

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

KIA CORP.,
TOYOTA MOTOR CORP.,
Petitioners,

v.

EMERGING AUTOMOTIVE LLC,
Patent Owner.

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

**EMERGING AUTOMOTIVE LLC'S
PATENT OWNER SUR-REPLY**

TABLE OF CONTENTS

	<u>Page</u>
I. Introduction.....	1
II. All <i>Kleve</i> -based grounds fail because <i>Kleve</i> lacks any “coded data from the mobile device ... the coded data includes privilege settings.”	4
A. Even if the “rental period” or any other alleged “privilege setting” were delivered to the vehicle with a virtual key, nothing in Reply shows any “privilege setting” included in coded data sent from the Temporary User’s mobile device.....	6
1. There is no dispute that, for any rental agreement made <i>after</i> a virtual key is generated, the virtual key cannot include any terms of the nonexistent rental agreement.	7
2. For any rental agreement made <i>before</i> a virtual key is generated, Petitioners claim the vehicle already has restrictions before the Temporary User’s arrival— <i>Kleve</i> does not teach to have the Temporary User send them to the vehicle and doing so would make no sense when the vehicle already has them.	10
3. Even if the virtual key were “only operable during a rental period,” Petitioners offer no reason for “re-sending” to the vehicle the already “delivered” rental period.....	16
4. Petitioners cannot identify a single disclosure in <i>Kleve</i> that the alleged coded data from a mobile device “includes privilege settings.”	17
a. Petitioners misstate Figure 3’s disclosure, but even if it were accurate, it would still fail to teach any privilege setting included in any coded data sent from the Temporary User’s mobile device.....	18
b. Petitioners mischaracterize Figure 7—nevertheless, the starting point of Figure 7A is	

after the virtual key has been generated and distributed.19

B. It is undisputed that *Kleve* does not disclose its alleged “e-key” having any alleged “privilege setting,” and even Petitioners’ hindsight-driven reasons to do so confirm no coded data with privilege settings is ever sent from the Temporary User’s mobile device.20

C. Petitioners do not rebut *Kleve*’s requirement that vehicle restriction limits are “initially set by the Owner at the beginning of the rental term” and therefore cannot be included as any “privilege setting” in a virtual key, which has already been generated.22

III. All *Mikan*-based grounds fail, as the Reply fails to rebut the lack of disclosure of any “coded data from the mobile device ... the coded data includes privilege settings.”24

IV. Petitioners fail to rebut the Petition’s deficiencies as to claims 6, 12-13, and 20.....29

V. Conclusion31

TABLE OF AUTHORITIES

	<u>Page(s)</u>
Cases	
<i>Qualcomm Inc. v. Apple Inc.</i> , 24 F.4th 1367 (Fed. Cir. 2022)	5
Statutes	
35 U.S.C. § 312(a)(3).....	5

I. Introduction

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

Instead, Petitioners hand-wave, urging that because *Kleve* discloses a virtual key and because the parties agree to a rental period, the virtual key must as a matter of “common sense” include a rental period as a “privilege setting” so that the vehicle can enforce the rental period before the Temporary User initiates the rental event. But Petitioners argue that *first* “the rental period would need to be communicated *to the vehicle* with the virtual key” so that “*afterwards*, when the Temporary User arrives at the vehicle within the scheduled rental time,” the vehicle can apply the already-received restrictions. Reply, 3-5. But this just goes to show that even with modification, the alleged privilege settings would not be sent from the Temporary

User's mobile device, as the vehicle would have them. Petitioners offer no evidence, no rationale, and no expert testimony as to why the vehicle would need to receive these alleged restrictions *a second time* from the Temporary User's mobile device.

Petitioners did not submit a reply declaration, leaving the opinions of Patent Owner's expert, Dr. Malek, unrebutted. Petitioners offer no evidence to refute Dr. Malek's testimony showing that the alleged coded data does not include any privilege setting, that it would not have been obvious to do so, and that the proposed combination of *Kleve* and *Hatton* fails.

Though the Institution Decision was preliminarily persuaded that the virtual key will include a rental period—something that *Kleve* does not disclose—that nevertheless does not mean that any alleged coded data from the Temporary User's mobile device would include the rental period, since Petitioners argue the vehicle would already have that information.

In Reply, Petitioners argue that *Kleve*'s virtual key, sent to the vehicle from a server following a rental agreement, ***should*** include a “rental period” to “increase security, efficiency,” and to “accomplish *Kleve*'s goal of establishing and enforcing a rental period.” Reply, 16. While this argument is not supported by any expert testimony, it would nevertheless not cure *Kleve*'s failure to teach that the vehicle receives “***coded data from the mobile device ... the coded data includes privilege settings.***” At best, Petitioners offer a basis for sending the rental period with a virtual

key sent to the vehicle from a *server* “following agreement”—not any reason to include any restriction for data sent from the mobile device of the Temporary User. Reply, 4-5. Indeed, according to Petitioners, the vehicle already knows the rental period or any other restriction and is able to enforce such restrictions—before the Temporary User even arrives at the vehicle—thereby obviating any need for the Temporary User to send to the vehicle the very restrictions it allegedly already has.

Mikan, alone or in combination, also fails to teach or suggest a vehicle receives “coded data from the mobile device when using the eKey ... the coded data includes privilege settings,” required by all claims. *Mikan* never teaches that any vehicle operation policy—the alleged privilege settings—is sent from the mobile device to the vehicle. In Reply, Petitioners fail to rebut *Mikan*’s express teachings (1) that any vehicle operation policy is stored on the master database and/or the vehicle’s local database, (2) that the databases synchronize, (3) that when a key is detected, the vehicle retrieves any vehicle operation policy from the vehicle itself, and (4) that because the vehicle already has these records before the vehicle’s detection and authentication of any key, *Mikan* obviates the need for, and the security risk of, a vehicle also receiving any policy from a mobile device. Petitioners’ motivation to modify *Mikan*’s more secure, more efficient solution, is simply not credible.

