

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

TOYOTA MOTOR CORP. AND KIA CORPORATION,
Petitioners,

v.

EMERGING AUTOMOTIVE LLC,
Patent Owner

Case IPR2024-01167
U.S. Patent No. 11,738,659

**PATENT OWNER'S
RESPONSE
UNDER 37 C.F.R. §42.107**

TABLE OF CONTENTS

	<u>Page</u>
I. Introduction.....	1
II. The '659 patent.....	3
III. <i>Kleve</i> (EX1005) discloses distinct operations for (1) forming a rental agreement, (2) setting up and distributing a virtual key, and finally, (3) setting user restrictions—available to only a Vehicle Owner and only at the beginning of the rental term, after the virtual key has been sent to the vehicle.	5
A. <i>Kleve</i> 's “terms and conditions for the rental period” reflect the agreed-to terms of a rental contract and are independent of any “virtual key.”	6
B. Neither the “set up” of a virtual key nor the distribution of a virtual key includes the rental agreement terms or any other restrictions.	9
C. To monitor and control vehicle usage, a Vehicle Owner may independently “set user restrictions”—an operation distinct from the rental agreement and “set up” and distribution of a virtual key credential.....	13
1. <i>Kleve</i> allows restrictions for monitoring and controlling usage to be set by the Owner at the beginning of the rental term.	14
2. “Rental period end time” is set by the Owner as a “user restriction” at step 214 which may be monitored, controlled, and even updated by returning to step 214.....	18
D. <i>Kleve</i> 's virtual key credential is operable independent of the agreed-upon rental period; the virtual key may be terminated before, or remain in use after, the agreed-upon rental period has ended.	21
IV. Petitioners failed to show that the challenged claims of grounds 1-2 are obvious over <i>Kleve</i> , alone or in combination.	26

A.	Each of the “restrictions” identified by Petitioners as alleged “privilege settings” are unavailable to be set until <i>after</i> the set up and distribution of the alleged “coded data,” a virtual key, and are thus not included in the coded data.	29
B.	<i>Kleve</i> flatly contradicts the conclusion that “rental agreement restrictions were sent with the request.”	42
C.	That a virtual key credential enables the keyless drive system during a given rental period does not suggest the “rental period” is included in the virtual key itself.	43
1.	Rental agreement terms are not included in the virtual key because a Temporary User uses the already-generated, already-distributed virtual key to access the vehicle and thereafter, “agree to rental terms.”	44
2.	<i>Kleve</i> cannot enforce compliance with rental agreement terms until after the virtual key is generated and distributed, where a Temporary User may “agree to rental terms” after accessing the vehicle with the virtual key.	45
3.	During cross examination, Dr. Almeroth admitted that <i>Kleve</i> ’s virtual key is not “always generated after the rental agreement.”	47
4.	<i>Kleve</i> has the Vehicle Owner send the “virtual key” to the vehicle “at rental time.”	48
5.	<i>Kleve</i> teaches a distinct solution for monitoring, controlling and updating the rental period—one that does not involve any such “restriction” in the virtual key itself.	49
6.	Dr. Almeroth’s obviousness opinions ignore and even contradict <i>Kleve</i> ’s solution for enforcing rental agreement terms and conditions.....	51
a.	Dr. Almeroth ignores the security of the enforcement solution already achieved by <i>Kleve</i> ’s steps 214-226.	51

b.	<i>Kleve</i> ’s solution renders nonsensical Dr. Almeroth’s hindsight demands to include rental agreement restrictions in the virtual key.	52
D.	It would not have been obvious to combine <i>Kleve</i> and <i>Hatton</i> as Petitioners propose.	54
V.	The <i>Mikan</i> Reference (EX1007).....	58
VI.	All challenged claims in grounds 3-6 must be upheld because <i>Mikan</i> ’s vehicle never “receives coded data from the mobile device ... the coded data includes privilege settings,” as claimed.	67
A.	Petitioners rely on a mobile device’s “secure ID 407” as alleged coded data, but the secure ID 407 does not include any alleged privilege settings.	69
B.	<i>Mikan</i> does not disclose, and discourages, a vehicle receiving any privilege settings from a mobile device.	73
C.	Dr. Almeroth’s opinions ignore and even contradict <i>Mikan</i> ’s solution to retrieve locally stored vehicle operation policies from the vehicle’s local database.	75
1.	The wireless device does not include or transmit to a vehicle any “associated vehicle operation policy,” as Dr. Almeroth suggests.	76
2.	Modifying <i>Mikan</i> “to transmit the vehicle operation policy as additional coded data, either as a part or in addition to <i>Mikan</i> ’s secure identifier” renders the data more vulnerable to “tampering,” not less, and vitiates existing efficiencies in <i>Mikan</i> ’s unmodified system.	77
VII.	The Petition’s additional deficiencies with respect to the dependent claims.	79
VIII.	Conclusion	82

TABLE OF AUTHORITIES

Page(s)

Cases

<i>C R Bard Inc. v. AngioDynamics, Inc.</i> , 979 F.3d 1372 (Fed. Cir. 2020).....	81
<i>In re Dow Chem. Co.</i> , 837 F.2d 469 (Fed. Cir. 1988).....	52
<i>In re Oetiker</i> , 977 F.2d 1443 (Fed. Cir. 1992).....	52, 78
<i>In re Ratti</i> , 270 F.2d 810 (CCPA 1959)	54
<i>Opticon Medical AB v. Cochlear Limited</i> , IPR2019-00975 (P.T.A.B. Oct. 14, 2020)	52, 79

Patent Owner's Updated Exhibit List	
EX2001	Declaration of Dr. Sam Malek
EX2002	<i>Curriculum Vitae</i> of Dr. Malek
EX2003	<i>Reserved</i>
EX2004	Cover pleading to Defendants' Preliminary Invalidity Contentions, <i>Emerging Automotive LLC v. Kia Corporation, et. al., and Toyota Motor Corp. et al.</i> , No. 2:23-cv-0437-JRG (lead case), No. 2:23-cv-0434-JRG (member case), served March 28, 2024
EX2005	<i>Reserved</i>
EX2006	Judicial Caseload Profile (June 30, 2024): Table C-5, <i>U.S. District Courts—Civil Federal Judicial Caseload Statistics</i> ; Table T-3, <i>U.S. District Courts—Median Time from Filings to Trial for Civil Cases in which Trials were Completed</i>
EX2007	Civil Docket Report for <i>Emerging Automotive LLC v. Kia Corporation, et. al., and Toyota Motor Corp. et al.</i> , No. 2:23-cv-0437-JRG (lead case)
EX2008	Civil Docket Report for <i>Emerging Automotive LLC v. Toyota Motor Corp. et al.</i> , No. 2:23-cv-0434-JRG (member case)
EX2009	U.S. Patent No. 11,295,564
EX2010	<i>Reserved</i>
EX2011	Related Applications Search results for US Patent 11,295,564 from United States Patent Office Global Dossier Public Access Portal
EX2012	U.S. Patent No. 10,493,953
EX2013	U.S. Patent No. 10,614,644
EX2014	U.S. Patent No. 11,094,149
EX2015	<i>Reserved</i>

EX2016	Docket Navigator Median Time-to-Trial Statistics for Judge Rodney Gilstrap (excluding transfers), August 26, 2019 through August 26, 2024
EX2017	Unified Patents, LLC Request for <i>Ex Parte</i> Reexamination of U.S. Patent No. 11,738,659 (Mar. 25, 2024)
EX2018	Unified Patents Website, Members Section, available at https://www.unifiedpatents.com/members
EX2019	Office Action in <i>Ex Parte</i> Reexamination, Application Number 90/019,456 (Sept. 4, 2024)
EX2020	Office Action Response Remarks from Robert B. Kleve (Aug. 14, 2014)
EX2021	Declaration of Dr. Sam Malek in Support of Patent Owner's Response
EX2022	Deposition Transcript of Kevin C. Almeroth, Ph.D., taken April 1, 2025 in <i>Toyota Motor Corp. & Kia Corp. v. Emerging Automotive, LLC</i> , IPR2024-01167 (Excerpted)

I. Introduction

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

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

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

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

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

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

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

II. The ’659 patent

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

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

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

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

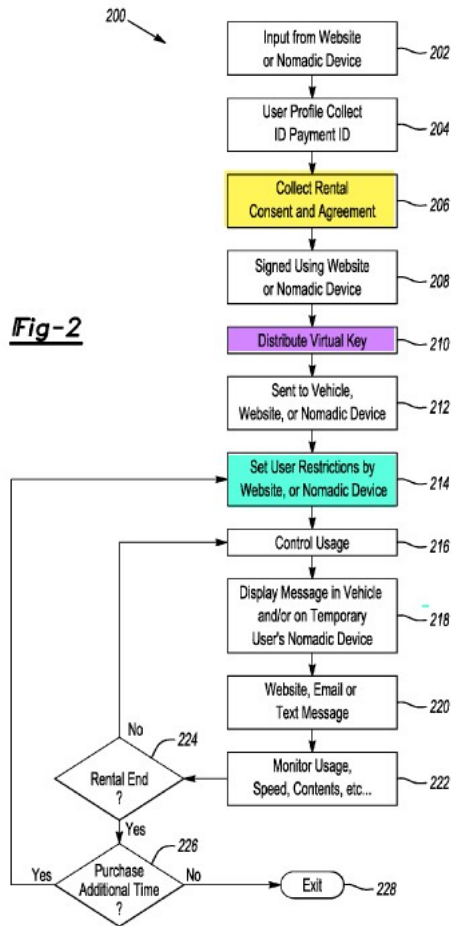
Kleve discloses a system to “check” a “credential” and use that “credential” as the “authorization” or “virtual key” for use of a “personal vehicle rental.” EX1005, face page, ¶ 36. *Kleve* discloses that parties negotiate and form a rental contract, allowing the parties to exchange identifying information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

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

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

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

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



EX1005, Fig. 2 (annot.).

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

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

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

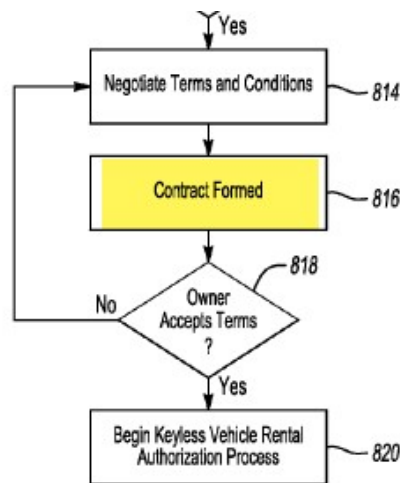


Fig-8

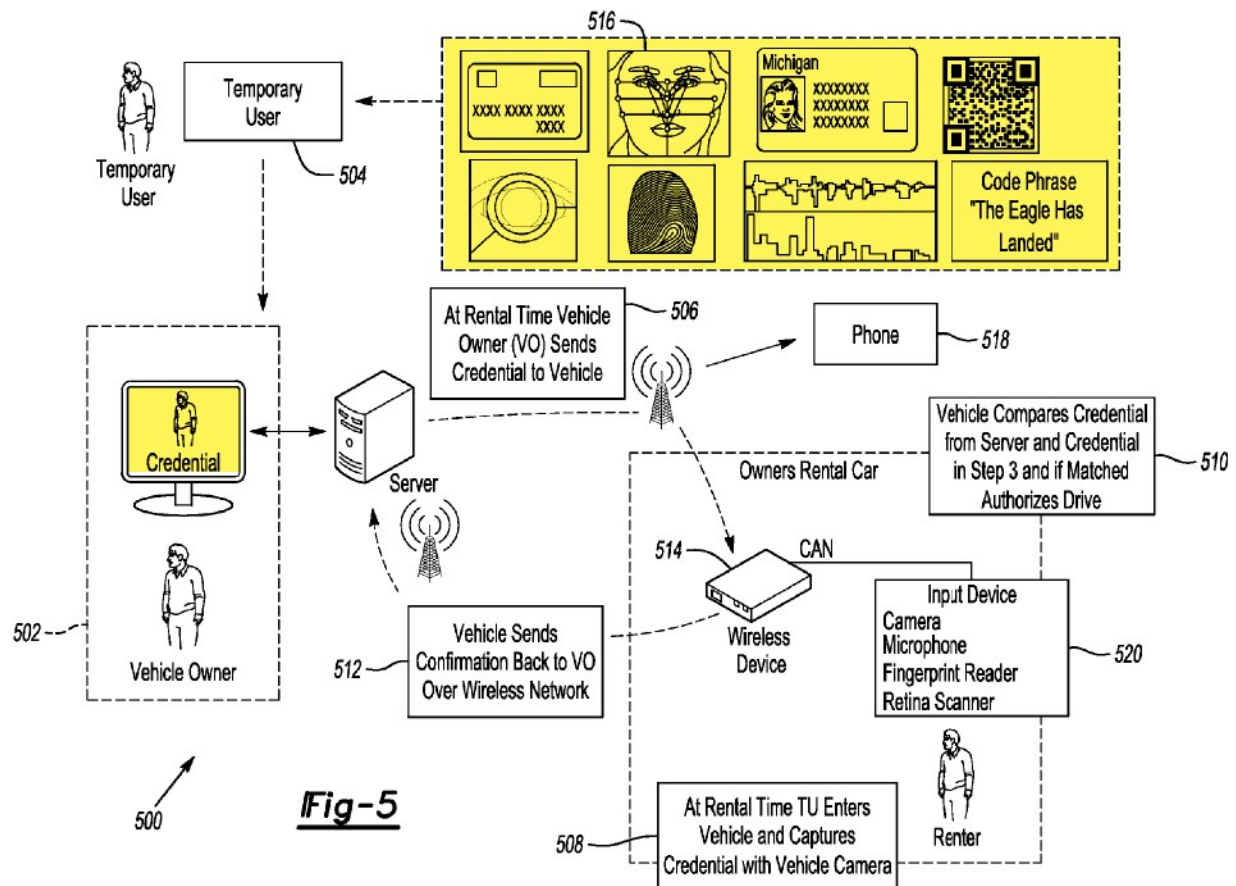
Id., Fig. 8 (annot.). Here, *Kleve* teaches nothing more than two parties forming an agreement. *Kleve* does not teach that the parties’ agreed-upon conditions are ever included in the set up or eventual distribution of a virtual key or provided to the

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

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

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

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

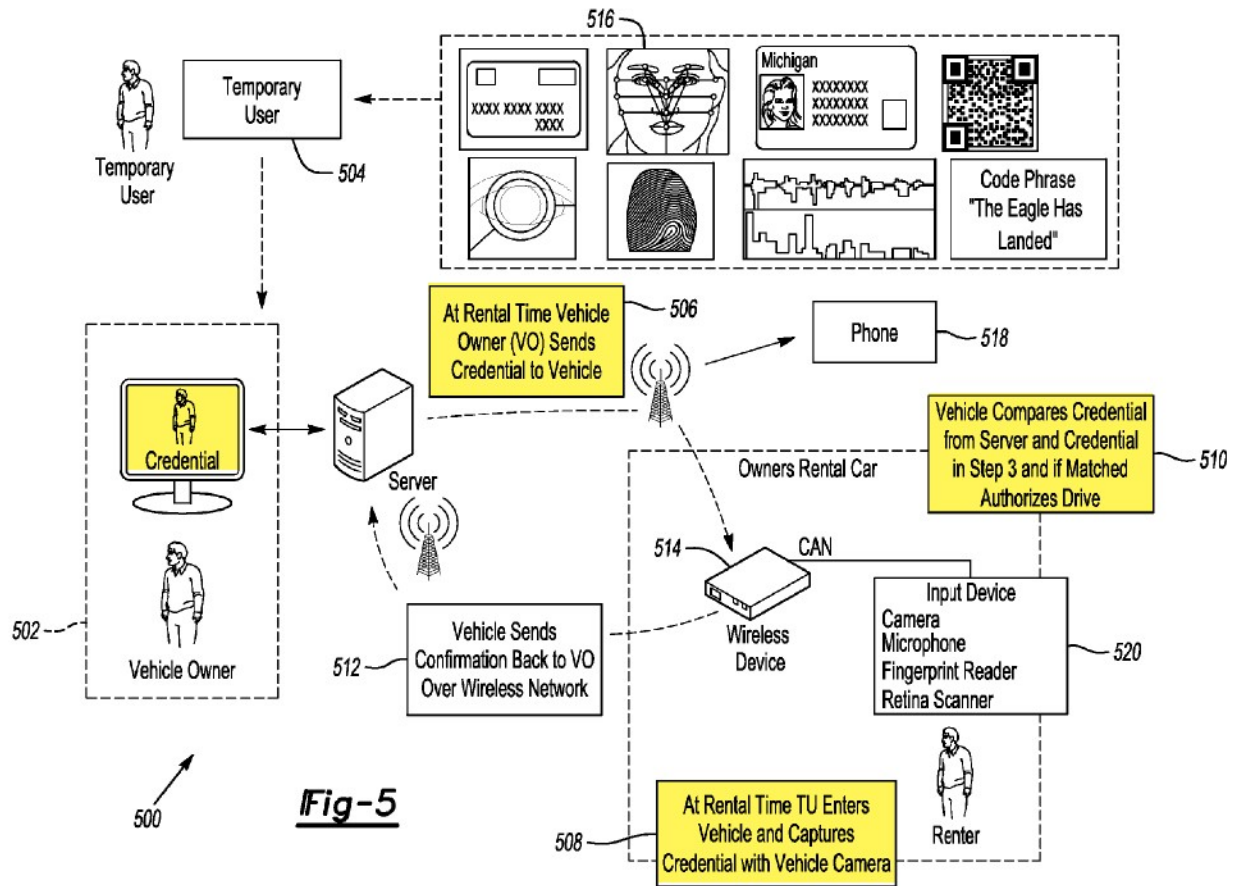


Id., Fig. 5 (annot.). This “credential” is the information collected from the Temporary User, such as “fingerprint recognition,” “photos of credit cards, photo of forms of ID, facial recognition, voice print recognition, matrix barcode [], code word or code phrase for speech recognition,” or “other types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

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

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

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



Id., Fig. 5 (annot.).

