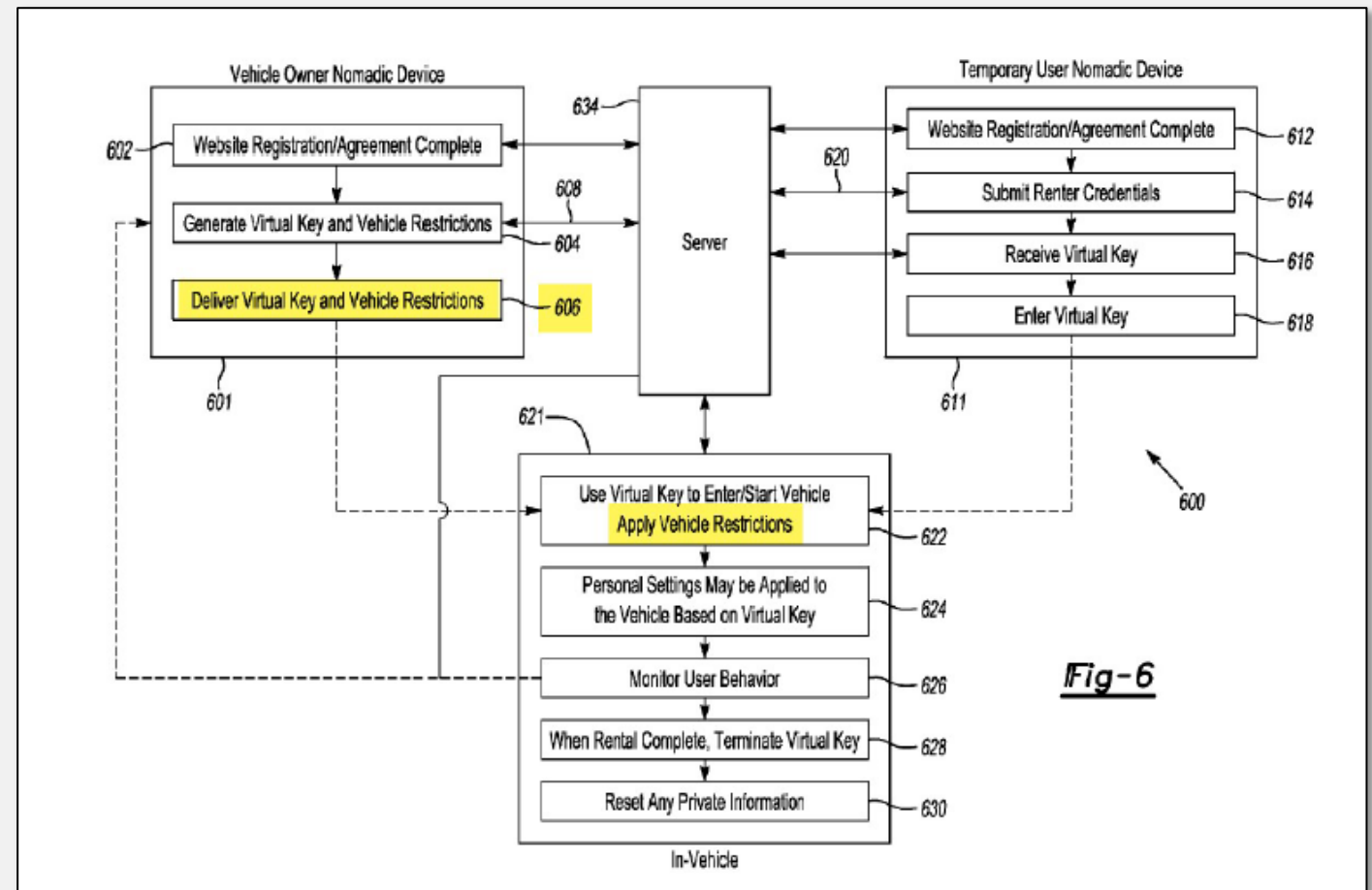


Fig-6

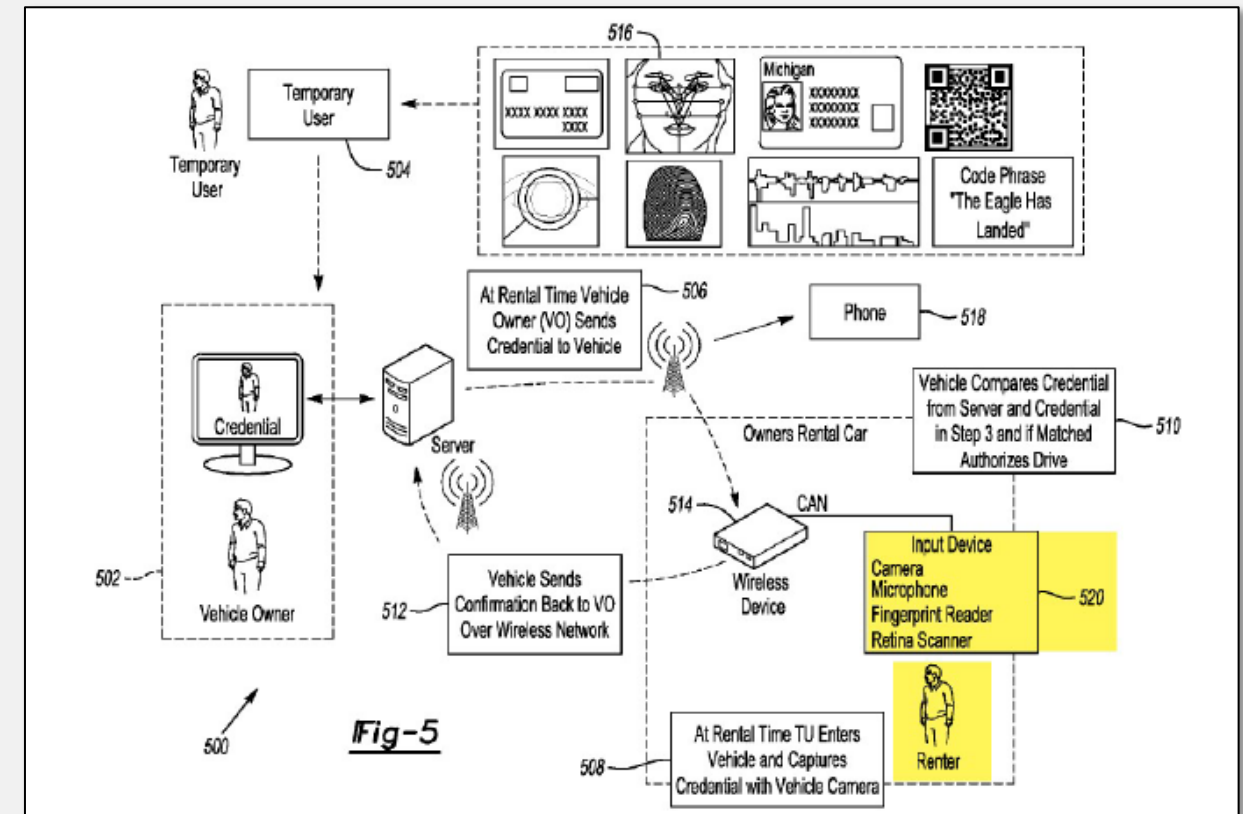
That Kleve's Virtual Key "Enables Keyless Drive System ... During a Given Rental Period" Fails to Show Vehicle Receipt of "Coded Data From the Mobile Device ... the Coded Data Includes Privilege Settings"

- **The Petition:** only the virtual key that is "sent to the vehicle" that enables a keyless drive "during a given rental period"
- Like Figure 6, Para. 39 fails to connect any "rental period" or other "restriction" to the virtual key sent to the Temporary User

[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.