All claims must be upheld.

II. All *Kleve*-based grounds fail because *Kleve* lacks any “coded data from the mobile device ... the coded data includes privilege settings.”

The challenged claims have two distinct requirements: (1) “the coded data includes privilege settings” and (2) a vehicle receives the “coded data *from the mobile device* when using the eKey.” *Kleve*’s virtual key—in whatever form and whether or not encrypted—does not include any restrictions whatsoever. In its Response, Patent Owner disproved each faulty premise relied upon by Petitioners—and credited by the Institution Decision—to allege that a “privilege setting” is included in *Kleve*’s virtual key. There is no disclosure of this in *Kleve*, moreover, *Kleve*’s enforcement solution provides that any use restriction is “initially set by the owner at the beginning of the rental period”—after any virtual key has already been generated.

In Reply, Petitioners actually rely on the undisputed inferiority of *Kleve*’s teachings, repeatedly highlighting, for obviousness, *Kleve*’s failure to teach many of the very security features and efficiencies enabled by the innovations of the ’659 Patent, and clearly unavailable in the prior art. But Petitioners offer no evidence or expert testimony in Reply to support the flawed bases on which their *Kleve*-based challenges rest. Petitioners’ unsupported attorney argument that *Kleve*’s virtual key, in hindsight, *should*, as a matter of alleged “common sense,” include a rental period,

does nothing to change the lack of disclosure fatal to all *Kleve*-based grounds.

Reply, 2-3, 12-13, 16.¹

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

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

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

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

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

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

the rental period that Petitioners contend was already “delivered to the vehicle.” *Id.*,

3.

1. **There is no dispute that, for any rental agreement made after a virtual key is generated, the virtual key cannot include any terms of the nonexistent rental agreement.**

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

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

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

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

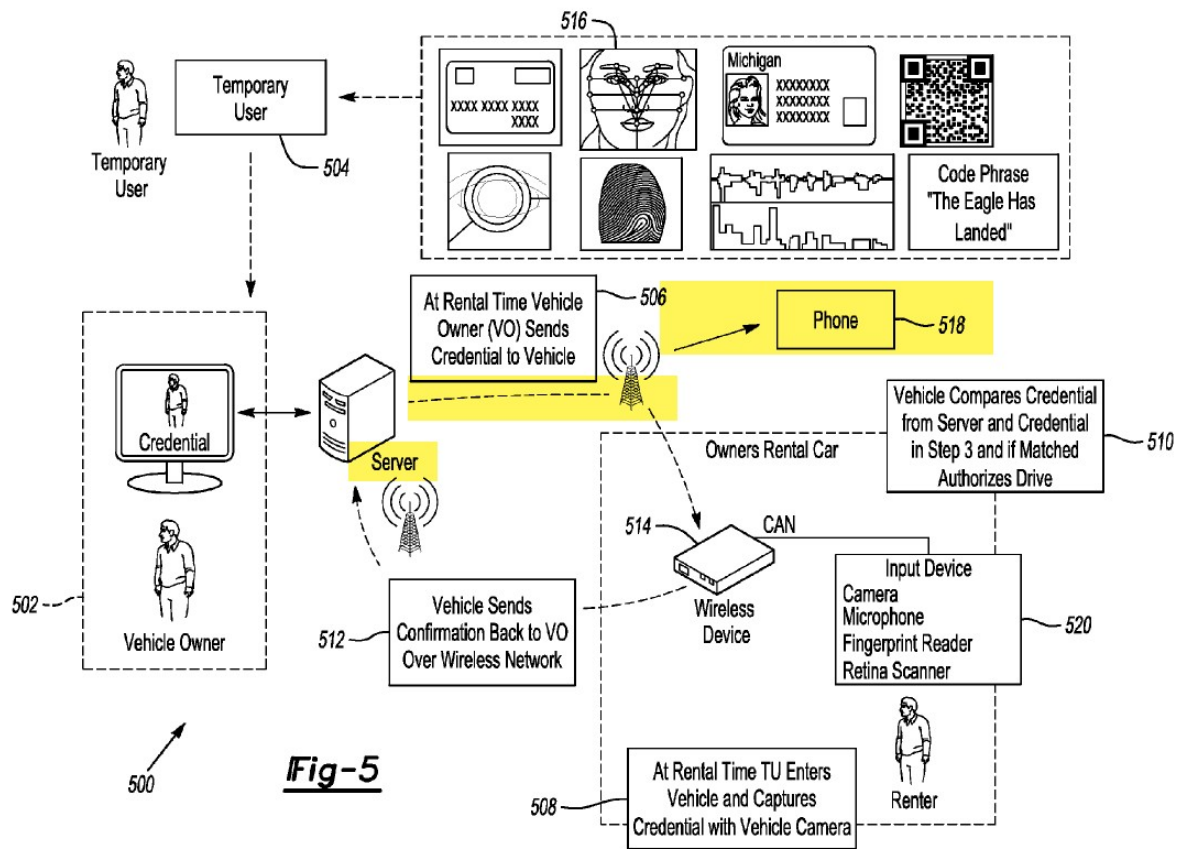
On cross-examination, however, Dr. Almeroth admitted his testimony was wrong. Response, 47-48.

For the alleged “coded data” recited by each independent claim, Petitioners rely on *Kleve*’s disclosure that a virtual key may be sent “in an encrypted message” (Pet., 19 (citing EX1005, ¶ 63)), however this “encrypted message” is sent via the

server “to the VCS, Temporary User’s nomadic device, and/or vehicle Owner[’]s nomadic device.” EX1005, ¶ 63:

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

Kleve’s Figure 5 further illustrates this *unilateral* direction of the alleged “encrypted message” to the VCS, or to the Temporary User’s nomadic device (“Phone – 518”):



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

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

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

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

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

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

has that information. As Petitioners argue, “following agreement, a virtual key is sent to the vehicle,” and “to restrict use of the virtual key to ‘rental time,’ the rental period would need to be communicated *to the vehicle* with the virtual key (or as part of it).” Reply, 4.