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

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

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

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

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

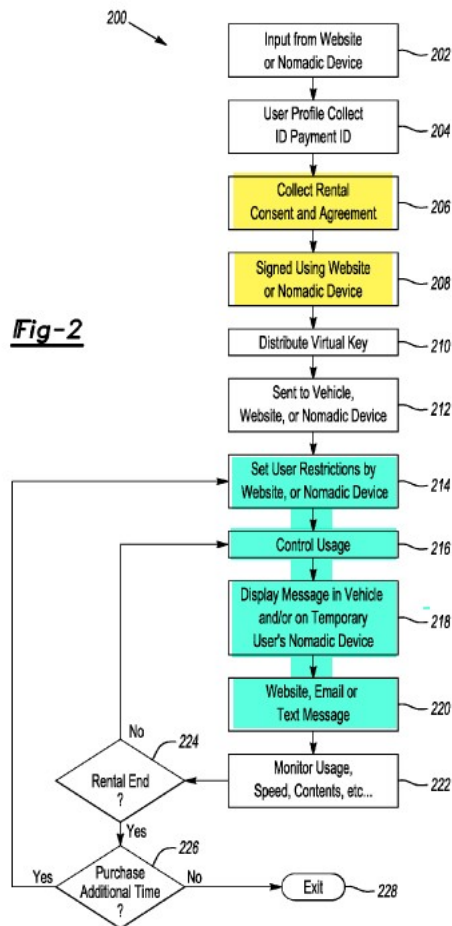
As *Kleve* explains, because a Vehicle Owner may be renting out a vehicle that “may be the only vehicle the Owner possesses,” “[c]ontrolling usage to enforce compliance with the rental agreement terms may be of more importance to a vehicle rental micro-business owner[.]” *Id.*, ¶ 51. Therefore, “at the beginning of the rental term,” *Kleve* provides the Vehicle Owner the option “to set rental restrictions,” which may be used by the vehicle’s VCS to “monitor,” “control” and/or “update” usage of the vehicle. *Id.*, ¶¶ 40-41, 43, 51.

1. *Kleve* allows restrictions for monitoring and controlling usage to be set by the Owner at the beginning of the rental term.

To enforce compliance with rental agreement terms or enforce any other user restrictions, *Kleve* makes clear that those vehicle restrictions may not be set when the rental agreement is formed, nor at any other time before the distribution of a virtual key. *Id.*, ¶¶ 51, 40, 43, 75, Figs. 2, 7A. Instead, these restrictions are “***initially set*** by the Owner at the beginning of the rental term,” which undisputably occurs after distribution of the virtual key credential, as discussed above. *Id.*, ¶ 43 (emphases added); *see also id.*, ¶ 40, Fig. 2. Because the Owner does not have the option to set rental restrictions until the beginning of the rental term at step 214—when those restrictions are “initially set”—neither the rental agreement terms themselves, nor the generation of a virtual key (each of which precedes the

distribution of the virtual key, at step 210) could possibly qualify as *Kleve*'s Owner-set restrictions. *Id.*, Fig. 2; ¶¶ 40-41, 43; EX2021, ¶¶ 46, 49-50.

Specifically, at **step 214**, shown in Figure 2 below, *Kleve*'s system allows the Owner to select parameters that enforce the parties' agreed-upon terms and conditions and/or add specific restrictions for the usage of the rental vehicle, such as cargo load weight restrictions, rental end time, or global position coordinates corresponding to restricted areas. *Id.* It would not be necessary for *Kleve* to have such a solution to "enforce" any rental agreement terms if somehow those terms were already included as some "privilege setting" in *Kleve*'s "set up," creation, or distribution of the virtual key, at step 210. EX1005, Fig. 2; ¶¶ 40-41, 43; EX2021, ¶¶ 48-50.



EX1005, Fig. 2 (annot.).

Likewise, it would not be necessary for *Kleve* to teach this distinct operation to “set user restrictions” at [step 214](#)—restrictions that may include *the very same restrictions* the parties had agreed to in [the rental agreement](#)—if somehow those rental agreement restrictions were already included as alleged “privilege settings” in *Kleve*’s creation or distribution of the virtual key, at step 210. *Id.*; *id.*, ¶¶ 84-85, 89-90, 40, 51; EX2021, ¶¶ 51-52.

For example, although the Vehicle Owner and Temporary User may have already agreed to specific “load weight restrictions” as part of the rental agreement (EX1005, ¶¶ 84-85, 89-90), *Kleve* provides for an Owner to “enforce” and “control” the agreed-upon “load weight restrictions” by separately inputting the “load weight restrictions” as “user restrictions” in the system’s website when the rental period begins (*id.*, ¶¶ 40, 51) (“owner may set user restrictions” e.g., “load weight restrictions”); EX2021, ¶¶ 51-53.

Kleve reiterates that these restrictions cannot be set when the rental agreement is formed, or at any point before the virtual key is distributed, but are instead “restrictions assigned by the Vehicle Owner *at the start of the rental period.*” EX1005, ¶ 75 (emphases added); ¶ 43 (“initially set by the Owner at the beginning of the rental term”). The restrictions’ corresponding “performance limitations” for the VCS to monitor and control the vehicle’s usage are downloaded to the VCS at step 708, after “the Temporary User initiates the rental event,” at step 706. *Id.*, ¶ 75, Fig. 7A.

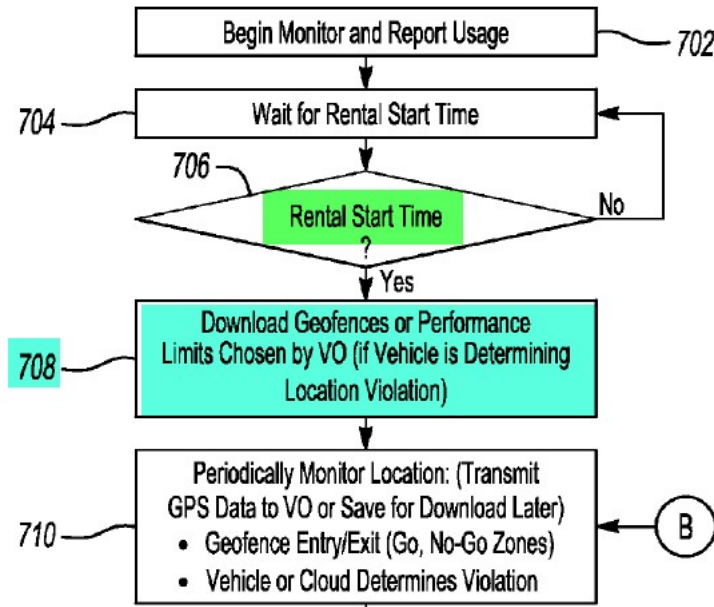


Fig-7A

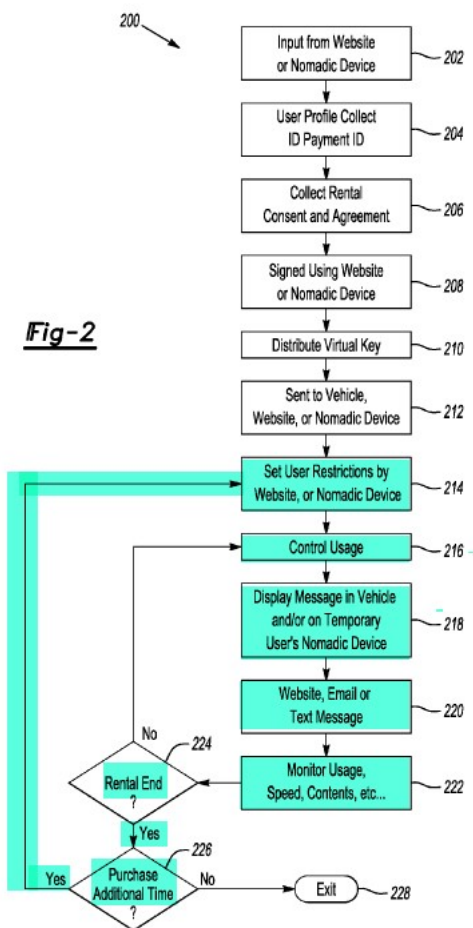
716

Id., Fig. 7A (annot.).

2. **“Rental period end time” is set by the Owner as a “user restriction” at step 214 which may be monitored, controlled, and even updated by returning to step 214.**

Kleve teaches that the “rental period end time” is one of the “user restrictions” which is set by the Owner at the beginning of the rental term, at step 214, where *Kleve*’s system enforces compliance with this restriction by monitoring usage of the vehicle, controlling actions to put the vehicle in a remedial action, and updating the rental period end time restriction. EX1005, ¶ 43. Specifically, “[a]t 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.” *Id.*, ¶¶ 43, 54; *see id.*, Fig. 2. Referring

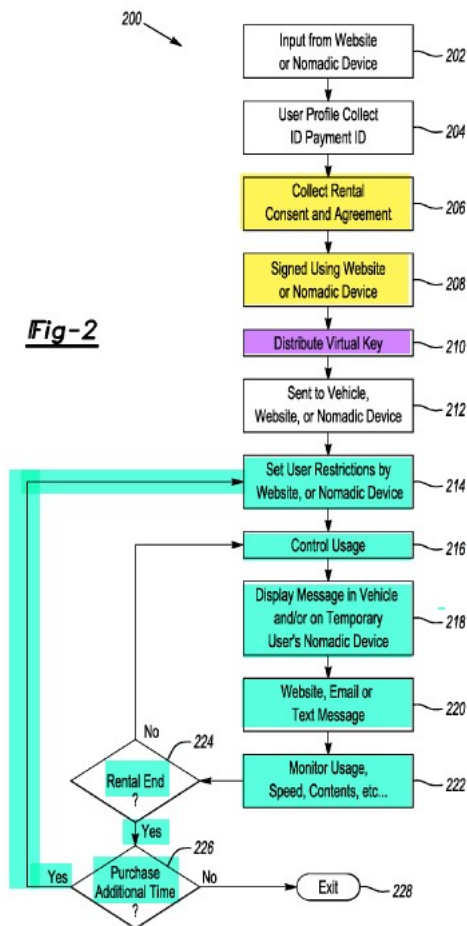
to Figure 2, the system will return to **step 214**, to “update the new rental period end time restriction.” *Id.*



Id., Fig. 2 (annot.).

Accordingly, *Kleve*’s system expressly links **step 214**, where the Vehicle Owner initially “set user restrictions,” with the updated “**new rental period end time restriction**” that has been extended by the user’s purchase at **step 226**. *Id.*, ¶¶ 43, 54, Fig. 2.

By contrast, *Kleve* offers no mechanism to “update” the rental period via the rental agreement (steps 206, 208) or the virtual key (step 210)—because *Kleve* teaches that only by the “user restrictions,” set at step 214, may rental agreement terms or other restrictions, such as rental time, be enforced or controlled. *Id.*



Id., Fig. 2 (annot.).

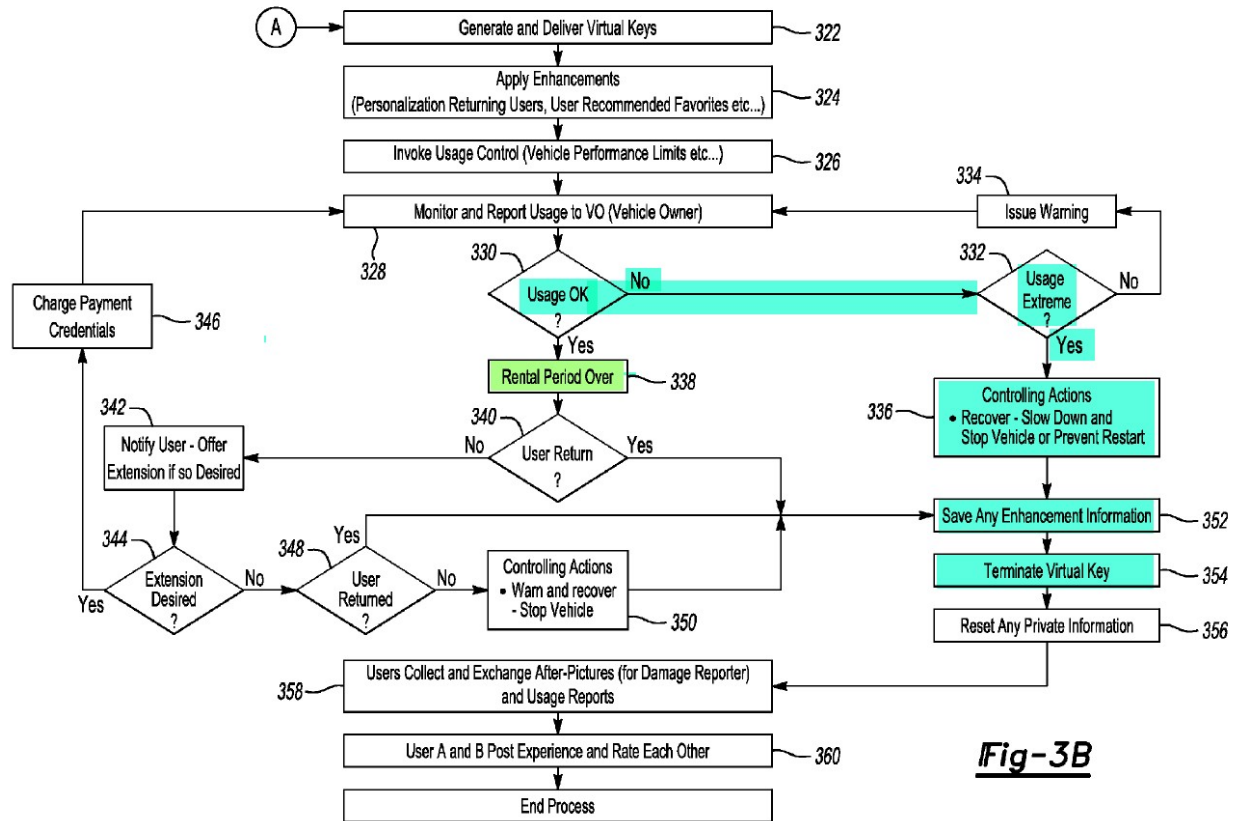
D. *Kleve*'s virtual key credential is operable independent of the agreed-upon rental period; the virtual key may be terminated before, or remain in use after, the agreed-upon rental period has ended.

As detailed in Section III.C., the virtual key is not only operable during the agreed-upon rental period; instead, *Kleve*'s system enables the Temporary User to extend the rental period “if the rental period has ended,” allowing the Vehicle Owner to update the “rental period end time restriction.” *Id.*, ¶ 43, Fig. 2. The virtual key is not only operable outside of the agreed-upon rental period, e.g., via a rental end time *update*, but may also be *terminated* either before or after the end of the agreed-upon rental period. EX2021, ¶ 54.

Kleve's system teaches several examples by which the vehicle rental “exit mode process,” which includes “terminating the virtual key” (EX1005, ¶ 80), is undertaken before or after the agreed-upon rental period expiration (*id.*, ¶¶ 43, 53-55, 79-80). These examples further demonstrate that the virtual key is *not* “only operable during a rental period.” Paper 14 at 37 (citing Pet. 15, EX1005, ¶ 83).

For example, if the Temporary User's usage of the vehicle exceeds the “user restrictions” set by the Vehicle Owner (e.g., EX1005, Fig. 2, step 214), the system may undertake remedial actions and terminate the virtual key—regardless of the parties' agreed-upon rental period. *Id.*, ¶ 53, Fig. 3B; EX2021, ¶¶ 55-56. As *Kleve* explains, if “a restriction threshold has been violated,” and the usage is “extreme,”

the VCS may “put the vehicle in a remedial action,” such as engine shut down and immobilization. EX1005, ¶ 53, Fig. 3B. The system will then “save any enhancement information” and “terminate [the] virtual key,” regardless of whether the agreed-to rental period has ended. *Id.* As illustrated in Figure 3B, the detection of “extreme” usage prompts the system to “terminate virtual key,” even before the “rental period [is] over.” *Id.*



Id., Fig. 3B.

As another example, if the vehicle detects an accident which renders the vehicle unsafe to drive, *Kleve*’s system will undertake the same vehicle rental exit

mode process, thereby terminating the virtual key—independent of “rental end” time. *Id.*, ¶¶ 79-80, 53, Fig. 7B; EX2021, ¶ 57.