Kleve's Input of a Matrix Barcode—Merely “Ensures the Temporary User is Who They Claim to Be”—But Fails to Disclose “Coded Data From the Mobile Device ... the Coded Data Includes Privilege Settings”

- **The Petition:** only the virtual key that is “sent to the vehicle” that enables a keyless drive “during a given rental period,” whereas input of matrix barcode merely “ensure[s] the TU is who they claim to be”
- **The Petition:** the matrix barcode input at device 520 is mere “credential” to “ensure the temporary user is who they claim to be”



Kleve, Hatton Combination Teaches Authentication

Hatton: Vehicle PEPS & PATS Controllers with Encrypted Data

Referring now to FIG. 2A, a system 110 in communication and/or embedded with the VCS 1 may program keys to a vehicle to establish primary and secondary drivers in accordance to one embodiment of the present invention is shown. The system 110 includes a vehicle interface display 112, a body electronics controller 114, and a passive anti-theft security (PATS) controller 116. The vehicle interface display 112

EX1008 (Hatton), 5:54-5:60

Referring now to FIG. 2B, a system 150 for programming keys to a vehicle to establish primary and secondary drivers in accordance to one embodiment of the present invention is shown. The system 150 includes the vehicle interface display 112, a passive entry passive start (PEPS) controller 152, and a backup slot 154. The PEPS controller 152 may be used in place of the PATS controller 116 as illustrated in FIG. 2A. While FIG. 2B generally illustrates that the PEPS controller 152 is positioned external to the vehicle interface display 112, other such implementations may include positioning the PEPS controller 152 within the vehicle interface display 112 or within any other such controller in the vehicle. The particular placement of the PEPS controller 152 may vary based on the desired criteria of a particular implementation.

EX1008 (Hatton), 9:4-17

Kleve, Hatton Combination Fails to Render Claims Obvious

Hatton: Vehicle PEPS & PATS Controllers with Encrypted Data

Prior to starting the vehicle, the key/mobile device serial number and the encrypted data are compared to known key/mobile numbers and/or encrypted data in a PEPS look up table in a manner similar to that described in connection with FIG. 2A. The manufacturing code is also checked to ensure the key/mobile device is used for a particular manufacturer of the vehicle. The PEPS LUT may be similar to the PATS LUT as shown in Table 1 and Table 2. As noted above, additional operations are performed as exhibited with the handshaking exercise in addition to matching the data received on the signal KEY_ID with the data in the LUT (e.g., key serial number and encryption data) to ensure that the user is properly authorized to enter the vehicle and to start the vehicle with the PEPS implementation. As noted above in connection

EX1008 (Hatton), 9:50-63

Kleve, Hatton Combination Teaches Authentication

Hatton Teaches Encrypted Data Is Assigned to a Vehicle During Manufacturing

The LUT in the PATS controller **116** assigns all of the keys and/or the associated mobile device as primary keys when the vehicle is manufactured in a default condition. The PATS controller **116** may update the key status for a key number in response to the driver changing the key status for a particular key via operations performed between the primary driver and the vehicle interface display **112** and/or configuring the software application **126** on the mobile device **124**. In another exemplary embodiment, the vehicle interface display **112** updates and changes may be communicated to the mobile device **124** software application **126** using the communication established between the mobile device **124** and VCS.

EX1008 (Hatton), 8:24-36

At step **302**, the vehicle key may be embedded with security codes associated with the vehicle during manufacturing and/or at a vehicle dealership. A user may initiate the transmission of the security codes from the vehicle key to a handheld device by pressing one or more buttons on the vehicle key at step **304**. To initiate a vehicle key for transmission of security codes may be a combination of button inputs received and recognized by the integrated circuit as the authorization to begin transmission of codes. For example, the authorization to begin transmission of security codes from the integrated circuit on the vehicle key may be the holding down of one or more buttons for a predefined amount of time.

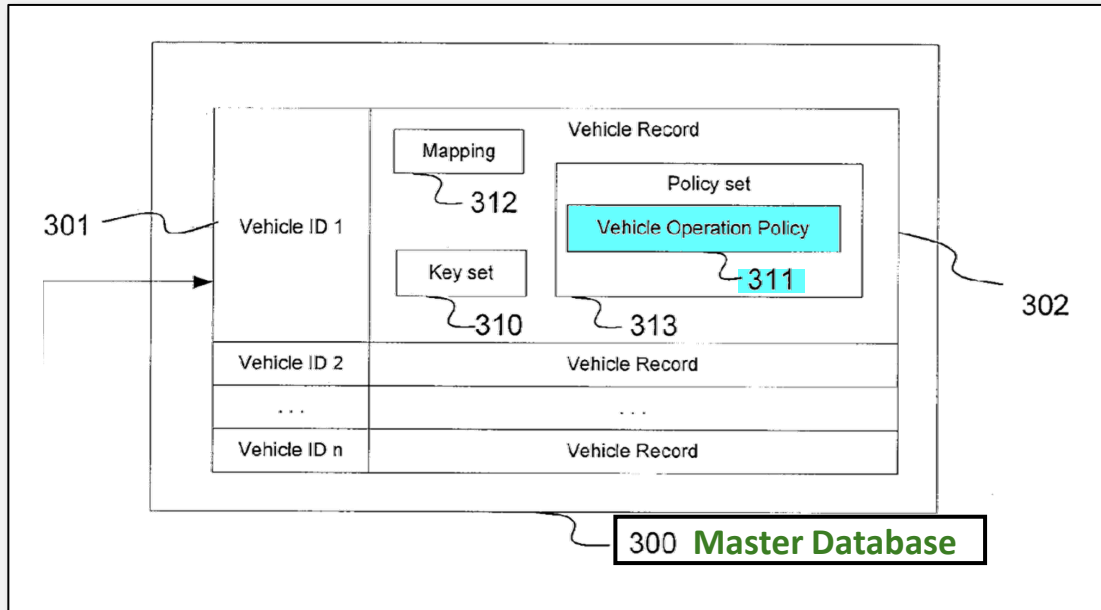
EX1008 (Hatton), 14:7-18

All Mikan-Based Grounds Fail to Disclose or Teach “Coded Data From the Mobile Device ... the Coded Data Includes Privilege Settings”

All Mikan-based grounds fail because:

1. Petitioners failed to show any disclosure or teaching of **coded data from the mobile device that includes privilege settings**
2. Petitioners’ relied upon disclosures for the alleged **coded data**—the wireless device’s secure ID—is used only for authentication and does not include any privilege settings
3. Petitioners’ relied upon disclosures for the alleged **privilege settings**—vehicle operation policy—are stored only in the master database and/or vehicle’s local database, not stored in the wireless device or at any time received from the wireless device, let alone in any **“coded data from the mobile device”**
4. Petitioners’ theories to modify **vitiates existing efficiencies in Mikan’s unmodified system** - Petitioners’ modifications render the data **more vulnerable to tampering**

All Mikan-Based Grounds Fail to Disclose or Teach “Coded Data From the Mobile Device ... the Coded Data Includes Privilege Settings”



EX1007 (Mikan), Fig. 3A

[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.

EX1007 (Mikan), ¶ 58

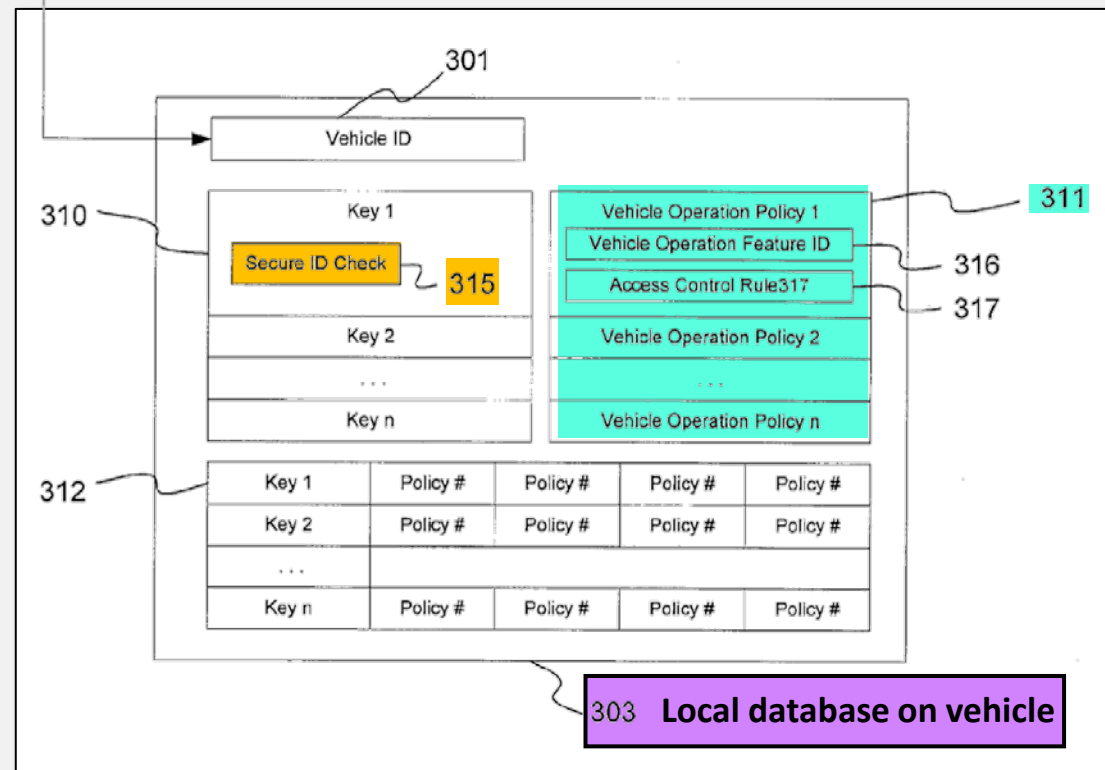
All Mikan-Based Grounds Fail to Disclose or Teach “Coded Data From the Mobile Device ... the Coded Data Includes Privilege Settings”