Petitioners state that the server generates *two virtual keys*: (1) at step 604: “the server simultaneously generates virtual key and vehicle restrictions,” and thereafter, (2) “the virtual key is *then generated* and sent to the Temporary User at step 616” (no restrictions mentioned). Reply, 3; EX1005, Fig. 6, Abstract. “Afterwards, when the Temporary User arrives at the vehicle within the scheduled rental time, the vehicle applies restrictions.” Reply, 3. By Petitioners’ argument, therefore, “the restrictions are delivered to the vehicle at step 606,” and the vehicle would already know which restrictions to apply well before step 622—when the Temporary User arrives at the vehicle.

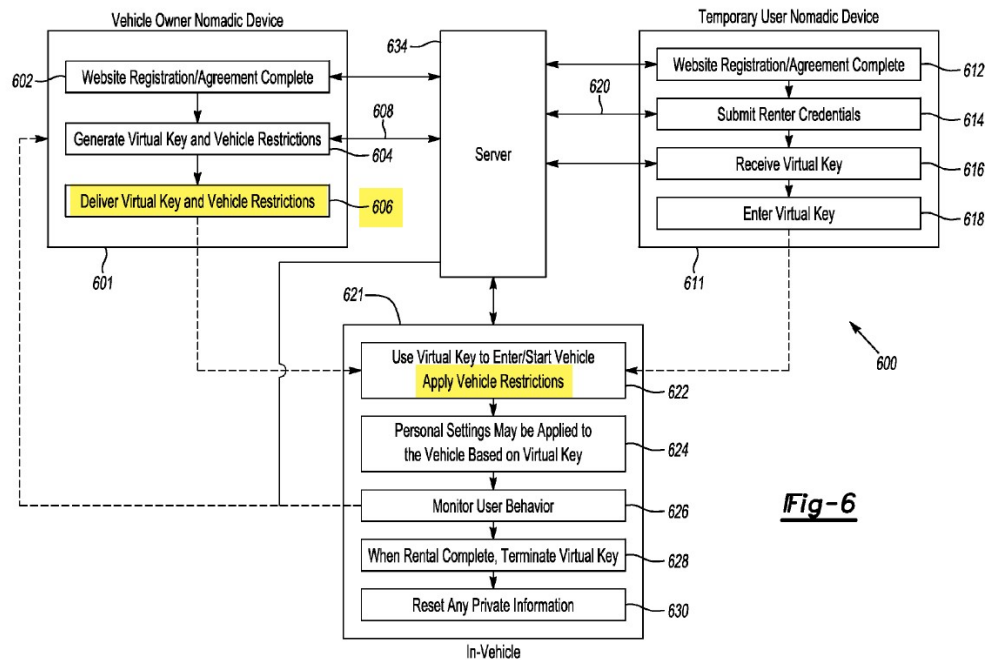


Fig-6

EX1005, Fig. 6.

According to Petitioners’ own argument, even if the vehicle’s “virtual key” included restrictions (it does not), the “virtual key” for the mobile device would not.

Not only does *Kleve* never disclose including any “privilege setting” in any coded data sent from a mobile device to a vehicle, by Petitioners’ own arguments *Kleve*’s system has no need to have the Temporary User’s mobile device re-send to the vehicle the very rental agreement, the very rental period, or any other restrictions, because they were *already delivered to the vehicle before the Temporary User’s arrival at the vehicle*.

Likewise, referring to Figure 7, Petitioners contend that the vehicle “would receive the rental period when the virtual key is sent”,² that “the virtual key includes restrictions, including the rental period,” and that “enforcement of the rental period begins *before step 704*.” Reply, 4-5. *Kleve* teaches that “once the Temporary User initiates the rental event, the system detects a rental time start *at step 706*.” EX1005, ¶ 75. According to Petitioners, therefore, the vehicle already has any alleged restrictions from the virtual key sent to the vehicle before the rental start time—i.e., before the Temporary User even initiates the rental event. By this rationale, Petitioners offer no reason—and no teaching from *Kleve*—to have the vehicle receive the restrictions a second time, from the Temporary User’s mobile device.

Petitioners urge that because *Kleve*’s virtual key will “enable the keyless drive system ... during a given rental period,” the rental period must be included in that virtual key. Reply, 3, 7-11. And indeed, the Board preliminarily relied upon *Kleve*’s disclosure, at paragraph 39, to conclude that the virtual key includes a “rental period.” Paper 14, at 38. But Petitioners contend that there are two virtual keys: (1) “the server simultaneously generates virtual key and vehicle restrictions,”—wherein that key and those “restrictions are delivered to the vehicle,” and thereafter, (2) “the virtual key is then generated and sent to the

² Reply, 4 (citing EX1005, ¶ 63, wherein server sends a virtual key to vehicle).

Temporary User” (no restrictions mentioned). Reply, 3. Paragraph 39, at most, would support Petitioners’ argument that only the virtual key that is sent to the vehicle is “configuring the VCS to enable the keyless drive system for the appropriate Temporary User during a given rental period,” as paragraph 39, like Figure 6, fails to connect any “rental period” or other restriction to the virtual key sent to the Temporary User. EX1005, Abstract, ¶ 39:

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

Accordingly, even if the Board accepts Petitioners’ arguments that “restrictions are delivered to the vehicle” via the virtual key “*sent to the vehicle* configuring the VCS to enable the keyless drive ... during a given rental period,” all *Kleve*-based grounds of the Petition fail regardless. There remains no evidence, nor reason for the Board to conclude that *Kleve*’s vehicle would *also receive* any restriction from the Temporary User’s mobile device.

