IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

_____

BEFORE THE PATENT TRIAL AND APPEAL BOARD

_____

KIA CORP. and TOYOTA MOTOR CORP.,

Petitioners,

v.

EMERGING AUTOMOTIVE LLC,

Patent Owner.

_____

Case No. IPR2024-01167

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

_____

PETITIONERS' REPLY

TABLE OF CONTENTS

I. Introduction....1

II. Ground 1: Kleve....1

A. PO's Summary of Kleve is Internally Inconsistent and Ignores its Full Disclosure....2

1. Kleve Teaches Assigning and Enforcing Restrictions Before the Rental Period....3

2. PO Conflates Kleve's Virtual Key with Its Credential....5

3. Step 214 Is Not the Only Mechanism for Setting Restrictions....7

4. The Virtual Key Is Not Unmoored from Restrictions....10

B. Kleve Discloses a Virtual Key that Includes Privilege Settings....11

C. Kleve Renders Obvious Including Privilege Settings in Coded Data Associated With a Virtual Key....16

D. PO's Arguments on Motivation to Combine Are Misplaced....17

III. Ground 3: Mikan....18

A. PO Relies on Exemplary Embodiments as Limiting....19

B. Mikan Renders Obvious Providing the Vehicle Operation Policy as Coded Data....21

IV. The Dependent Claims Are Obvious....22

V. Conclusion....23

EXHIBIT LIST

Exhibit	Description
Ex. 1001	U.S. Patent No. 11,738,659 to *Penilla* et al.
Ex. 1002	Prosecution File History for U.S. Patent No. 11,738,659.
Ex. 1003	Curriculum Vitae of Dr. Kevin Almeroth.
Ex. 1004	Declaration of Dr. Kevin Almeroth.
Ex. 1005	U.S. Patent Pub. No. 2014/0129053 to Kleve et al.
Ex. 1006	Japanese Laid Open Patent Application Publication No. 2010-126949 to Sekiyama
Ex. 1007	U.S. Patent Pub. No. 2008/0150683 to Mikan et al.
Ex. 1008	U.S. Patent No. 9,002,536 to Hatton
Ex. 1009	U.S. Patent No. 7,868,736 to Fukushima et al.
Ex. 1010	U.S. Patent No. 8,737,913 to Xiao et al.
Ex. 1011	U.S. Patent Application No. 61/478,436
Ex. 1012	U.S. Patent Application No. 61/745,729
Ex. 1013	U.S. Patent Application No. 13/452,882
Ex. 1014	U.S. Patent Application No. 13/842,158
Ex. 1015	U.S. Patent Application No. 14/063,638
Ex. 1016	U.S. Patent Application No. 15/344,566
Ex. 1017	U.S. Patent Application No. 15/180,306
Ex. 1018	U.S. Patent Application No. 14/303,442
Ex. 1019	U.S. Patent Application No. 16/653,958
Ex. 1020	U.S. Patent Application No. 15/854,241

Exhibit	Description
Ex. 1021	U.S. Patent Application No. 15/607,418
Ex. 1022	Text Comparison of U.S. Pat. App. No. 13/842,158 to U.S. Pat. App. No. 14/063,638
Ex. 1023	Order Granting Request For Ex Parte Reexamination, Reexamination Control No. 90/019,456, Patent No. 11,738,659 (April 15, 2024)
Ex. 1024	Docket Control Order in *Emerging Automotive LLC v. Kia Corp.*, No. 2:23-CV-00437-JRG (E.D. Tex.) (Feb. 6, 2024)
Ex. 1025	Notice of Hearing in *Emerging Automotive LLC v. Kia Corp.*, No. 2:23-CV-00437-JRG (E.D. Tex.) (Jan. 6, 2025)
Exs. 1026-1047	Intentionally Left Blank
Ex. 1048	Transcript of Deposition of Dr. Sam Malek, June 25, 2025

I. INTRODUCTION

PO's Response retreads its preliminary response arguments: that Kleve's optional mechanism for setting restrictions (*i.e.* the claimed **privilege settings**) after the rental period begins is the ***only*** mechanism for setting restrictions, and that a POSITA would not add encryption to Kleve because Hatton only uses encryption for "authentication" and not "confidentiality." The Board rejected both arguments, finding that Kleve's virtual key is only usable during a rental period, which requires enforcing such a restriction ***before*** the rental period begins, and that a POSITA would have understood, based on Hatton, that encrypted wireless communications would be effective in preventing unauthorized access to a vehicle.

PO's arguments on Mikan are premised on the legally incorrect argument that because Mikan discloses transmitting restrictions to the vehicle by synchronizing a master and local database, a POSITA would be discouraged from using other well-known techniques, such as including the same information in the coded data communicated via the electronic key. PO's expert admitted that Mikan discloses a disadvantage in this approach that is solved by the proposed modification.