[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

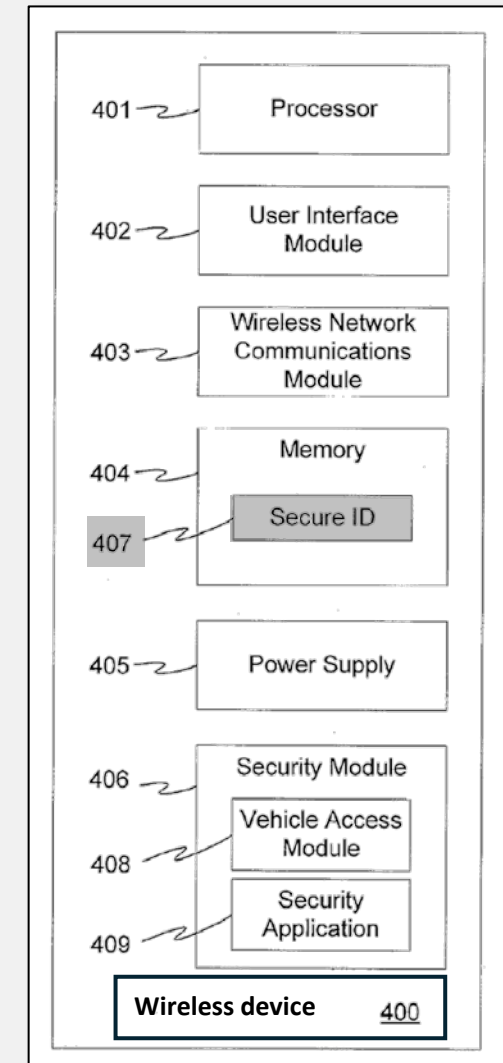
related vehicle operation feature. Access control rule 317 may include advanced criteria relating to the manner and conditions under which the vehicle may be operated. For example, access control rule 317 may establish a maximum acceleration for the vehicle, a maximum distance traveled for the vehicle, a range of time within which the vehicle may be operated, a geographic range within which the vehicle may be operated and the like. 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.

All Mikan-Based Grounds Fail to Disclose or Teach “Coded Data From the Mobile Device ... the Coded Data Includes Privilege Settings”

The alleged “data” the vehicle receives from the wireless device is “secure ID 407” (right)—by contrast, it is the vehicle’s local database (left) which includes a “secure ID 315” associated with the key set, as well as the records of vehicle operation policies 311. Id., ¶¶ 59, 64, Figs. 3B, 4.

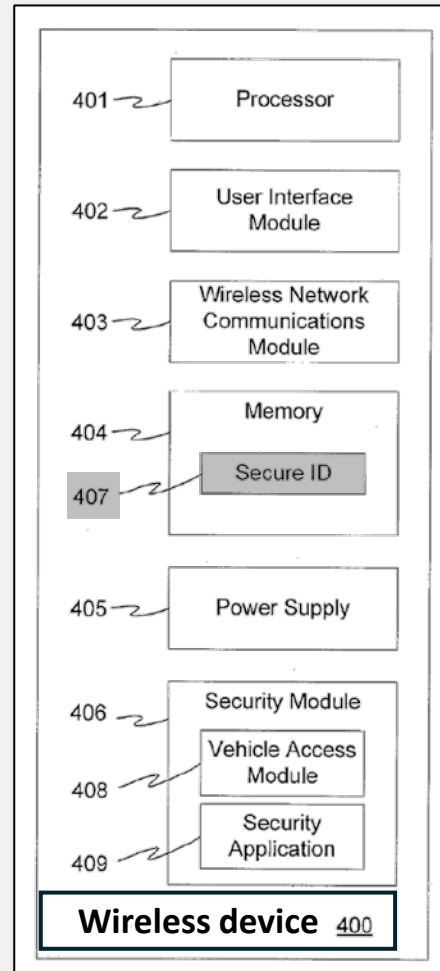


EX1007 (Mikan), Fig. 3B

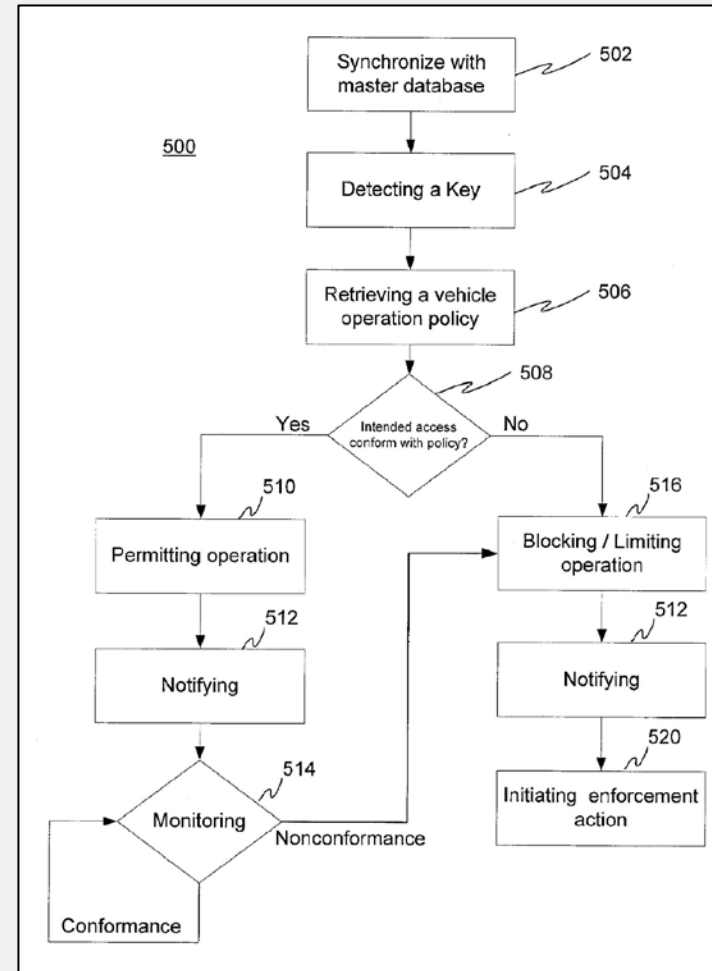


EX1007 (Mikan), Fig. 4

Mikan's Alleged Coded Data, Secure ID 407, Does Not Include Any Privilege Settings



EX1007 (Mikan), Fig. 4



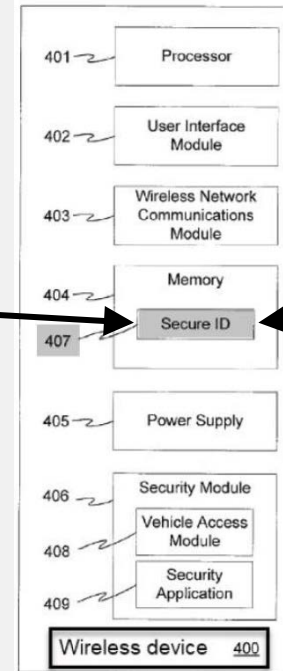
EX1007 (Mikan), Fig. 5

Mikan's Alleged Coded Data, Secure ID 407, Does Not Include Any Privilege Settings

Mikan's phone includes secure ID 407, which is merely used by the vehicle to authenticate the key

[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.