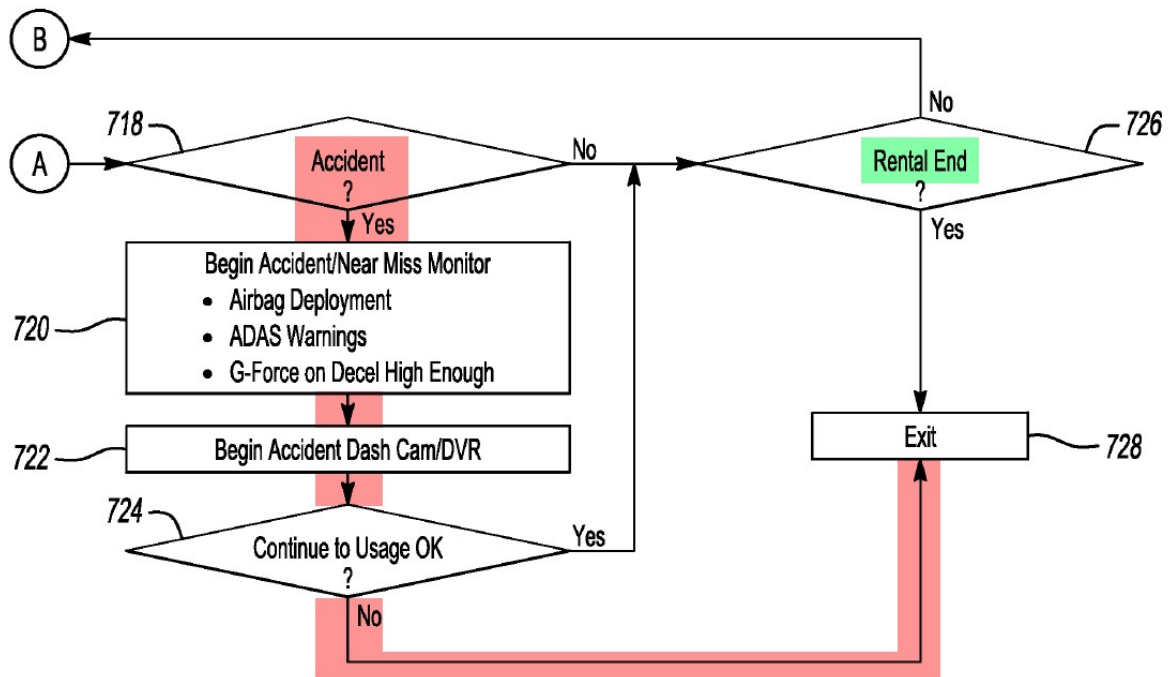
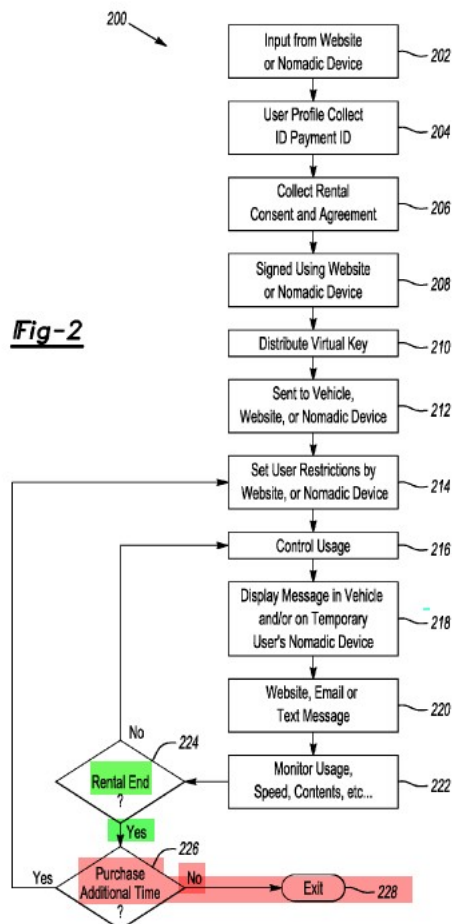


Fig-7B

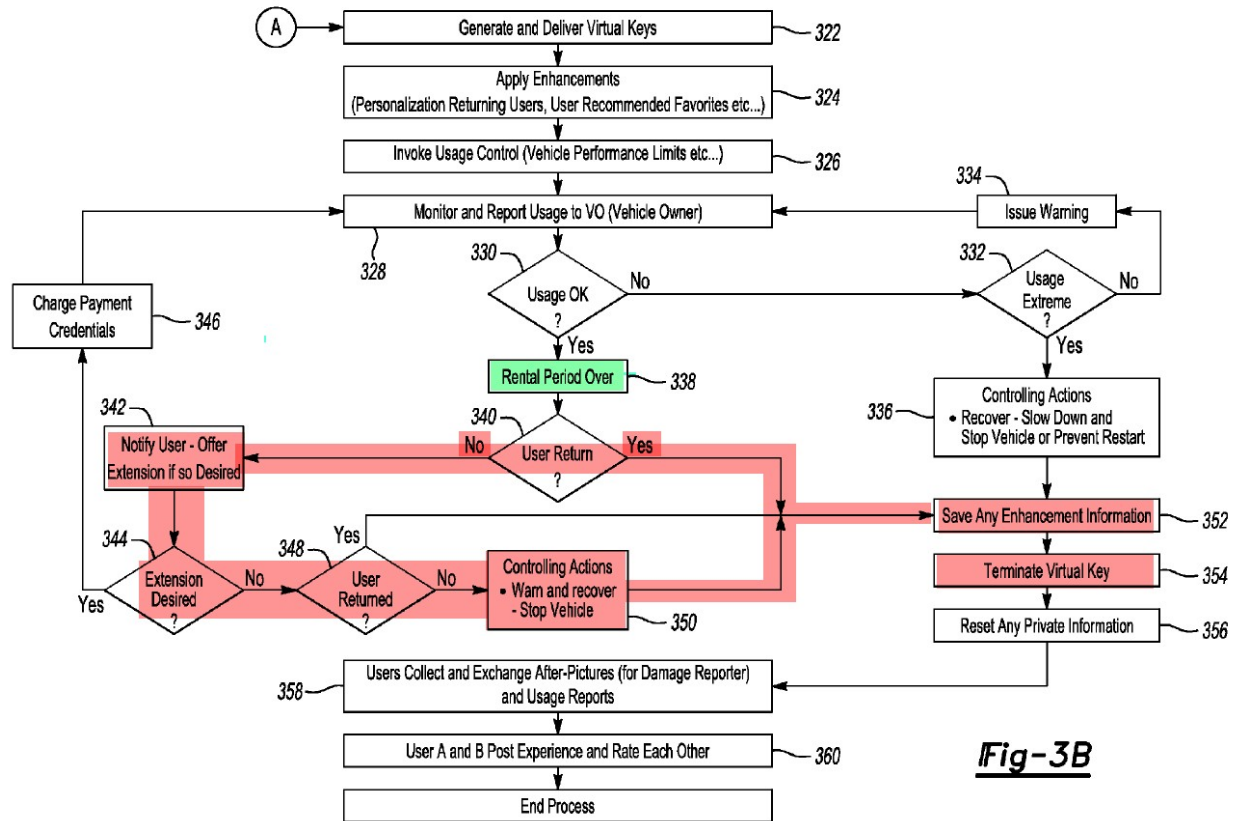
EX1005, Fig. 7B (annot.).

Kleve also provides examples where the virtual key remains operable *after* the rental term has ended and will not be terminated until the vehicle rental exit process, after the rental period is over. *E.g., id.*, ¶ 54; EX2021, ¶ 58. In each of these scenarios, terminating the virtual key is one step of *Kleve*’s vehicle rental exit process—occurring (1) *after the rental period ends*, (2) *after* the user has either returned the vehicle, or having failed to return it, *after* controlling actions of the VCS warn the user and/or stop the vehicle, and (3) *after* the system saves “any

enhancement information” based on the Temporary User’s settings. EX1005, ¶ 54; *id.*, ¶¶ 80, 49. Then, after terminating the virtual key, the system will “reset private information stored on the vehicle-based computing system.” *Id.*, ¶¶ 80, 49 (same). For example, “[i]f the rental term has ended, and no additional time is purchased, the system may begin the vehicle rental exit process within the VCS.” *Id.*, ¶ 43, Fig. 2. This vehicle rental exit process, at step 228, occurs after the rental period has expired, as detailed further below. *Id.*; EX2021, ¶ 59.



EX1005, Fig. 2 (annot.). It is after “the rental period has ended, [that] the monitoring and control system of the vehicle rental micro-business may begin to start its Temporary User vehicle rental exit mode process.” *Id.*, ¶ 80. As illustrated in Figure 3B, after “the Temporary User has completed the rental period” and after the Temporary User “has returned the vehicle to the appropriate drop off, the virtual key may terminate.” *Id.*, ¶¶ 55, 49 (same), Fig. 3B; EX2021, ¶ 60.



EX1005, Fig. 3B (annot.).

Alternatively, if “the rental period has expired,” but the Temporary User has not yet returned the vehicle, and an extension of time is not desired or authorized,

“the system may transmit controlling action to warn and induce remedial actions at step 350.” *Id.*, ¶ 54, Fig. 3B. Then, after terminating the virtual key, the system will reset any private information stored on the VCS. *Id.*, ¶¶ 80, 49, Fig. 3B; EX2021, ¶ 61.

Kleve therefore refutes the notion that its virtual key is “only operable during a rental period.” Paper 14 at 37 (citing Pet. 15); EX2021, ¶¶ 54-61. Indeed, these examples affirm that it is *Kleve*’s operation to “set user restrictions,” available to the Vehicle Owner initially at step 214, which empowers the Owner, alone, to dictate restrictions and gives the Owner flexibility to terminate usage (1) before the agreed-upon rental period ends, (2) after the agreed-upon rental period ends, and/or (3) update the rental period end time.

IV. Petitioners failed to show that the challenged claims of grounds 1-2 are obvious over *Kleve*, alone or in combination.

The claims require that a vehicle receive “coded data from a mobile device” and that “the coded data include[] privilege settings set for limiting types of use of the vehicle when using the vehicle via [an] eKey.” Claims 1[d-e], 11[d-e], 18[d-e]. Petitioners allege that *Kleve*’s “virtual key” discloses an “eKey.” Pet. 19. *Kleve*’s “virtual key,” however, is merely a credential, such as a user’s face, fingerprint, or other identifying information. EX1005, ¶ 62; EX2021, ¶ 62. Petitioners allege that the virtual key also discloses “coded data” when it is in the form of an encrypted

message or matrix barcode. Pet. 19-20. However, *Kleve*'s "virtual key," in whatever form, is independent of any alleged "privilege settings." EX2021, ¶¶ 62, 77. Petitioners fail to show that *Kleve*'s system includes any "privilege setting" in any "virtual key." This deficiency is fatal to grounds 1-2, as Petitioners rely on *Kleve* alone for this claimed functionality. Pet. 20-21, 28, 35.

The Board preliminarily credited Dr. Almeroth's testimony that "*Kleve* discloses that certain restrictions are sent with the request to generate a virtual key." Paper 14 at 38 (citing EX1004, ¶¶ 119-123 [sic]¹). However, Dr. Almeroth's testimony is incorrect and contrary to the express disclosures of *Kleve*. Unlike the Preliminary Response, which did not delve into the details of *Kleve*'s "credential check and authorization solution for personal vehicle rental," Patent Owner does so here, demonstrating below that each of the premises on which Dr. Almeroth bases his conclusions are directly refuted by *Kleve* itself.

At bottom, *Kleve* teaches that the creation and distribution of the virtual key both occur before, and independently of, any input of "user restrictions" at step 214 (section III.B.-C., *supra*). Regardless of whether *Kleve*'s virtual key is sent as an

¹ The ID quoted testimony of Dr. Almeroth which appears in his declaration from the IPR2024-00981.

encrypted message or a matrix barcode, no “restrictions” are included in the request to generate a virtual key, in the virtual key itself, nor in any encrypted data associated with the virtual key. Pet.19-21; EX1004, ¶¶ 138-140.

Dr. Almeroth opines that “restrictions” are included in *Kleve*’s virtual key. But as shown below, not a single one of Dr. Almeroth’s alleged “restrictions” is included in the creation of a virtual key, and certainly not in the virtual key itself, as required under Dr. Almeroth’s theory. EX1004, ¶¶ 138-139. Instead, *Kleve* makes clear that “user restrictions” are “initially” set at the beginning of the rental term—a point at which the virtual key has already been requested, generated and distributed. EX1005, ¶ 43, Fig. 2.

As an alternative theory, Dr. Almeroth opines that a POSITA would have included the restrictions on types of use of the vehicle as part of the coded data associated with a virtual key, e.g., as part of the encrypted data described in *Hatton*, “so that the Temporary User cannot modify those restrictions at his or her mobile device and circumvent the restrictions.” EX1004, ¶ 140. But this opinion disregards and contradicts *Kleve*’s discrete solution “to enforce compliance with rental agreement terms”—a solution that gives the Vehicle Owner—and the Owner alone—sole discretion to set “user restrictions” and control use of the vehicle, which the Owner performs by inputting restrictions via a website, nomadic device

or direct communication with the vehicle—never sending those restrictions to the Temporary User’s mobile device. EX1005, ¶¶ 40, 43, 51, 75. Dr. Almeroth’s proposed benefit is incorrect, as *Kleve*’s functionality already, and more securely, prevents a Temporary User from modifying restrictions. Indeed, Dr. Almeroth’s proposed motivation to modify *Kleve*’s solution would actually render the virtual key *more* vulnerable to “tampering,” not less, as *Kleve*’s existing solution never transmits any restrictions to the Temporary User—not in any virtual key or otherwise. EX1004, ¶¶ 111, 140.

Kleve explicitly teaches that a Vehicle Owner, alone, provides any use restrictions, the alleged “privilege setting” to the device, and makes clear that the Temporary User does not provide any restrictions to the vehicle merely by using a virtual key.

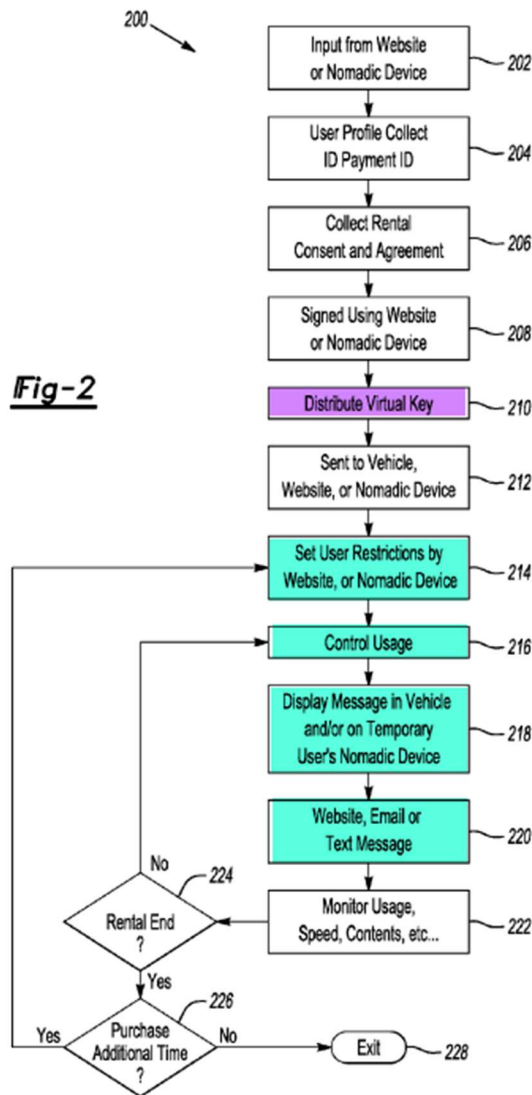
Though the Petition adds references *Hatton* and *Sekiyama* to grounds 1-2, these references do not cure *Kleve*’s lack of disclosure or suggestion on these elements, and Petitioners offer no argument or analysis to the contrary.

A. Each of the “restrictions” identified by Petitioners as alleged “privilege settings” are unavailable to be set until *after* the set up and distribution of the alleged “coded data,” a virtual key, and are thus not included in the coded data.

As the alleged “coded data,” Petitioners identify *Kleve*’s disclosure of a virtual key in the form of a matrix barcode or encrypted message, sent from a renter

to a vehicle to access the vehicle. Pet. 19-20. *Kleve* teaches that the “distribution” of this virtual key credential occurs at step 210. EX1005, ¶¶ 62, 39, Fig. 2. As the alleged “privilege settings,” Petitioners cite a variety of “restrictions,” but *Kleve* teaches such restrictions are independent of the virtual key: they are *initially* set by the Vehicle Owner “at the beginning of the rental term,” *after* the virtual key has been distributed. Pet. 20-21 (citing EX1005, ¶¶ 40, 83, 76); EX1004, ¶¶ 138-140 (verbatim). Accordingly, neither the alleged virtual key nor its representation as encrypted data or a matrix barcode includes any of the alleged “privilege settings” as required by each of the independent claims.

Petitioners and Dr. Almeroth repeatedly misstate that *Kleve*’s “user restrictions” are included in the virtual key. However, *Kleve* is explicit that this is incorrect, as the “virtual key” is distributed at **step 210**, before any “restrictions” are even **set by the Owner at step 214**. Pet. 19-21; EX1004, ¶¶ 138-140.