Even assuming, arguendo, that each of Petitioners’ security concerns were legitimate (e.g., Reply, 10, 15, key “unmoored for the rental period” or “detrimental

to the security of the vehicle”), *Kleve*’s server could associate the rental period with the virtual key “*sent to the vehicle*”—readily addressing each of Petitioners’ concerns without using the mobile device.

Likewise, *Kleve* can readily achieve Dr. Almeroth’s stated end of “increas[ing] security and efficiency,” and “preventing a Temporary User from tampering” or “circumventing restrictions” without including any restrictions in any data sent by the Temporary User’s mobile device. Reply, 16. Indeed, sending from the server would be more secure, more efficient and further reduce any tampering by the Temporary User. *Id.*, 3.

Similarly, Petitioners allege, without expert testimony, that a “POSITA would understand there is a mechanism to enforce the rental period that does not require the use of step 214”—when use restrictions are “initially set.” But, again, by Petitioners’ account, restrictions are generated before the user receives their virtual key—when another virtual key and vehicle restrictions were “delivered to the vehicle” before the Temporary User arrives at the vehicle—and therefore the vehicle would already have the rental period without any need to have the Temporary User send the rental period to the vehicle as well. *Id.*, 3, 7-8, 10. Therefore, Petitioners’ concern about “prevent[ing] the user from using the virtual key before the rental period begins”—like the cited security, efficiency, and tampering concerns of Dr. Almeroth—does not suggest that the Temporary User

should send to the vehicle the rental period that Petitioners state was already delivered to the vehicle. *Id.*, 3, 13.

Accordingly, whether the Board accepts Petitioners’ attorney arguments as to what *Kleve* *should* have, but does not disclose, as opposed to Patent Owner’s reliance on *Kleve*’s express teachings of *when* use restrictions are set by the vehicle owner, all *Kleve*-based grounds of the Petition fail regardless. EX1005, ¶¶ 43 (“initially set by the Owner at the beginning of the rental term”), 75 (“performance limitations and restrictions assigned by the vehicle owner at the start of the rental period”).

Even under Petitioners’ theories to modify *Kleve*—having no basis in any asserted reference—the server can generate a virtual key, “*sent to the vehicle*” with the alleged restrictions “delivered to the vehicle,”—all without any need to *re-send* to the vehicle the rental agreement or rental period already delivered to the vehicle. Reply, 3, 4. There remains no disclosure of, nor any reason for, *Kleve*’s Temporary User’s mobile device to send coded data that includes the restriction already delivered to the vehicle.

3. Even if the virtual key were “only operable during a rental period,” Petitioners offer no reason for “re-sending” to the vehicle the already “delivered” rental period.

Kleve provides no fewer than seven examples disproving Petitioners’ misstatement that the virtual key is “only operable during a rental period.” EX1005,

¶¶ 43, 53-55, 79-80. As the Institution Decision credited Petitioners’ misstatement, the Response detailed *Kleve*’s disclosure that the virtual key is terminated beyond the end of the rental period and terminated before the rental end time. Response, 21-26. Petitioners offer no rebuttal on this point, but instead merely repeat the Institution Decision’s reliance on Petitioners’ misstatement. Reply, 1-3, 8.

Kleve’s disproving examples notwithstanding, even if the virtual key were “only operable during a rental period,” Petitioners still fail to show any reason why the vehicle would need to re-receive the rental period from the Temporary User if—as Petitioners contend—that rental period was already “delivered to the vehicle” beforehand. *Id.*, 3.

4. Petitioners cannot identify any disclosure in *Kleve* that the alleged coded data from a mobile device “includes privilege settings.”

The Petition failed to point to any disclosure of *Kleve* that the alleged coded data from the Temporary User includes any alleged “privilege setting.” While Petitioners try to supplement the Petition in Reply, without expert testimony, the attempted supplementation fails.

- a. **Petitioners misstate Figure 3’s disclosure, but even if it were accurate, it would still fail to teach any privilege setting included in any coded data sent from the Temporary User’s mobile device.**

Petitioners invent a disclosure in *Kleve*, arguing that “limitations are pre-assigned before the start of the rental term.” Reply, 9-10. In reality, *Kleve* states: “at 326, the VCS may **implement assigned** vehicle control restrictions **during the use of the rental term** by mitigating vehicle performance while preventing the Temporary User to exceed a limitation set by the Owner.” EX1005, ¶ 51. During the rental term, therefore, the VCS implements restrictions. But *Kleve* dictates such restrictions are “**assigned by the vehicle owner at the start of the rental period.**” *Id.*, ¶ 75. Like Figure 3, Figure 7 teaches that after the Temporary User initiates the rental event, the VCS downloads the restrictions assigned by the vehicle owner at the start of the rental period. *Id.* Accordingly, Figure 3 does nothing to undermine *Kleve*’s unequivocal disclosure that “restriction limits [are] initially set by the Owner at the beginning of the rental term.” *Id.*, ¶ 43.

Even if Petitioners’ fictional disclosure were accepted, Petitioners’ argument would still fail to show that any coded data sent from a Temporary User’s mobile device ever includes any privilege setting. Petitioners’ arguments about the “rental start time” of various figures does nothing to change the fact that by that start time,

the virtual key has already been generated. *E.g., id.*, ¶ 75 (vehicle detects start time when Temporary User initiates rental event).