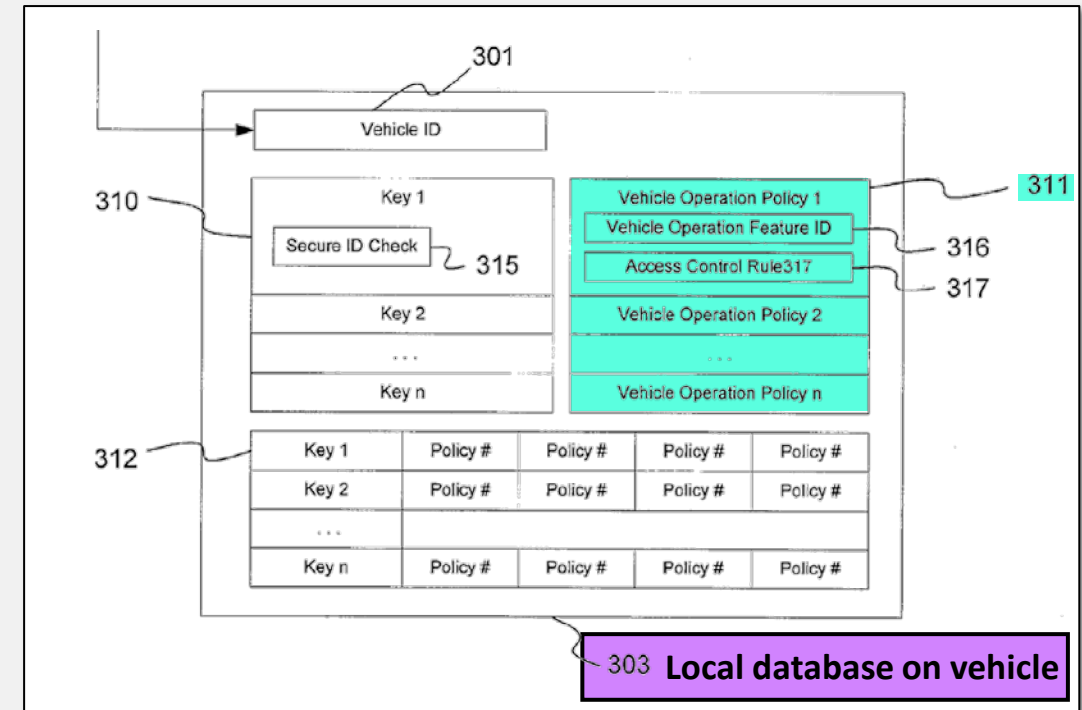
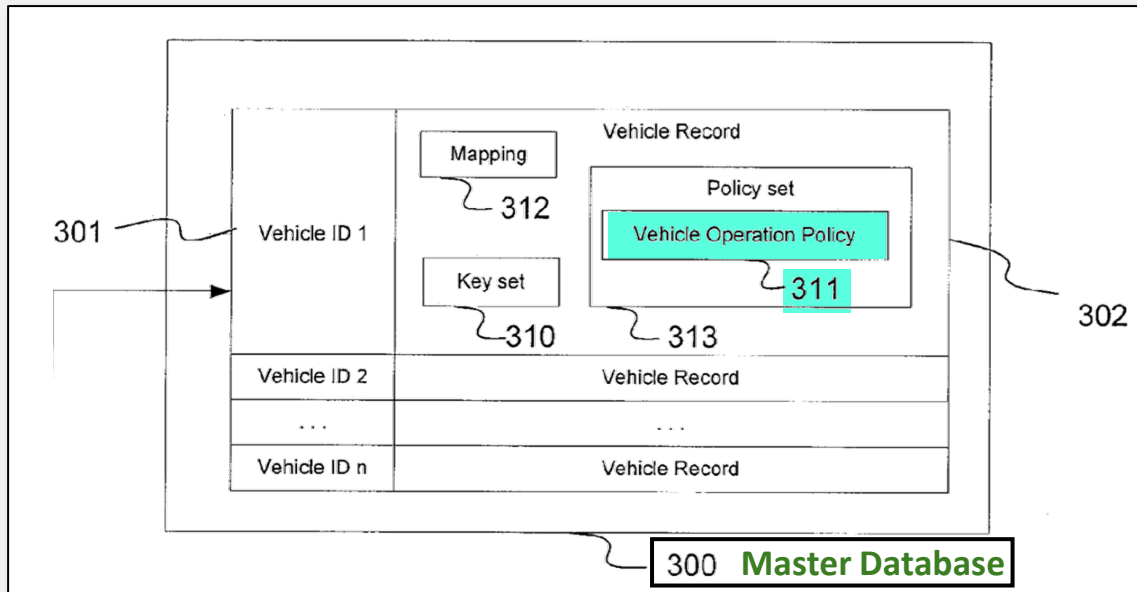
[0065] Memory 404 may be a subsystem suitable for storing and retrieving data. Memory 404 may be random access memory (RAM) or read only memory (ROM), or the like. In one embodiment, memory 404 may provide non-volatile storage of secure identifier 407 of wireless device 400. In another embodiment, memory 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).



FIG. 3B

Mikan's Vehicle Operation Policy is Never Received From a Mobile Device

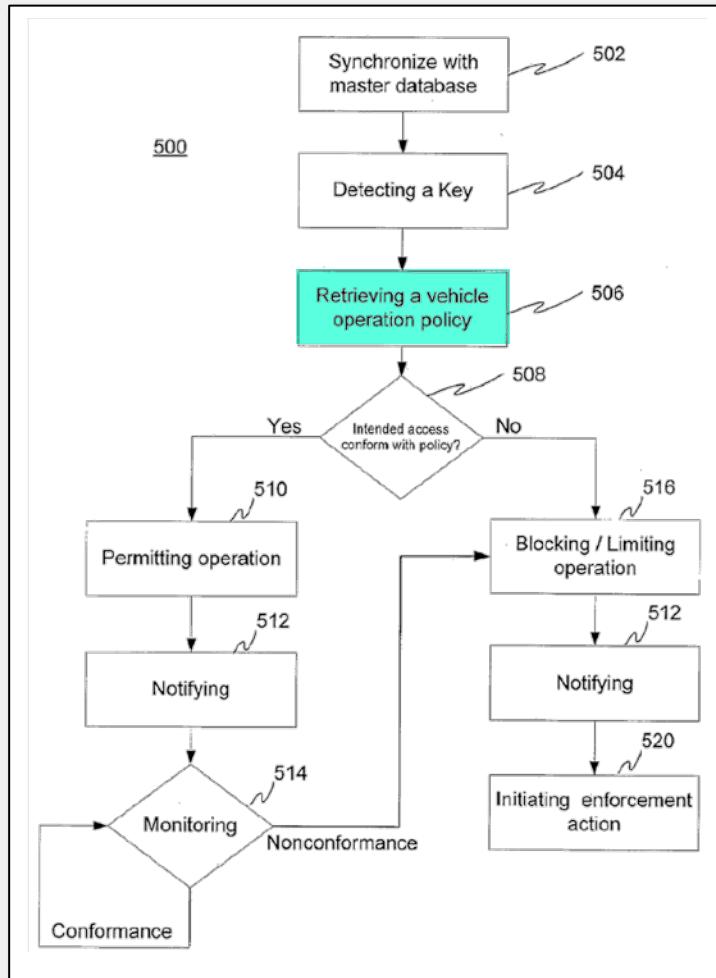
- Mikan teaches that the master database and/or local database store any vehicle operation policy
- The local database of the vehicle is kept consistent with records of the master database through synchronization
- Mikan never discloses the wireless device sending any vehicle operation policy to a vehicle
- Instead, after authentication the vehicle retrieves the policy from the vehicle itself



EX1007 (Mikan), Fig. 3A, 3B

Mikan's Vehicle Control Unit Processes Any Access Request Based on Locally-Retrieved Vehicle Operation Policy

- Mikan's vehicle never receives any alleged privilege setting "from the mobile device"
- Mikan's vehicle **control unit 202** processes access requests using the locally stored operation policy