II. GROUND 1: KLEVE

As the Board correctly concluded in its institution decision, Kleve "describes an e-key that is only operable during a rental period." ID 37; EX1005, ¶39. As a result, the rental period is set as part of the virtual key. Pet. 15-16, 20. Nothing in

PO's Response (Paper 17, "POR") refutes Kleve. As it did in its preliminary response, which the Board rejected, PO relies on step 214 of Figure 2 where the vehicle owner can set restrictions after the rental period begins. These teachings, however, do not preclude setting at least the rental period in advance to ensure the virtual key is only operable during the rental period. And it makes no sense for Kleve to require the rental period to begin before the rental period can be set.

A. PO's Summary of Kleve is Internally Inconsistent and Ignores its Full Disclosure

PO provides a "summary" of Kleve that selectively ignores Kleve's teachings and is internally inconsistent. POR 5-26. PO concedes that prior to generating a virtual key, the owner and renter agree on a set of restrictions ***including*** the rental period. POR 5-9; *see also* EX1001, 3:21-23 ("privileges" include "period of time" that electronic key is active). Yet PO argues that such restrictions are not assigned to the vehicle until ***after*** the rental period begins. POR 14-16. Such a strained reading contradicts Kleve's teachings, and it is nonsensical to require restrictions be set ***only*** during the rental period when the rental period ***itself*** is a restriction. Moreover, PO's reading makes no sense in terms of operational security, as the virtual key is delivered to the renter before any restrictions are set, and would therefore be unmoored from any timing and use restriction.

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

Enforcing the rental period before the rental period begins is both common sense and made clear in Kleve. As the Board found, Kleve's virtual key is "only operable during a rental period." ID 37; EX1005, ¶39 ("The virtual key … enable[s] the keyless drive system for the appropriate Temporary user ***during a given rental period***."). Thus, the virtual key and its associated coded data includes (or it would have been obvious to include) at least the rental period so that access to vehicle is limited to "a given rental period." Pet. 15, 20; EX1004, ¶¶96, 111, 139-140.

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

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

rental term. *Id.*; *see also* EX1005, Figs. 8-9, ¶¶84-85, 89-90 ("load weight" and "amount of miles" restrictions assigned *before* "begin[ning] the keyless vehicle rental authorization process"). Kleve further notes "[c]ontrolling usage to enforce compliance with the rental agreement terms," which would include the rental period. EX1005, ¶51. The enforcement of any rental period, including limiting usage of a virtual key to that period, requires that the rental period be communicated to the server before it begins.

Kleve also teaches "monitor[ing] the vehicle for the ***entire*** rental period." EX1005, ¶54. Restrictions must therefore be assigned ***prior*** to the start of the rental period in order to monitor usage for the entire period.

In addition, Kleve states that following agreement, a virtual key is "sent to the vehicle allowing Temporary user access to the Owner's vehicle" but only "[a]t rental time." *Id.*, ¶62, Fig. 5. 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).

Kleve further describes in Figure 7 that the VCS "may begin monitoring and report usage" at step 702 and then "wait for the rental period to start at step 704." EX1005, ¶75. Thus, enforcement of the rental period begins before step 704. The VCS would receive the rental period when the virtual key is sent, *e.g.*, "in an encrypted message to the VCS." *Id.*, ¶63. Thus, the virtual key includes restrictions,

including the rental period. Following "the start of the rental period at step 708," the "system may begin to download performance limitations and restrictions assigned by the vehicle," indicating that such restrictions were assigned prior to the start of the rental period. *Id.*, ¶75.

PO's summary of Kleve ignores such teachings, instead elevating a single, admittedly optional, step from Figure 2 to argue that Kleve's restrictions can ***only*** be set after the rental period starts. Kleve's system is not so limited.

2. PO Conflates Kleve's Virtual Key with Its Credential

First, PO argues that Kleve's virtual key consists only of a Temporary User "credential" (such as a photo ID, fingerprint or passcode) and therefore that is the only information sent when requesting a virtual key. POR 9-13. PO's argument is not consistent with Kleve's other disclosures as discussed above. Moreover, PO selectively quotes Kleve, which expressly states that the credential can be "used as a virtual key, ***or in addition to the virtual key***." EX1005, ¶63. PO further conflates the virtual key with Kleve's credential-checking process. While Kleve contemplates that the credential ***may*** itself be a virtual key, Kleve also discloses the credential can be "in addition to the virtual key" and verified "inside of the vehicle" ***after*** the user has unlocked the vehicle with the virtual key—confirming the credential and the key can be separate. *Id.*, ¶¶63, 64, 67 ("Once the Temporary User enters the vehicle and captures the credentials … the vehicle may verify that the Temporary User has

approval to use the vehicle."), Fig. 5 ("At Rental Time TU Enters Vehicle and Captures Credential with Vehicle Camera"). Regardless, Kleve does not foreclose additional information being included as part of the virtual key and its associated coded data—and as discussed above, the vehicle limits entry to the "rental time," requiring at least that privilege setting to be assigned prior to the rental period and included.