Likewise immaterial to the Petition’s failure is whether Figure 3 shows any “equivalent to step 214” to extend the rental period. Reply, 10. Figure 3 does teach a mechanism for extending the rental term, and like Figure 2, the rental time extension actions are unrelated to the generation of a virtual key. EX1005, ¶ 54, Fig. 3. But whether it does or not fails to contradict *Kleve*’s teaching that restriction limits are “initially set by the Owner at the beginning of the rental term,” and likewise fails to show any “privilege setting” sent in coded data from the Temporary User’s phone to the vehicle. Reply, 10; EX1005, ¶ 43.

b. Petitioners mischaracterize Figure 7—nevertheless, the starting point of Figure 7A is *after* the virtual key has been generated and distributed.

Petitioners’ new reliance on Figure 7 is also unavailing and certainly fails to cure the Petition’s deficiencies since the starting point of Figure 7A proceeds *after* the vehicle has been rented and a virtual key has already been generated and distributed. *Id.*, ¶¶ 17, 75. Step 702’s “monitoring and report[ing] usage” cannot include the vehicle’s monitoring and reporting of any “performance limitations and restrictions assigned by the vehicle owner,” since the vehicle does not even “*download* performance limitations and restrictions assigned by the vehicle owner” until step 708. *Id.*, ¶ 75. Likewise, step 702’s “monitoring and report usage” cannot

be monitoring the not-yet-downloaded performance limitations and restrictions, since that monitoring does not even commence until step 710, and is further detailed in steps 712-718. *Id.*, ¶¶ 76-79. Indeed, regardless of timing, *Kleve* discloses that any “restrictions” are “downloaded” by the vehicle separate and apart from any “virtual key.” *Id.*, ¶ 75, Fig. 7A.

Notwithstanding, neither Figure 7A nor its accompanying disclosures ever mention a Temporary User sending coded data to the vehicle, which certainly fails to suggest that this *unmentioned* coded data should include any “privilege setting.” *Id.*, Fig. 7A, ¶¶ 75-80.

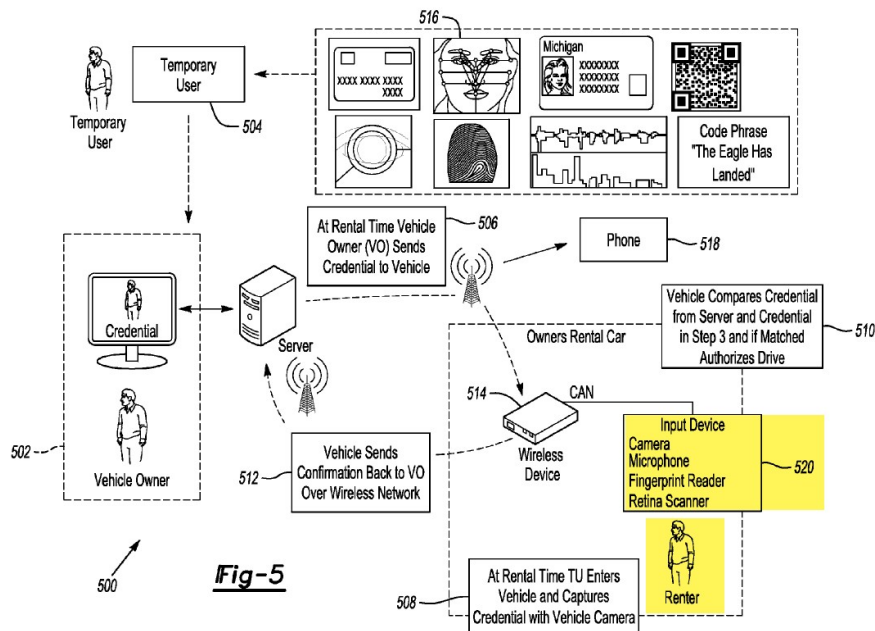
B. It is undisputed that *Kleve* does not disclose its alleged “e-key” having any alleged “privilege setting,” and even Petitioners’ hindsight-driven reasons to do so confirm no coded data with privilege settings is ever sent from the Temporary User’s mobile device.

Kleve never discloses its “virtual key” as having any privilege setting. *Kleve* teaches setting and applying use restrictions *after* the virtual key is already generated. Response, 5-41. Nevertheless, Petitioners argue that the “virtual key” *should* include alleged privilege settings for alleged security concerns. Petitioners contend there is some security difference between a virtual key and a credential, such that “the virtual key and the credential have complementary purposes: the former allows access (but only at rental time, see Fig. 5) and the latter is an

additional security check to ensure the temporary user is who they claim to be.”

Reply, 6.

But by Petitioners’ own argument, then, the user’s input of a matrix barcode at input device 520 (EX1005, ¶ 66, Fig. 5) merely “ensure[s] the temporary user is who they claim to be,” whereas the vehicle had already received any restrictions alongside *its virtual key*—sent before another virtual key was generated and sent to the Temporary User—and likewise before the Temporary User had already used *their* virtual key to “access the vehicle (but only at rental time),” as “the vehicle limits entry to the rental time.” Reply, 6, 3-4 (describing two virtual keys generated, one at step 604 “sent to the vehicle,” and thereafter, at step 616, “the virtual key is *then generated* and sent to the Temporary User”).



EX1005, Fig. 5 (showing “input device” 520), ¶ 66 (“matrix barcode” entered at 520).

By Petitioners’ sequence of events, the vehicle already had restrictions delivered to the vehicle before the Temporary User ever used their virtual key, and certainly before the “credential verification” of the matrix barcode—alleged coded data—inputted at input device 520. But Petitioners do not—and cannot—explain why any “matrix barcode” inputted by the Temporary User at input device 520 should include any restriction, where Petitioners contend that the vehicle has not only already received any vehicle restrictions, but also already allowed the Temporary User access to the vehicle by their virtual key.

Accordingly, whether or not there is some security difference between *Kleve*’s virtual key and its credential, there remains no reason for the alleged coded data—a matrix barcode—to include any privilege settings.