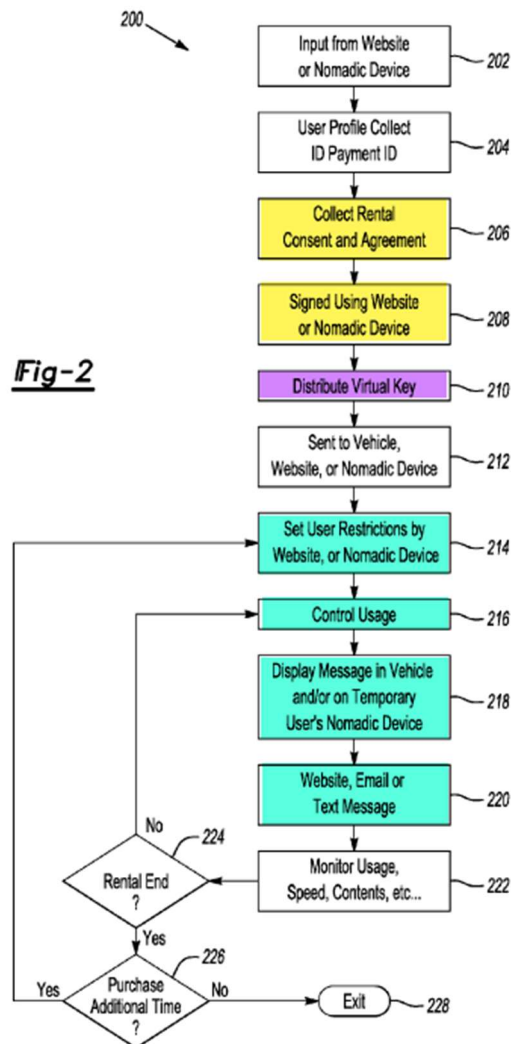


Id., Fig. 2 (annot.).

Kleve's restrictions are not predicated on any rental agreement or review of a rental request. As detailed in sections III.A., C.-D., *supra*, *Kleve* teaches that among the terms that may be agreed to as part of the parties' rental agreement are "load weight restrictions" (*id.*, ¶¶ 84, 89) and "rental period" (*id.*, ¶ 38). However,

Kleve never discloses or suggests that **any rental agreement terms** are somehow “included” in the generation or distribution of the virtual key or otherwise “enforced” by the virtual key itself. *Id.*, ¶ 51; EX2021, ¶¶ 79-82.

In fact, it would be wholly unnecessary for *Kleve* to teach “load weight restrictions” (EX1005, ¶ 40) and “rental end time restriction” (*id.*, ¶ 43) as express examples of how the parties’ *already agreed to rental agreement terms* may be “enforce[d]” (*id.*, ¶¶ 51, 40, 43) by the Owner setting “user restrictions” **at step 214**, were these terms (*id.*, ¶¶ 84, 89, 38) somehow included in the set up and/or distribution of the virtual key, at step 210. *See also id.*, Fig. 2; EX2021, ¶¶ 79-80; *and see, supra*, section III.C.



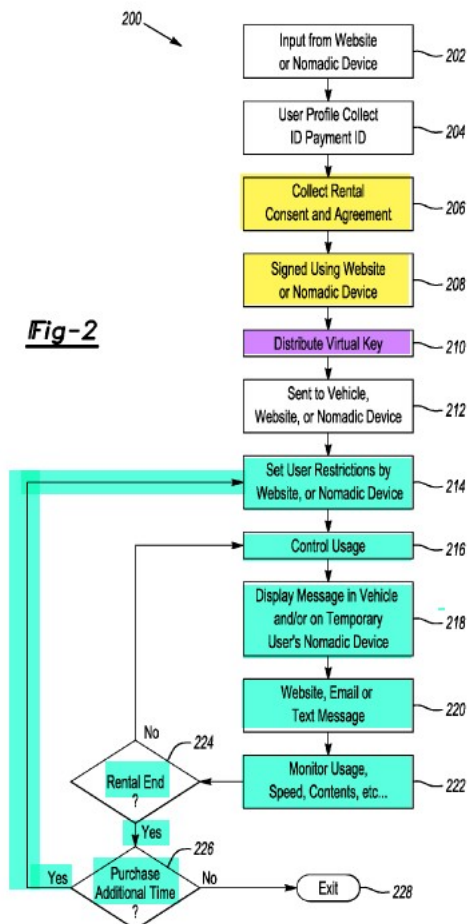
EX1005, Fig. 2 (annot.).

As the “restrictions” allegedly included in the virtual key, the Institution Decision identifies “a rental period restriction.” Paper 14 at 37-38 (citing EX1005, ¶¶ 38-39 and EX1004, ¶¶ 119-120 [sic]). But *Kleve*, at paragraph 38, describes **steps 206 and 208** (EX1005, ¶ 38, Fig. 2), in which the “terms and conditions for the rental period” may be agreed to by the parties, but “the rental period” described in

paragraph 38 is not disclosed or suggested to be “included as a restriction when the virtual key is created at step 206.” Paper 14 at 38; EX2021, ¶ 81. Indeed, *Kleve*’s discrete solution “to enforce compliance with rental agreement terms”— is a solution that (1) would be unnecessary were the rental agreement terms, e.g. rental period, already included in the virtual key, (2) requires the Vehicle Owner to input as “user restrictions” the very same restrictions/conditions already agreed to by the parties’ rental agreement, (3) gives the Vehicle Owner (and the Owner alone) full discretion, flexibility and control to set “user restrictions” that *Kleve*’s system will use to monitor, control and update the vehicle usage, and (4) updates the “rental period end time” as a “user restriction,” input at step 214, not involving the virtual key or rental agreement at all. *Id.*; see sections III.A.-D., *supra*. Moreover, there can be no restriction on vehicle use before the distribution of the virtual key (step 210), since *Kleve* is clear that user restrictions for monitoring and controlling vehicle usage cannot even be set until “the beginning of the rental term.” EX1005, ¶ 43 (“initially set ... at the beginning of the rental term”), ¶ 75 (“restrictions assigned ... at the start of the rental period”).

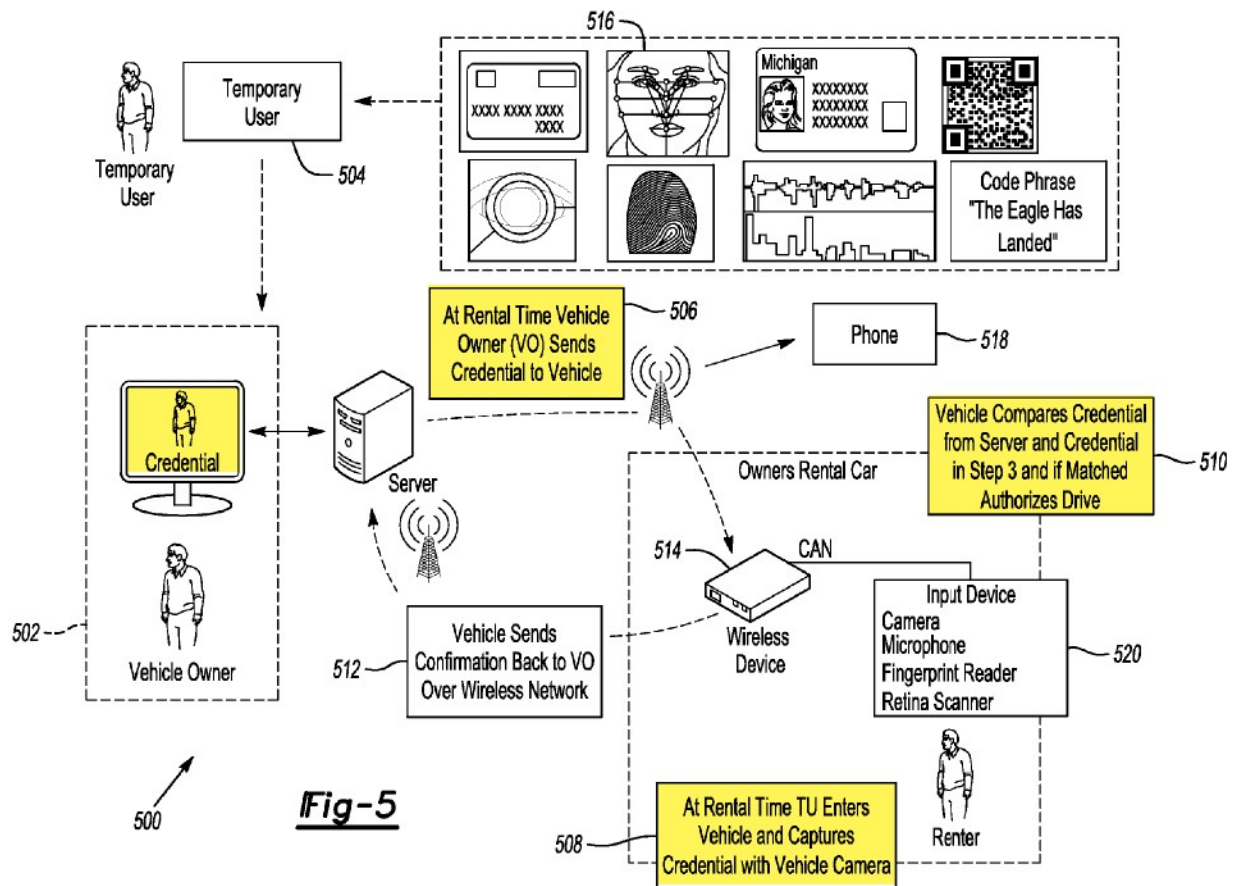
Instead, to “enforce” any “rental end time restriction” which may have been agreed to by the parties in their rental agreement, this “rental period end time” is a separate “restriction” that may be set by the Owner, at 214, and, if extended, the

“system may update the new rental period end time restriction”—in step 214—and “continue to monitor usage of the vehicle.” See section III.C.; EX2021, ¶ 82; see also EX1005, ¶ 43, Fig. 2. Again, were the “rental period” somehow included in the virtual key, at step 210 (or even earlier, i.e. at steps 206 or 208), it would make no sense for *Kleve* to update only step 214, in order to “update the new rental period end time restriction,” step 226 → step 214, but *not* at step 210 or steps 206 or 208. EX1005, ¶ 43, Fig. 2; EX2021, ¶ 83.



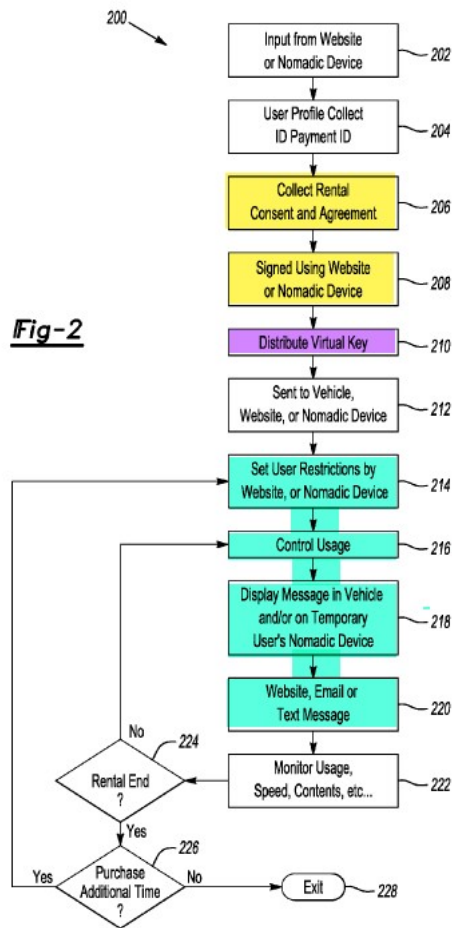
EX1005, Fig. 2 (annot.).

Moreover, by sending the authorization “credential” to the vehicle “at Rental Time,” the Owner ensures “the scheduled rental period of time begins” (*id.*, ¶ 66, Fig. 5) according to the agreed-upon rental period via sending the credential (*id.*, ¶ 62, Fig. 5) and via receipt of the credential by the vehicle. “At Rental Time” the Temporary User enters the vehicle, the vehicle captures the User’s credential, the vehicle compares the two credentials, and “if matched authorizes drive.” *Id.*, ¶ 66, Fig. 5. Were this “rental time” somehow included in the set up or distribution of the virtual key, it would be unnecessary that the “Vehicle (VO) Owner sends [the] credential to [the] vehicle” (*id.*, ¶ 66, Fig. 5) “[w]hen the scheduled rental period of time begins” (*id.*, ¶ 66, Fig. 5); EX2021, ¶ 84.



EX1005, Fig. 5 (annot.).

Dr. Almeroth also points to *Kleve*'s description of "speed, global position coordinates, or load weight restrictions," at paragraph 40, as alleged "restrictions" included in its virtual key. EX1004, ¶ 139. But at paragraph 40, *Kleve* describes steps 214, 216, 218 and 220—all of which are steps *subsequent* to the set up and distribution of the virtual key. EX1005, ¶ 40, Fig. 2; EX2021, ¶ 85.



EX1005, Fig. 2 (annot.). Indeed, at paragraph 40, *Kleve* describes how, starting with step 214, an “Owner may set user restrictions,” how these “use restrictions may be monitored,” and how, when usage exceeds those restrictions, notifications are sent. *Id.*, ¶ 40. Moreover, these are “restriction limits initially set by the Owner at the beginning of the rental term,” not at any time prior. *Id.*, ¶ 43; EX2021, ¶ 86.

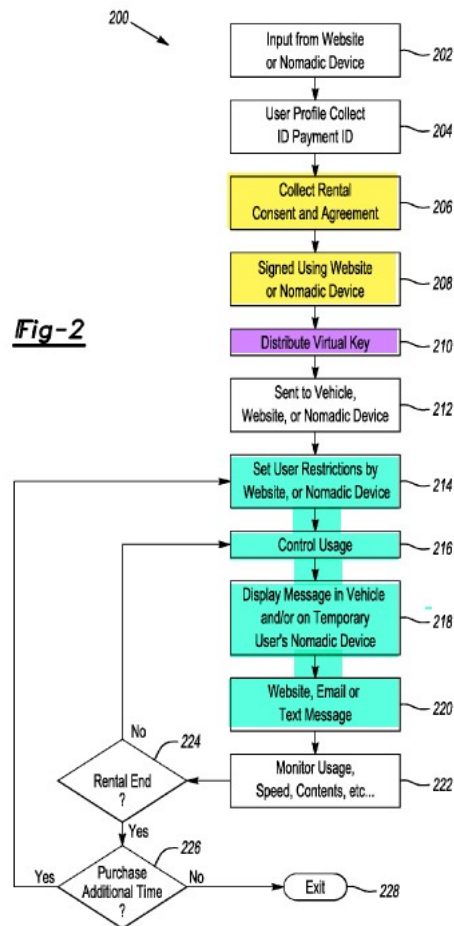
Dr. Almeroth erroneously claims that because “the Temporary User may request to rent a vehicle for running errands, and not for towing and hauling cargo,

[] the virtual key may thus be configured to monitor for unauthorized cargo or an unauthorized trailer tow.” EX1004, ¶ 139 (citing EX1005, ¶¶ 83, 76). *Kleve* never suggests to “configure” the virtual key for any use, restriction, or rental request whatsoever. EX2021, ¶ 87. Instead, *Kleve* explains the process by which an Owner may review a Temporary User’s “rental request,” which may include information such as “*what* the Temporary User is looking to use the vehicle for (e.g., ... for towing, hauling, or errands), *when* the requested use will be taking place, and *where*.” EX1005, ¶ 83 (emphases added). *Kleve* goes on to instruct that the Owner can either accept or decline the rental request. *Id.*, ¶ 84.

However, *Kleve* offers no mention or suggestion regarding a virtual key when teaching this process of submitting, reviewing or accepting/rejecting a “rental request,” no matter the *what*, *when*, or *where* details specified in that “rental request.” *Id.*, ¶¶ 83-84; EX2021, ¶ 87. Instead, as discussed in Section III.C., *Kleve*’s solution to “control the vehicle with the use of vehicle restriction limits,” gives the Owner the option to set user restrictions *after the virtual key has already been distributed*—as the restrictions are “*initially* set by the Owner at the beginning of the rental term”—and therefore cannot be sent or “include[d]” as an alleged “privilege setting” in the creation or distribution of that virtual key. EX1005, ¶¶ 51, 43, Fig. 2; EX1001, claims 1[d-e], 11[d-e], 18[d-e]; EX2021, ¶ 88.

Likewise incorrect is Dr. Almeroth's conclusion that the virtual key is "configured to monitor for unauthorized cargo or an unauthorized trailer tow," merely because *Kleve*'s vehicle may monitor restrictions related to unauthorized cargo or unauthorized trailer tow. Instead, such restrictions are assigned at the start of the rental term—after the virtual key has already been created and distributed. EX1005, ¶¶ 76, 75; EX2021, ¶ 89. Specifically, the cited disclosure of *Kleve* describes monitoring "performance limitations and restrictions assigned by the vehicle owner at the start of the rental period at step 708." EX1005, ¶¶ 75-76. This monitoring, *Kleve* explains, may include "unauthorized objects or cargo, unauthorized driving behavior, unauthorized driver, and/or an unauthorized trailer tow," but are clearly based upon the restrictions downloaded by the VCS at step 708—restrictions that are "assigned by the Owner at the start of the rental period"—not at any time prior. *Id.*, ¶¶ 75-76, Fig. 7A; EX2021, ¶ 89.