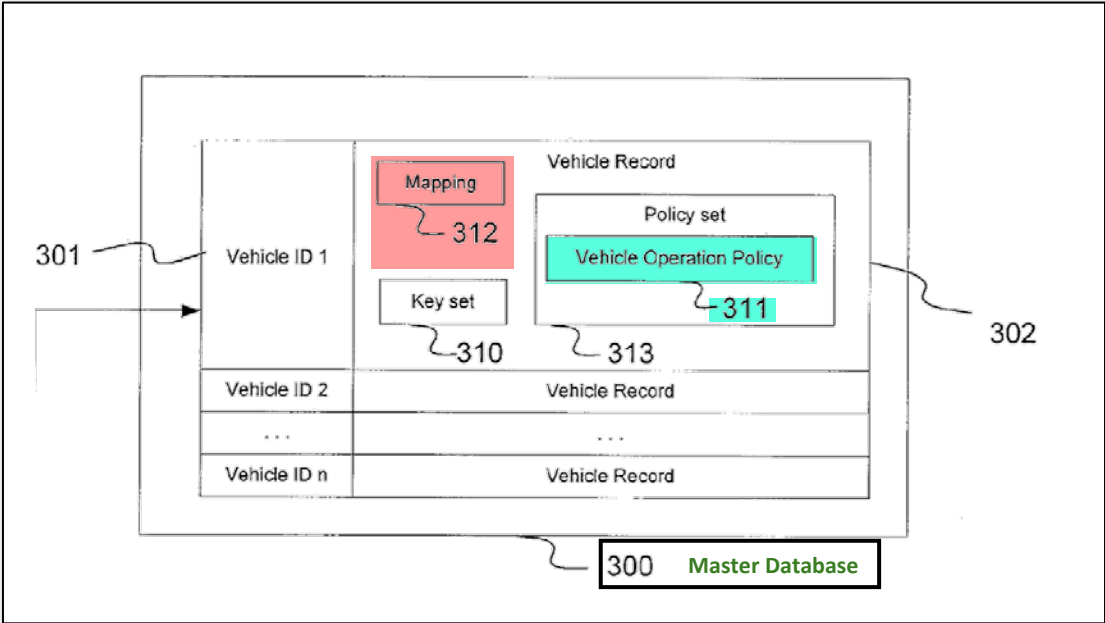
[0074] At 508, control unit 202 may process the access request and compare the access request with retrieved vehicle operation policy 311. Where the access request is consistent with retrieved vehicle operation policy 311, control unit 202 may permit the operation of the vehicle at 510. Where the access 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.

EX1007 (Mikan), ¶ 74

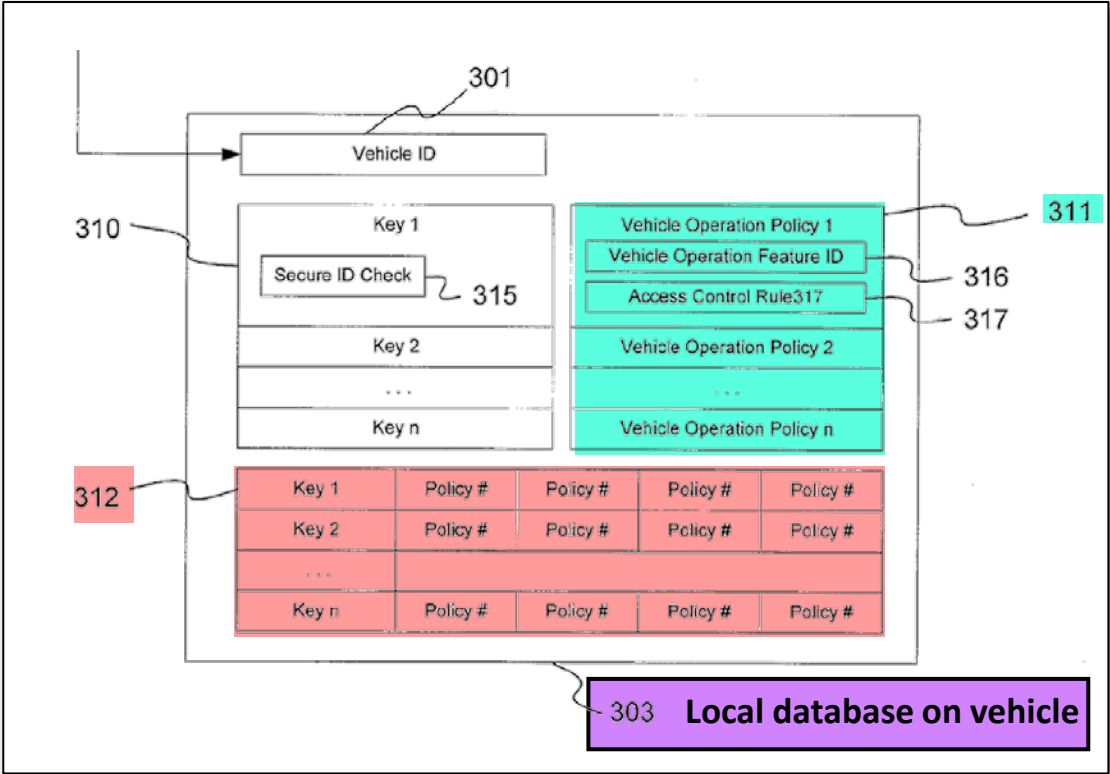
EX1007 (Mikan), Fig. 5

Mikan’s Vehicle Operation Policy—the Alleged “Privilege Settings”—are Stored in the Master and/or Vehicle Local Database, Linked by Mapping Function—Not Received From Any Mobile Device

- Mikan’s vehicle never receives any alleged privilege setting “from the mobile device”
- Master database has mapping function to link vehicle operation policy to vehicle keys
- Vehicle’s local database has mapping function to link vehicle-stored vehicle operation policies to vehicle-stored key set



EX1007 (Mikan), Fig. 3A



EX1007 (Mikan), Fig. 3B

Petitioners' Proposed Modifications to Mikan Undermine Security and Efficiencies of Existing System and Would In Fact Render Mikan *More Vulnerable to Tampering*

131. I also disagree with Dr. Almeroth's statement that a POSITA would 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." EX1004, ¶ 221. But Mikan does not disclose any such transmission. Indeed, by retrieving the vehicle operation policy 311 records from its local database 203, the vehicle need not rely on the "transmission" of any vehicle operation policy from the wireless device.

EX2021, ¶ 131

132. I also disagree with Dr. Almeroth's proposed modification of Mikan "to transmit the vehicle operation policy" "either as part of or in addition to Mikan's secure identifier." EX1004, ¶¶ 221-222. It would not make sense to make such a modification, since doing so would render Mikan's local database and its synchronization with the master database superfluous. The point of having a local database and synchronizing it with the master database in Mikan is to then use it for retrieving the vehicle operation policy. Mikan discloses an efficient solution, where vehicle operation policy changes are communicated to a vehicle as part of the synchronization process. Therefore, each policy change is communicated only once. A POSITA would not have modified Mikan as proposed by Dr. Almeroth because they would have realized it would make the system less efficient. In the modified system, the vehicle operation policy would need to be sent every time the wireless device is used to enter the vehicle, even if there has been no change to the vehicle operation policy.

EX2021, ¶ 132

Petitioners' Proposed Modifications to Mikan Undermine Security and Efficiencies of Existing System and Would In Fact Render Mikan *More Vulnerable to Tampering*

133. I also disagree with Dr. Almeroth's *proposed motivation* "to transmit the vehicle operation policy" "either as part of or in addition to Mikan's secure identifier," since Dr. Almeroth's proposed modification actually renders the vehicle operation policy records *more* vulnerable to "tampering" by the user, not less.

EX1004, ¶¶ 221-222. Mikan teaches that the wireless device does not transmit to the vehicle any vehicle operation policy that limits the types of use of the vehicle when the vehicle is accessed using the electronic key. By modifying Mikan to not only include such vehicle operation policy records in the user's wireless device itself, but also to have the user transmit the vehicle operation policies via the wireless device, would inject *additional security vulnerabilities* into Mikan's system. As I discussed in Section X.C., above, Dr. Almeroth's concern about tampering and unauthorized access actually demonstrates why it would not have been obvious to modify Mikan to include vehicle operation policies as part of Mikan's "secure ID 407" because including the vehicle operation policies on the wireless device and having that device transmit those policies leads to an additional point of security vulnerability and would provide a wireless device user an opportunity to modify his or her own device to tamper with privilege settings.