C. Petitioners do not rebut *Kleve*’s requirement that vehicle restriction limits are “initially set by the Owner at the beginning of the rental term” and therefore cannot be included as any “privilege setting” in a virtual key, which has already been generated.

Even after Reply, Petitioners failed to identify *any disclosure* whereby *Kleve* teaches or suggests including any rental period or any other restriction in any coded data sent to the vehicle from the Temporary User’s mobile device. Indeed, Patent Owner demonstrated that this would be contrary to the express teachings of *Kleve*,

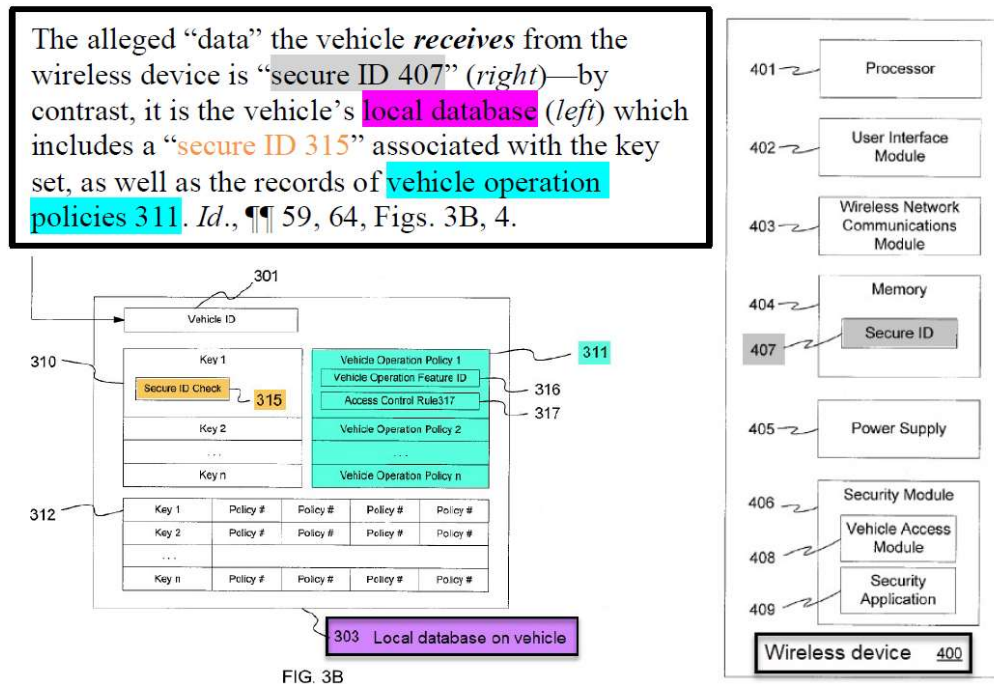
which teach to set and implement any restrictions *after* the virtual key has been generated: “initially set by the Owner at the beginning of the rental term.” Response, 5-41.

Kleve’s timing is not limited to what Petitioners characterize as “optional step 214.” Reply, 11, 14. For example, *Kleve* reiterates this required timing when describing Figure 7: “performance limitations and restrictions assigned by the Vehicle Owner *at the start of the rental period.*” EX1005, ¶ 75. And to the extent the owner’s *discretion* in setting restrictions is somehow suggested to undermine the Petition’s failures, *Kleve* again proves Petitioners wrong. First, equally “optional” is *Kleve*’s generation of a virtual key and whether the parties may agree to rental terms. *Id.*, ¶¶ 39 (“system *may* generate a virtual key”), 84 (“*may* agree to terms”), 38 (same). Indeed, *Kleve* teaches the vehicle may not download any restrictions until the Temporary User has initiated the rental period, which makes sense, as the vehicle would not be able to apply any restrictions for an earlier renter. *Id.*, ¶ 75, Fig. 7A.

Second—optional or not—*Kleve* would have no reason to teach setting use restrictions to be “monitored” and “enforced” (e.g., *id.*, ¶¶ 43, 75) were those very same restrictions—which were agreed to in the rental agreement—somehow already included in the generated virtual key. *E.g.*, Response, 1-2, 16, 34.

III. All *Mikan*-based grounds fail, as the Reply fails to rebut the lack of disclosure of any “coded data from the mobile device ... the coded data includes privilege settings.”

The Response showed—and the Reply fails to rebut—that *Mikan*’s vehicle never receives any coded data that includes privilege settings from a mobile device. Instead, *Mikan* makes clear that it is the *vehicle itself* 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 vehicle’s locally retrieved vehicle operation policy. Response, 58-75. While Petitioners repeatedly seek to conflate the “secure ID check 315” of the vehicle’s local database with the “secure ID 407” of *Mikan*’s wireless device (e.g., Reply, 20)—the alleged “coded data”—the phone’s secure ID 407 is merely used as an authenticator of the key, which is “checked” by the vehicle’s “secure ID 315.” *Id.*; EX1007, ¶¶ 70-71. And, in any event, no privilege settings are included in the phone’s “secure ID 407.” Response, 62-73.



Response, 67.

Indeed, Petitioners cannot rebut *Mikan*’s unambiguous teachings that any vehicle operation policies, and their included access control rules, are stored and provided to the vehicle’s local database, which receives the policies not from any mobile device, but by syncing with a remote master database. *Id.*, 58-75. Moreover, Petitioners offer no evidence to refute Dr. Malek’s testimony establishing that *Mikan* discourages sending any vehicle operation from a user’s mobile device. By *avoiding* storing on or sending from the user’s phone any vehicle operation policies, *Mikan*’s solution to store vehicle operation policies on the master database and the

local database is already *more secure*, and *less vulnerable* to Dr. Almeroth's concerns of a user "tampering with" or circumventing use restrictions. *Id.*, 73-79.