Kleve teaches that these restrictions, and the control parameters on which they are based, "enforce compliance with the rental agreement terms" and enforce any other user restrictions set by the Owner, but the Owner cannot input such restrictions until [step 214](#), at "the beginning of the rental term," *after* the creation and distribution of a virtual key. EX1005, ¶¶ 51, 43, 75-76, Figs. 2, 7A; EX2021, ¶¶ 89-90.



EX1005, Fig. 2 (annot.).

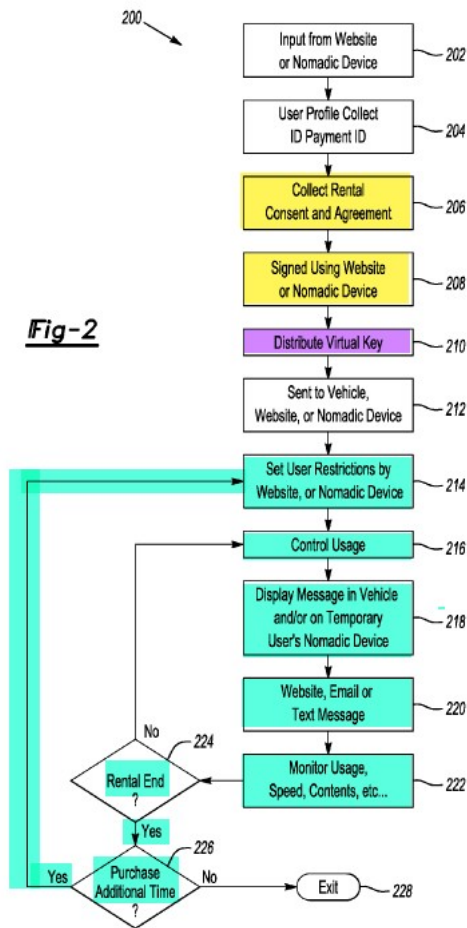
Accordingly, not one of the alleged “restrictions” identified by Petitioners and Dr. Almeroth is included in a virtual key, let alone within any alleged coded data, “the encrypted data associated with the virtual key.” Pet. 21 (citing EX1005, ¶¶ 40, 83, 76); EX1004, ¶¶ 138-140 (same); EX2021, ¶ 91.

B. *Kleve* flatly contradicts the conclusion that “rental agreement restrictions were sent with the request.”

While the Institution Decision credits Dr. Almeroth’s opinion that “rental agreement restrictions were sent with the request,” this notion is fundamentally belied by *Kleve*’s specific and discrete solution “to enforce compliance with rental agreement terms.” Paper 14 at 38 (citing EX1004, ¶¶ 119-123 [sic], 152); EX1005, ¶ 51. This independent functionality would be wholly unnecessary were those terms somehow included in the creation or distribution of the virtual key.

Likewise, it would not be necessary for *Kleve* to have the Vehicle Owner input “user restrictions” at **step 214**—such as “load weight restrictions” (*id.* ¶ 40) and the “rental period end time restriction” (*id.*, ¶ 43)—if those *same restrictions*, agreed to as part of the parties’ **rental agreement**—*id.*, ¶ 84 (“terms and conditions of the rental period include “load weight restrictions”), ¶ 89 (same), ¶ 38 (parties may agree to “terms and conditions for the rental period”)—were already sent in *Kleve*’s creation and distribution of a virtual key, at step 210. *See* sections III.C.-D., *supra*; EX2021, ¶ 90.

Further, as described in section III.C., Dr. Almeroth’s conclusion makes no sense where *Kleve* teaches that in order to *extend* a rental period, a user may purchase additional time at step 226, and, by doing so, at **step 214**, “a new rental period end time restriction” is “update[d].” *Id.*, ¶ 43, Fig. 2.



Id., Fig. 2 (showing arrow linking step 226, “yes,” back to step 214). By contrast, *Kleve*’s extension of the rental period, at step 226, does not “update” *Kleve*’s virtual key (step 210) or its rental agreement (steps 206, 208). *Id.*; EX2021, ¶ 83.

C. That a virtual key credential enables the keyless drive system during a given rental period does not suggest the “rental period” is included in the virtual key itself.

As detailed above, *Kleve*’s system includes solutions for the Owner to allow access and/or a drive-away, during the rental period, without having “the rental

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

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

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

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

and there is no dispute that the Temporary User cannot access the Owner's vehicle without first having received and used the already-distributed virtual key (EX1005, ¶ 63; Pet. 19). Accordingly, where a Temporary User may "agree to rental terms" *after* accessing the vehicle, there can be no rental agreement terms in this already-generated, already-distributed, and already-used virtual key. EX2021, ¶ 93.

2. *Kleve* cannot enforce compliance with rental agreement terms until after the virtual key is generated and distributed, where a Temporary User may "agree to rental terms" after accessing the vehicle with the virtual key.

As detailed in Section III.C., *Kleve* discloses a solution "to enforce compliance with the rental agreement terms," in which the Owner has "the options to set rental restrictions," at step 214, after the virtual key has been generated and distributed. EX1005, ¶¶ 51, 40; EX2021, ¶ 94; *see supra* sections III.C. By contrast, the virtual key itself cannot "enforce compliance with the rental agreement terms," where the virtual key is already generated, distributed to the Temporary User, and used by the Temporary User to access the vehicle—all *before* the Temporary User has even agreed to rental terms. EX1005, ¶ 67 ("Temporary User may use their virtual key credential to access the vehicle"), ¶ 65 (Temporary User "may agree to rental terms" "at a vehicle with the use of hardware integrated with the VCS").

Apart from the optional Owner-set restrictions, "chosen by VO" and "set" by the Owner at step 214—*after* the generation and distribution of the virtual key—

Kleve offers no other option for “controlling usage to enforce compliance with rental agreement terms.” *Id.*, ¶¶ 51, 40, 75, Figs. 7A, 2; EX2021, ¶ 95. Indeed, those “vehicle restrictions,” *Kleve* instructs, are not set before the virtual key is distributed, but are instead “initially set by the Owner at the beginning of the rental term.” *Id.*; *id.*, ¶¶ 43, 75 (“restrictions assigned by the Vehicle Owner at the start of the rental period”). The performance limits chosen by the Owner are downloaded to the VCS at **step 708**, after “the Temporary User initiates the rental event,” at **step 706**. *Id.*, ¶ 75, Fig. 7A.

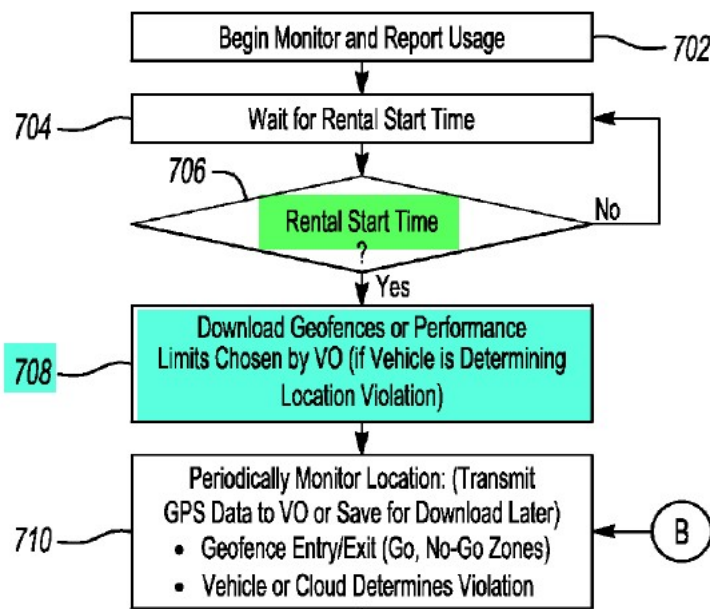


Fig-7A

Id., Fig. 7A (annot.). Because the virtual key is already generated, distributed to the Temporary User, and used by the Temporary User to access the vehicle—all before the beginning of the rental term—the virtual key cannot include any restrictions, let alone any rental agreement restrictions. *Id.*, ¶¶ 43, 51, 75, Fig. 7A. *Kleve*’s system

will monitor and control usage—i.e. enforce any rental agreement terms—according to the “vehicle restriction limits initially set by the Owner at the beginning of the rental term.” *Id.*

3. During cross examination, Dr. Almeroth admitted that *Kleve*’s virtual key is not “always generated after the rental agreement.”

As described in Sections IV.C.1.-2., *Kleve* teaches that the virtual key is not always generated after the rental agreement. *See, e.g.*, EX1005, ¶ 65 (after virtual key distributed, user may access vehicle and, at the vehicle, “agree to rental terms”). But even in the situations where a virtual key may be generated after the rental agreement has been signed by the parties, this alone has no bearing on whether the virtual key includes “privileges settings.” *Kleve* teaches it does not, as discussed above. *See, supra*, sections III.C.-D., IV.A.-C.1.-2. Indeed, by *Kleve*’s express disclosure, the virtual key is not “always generated after the rental agreement,”² and indeed, Dr. Almeroth admits the key is not always generated after the rental agreement. EX2022, 27:5-10 (“I don’t think *Kleve* is limited in all of its embodiments where a POSITA reading *Kleve* would understand that every

² The ID appears to rely on a statement from Dr. Almeroth’s declaration in IPR2024-00981; this testimony does not appear in his declaration submitted in this matter.

embodiment, the only way the e-key could be generated is after the rental agreement”); *id.*, 27:21-28:1; EX2021, ¶ 96.

Regardless, as shown above, *Kleve*’s system expressly teaches a virtual key is generated and distributed to the Temporary User *before* there is a rental agreement between the parties. *Id.*; EX1005, ¶ 65. For example, *Kleve* teaches that the Temporary User agrees to rental terms *at the vehicle*, using the vehicle’s hardware, *after Kleve*’s system has already generated and distributed the virtual key to a Temporary User, and *after* the Temporary User uses the virtual key to access the vehicle. *Id.*, ¶¶ 65, 67.

Accordingly, *Kleve* itself belies the notion that a virtual key is “always generated after the rental agreement.” Paper 14 at 38. This demonstrates what is already explicit in *Kleve*: that setting any restrictions is independent of generating and distributing a virtual key—*Kleve*’s “virtual key” does not and cannot include any restrictions at all.

4. *Kleve* has the Vehicle Owner send the “virtual key” to the vehicle “at rental time.”

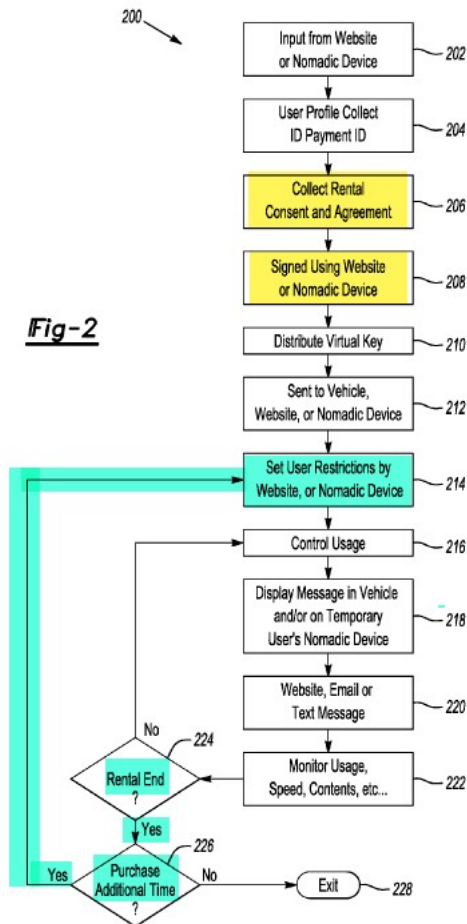
As described above, *Kleve*’s Vehicle Owner sends credentials to the vehicle “at rental time,” which would be wholly unnecessary were the “rental period” itself already included in the creation or distribution of the alleged coded data that a Temporary User uses to access the vehicle. *See* sections III.B., IV.A.-B., *supra*;

EX2021, ¶ 97. *Kleve* teaches that a virtual key credential may allow “entry of the vehicle” (EX1005, ¶¶ 48, 67), however, “at rental time,” *Kleve* teaches that the “Vehicle Owner sends the credential to [the] vehicle” (e.g., by the server). *Id.*, ¶ 66, Fig. 5. Had the virtual key already included the agreed-upon rental period when created or distributed, it would be unnecessary for *Kleve* to direct the Vehicle Owner to send information to the vehicle “at rental time.” *Id.*

5. *Kleve* teaches a distinct solution for monitoring, controlling and updating the rental period—one that does not involve any such “restriction” in the virtual key itself.

As shown in section III.D., *Kleve* offers numerous examples in which the virtual key’s operability is not at all dependent on the “rental period” agreed upon in the rental agreement, but instead: (1) the virtual key is terminated before a rental end time, e.g., due to extreme usage which exceeds a “user restriction” set after the set up and distribution of the virtual key (*id.*, ¶ 53, Fig. 3B) or due to a detected accident (*id.*, ¶¶ 79, 53, Fig. 7B), (2) the rental period end time may be updated where extended time is purchased and authorized (*id.*, ¶ 43, Fig. 2), or (3) the virtual key is terminated *after* the agreed upon rental period has expired (*id.*, ¶¶ 43, 53-55, 79-80); EX2021, ¶ 98. At bottom, *Kleve*’s solution enforces the end of the rental period, not by including the agreed upon period into the virtual key itself, but by

the Owner's input, at step 214, of a "rental period end time restriction." *Id.*; EX1005, ¶ 43.



Id. at Fig. 2 (annot.). Accordingly, while *Kleve* teaches that a virtual key credential allows the Temporary User to access and/or drive the vehicle, the rental period is not restricted or enforced via the virtual key itself, but is controlled by the Vehicle Owner alone, when the "rental period end time restriction" is "set" by the Owner as a "user restriction," "at the beginning of the rental term." *Id.*; *id.*, ¶¶ 43, 40.

6. Dr. Almeroth’s obviousness opinions ignore and even contradict *Kleve*’s solution for enforcing rental agreement terms and conditions.

By its express disclosure of a solution “to enforce compliance with the rental agreement terms”—i.e., setting “user restrictions” at step 214, which may be monitored, controlled and updated—*Kleve* itself flatly contradicts Dr. Almeroth’s obviousness opinions. *E.g., id.*, ¶¶ 40-41, 43, 51.

a. Dr. Almeroth ignores the security of the enforcement solution already achieved by *Kleve*’s steps 214-226.

Dr. Almeroth’s logic is fundamentally flawed. He opines that a POSITA would have been motivated to “include data identifying restrictions on a Temporary User’s use of the vehicle as part of the encrypted data transmitted with the electronic key or as part of the electronic key, *so that* the Temporary User cannot modify those restrictions at his or her mobile device” (EX1004, ¶¶ 140, 111-112) (emphasis added). But *Kleve*’s solution already provides this benefit, and in a more secure way. *Kleve* never includes any “data identifying restrictions on a Temporary User’s use of the vehicle” in or as part of any virtual key transmitted to the Temporary User. EX2021, ¶¶ 99-100, 106. Instead, *Kleve* teaches that the restrictions used to control and monitor vehicle usage are “initially set at the beginning of the rental term,” *after* the virtual key has already been created and distributed, and in fact, are never transmitted to the Temporary User. EX1005, ¶¶ 40-43, Fig. 2; *see* section

III.C, *supra*. Apart from hindsight knowledge based on the '659 patent, Dr. Almeroth never offers any benefit that would be achieved by modifying *Kleve* to include restrictions in its virtual key and then encrypt those restrictions. *Id.*; EX1004, ¶¶ 140, 111-112. Citing to benefits already achieved by *Kleve*'s solution is "insufficient to present a prima facie case of obviousness." *In re Oetiker*, 977 F.2d 1443, 1447 (Fed. Cir. 1992); *see also In re Dow Chem. Co.*, 837 F.2d 469, 473 (Fed. Cir. 1988) ("[t]here must be a reason or suggestion in the art for selecting the procedure used, other than the knowledge learned from the applicant's disclosure"); *Opticon Medical AB v. Cochlear Ltd.*, IPR2019-00975, Paper 154 at 29-30 (P.T.A.B. Oct. 14, 2020) (proposed modification was based on improper hindsight).

b. *Kleve*'s solution renders nonsensical Dr. Almeroth's hindsight demands to include rental agreement restrictions in the virtual key.

Kleve's system of enforcing compliance with rental agreement terms ensures that *only the Vehicle Owner* may set user restrictions that the vehicle will monitor and/or control via remedial actions. EX1005, ¶¶ 40, 51, Fig. 7A. While *Kleve*'s system provides both parties—the Temporary User and the Vehicle Owner—with the opportunity to negotiate, agree to and ultimately sign a rental agreement (*id.* ¶¶ 38, 84, 89), *Kleve* puts the "controlling usage" discretion solely in the hands of *the Vehicle Owner* (*id.*, ¶¶ 40-41, 51, Figs. 2, 7A).