EX2021, ¶ 133

Petitioners' Proposed Modifications to Mikan Undermine Security and Efficiencies of Existing System and Would In Fact Render Mikan *More Vulnerable to Tampering*

134. As I discussed above, the vehicle operation policies are not sent to the vehicle from the wireless device. Instead, the local database of the vehicle synchronizes with the master database, then when the vehicle detects a key, the vehicle retrieves vehicle operation policy records from its own local database.

EX2021, ¶ 134

135. While Dr. Almeroth provides no sufficient reason why a POSITA would have modified Mikan to instead have the wireless device send to the vehicle with the device's secure ID 407 vehicle operation policies, a POSITA would understand that making such a modification (not taught by the reference) would be undesirable. By having the wireless device send vehicle operation policies to the vehicle, the wireless device user would have an opportunity to "tamper" with or gain "unauthorized access" to the vehicle operation policies—the reason Dr. Almeroth proposed to do so. EX1004, ¶¶ 111, 221. A POSITA would understand Mikan to already avoid the problems that Dr. Almeroth identified: as the wireless device does not ever send vehicle operation policies to the vehicle in Mikan, the wireless device user cannot tamper with or gain unauthorized access to those vehicle operation policies.

EX2021, ¶ 135

Petitioners' Proposed Modifications to Mikan Undermine Existing Solutions of Mikan's System

[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.

EX1007 (Mikan), ¶ 85

Claim 6 Must be Upheld, as Neither Kleve Nor Mikan Discloses the Required “Application ... Configured to Enable Sharing of Said eKey”

- Petitioners fail to show disclosure or suggestion of an application enabling eKey sharing via a message from the mobile device.

6. The sub-system of the vehicle of claim 1, wherein an application associated with said mobile device is configured to enable sharing of said eKey with a recipient user having a recipient mobile device, the sharing is enabled via a message initiated from said mobile device.

EX1001 ('659 Patent), Claim 6

Claim 6 Must be Upheld, as Kleve Does Not Teach, and Actually Discourages, a Temporary User Sharing a Virtual Key with Another User

- Kleve highlights the Vehicle Owner has the sole ability to exercise complete control over their vehicle.

[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.

EX1005 (Kleve), ¶ 40

[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.

EX1005 (Kleve), ¶ 51

Claim 6 Must be Upheld, as Kleve Does Not Teach, and Actually Discourages, a Temporary User Sharing a Virtual Key with Another User

- Kleve highlights the Vehicle Owner's ability to exercise complete control over their asset.

[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.

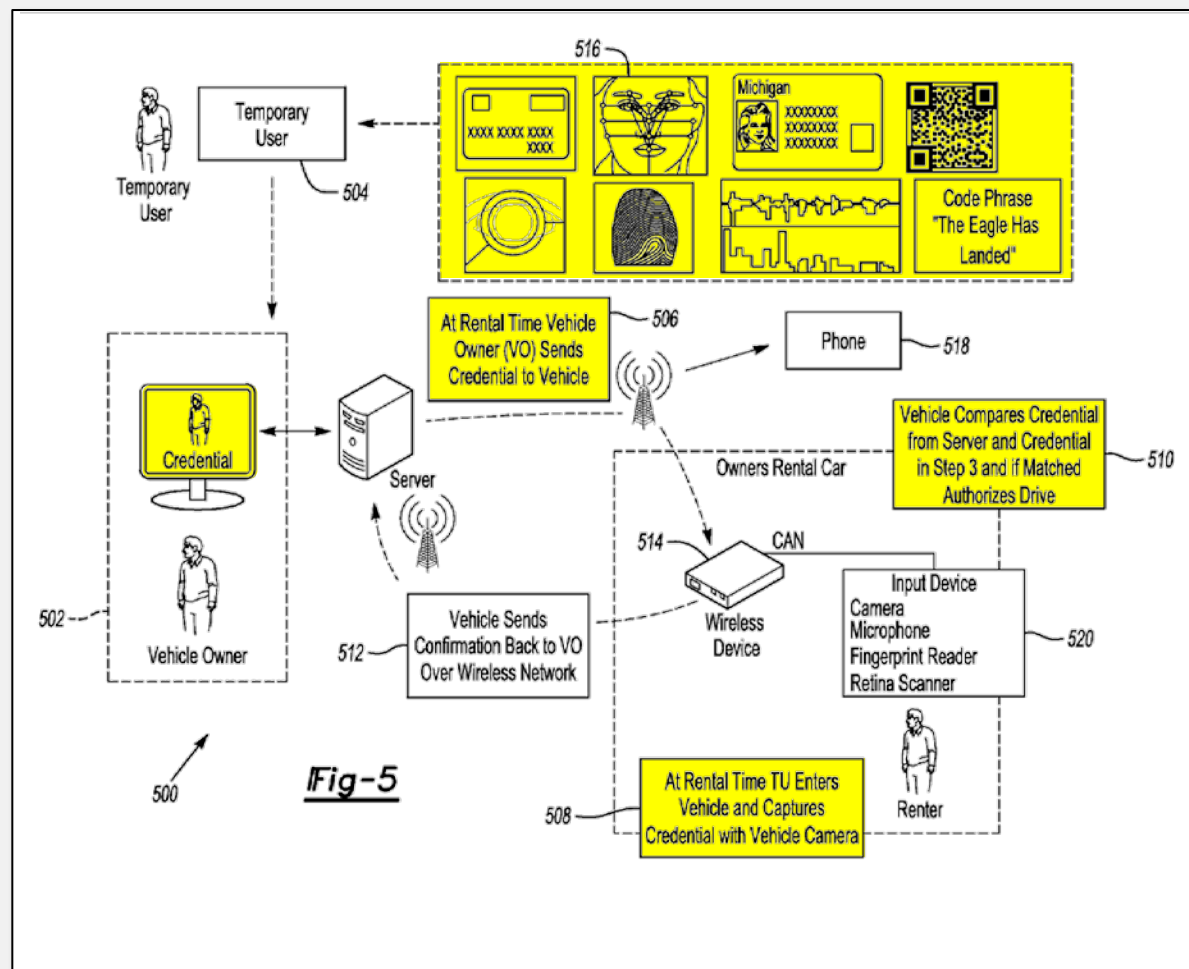
EX1005 (Kleve), ¶ 43

[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.

EX1005 (Kleve), ¶ 75

Claim 6 Must be Upheld, as Kleve Does Not Teach, and Actually Discourages, a Temporary User Sharing a Virtual Key with Another User

- Kleve teaches that at rental time the Owner sends the credential to the vehicle, and the Temporary User enters their credential at the vehicle.



EX1005 (Kleve), Fig. 5

[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.

Claim 6 Must be Upheld, as Kleve Does Not Teach, and Actually Discourages, a Temporary User Sharing a Virtual Key with Another User

- **Kleve discourages allowing a Temporary User—whose use is monitored and controlled by the Owner— to share an e-Key with others.**

137. In my opinion, Petitioners and Dr. Almeroth failed to show that any reference discloses or suggests claim 6's recited "application associated with said mobile device is configured to enable sharing of said eKey with a recipient user having a recipient mobile device, the sharing is enabled via a message initiated from said mobile device." EX1001, claim 6.

EX2021, ¶ 137

138. I disagree with Dr. Almeroth's opinion that it would have been obvious that the smartphone application of Kleve "may also be used to enable multiple authorized temporary users to share virtual keys with each other." In fact, Kleve teaches the opposite. As I discussed in Section V, above, Kleve teaches specific features to allow the Vehicle Owner, and the Vehicle Owner alone, full control over the usage of their vehicle, "as this may be the only vehicle the Owner possesses." EX1005, ¶ 51. Kleve highlights the Vehicle Owner's ability to exercise complete control over their asset, e.g. disclosing a solution by which the Owner can set user restrictions, which will be monitored and controlled by the vehicle's VCS, thereby providing the Owner with notifications of the vehicle's usage and any violations of set user restrictions. Kleve also teaches that even after a virtual key is distributed to the Temporary User, the Vehicle Owner sends the "credential" to the vehicle "at rental time," and, "at rental time," the Temporary User inputs their "credential" at the vehicle. *Id.*, Fig. 5, ¶ 66. That is, the vehicle must compare and confirm a "match" between these two credentials before authorizing the Temporary User's drive. *Id.*

EX2021, ¶ 138

Patent Owner Response at pp. 79-82 | 63

Claim 6 Must be Upheld, as Kleve Does Not Teach, and Actually Discourages, a Temporary User Sharing a Virtual Key with Another User

Petitioners fail to explain how one user's unique Temporary User ID could be altered to activate the vehicle for another, given that Kleve's user identifiers are individual-specific, and fail to provide any motivation or expectation of success for such modification.