Neither Petitioners, nor *Mikan* itself, offer any reason to transmit the vehicle operation policy from the wireless device to the vehicle, as *Mikan* teaches that the vehicle itself already has synched with the master database before the detection and authentication of the mobile phone key and the vehicle's local database already has any vehicle operation policy associated with any key for that vehicle.

Ultimately, Petitioners fail to rebut that *Mikan*'s wireless device does not transmit any vehicle operation policy to the vehicle *at all*, let alone transmit it in or with the secure ID 407. Instead, Petitioners misunderstand their burden on obviousness, claiming that the reference "does not preclude" modifying its teachings to satisfy the recited limitations of the '659 Patent, even though that is not disclosed and discouraged. Reply, 19-20. Each of Petitioners' unsupported attorney arguments in Reply are contradicted by *Mikan* itself.

The alleged privilege settings—vehicle operation policies—are only stored in the master database 300 or the local database 303. *Id.*, 58-67 *Mikan* makes clear that the two databases sync, and the vehicle retrieves any vehicle operation policy from its own database. *Mikan*'s Figures alone further illustrate that fact. Figures 3A and 3B disclose the master and local database's storage of vehicle operation policy records and the mapping function to associate each policy with its key; they stand

in stark contrast to the absence thereof in *Mikan*'s phone, depicted in Figure 4.

Compare EX1007, Figs. 3A-3B with *id.*, Fig. 4:

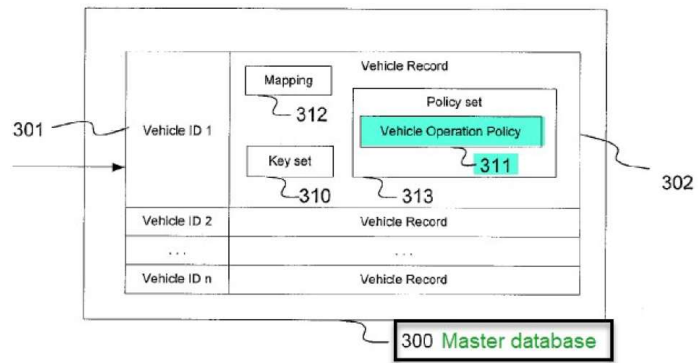


FIG. 3A

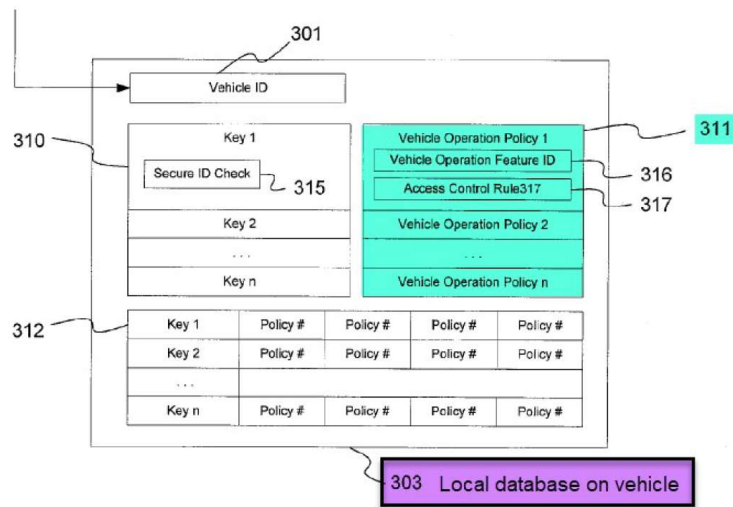


FIG. 3B

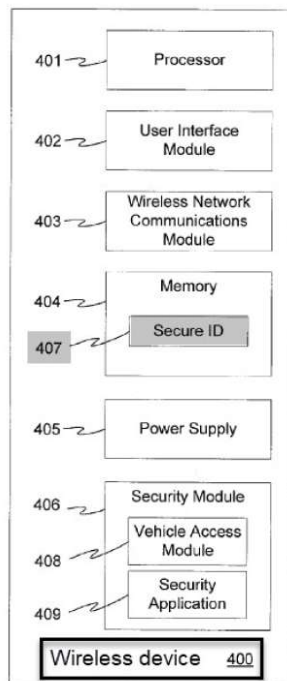


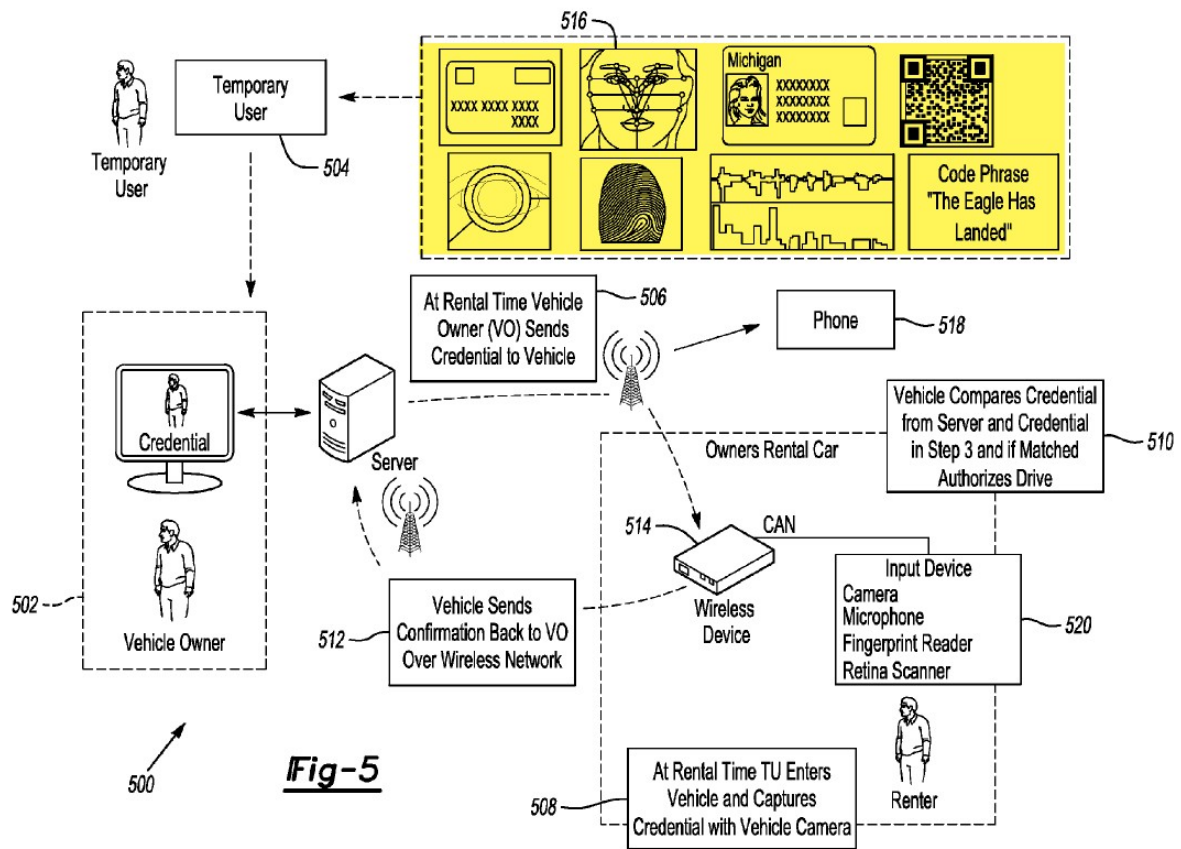
FIG. 4

In Reply, Petitioners argue that their proposed modification allegedly solves *Mikan*'s problem when the vehicle is "out of range of wireless network" (Reply, 22)—but first, this solves nothing, as the phone would be out of range as well. Second, *Mikan* itself actually provides a real solution to this problem—one that is consistent with keeping any vehicle operation policy stored in a master or local database: "when communication cannot be established, master application 209 or master database 208 may queue the request for a later time." EX1007, ¶ 85. Ultimately, Petitioners do nothing to cure their incredible motivation to modify. Storing the vehicle operation policy records in the master and local database is already more secure and more efficient than Petitioners' unjustified proposal to

have the phone send to the vehicle the very vehicle operation policy records it already has.

IV. Petitioners fail to rebut the Petition’s deficiencies as to claims 6, 12-13, and 20.

Petitioners offer neither expert testimony nor evidence to rebut Patent Owner’s showing that *Kleve* does not teach, and in fact discourages, its Temporary User sharing a virtual key with another user. Response, 79-80. Petitioners leave unexplained how one user’s *unique Temporary User identification* would be modified to activate the vehicle for another user—as *the user identifier* of *Kleve* is unique to each individual user—let alone any reference-based motivation to modify or any reasonable expectation of success. *Id.*; EX1005, ¶¶ 69, 37, 63. Apart from hindsight-bias, Petitioners offer no reason why *Kleve* should be modified to share a virtual key with another user. Response, 79-80.



EX1005, Fig. 5.

Petitioners further fail to cure the relied-upon misstatements for the proposed *Mikan/Sekiyama* combination, as *Mikan* teaches that each wireless device may have only one embedded “key” at a time—even if that key can be any one of keys 205A-C—that each device has its own secure ID 407, for authorization, and in any event, the secure ID 407 does not include any privilege settings. Response, 80-81; EX1007, ¶¶ 5, 50, 60, 69, claim 3.

Accordingly, claim 6 must be upheld.

Claims 12-13 and 20 must be upheld, as Petitioners failed to offer evidence that any reference discloses or suggests the recited “server associated with a manufacturer of the vehicle”—instead relying on the hindsight-driven, conclusory assertions of Dr. Almeroth. Pet., 30-32, 58-60. Moreover, Petitioners do not even attempt to rehabilitate their failed reliance on the “printed matter doctrine.” Response, 81-82.

V. Conclusion

The Board should uphold each of the challenged claims.

Dated: September 10, 2025

Respectfully submitted,

/Jerry D. Tice II/

Jerry D. Tice II

Reg. No. 73,582 (Lead counsel)

Brenda Entzminger

Reg. No. 76,896 (Back-up counsel)

Aaron R. Hand

Reg. No. 80,694 (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

bentzminger@bdiplaw.com

Counsel for Patent Owner

37 C.F.R. §42.24(d) CERTIFICATION

The undersigned hereby certifies that this submission, excluding the tables of contents, certificate of word count, exhibit list, and certificate of service, contains 5,598 words, as determined using the standard word counting feature of the Microsoft Word program.

Dated: September 10, 2025

/Jerry D. Tice II/

Jerry D. Tice II

Reg. No. 73,582 (Lead counsel)

Brenda Entzminger

Reg. No. 76,896 (Back-up counsel)

Aaron R. Hand

Reg. No. 80,694 (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

bentzminger@bdiplaw.com

Counsel for Patent Owner

CERTIFICATE OF SERVICE

Petitioner has consented to e-mail service in this proceeding. Pursuant to 37 C.F.R. §42.6, the undersigned certifies that on September 10, 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
Ryan Davies – ryan.davies@finnegan.com

Quinn, Emanuel, Urquhart & Sullivan LLP
James M. Glass – jimglass@quinnemanuel.com
Quincy Lu – quincylu@quinnemanuel.com
Ron Hagiz – ronhagiz@quinnemanuel.com
Jeffrey S. Gerchick – jeffgerchick@quinnemanuel.com
Brett Watkins – brettwatkins@quinnemanuel.com

Dated: September 10, 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
bentzminger@bdiplaw.com

Counsel for Patent Owner