First, *Kleve* allows only the Vehicle Owner to decide whether to control usage, by inputting “user restrictions,” available at step 214, and second, *Kleve* lets only the Vehicle Owner choose which “user restrictions” will best protect the Vehicle Owner’s asset. *Id.* *Kleve* makes clear that this system design is not the result of any mere coincidence, but is instead purposefully designed to permit *only Vehicle Owners* to input restrictions to control usage. *Id.*, ¶¶ 51, 43 (restriction limits initially set *by the Owner* at the beginning of the rental term”), 75 (“restrictions assigned *by the Vehicle Owner* at the start of the rental period”). As *Kleve* explains, “[c]ontrolling 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.” *Id.*

For example, *Kleve* dictates that the “performance limits *chosen by the VO [Vehicle Owner]*” (*id.*, Fig. 7A) (emphasis added) are not sent by the Temporary User, but downloaded by the vehicle, and monitored by the vehicle, “alerting the vehicle owner if the driver enters an area *deemed to be prohibited by the owner*” (*id.*, ¶ 75) (emphasis added). Likewise, *Kleve* teaches that “the monitoring of the vehicle’s location may be done to reassure the Vehicle Owner that their asset is being driven in an approved manner and area.” *Id.*, ¶ 76. *Kleve* leaves no room for ambiguity that the “user restrictions,” which may be set only by the Vehicle Owner,

are intended to provide the Vehicle Owner alone with the discretion and flexibility to monitor and control their asset in the manner the Vehicle Owner deems appropriate. EX2021, ¶¶ 101-103.

To accept Dr. Almeroth’s opinion, in which restrictions of vehicle use are actually sent to the Temporary User, as part of the user’s a virtual key, ignores *Kleve*’s express design and purpose of giving the Vehicle Owner—and the Vehicle Owner alone—full access and control to vehicle usage restrictions. *Id.*; *see, e.g., In re Ratti*, 270 F.2d 810, 813 (CCPA 1959) (holding the suggested modifications “would require a substantial reconstruction and redesign of the elements shown in [a prior art reference] as well as a change in the basic principles under which [that reference’s] construction was designed to operate”).

D. It would not have been obvious to combine *Kleve* and *Hatton* as Petitioners propose.

Even assuming the proposed *Kleve* / *Hatton* combination taught or suggested the elements of the independent claims (it does not), it would nevertheless not have been obvious to a POSITA to modify *Kleve* in view of *Hatton* as Petitioners propose. EX2021, ¶¶ 104, 112-117. In a short summary of *Hatton*, Petitioners generally argue that the reference discloses communicating with “encrypted data” and generating an alleged “electronic key” using “encrypted data.” Pet. 11-12. Petitioners then broadly argue that it would have been obvious to use “encrypted

data for wireless communications,” to provide various benefits. Pet. 12-14; EX2021, ¶¶ 105-109. Not only would encrypting *Kleve*’s virtual key fail to cure *Kleve*’s deficiencies, the purported benefits that Petitioners and their expert describe are a result of encryption for **confidentiality**, which is not taught by *Hatton*. EX2021, ¶¶ 109-113. *Hatton* instead teaches using encryption for **authentication**. *Id.*, ¶¶ 113-114.

Authentication involves verifying or determining the authenticity of something, such as a communication, to, e.g., confirm that it is proper, such as from an authorized entity. *Id.* Confidentiality is a distinct concept involving the protection of information from unauthorized disclosure. *Id.*, ¶ 109. *Hatton*’s encryption is related to the former. *Id.* *Hatton* discloses a vehicle having entry passive start (PEPS) and passive anti-theft security (PATs) controllers, which include certain encrypted data. EX1008, 5:54-7:60, 9:4-17, 9:50-63. *Hatton* discloses that encrypted data sent from the key/mobile device is checked against the encrypted data in a PEPS by using a look up table that is stored on the vehicle computing system (VCS). EX1008, 9:50-63. This check authenticates that the key/mobile device is authorized to access the vehicle. EX2021, ¶ 114. *Hatton*’s “encryption” is unrelated to confidentiality, does not prevent any unauthorized disclosure, and, as *Kleve* already teaches authentication, a POSITA would not have

been motivated to modify *Kleve* in view of *Hatton* to add authentication. *Id.*³ Thus, Petitioners’ argument that “[t]here were well-known benefits of using encrypted data for wireless communications” provides no reason why a POSITA would have combined *Kleve* and *Hatton* as proposed. *Id.* And as *Hatton*’s encryption is not for confidentiality, Petitioners are incorrect that it would prevent unauthorized users from “view[ing] the contents of the messages,” as the “content” is what is sent and checked. *See* Pet. 12.

Moreover, Petitioners do not explain how *Kleve* could be modified in view of *Hatton* as proposed. *Hatton* does not disclose generating any encrypted data at a mobile device. EX2021, ¶ 115. *Hatton* discloses that encrypted data is assigned to a vehicle at the manufacturing process. EX1008, 8:24-36, 14:7-18. Thus, it would not have been obvious in view of *Hatton* to generate encrypted data to include restrictions for use in a rental vehicle because the encrypted data would have

³ As discussed above, *Kleve* teaches receiving the “virtual key” at the vehicle and providing it to the “rental authorization server” or vehicle Owner for authentication, e.g., by checking the credentials such as a fingerprint. EX1005, ¶ 70. Indeed, during prosecution, *Kleve* attempted to distinguish art using its “authenticating input [for] identifying a user.” EX2020.

already been generated. EX2021, ¶ 115. Under Petitioners’ theory, encrypted data would need to be generated each time “restrictions” were created or modified, but *Hatton* does not have a mechanism for doing this. *Id.*

Petitioners further state that encrypting the data would “simplify[] and facilitate[] use of the virtual key for end users,” but they provide no reason what this means or why it would be. In fact, it would not. EX2021, ¶ 116. Petitioners also state that encrypting data would allow key usage “when the vehicle and mobile device cannot connect to a remote server.” Pet. 13. However, the Petition provides no explanation or cite for this proposition. As discussed above in Section III.A.2, *Kleve*’s vehicle communicates with the server to receive a credential at rental time, and merely including “restrictions” in the virtual key and encrypting it would not eliminate this (EX2021, ¶¶ 114-117), and Petitioners offer no reason or citation to the contrary. Petitioners’ expert offers conclusory reasons for the benefits of the proposed combination, but, as Dr. Malek explains, a POSITA would not have found any of those purported benefits to lead to fruition. *Id.* Instead, a POSITA would have understood that the proposed combination would have resulted in a slower, less efficient system with a poorer user experience—all with no identified benefits. EX2021, ¶¶ 113-117.

V. The *Mikan* Reference (EX1007)

Mikan (EX1007) is related to a wireless vehicle security system, in which an electronic key to access a vehicle may be embedded in a traditional metal key, a phone, or a personal digital assistant (PDA). EX1007, Abstract, ¶ 50. *Mikan*'s system includes keys 205A-C, shown in Figure 2 below, which may communicate directly with the vehicle's control unit 202 in order to request to access the vehicle, or may communicate with a wireless network 207, for example, via an application, to manage and monitor the system. *Id.*, ¶¶ 50-51, 56. *Mikan*'s system further includes a local database 203, included *in the vehicle* 201, which communicates with the vehicle's control unit 202, as well as a master database 208, which is included in the system's wireless network 207. *Id.*, ¶¶ 50-51, 54; EX2021, ¶ 66.

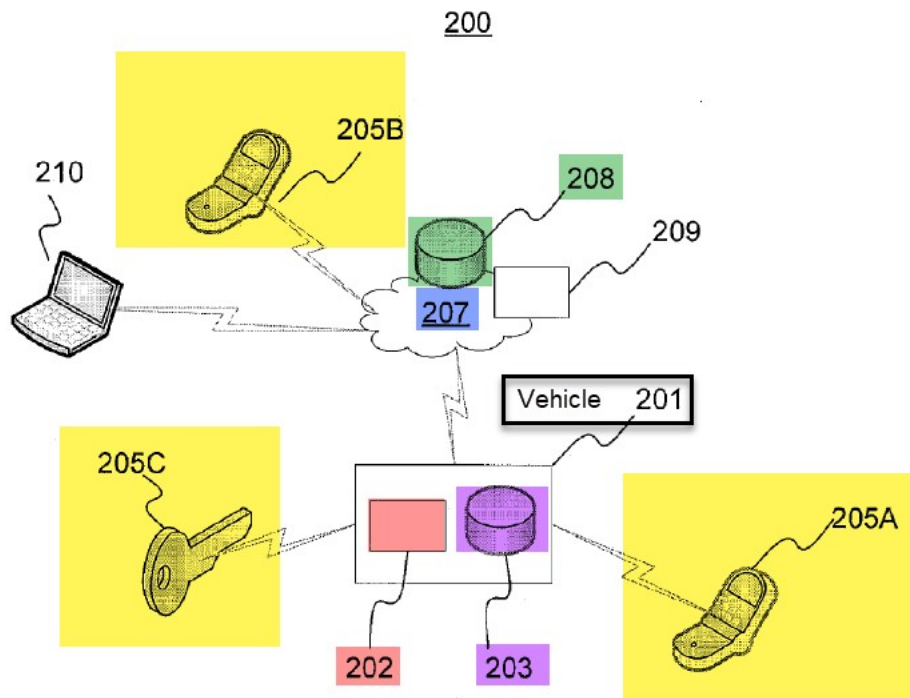


FIG. 2

EX1007, Fig. 2 (annot.). *Mikan*'s system further includes "a vehicle operation policy," which may "indicate to enable, partially enable, or disable a vehicle operation feature." *Id.*, ¶¶ 5, 57. *Mikan* teaches that this vehicle operation policy 311 may be stored in the master database 208, on the wireless network 207, and after syncing with the vehicle, the vehicle operation policy 311 is also stored in the local database 203 on the vehicle 201. *Id.*, ¶¶ 58-59, 72, 81, Figs. 3A-3B; EX2021, ¶ 67.

Specifically, the master database may include records for each “vehicle ID,” including a key set 310, which is “data representing a collection of keys 205A-C,” as well as a policy set of vehicle operation policies 311. EX1007, ¶ 58, Fig. 3A; EX2021, ¶ 68. The master database also includes a “mapping 312,” which relates individual keys from the records of the key set 310 with specific vehicle operation policies 311. *Id.*; EX1007, ¶ 58, Fig. 3A.

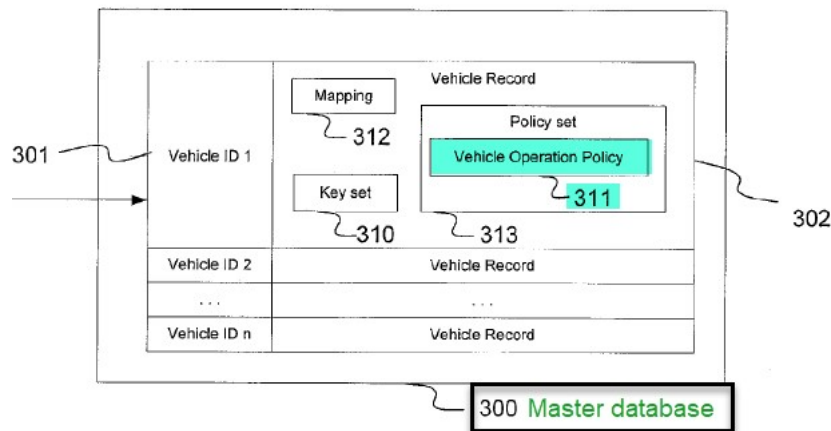


FIG. 3A

Id., Fig. 3A (annot.).

Likewise, the local database on the vehicle stores that vehicle’s “vehicle ID,” which corresponds to a specific vehicle ID record on the master database, and the local database further stores a key set 310, and a policy set of vehicle operation policies 311, with access control rules 317 for associated vehicle operations. *Id.*, ¶¶ 59-60; EX2021, ¶ 69.

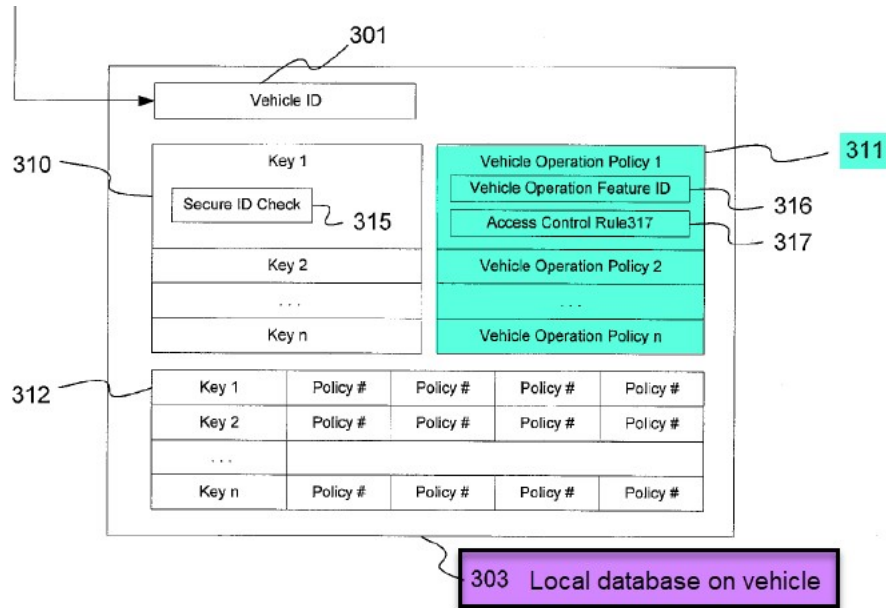


FIG. 3B

EX1007, Fig. 3B (annot.). Like the master database, the vehicle's **local database** includes a “mapping 312” that relates a **vehicle operation policy 311** to a specific key in the key set stored on the vehicle. *Id.*, ¶ 61; EX2021, ¶ 70. For example, the mapping can indicate whether a given key in the key set is related to a **vehicle operation policy 311** that enables all vehicle operation features, while relating another key to a **vehicle operation policy 311** that may restrict that key holder's access to certain vehicle operation features via access control rules 317, e.g. restricting access to the glove box or trunk. *Id.*; EX1007, ¶ 61.

Mikan teaches that the **local database 203** may be synchronized with records in the **master database**, so that the vehicle receives the updated data that is relevant to the vehicle since the last synchronization. *Id.*, ¶ 69; EX2021, ¶ 71. In this way,

the data in the master database and local database are kept consistent, e.g. which keys are associated with a particular vehicle ID and/or which vehicle operation policies relate to a particular key. *Id.*; EX1007, ¶¶ 54, 68-69. Because the synchronization between the databases precedes a vehicle's detection and authentication of a key 205A-C, the vehicle control unit need only access *locally stored records*, e.g. vehicle operation policy 311 and any included access control rule 317, to process and permit/block specific access requests, as detailed further below. *Id.*; *id.*, Fig. 5; EX2021, ¶ 72.

In order to authenticate a key 205A-C, *Mikan*'s vehicle local database further includes a “secure ID check 315” associated with a key in the key set 205A-C. EX1007, ¶¶ 59, 70-71; EX2021, ¶ 73. This “secure ID check 315” may be a serial number, identifier of the key, or a digital signature associated with a key 205A-C. EX1007, ¶¶ 59, 70-71. For example, the secure ID may be used in a “challenge-handshake authentication protocol (CHAP)” to authenticate a user's key. *Id.*

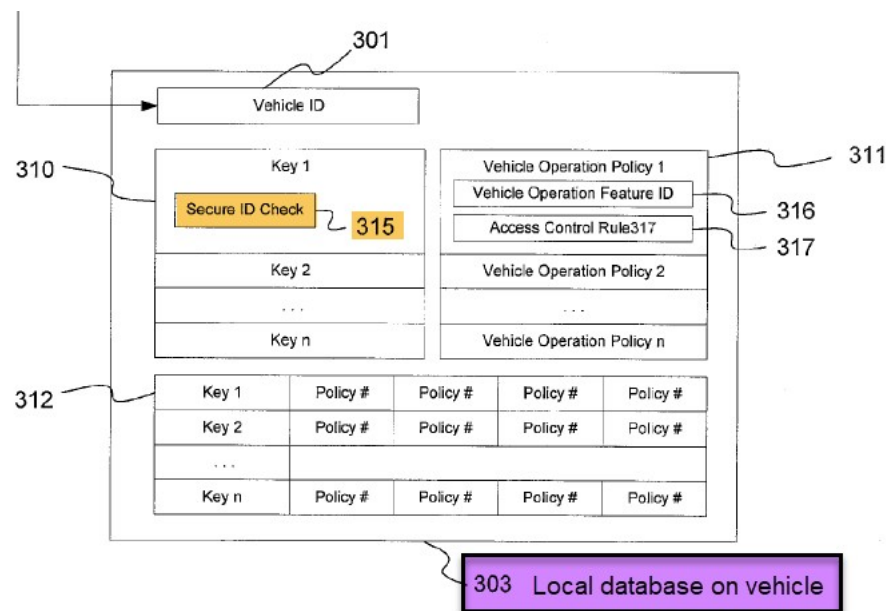


FIG. 3B

Id., Fig. 3B (annot.).

When a user approaches a vehicle and attempts to access that vehicle, e.g. unlock the vehicle using a wireless device as a **key 205A-B**, the vehicle receives a **secure key identifier 407** from the wireless device. *Id.*, ¶ 70, Fig. 5; EX2021, ¶ 74. This **secure key identifier 407** is used by the vehicle to authenticate the user's wireless device as a **key 205A-B** to access the vehicle. EX1007, ¶¶ 60, 70. The **secure key identifier 407** is stored in memory of the wireless device, as shown in Figure 4 below. *Id.*, ¶ 70, Fig. 4; EX2021, ¶ 74.