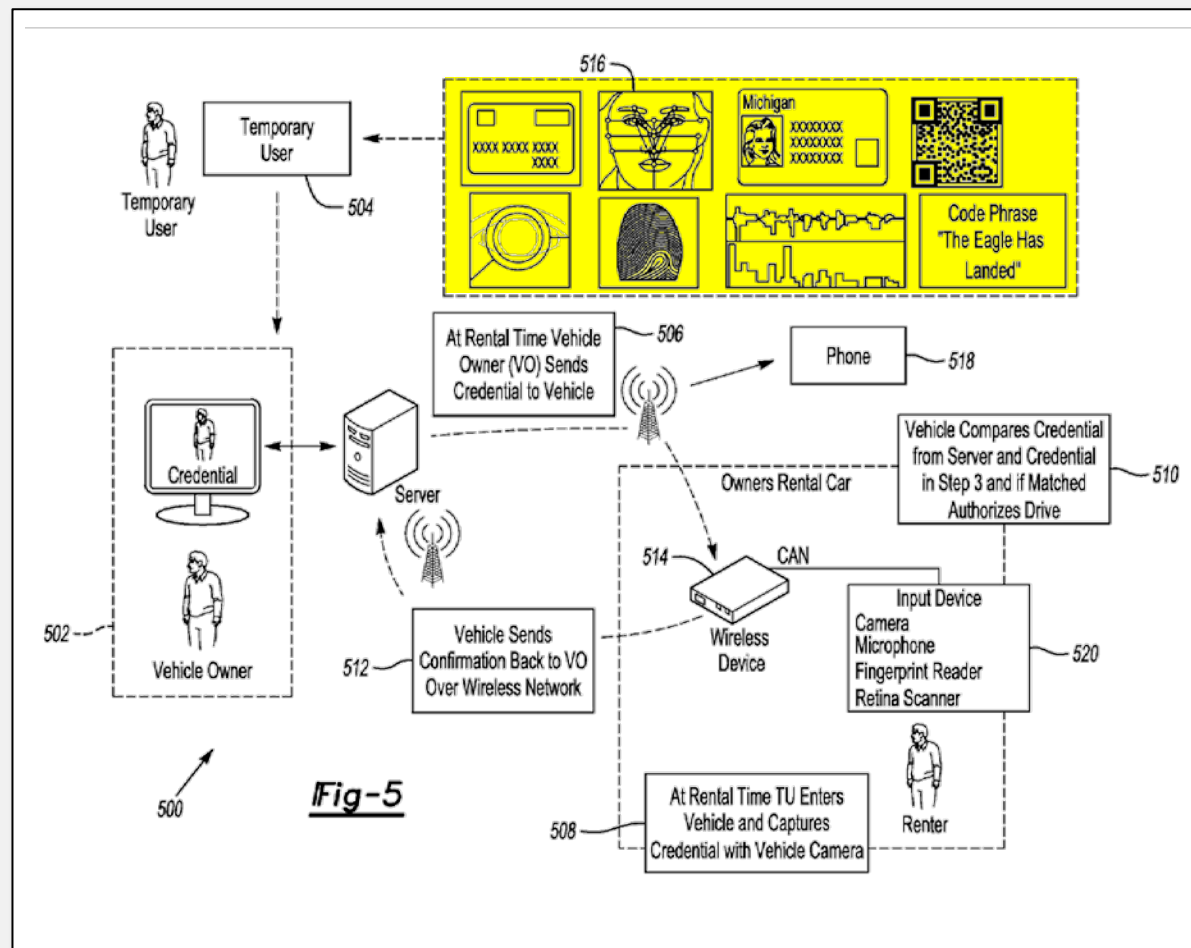
[0069] FIG. 6 is an exemplary embodiment of the vehicle rental micro-business distributing and controlling virtual keys using a nomadic device with a vehicle. The vehicle rental micro-business administrative system may consist of a computer system configured to host one or more websites for interaction 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.

[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.

EX1005 (Kleve), ¶ 37

Claim 6 Must be Upheld, as Kleve Does Not Teach, and Actually Discourages, a Temporary User Sharing a Virtual Key with Another User

Petitioners fail to explain how one user's unique Temporary User ID could be altered to activate the vehicle for another, given that Kleve's user identifiers are individual-specific, or provide any motivation or expectation of success for such modification.



[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.

EX1005 (Kleve), ¶ 63

EX1005 (Kleve), Fig. 5

Claim 6 Must be Upheld Because Mikan Limits Each Phone Having Only One “Secure ID 407”

- Mikan does not teach that multiple electronic keys can be incorporated into mobile devices for vehicle use
- Each wireless device has its own secure ID 407, which is transmitted to the vehicle for authentication.

140. I also disagree that Mikan teaches a “plurality of electronic keys may be incorporated into mobile devices for use with a vehicle.” Pet. 65. Instead, each wireless device includes its own “secure ID 407,” and it is this “secure ID 407” that is transmitted to the vehicle for authentication. EX1007, ¶ 65. Because Mikan’s secure ID 407 does not include any privilege settings, as I discussed in Section XI above, the Petition’s proposed combination with Sekiyama does not cure Mikan’s failure to disclose or suggest coded data from the mobile device that includes privilege settings. Therefore, any sharing of the key, as proposed in this combination, would nonetheless lack the requisite privilege settings included in coded data.

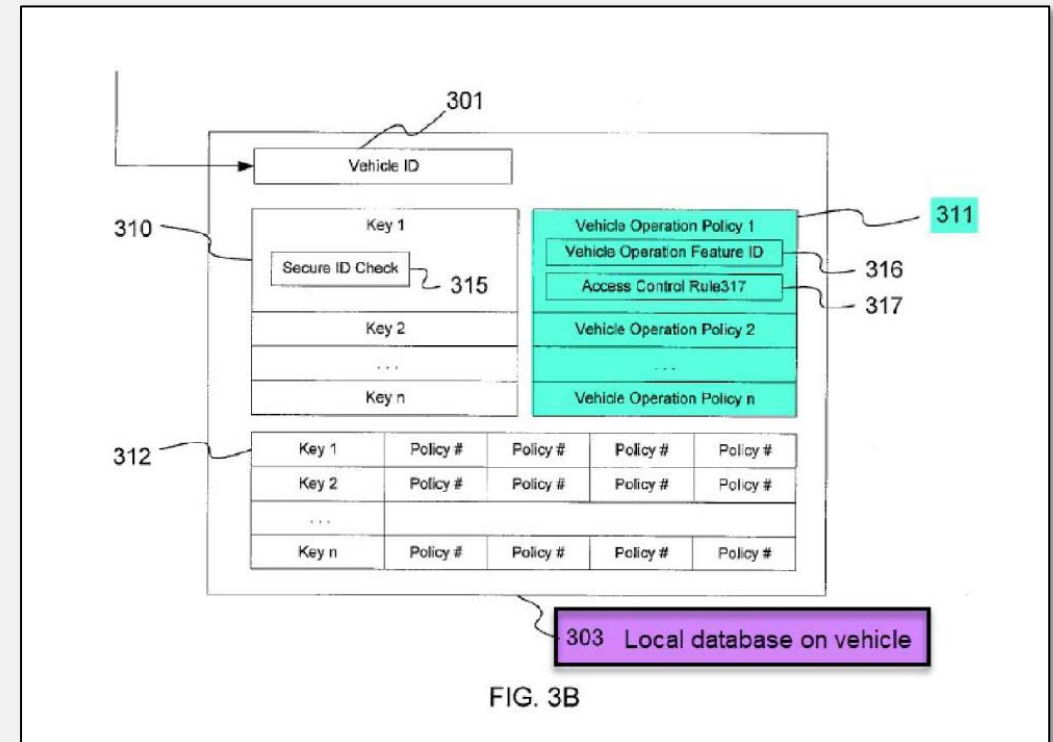
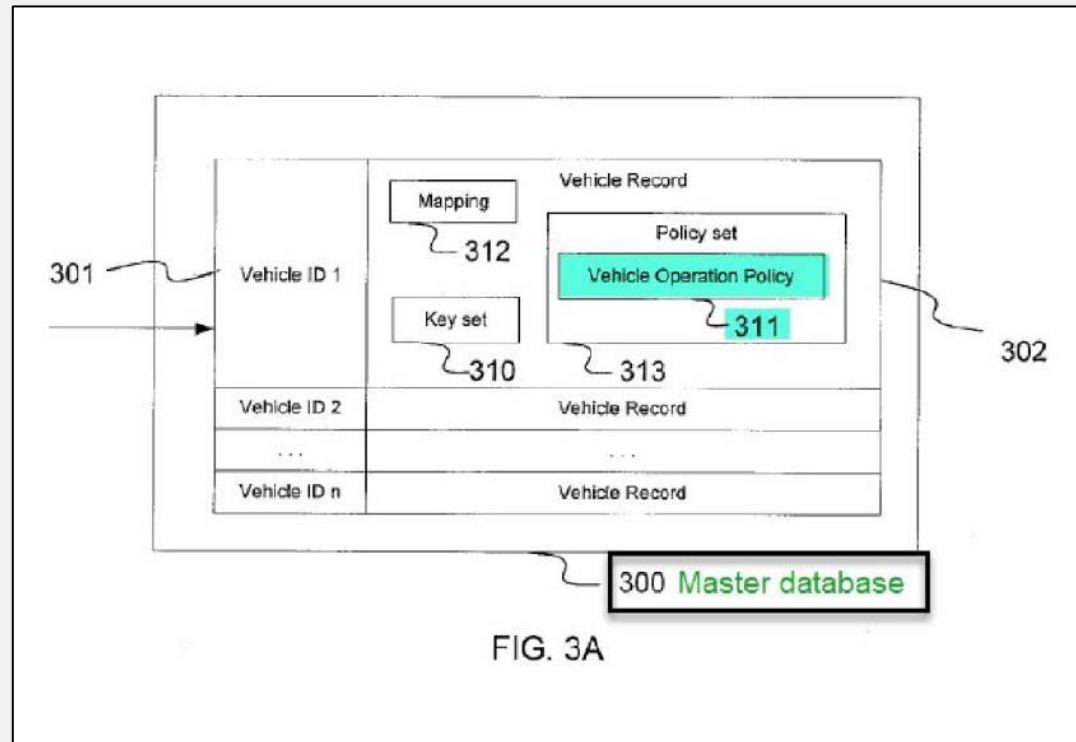
EX2021, ¶ 140