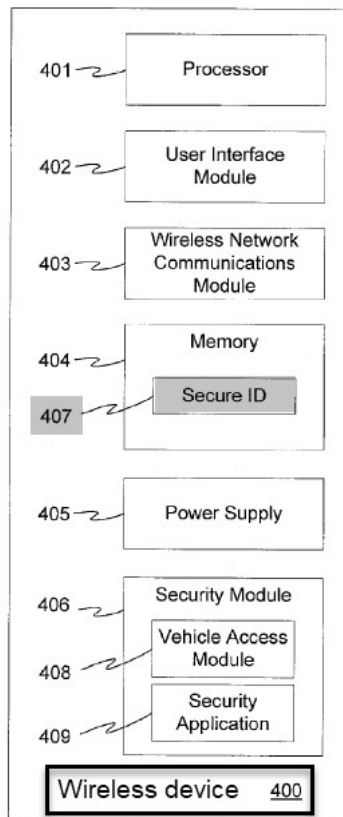


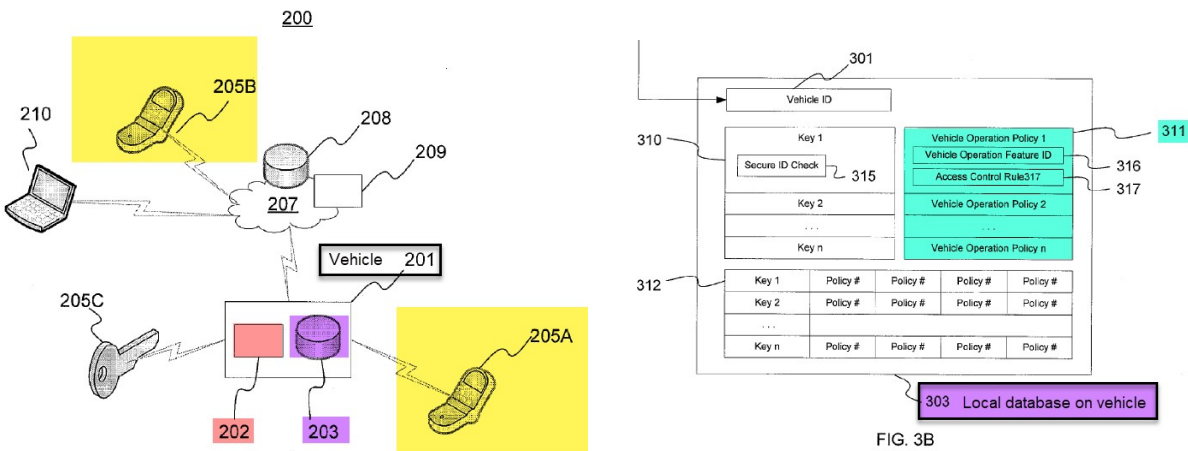
FIG. 4

EX1007, Fig. 4 (annot.).

Importantly, the wireless device's secure key identifier 407 does not include any vehicle operation policy or any access control rule thereof, nor does *Mikan* ever teach or suggest that the vehicle receives any vehicle operation policy or access control rule *from the wireless device*. EX2021, ¶ 75. Instead, *Mikan* makes clear that the wireless device's secure ID 407 is simply used to authenticate the device as a key. *Id.*; EX1007, ¶ 65. And, when that wireless device delivers its secure ID 407 as a signal to be authenticated by the vehicle, *Mikan* teaches that the vehicle

“retrieves” a vehicle operation policy, not from the wireless device, but from the vehicle’s **local database**. *Id.*, ¶ 72.

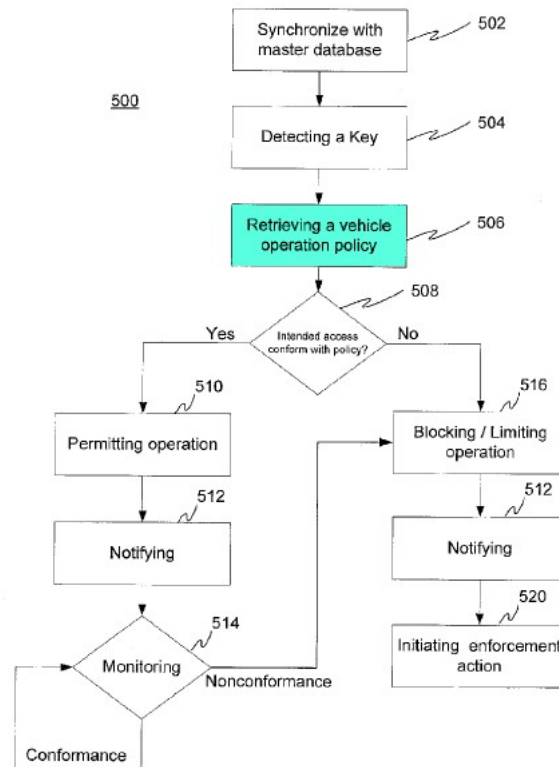
For example, when the vehicle detects a user’s wireless device as a key (e.g. **205A-B**), via the wireless device’s **secure ID 407**, the vehicle’s **control unit 202** “retrieve[s]” the **vehicle operation policy 311** by querying the vehicle’s **local database 203**. *Id.*, ¶ 72, Figs. 2, 3B, 5.



Id., Figs. 2, 3B (annot.). The vehicle’s **control unit 202** queries **local database 203/303** records, using mapping 312 to retrieve any **vehicle operation policy 311** that may be in effect with relation to the authenticated key. *Id.*, ¶¶ 71-72, Fig. 5; EX2021, ¶ 76.

Whether the vehicle’s database must first sync with the **master database** to obtain from the **master database** a **vehicle operation policy 311**, or whether the **vehicle operation policy 311** is “retrieved” from the vehicle’s own **local database**

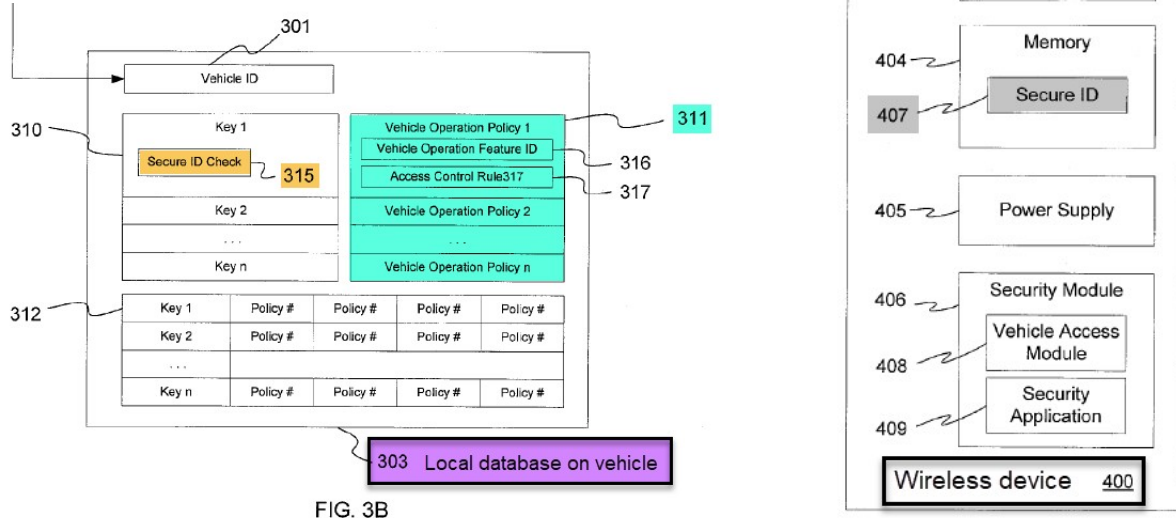
203 by the vehicle's control unit 202 (EX1007, Fig. 5, step 506), Mikan's vehicle never receives any vehicle operation policy from any mobile device. *Id.*, ¶ 59 (“At 506 vehicle operation policy 311 may be retrieved by, for example, querying local database 203.”); *id.*, ¶¶ 71-72, Figs. 5, 3A-B.



Id., Fig. 5 (annot.).

Mikan's vehicle **receives only** a secure ID 407 from the mobile device, not any secure ID 407 including any vehicle operation policy, nor does the vehicle ever receive any vehicle operation policy from the mobile device at all. *Id.*, ¶¶ 59, 64, Figs. 3B, 4.

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.



Id., Figs. 3B, 4 (annot.).

Accordingly, *Mikan*’s vehicle never “receives coded data from the mobile device ... the coded data includes privilege settings,” as the independent claims require. EX1001, claims 1[d-e], 11[d-e], 18[d-e].

VI. All challenged claims in grounds 3-6 must be upheld because *Mikan*’s vehicle never “receives coded data from the mobile device ... the coded data includes privilege settings,” as claimed.

While the Board preliminarily credited Dr. Almeroth’s opinion “[a]s part of the electronic key authentication process, the vehicle receives the vehicle operation policy associated with the authenticated key” (Paper 14 at 47), as detailed in Section

V., it is *the vehicle* that retrieves any vehicle operation policy *from the vehicle's own local database*, *the vehicle* stores those records in the vehicle control unit, and, in order to permit or block any requested action, *the vehicle* compares *each* access request from the wireless device to the locally retrieved vehicle operation policy.

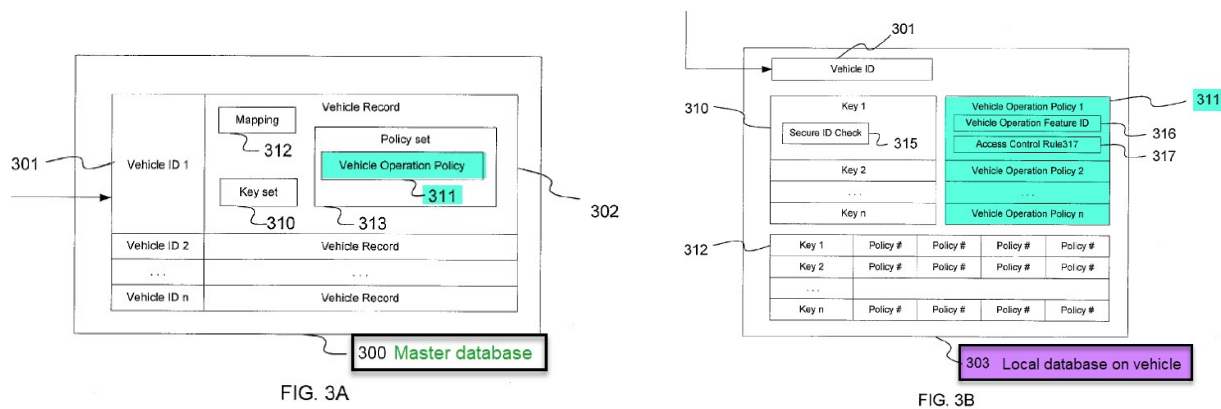
The Board also credited Dr. Almeroth's testimony that *Mikan's* secure identifier 407 "enables the key" to perform certain functions, such as unlocking and using the vehicle (Paper 14 at 44), however *Mikan's* secure ID 407 is merely used as an authenticator of the key, which is "checked" by the vehicle's "secure ID 315." EX1007, ¶¶ 70-71. Thereafter, the wireless device is used merely to transmit individual "access requests" to the vehicle via a "user interface module 402," not via any secure ID. *Id.*, ¶¶ 73-74. *Mikan's* vehicle operation policies, and their included access control rules, are stored and provided to the vehicle's local database, which receives the policies by syncing with a remote master database. When *Mikan's* vehicle receives a secure ID from the alleged mobile device the vehicle may retrieve alleged "privilege settings" from its own database, not "from the mobile device," as required. The wireless device does not transmit any vehicle operation policy to the vehicle at all, let alone transmit them in or with the secure ID 407. *Id.*, ¶¶ 70-71. Therefore, even if the mobile device's secure ID 407 constitutes "coded data," it does not include the vehicle operation policies alleged

to be “privilege settings.” Accordingly, *Mikan*’s vehicle does not receive any “privilege settings” “from the mobile device,” as recited by the claims, let alone any “coded data includes privilege settings.” EX1001, claims 1, 11, 18.

Petitioners rely on *Mikan* alone for alleged disclosure of this independent claim element for all ground 3-6 challenged claims. Pet. 43-45, 57, 62. Petitioners’ addition of the *Xiao* and *Sekiyama* references for grounds 4-6 do not cure *Mikan*’s failures, and Petitioners offer no argument or analysis to the contrary.

A. Petitioners rely on a mobile device’s “secure ID 407” as alleged coded data, but the secure ID 407 does not include any alleged privilege settings.

As shown in Section V., *Mikan* teaches that vehicle operation policies—identified by the Petition as the recited “privilege settings”—are “records” which are stored to in a remote master database, synced with the vehicle’s local database. After synchronization, the vehicle may “retrieve” any vehicle operation policy from its own local database—not from the alleged mobile device. Neither database is in or part of *Mikan*’s wireless device and Petitioners do not argue otherwise. Nor does *Mikan* ever disclose or suggest its wireless device sends any vehicle operation policy to a vehicle. *E.g.*, EX1007, ¶¶ 59, 64, 71-72, Figs. 3A-3B, 4-5. Accordingly, *Mikan*’s vehicle never receives any alleged privilege setting from the alleged mobile device. EX2021, ¶ 121.



EX1007, Figs. 3A-B (annot.).

To use the **key 205A-C**, *Mikan* teaches that the vehicle does not ever *receive* any coded data with privilege settings from the mobile device, but instead the vehicle itself stores the vehicle operation policies. *Id.*, ¶ 72. First, after detecting and authenticating the user's wireless device, vehicle **control unit 202** retrieves any applicable **vehicle operation policy 311** record by querying the vehicle's **local database 203**. *Id.*, ¶ 72. Thereafter, the vehicle's **control unit 202** may "temporarily store or cache the records for the duration of the user[']s operation of the vehicle." *Id.*, ¶ 72. Whether retrieved from the vehicle **local database** or retrieved from the **local database** and then temporarily stored to the vehicle **control unit 202**, the vehicle operation policy 311 records remain *in the vehicle*, and never are, nor need be, "received" from any mobile device. *Id.*, ¶¶ 59, 64, 71-72, Figs. 3A-3B, 4-5; EX2021, ¶¶ 122-123.

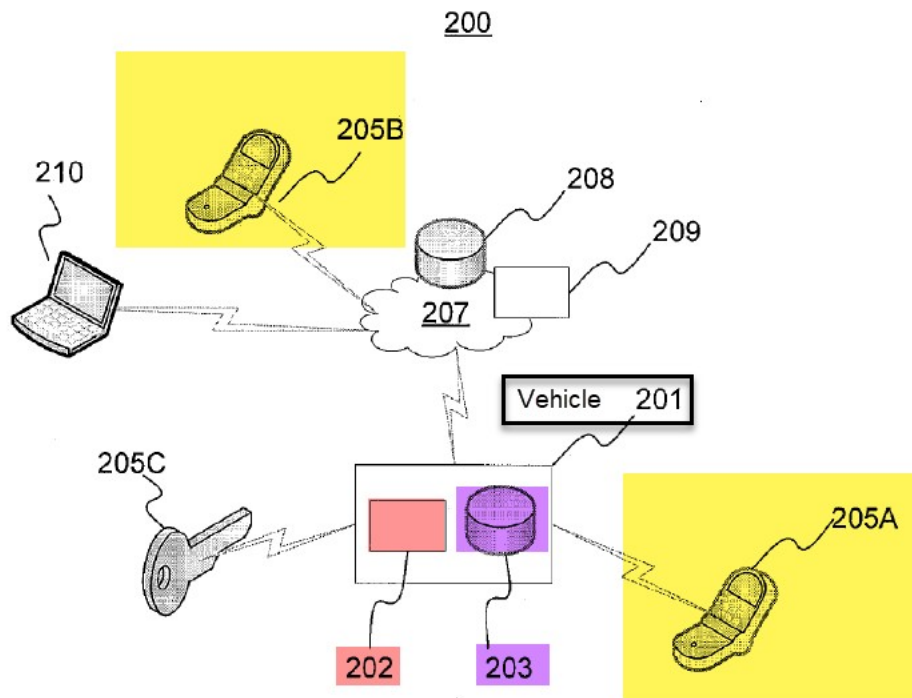
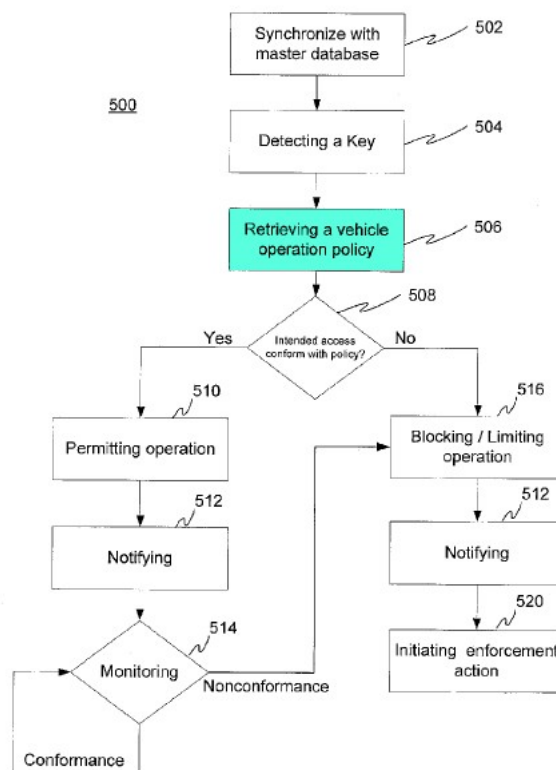


FIG. 2

EX1007, Fig. 2 (annot.).

By maintaining the vehicle operation policy 311 local to the vehicle, *Mikan* teaches that the vehicle itself processes any access request from a user according to the vehicle's locally stored vehicle operation policy. EX2021, ¶ 124. For example, after the master database and local database have synchronized (step 502), a user may approach the vehicle 201, the vehicle detects the secure ID 407 of the wireless device (step 504) and the user sends a user request, or access request, to unlock a vehicle door. EX1007, ¶¶ 72-73, Fig. 5. The vehicle control unit then processes the

access request, comparing the access request with the vehicle operation policy it retrieved from the **local database 203**. *Id.*, ¶¶ 72-74. “Where the access request is consistent with the **retrieved operation policy 311**, control unit 202 may permit the operation of the vehicle at 510,” as shown in Figure 5. *Id.*, ¶ 74. Conversely, where the access request is inconsistent with the **vehicle operation policy 311** the control unit retrieved from the local database, then the control unit 202 may block and/or limit the operation of the vehicle. *Id.*



Id., Fig. 5 (annot.). *Mikan* makes clear that to perform these comparison functions, the vehicle always compares each user access request with the **vehicle operation**

policy 311 “retrieved” from the vehicle’s local database. *Id.*, ¶¶ 72-74; EX2021, ¶ 125.

B. *Mikan* does not disclose, and discourages, a vehicle receiving any privilege settings from a mobile device.

Mikan teaches a vehicle-controlled solution for determining the relationship between any detected key and the vehicle’s locally stored vehicle operation policies, and in turn, retrieving those related vehicle operation policy records during a user’s operation of a vehicle. *E.g.*, EX1007, ¶¶ 59, 72-74. As detailed in Section V., both the master database and the vehicle’s local database include “mapping 312” which “may link vehicle operation policy 311 to keys 205A-C” in the key set records stored to each database. *Id.*, ¶¶ 59, 61, 81, Figs. 3A-B; EX2021, ¶ 126.

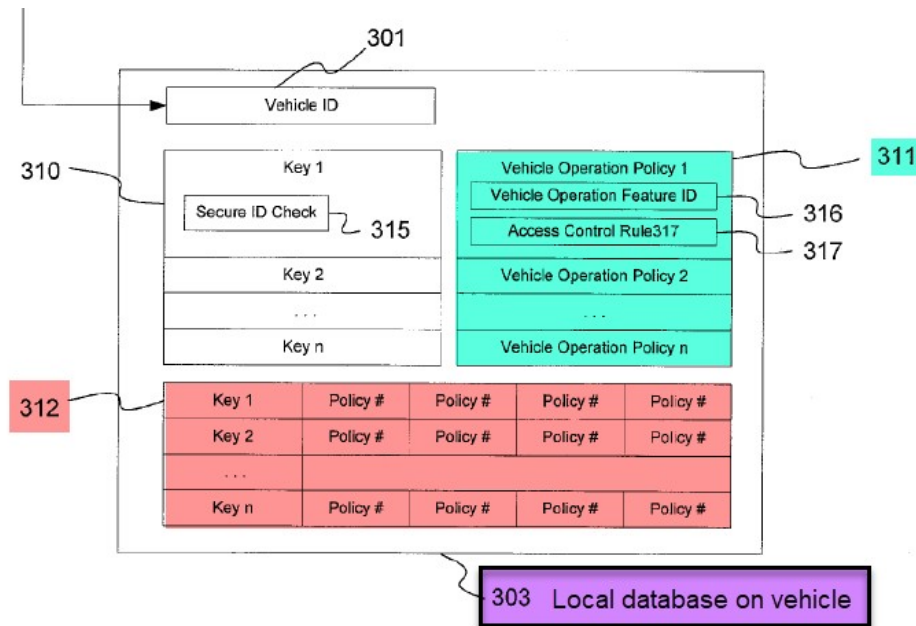


FIG. 3B

EX1007, Fig. 3B (annot.).

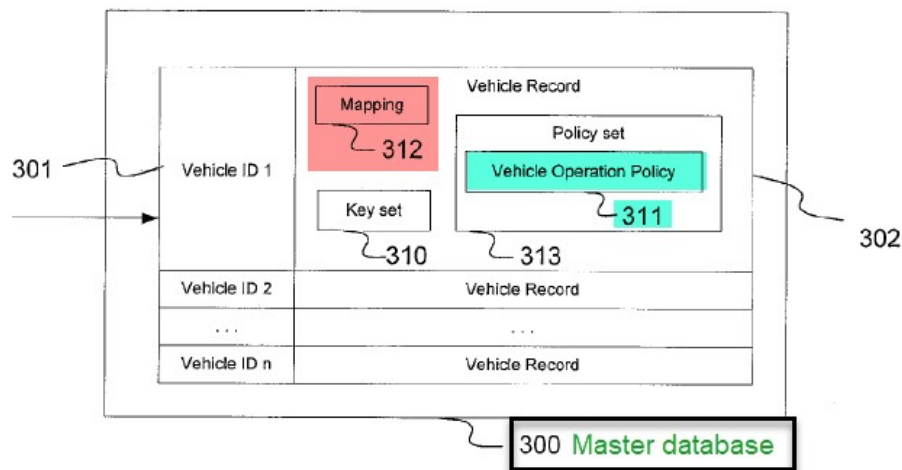


FIG. 3A

Id., Fig. 3A (annot.).

Accordingly, when a vehicle syncs its records with those of the master database, the master database mapping 312 may link which key in a key set relates to which vehicle operation policy/policies 311. *Id.*, ¶¶ 81, 84, Fig. 3A; EX2021, ¶ 127. Likewise, when a vehicle detects a wireless device using its secure ID 407, and authenticates that device as a key 205A-C, mapping 312—which is stored to the vehicle’s local database—determines the relationship between any locally stored vehicle operation policy to that detected and authenticated key. EX1007, ¶¶ 59, 61. No such mapping 312 would be needed by the vehicle were any vehicle operation policies, let alone any “privilege settings,” already received by the vehicle from the mobile device when it received the secure ID 407. *Id.*; EX2021, ¶ 127.

Indeed, were the vehicle operation policy somehow included in any data sent by the mobile device to the vehicle, the vehicle itself would not need to (1)

“retrieve[]” the vehicle operation policy 311 at step 506 by “querying the local database 203,” (2) perform the “mapping” to determine the relationship between a given key from the database’s “key set” with individual operation policies from the database’s “policy set,” or (3) perform the comparison functions between the “retrieved vehicle operation policy 311” and each user access request. EX1007, ¶¶ 72-74, 60-61, Fig. 5; EX2021, ¶ 128. Neither the wireless device itself, nor the secure ID 407 stored in the wireless device, ever transmits any vehicle operation policy to the vehicle. *Id.*

C. Dr. Almeroth’s opinions ignore and even contradict *Mikan*’s solution to retrieve locally stored vehicle operation policies from the vehicle’s local database.

Dr. Almeroth is incorrect in stating that “*Mikan* discloses that the coded data includes privilege settings for the electronic key that limit the types of use of the vehicle.” EX1004, ¶ 220; EX2021, ¶ 129. As detailed in Sections V.VI.A.-B., *Mikan* fails to disclose or suggest any vehicle that receives any “***coded data includes privilege settings,***” let alone “receive coded data ***from the mobile device***” that includes privilege settings. EX1001, claim 1[d-e], 11[d-e], and 18[d-e] (emphases added). Instead, *Mikan* uses locally stored mapping 312 to relate any key in its locally stored key set to its locally stored vehicle operation policies.

EX1007, ¶¶ 59, 61, 72; EX2021, ¶ 129; *see also* sections V.-VI.A-B, *supra*. *Mikan* further contradicts Dr. Almeroth’s additional opinions, as illustrated below.

1. The wireless device does not include or transmit to a vehicle any “associated vehicle operation policy,” as Dr. Almeroth suggests.

Notwithstanding *Mikan*’s express disclosures, Dr. Almeroth erroneously opines that “[t]he wireless device operating as an electronic key be used to unlock and start a vehicle. ... *Mikan* discloses that each electronic key has an associated ‘vehicle operation policy.’” EX1004, ¶ 217 (citing EX1007, ¶ 52). However, paragraph 52 offers no such teaching, and instead describes the communication connections involving the vehicle’s control unit. EX1007, ¶ 52; EX2021, ¶ 130.

Further, Dr. Almeroth failed to appreciate express disclosures of *Mikan*, which teach that any “association” is performed *on the vehicle*, using locally stored mapping 312 to relate vehicle operation policies 311—*stored on the vehicle*—to locally stored keys 205A-C. *Id.*; EX1007, ¶¶ 59-60, 72. In this way, the vehicle itself uses the identifier received from the detected phone for authentication, then the vehicle itself determines from the locally stored records “the vehicle operation policy 311 that may be in effect with relation to the key 205A-C being used.” *Id.*, ¶ 72.

2. Modifying *Mikan* “to transmit the vehicle operation policy as additional coded data, either as a part or in addition to *Mikan*’s secure identifier” renders the data more vulnerable to “tampering,” not less, and vitiates existing efficiencies in *Mikan*’s unmodified system.

As detailed in Sections V.-VI.A.-B., *Mikan*’s vehicle locally stores the vehicle operation policy 311 records it retrieves when a wireless device key is detected. *See* Sections V.VI.A.-B., *supra*; *see e.g.*, EX1007 ¶¶ 71-72; 60-61. By retrieving the vehicle operation policy 311 records from its local database 203, the vehicle does not rely on the “transmission” of any vehicle operation policy from the wireless device, as Dr. Almeroth erroneously states. EX1004, ¶ 221. Accordingly, because the vehicle operation policy is not transmitted to the vehicle from the wireless device, but is instead locally stored and retrieved from the vehicle’s local database, Dr. Almeroth’s asserted motivation to modify this non-existent transmission is nonsensical. EX2021, ¶ 131.

Moreover, no POSITA would have modified *Mikan* “to transmit the vehicle operation policy” “either as part of or in addition to *Mikan*’s secure identifier,” because doing so would render *Mikan*’s local database and its synchronization with the master database superfluous. EX1004, ¶¶ 221-222; EX2021, ¶ 132. *Mikan*’s solution is *more* efficient than Dr. Almeroth’s proposed modification, where vehicle operation policy changes are communicated to a vehicle as part of the

synchronization process, and thus each policy change need only be communicated once. *Id.* The modified system, by contrast, requires the vehicle operation policy to be sent every time the wireless device is used to enter the vehicle, regardless of any change to the policy. *Id.*

Indeed, were *Mikan* modified as Dr. Almeroth proposes, the vehicle operation policy records would be **more** vulnerable to “tampering” by the user, not less. EX2021, ¶ 133. *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. *Id.* 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 multiple times via the wireless device, would inject **additional security vulnerabilities** into *Mikan*’s system. *Id.* Accordingly, a POSITA would not have been motivated to modify *Mikan*’s method of having a vehicle retrieve from its own local database locally stored and locally linked vehicle operation policies in order to reduce “tampering” and “unauthorized access” by users, as Dr. Almeroth speciously claims. EX2021, ¶¶ 133-135.

Dr. Almeroth’s nonsensical and contradictory modifications to *Mikan*’s **more efficient, more secure** solution is “insufficient to present a prima facie case of

obviousness.” *In re Oetiker*, 977 F.2d at 1447; see *Opticon Medical AB*, IPR2019-00975, Paper 154 at 29-30 (finding Petitioner’s proposed modification based on improper hindsight and failed to prove its stated rationale for the proposed modification).

VII. The Petition’s additional deficiencies with respect to the dependent claims.

Claim 6 must be upheld as valid because Petitioners fail to show that any reference discloses or suggests the 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.

While Petitioners argue 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,” *Kleve* teaches the opposite. As detailed in Sections III.-IV., *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. Indeed, *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. *Id.*; *id.*, ¶¶ 40, 43, 75; EX2021, ¶ 137. Moreover, *Kleve* 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.*; EX1005, 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.*

Accordingly, *Kleve* discourages that its Temporary User—whose own vehicle usage will be specifically monitored and controlled by the Vehicle Owner’s actions—can share an eKey for the vehicle with some other user. EX2021, ¶¶ 137-138. Likewise, such sharing among Temporary Users would render meaningless *Kleve*’s disclosures that even for an already-authorized Temporary User, an additional credential match must occur before the drive is authorized. *Id.*, ¶ 139; EX1005, Fig. 5.

Petitioners’ reliance on *Mikan* and *Sekiyama* for alleged obviousness of claim 6 fares no better. First, *Mikan* does not teach a “plurality of electronic keys may be incorporated into mobile devices for use with a vehicle,” as Petitioners erroneously contend. Pet. 65; EX2021, ¶ 140. 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. *Id.*; EX1007, ¶ 65. Because *Mikan*'s secure ID 407 does not include any privilege settings, Petitioners' proposed combination with *Sekiyama* fails to cure the deficiencies of *Mikan*. Any sharing of the key would nonetheless lack the requisite privilege settings included in coded data. Accordingly, neither *Mikan* itself, nor *Mikan* modified in view of *Sekiyama*, renders obvious claim 6.

Claims 12, 13 and 20 must also be upheld. Petitioners fail to offer evidence that any reference discloses or suggests the recited "server associated with a manufacturer of the vehicle" or the mobile device application being "associated with a manufacturer of the vehicle." Pet. 30-32, 58-60. Instead, Petitioners argue that any limitation requiring that components of the recited system and vehicle be associated with "a manufacturer of the vehicle" have no patentable weight because this is somehow "printed matter." *Id.* As an initial matter, "printed matter must be matter claimed for what it communicates." *C R Bard Inc. v. AngioDynamics, Inc.*, 979 F.3d 1372 (Fed. Cir. 2020). Petitioners offer no explanation how the limitations of claims 12, 13 and 20 meet this threshold inquiry of the "printed matter doctrine." Pet. 30-32, 36.

Petitioners' burden of proof notwithstanding, these limitations cannot implicate the printed matter doctrine where the specification provides numerous

examples describing how applications, servers, and vehicles of the vehicle manufacturer are functionally related to the other claimed components of the system/vehicle. *E.g.*, EX1001, 15:15-37 (describing “applications can be augmented with restrictions made by the vehicle manufacturer ... to ensure safety during driving”), 13:20-49 (describing how manufacturer applications “cooperate to provide functionality to the application features and interfaces, while maintaining safety parameters defined by rules”), 13:50-14:2, 47:35-48:2 (the vehicle manufacturer’s provision of cloud services aids in achieving greater simplicity and security for the user). Reading the claims as a whole, the limitations of claims 12, 13 and 20 add these functional characteristics to the claimed systems and vehicle. *Id.*, claims 12, 13, and 20.

Accordingly, claims 12, 13, and 20 must be upheld as valid.

VIII. Conclusion

For the foregoing multitude of reasons, all challenged claims should be upheld as valid.

Dated: April 23, 2025

/Jerry D. Tice II/
Jerry D. Tice II
Reg. No. 73,582 (Lead counsel)
Brenda Entzminger
Reg. No. 76,896 (Back-up counsel)
BUNSOW DE MORY LLP
701 El Camino Real

Redwood City, CA 94063
Telephone: 650-318-6774
Facsimile: 415-426-4744
jtice@bdiplaw.com

Counsel for Patent Owner

37 C.F.R. §42.24(d) CERTIFICATION

The undersigned hereby certifies that this submission, excluding the table of contents, table of authorities, exhibit list, certificate of word count, and certificate of service, contains 13,873 words, as determined using the standard word counting feature of the Microsoft Word program.

Dated: April 23, 2025

/Jerry D. Tice II/

Jerry D. Tice II

Reg. No. 73,582 (Lead counsel)

BUNSOW DE MORY LLP

701 El Camino Real

Redwood City, CA 94063

Telephone: 650-318-6774

Facsimile: 415-426-4744

jtice@bdiplaw.com

Counsel for Patent Owner

CERTIFICATE OF SERVICE

Petitioners have consented to e-mail service in this proceeding. Pursuant to 37 C.F.R. §42.6, the undersigned certifies that on April 23, 2025, a copy of the foregoing document was served by email upon the following counsel at the below email addresses:

Finnegan, Henderson, Farabow, Garrett & Dunner LLP
Joshua L. Goldberg – joshua.goldberg@finnegan.com
James R. Barney - james.barney@finnegan.com
Aidan Skoyles - aidan.skoyles@finnegan.com
Nicholas Eitsert - nicholas.eitsert@finnegan.com

QUINN EMANUEL URQUHART & SULLIVAN, LLP
James M. Glass – jimglass@quinnemanuel.com
Quincy Lu - jimglass@quinnemanuel.com
Jeffrey S. Gerchick - jeffgerchick@quinnemanuel.com
Brett Watkins - brettwatkins@quinnemanuel.com

Dated: April 23, 2025

/Jerry D. Tice II/
Jerry D. Tice II
Reg. No. 73,582 (Lead counsel)
BUNSOW DE MORY LLP
701 El Camino Real
Redwood City, CA 94063
Telephone: 650-318-6774
Facsimile: 415-426-4744
jtice@bdiplaw.com

Counsel for Patent Owner