[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).

EX1007 (Mikan), ¶ 65

Claim 6 Must be Upheld Because Any Key Sharing Would Still Lack Privilege Settings

- Mikan's vehicle operation policy is stored only in the Master Database or Local Database
- The user's phone does not store or transmit any privilege settings
- When phone used as key, vehicle retrieves policy from its own local database



EX1007 (Mikan), Figs. 3A-3B, ¶¶ 58-59, 72, 81

Claims 12, 13 and 20 Must be Upheld as Petitioners Failed to Meet their Burden

Petitioners failed to meet their threshold burden on claims 12, 13, and 20 because:

- Petitioners failed to show any reference discloses or suggests the recited “**server associated with a manufacturer of a vehicle**”
- Petitioners likewise failed to show any reference discloses or suggests the recited mobile device application being “**associated with a manufacturer of the vehicle**”
- Petitioners failed to meet the threshold inquiry of the “printed matter doctrine”



“printed matter must be matter claimed for what it communicates.”

C R Bard Inc. v. AngioDynamics, Inc., 979 F.3d 1372 (Fed. Cir. 2020)

Claims 12, 13 and 20 Must be Upheld as Petitioners Failed to Meet their Burden

- Despite Petitioners' burden, the server and application associated with the vehicle manufacturer don't implicate the printed matter doctrine, as the specification shows their functional connection to other system components.

In one embodiment, certain third-party applications can be reviewed by the vehicle site administrators before they are made available to users for selection. In other embodiments, the third-party applications can be approved or disapproved. In still other embodiments, the third-party applications can be augmented with restrictions made by the vehicle manufacturer, or dictated by law. The restrictions can be applied, based on the anticipated interfacing with the vehicle interfaces, to ensure safety during driving. For instance, if a particular application requires entry of text, navigation of controls, or other activities that would distract the driver during operation of the vehicle, such vehicle controls or application controls for application interfaces can be temporarily disabled, or can be automatically transferred to a heads up display, or can switch to take audio vocal input from the user. In some embodiments, when the vehicle has come to a stop or is place to park, certain controls or interfaces can be re-enabled, or moved back to original display location or converted back from voice input to touch input. In one embodiment, tools provided by the vehicle site or third-party site can provide for customization of the layout of the display screens of the user interface.

EX1001 ('659 Patent), 15:15-37

In one embodiment, the functions of the specific applications illustrated in the display will be monitored and restricted depending on safety considerations while driving. For example, if the interfacing functionality requires more interactivity with the display, or requires a reading of text or inputting text, those functions will be disabled during operation of the vehicle. Once the vehicle comes to a stop, or is placed in Park, certain of these functions will be activated. In other embodiments, other safety considerations will allow for applications to shift from outputting text to outputting audio or voice. The input can also be changed from touch-screen, button touches, selections, and/or voice input. In still other embodiments, safety considerations can allow certain user interface components to move about the display to provide easier reading while driving or automatic conversion of text to audio.

For example, content being displayed in the center panel display of the vehicle, can be automatically shown in the dashboard display region of the vehicle, such as in front of the steering wheel. In still other embodiments, some content or display data can be moved from the center console or the display in front of the steering wheel to the windshield of the vehicle in a heads-up display area. Accordingly, algorithms executed by the applications and applications of the manufacturer, can cooperate to provide functionality to the application features and interfaces, while maintaining safety parameters defined by rules. The safety parameters will therefore allow content of the user interface to be shifted around to various displays of the vehicle, or translated to voice or audio at certain points in time.

EX1001 ('659 Patent),
13:20-49

Claims 12, 13 and 20 Must be Upheld as Petitioners Failed to Meet their Burden

- Despite Petitioners' burden, the server and application associated with the vehicle manufacturer don't implicate the printed matter doctrine, as the specification shows their functional connection to other system components.

These settings and customizations can be made through the web/cloud services and tools provided by the website of, for example the manufacturer of the vehicle. In one embodiment, the cloud services provided by the manufacturer can be provided by a partner of the manufacturer. The partners of the manufacturer can include software companies that develop, host, or manage certain functionality provided by the vehicle manufacturer. In other embodiments, the partner software companies can integrate tools or components with tools and components of the vehicle manufacturer. This provides for integration with one or more cloud services, software services, Internet services, and services provided by systems of vehicles or systems of the vehicle manufacturer. In either case, whether the software and logic is designed and constructed by one or more entities, the cloud services provided by the vehicle manufacturer or the website that provides the tools for customization will appear as a unified simple to use interface for the user. As mentioned above, the cloud services can provide databases for saving the user profile and data associated with the user account.

EX1001 ('659 Patent), 13:50-14:2

For security purposes, e-keys are generated at a server, which may be managed by a server to execute cloud services. The server may receive requests from registered users who may wish to assign e-keys to some individual or entity. The request is associated to the user account, as managed by the service. If the user has multiple vehicles, the request may further include identification of the vehicle, such as CAR-A or CAR-B, etc. At the server, the server is configured to execute the generation of access codes for a particular request. The access codes can be uniquely generated by the server, for each received request. In one embodiment, the access code format or form is set, so that a vehicle knows what to expect and reject access codes that do not meet the format or form. Once the access code is generated for the request, the access code is encrypted using a public key of the vehicle, which is assigned a public/private key pair.

In one embodiment, the public/private key pair can be re-generated from time to time, if the user feels that a security breach has taken place. Usually, however, one public/private key pair may serve for a life of a vehicle. The server keeps and maintains the public key and the private key is stored in storage/memory of the electronics of the vehicle. Although traditional encryption may make the public key freely available, in one embodiment, the public key is only referred to as "public" for purposes of defining the encryption logic, but preferably the public key is kept private or securely held by the server. The private key can be stored or programmed when the vehicle is registered with a service or at any other time, when the public/private key pair are re-generated for security purposes. The transfer of the private key to the vehicle can take place over any wired or wireless network, or by transfer via some connector, plug, memory card, thumb drive, etc. In any event, the private key is stored and kept secure by the vehicle.

EX1001 ('659 Patent),
47:35-48:2