PO argues that if the rental period were included in the virtual key request, "it would not be necessary for the Vehicle Owner to send the credential to the vehicle 'at rental time.'" POR 12-13. But this is not a reasonable interpretation of the reference. Kleve states that at step 502 "[t]he virtual key may be sent to the vehicle allowing Temporary User access to the Owner's vehicle" and later at step 506, "[w]hen the scheduled rental period of time begins the vehicle Owner may send the credentials to the vehicle." EX1005, ¶¶62, 66. Thus, even where "the vehicle Owner may send the credentials to the vehicle," the virtual key and the credential have complementary purposes: the former allows access (but only "[a]t rental time," *see* Fig. 5) and the latter is an additional security check to ensure the temporary user is who they claim to be. Having the virtual key include the rental period is necessary to limit its use to the "rental time" as taught in Kleve, and sending the credential "at rental time" does not contradict this teaching.

3. Step 214 Is Not the Only Mechanism for Setting Restrictions

Second, PO argues that Kleve "provides a separate, ***optional*** operation to allow only the Owner to 'set user restrictions'" after the rental period starts, relying on step 214 from Figure 2. POR 13-18 (citing to EX1005, ¶40, Fig. 2). But by PO's own admission, step 214 is an ***optional*** process. EX1005, ¶40 ("At step 214, the Owner … ***may*** set user restrictions by use of the website or nomadic device."). Yet enforcement of the rental period is ***not*** optional. *Id.*, ¶8 ("enabling a keyless vehicle drive-away during a scheduled rental period"), ¶39 ("The virtual key may also be sent to the vehicle … to enable the keyless drive system for the appropriate Temporary user during a given rental period."), ¶51 ("Controlling usage to enforce compliance with the rental agreement terms may be of more importance to a vehicle rental micro-business owner as this may be the only vehicle the Owner possesses."); ¶54 (describing enforcement of the end of the rental period). Accordingly, a POSITA would understand there is a mechanism to enforce the rental period that does not require the use of step 214—and notably, Kleve does not include the rental period in the exemplary list of restrictions described for step 214. EX1005, ¶40; EX1048, 13:18-14:4.

PO's argument that step 214 is the only mechanism for assigning restrictions is neither stated by Kleve, nor consistent with Kleve's other teachings that the rental period must be enforced or the understanding of a POSITA that limitations that begin

with the rental term would have to be assigned before the rental term. Again, as the Board found, the virtual key is "only operable during a rental period." ID 37. Since the virtual key is sent before the beginning of the rental period, there must be a mechanism outside of step 214 that disallows its use before the rental period. As discussed above, Kleve provides numerous teachings where such privilege settings are assigned before the rental period begins. *See, e.g.*, EX1005, ¶39 ("The virtual key … enable[s] the keyless drive system … during a given rental period."); Fig. 6 (generating restrictions before user receives virtual key). More fundamentally, PO's argument contradicts itself. If Kleve requires that privilege settings be assigned at "the beginning of the rental term at step 214" (POR 14), then there is no mechanism for the system to allow the setting of privilege settings unless and until it knows the rental period. Thus, prior to step 214, there must be some mechanism for setting the rental period so that the system can allow the owner to set restrictions at the beginning of the rental term.

PO argues that if the rental agreement terms are included with the virtual key, step 214 "would not be necessary." POR 15. But by PO's own admission, step 214 is "optional" (POR 13)—and it is only described for Figure 2. As discussed above, other teachings make clear that the rental agreement terms can be assigned before the rental period begins. *See, e.g.*, EX1004, ¶39 ("The virtual key … enable[s] the keyless drive system … during a given rental period."); Fig. 6 (generating

restrictions before user receives virtual key). In addition, as PO concedes, it is entirely plausible that step 214 is used for assigning restrictions that are ***not*** part of the rental agreement. POR 31-32 (arguing that Kleve's "restrictions are not predicated on any rental agreement"). Moreover, Kleve does not describe the rental period as a restriction that the owner sets at step 214. EX1005, ¶40. Thus, assuming (incorrectly) that step 214 is even "necessary" for enforcing rental term agreements, it could be used for initially assigning what Kleve describes elsewhere as geofencing or performance restrictions—*e.g.*, speed, location, or load weight restrictions—not the rental period. EX1005, ¶¶40, 75 ("performance limitations and restrictions"), Fig. 7-A ("Geofences").

PO further argues that step 214 is "link[ed]" with the rental period, because if the temporary user wishes to extend the rental period end time, Figure 2 depicts a return to step 214. POR 18-20; EX1005, ¶43, Fig. 2. As Kleve makes clear, step 214 is used for extending the "rental period ***end time***." EX1005, ¶43. This underscores the point that Kleve does ***not*** disclose that step 214 is used for assigning the ***start*** of the rental period—nor could it be for the reasons explained above. *See, e.g.*, EX1005, ¶39 ("The virtual key … enable[s] the keyless drive system … during a given rental period."), Fig. 6 (generating restrictions before user receives virtual key). Moreover, other figures do not have a similar "step 214." For example, in Figure 3, at step 326 "the VCS may implement ***assigned*** vehicle control limitations

during the use of the rental term," *i.e.* such limitations are ***pre-assigned*** before the start of the rental term. If a user desires to extend the rental period, that is done at step 346 (or possibly step 328). *See id.*, Fig. 3B. There is no equivalent to step 214 in Figure 3.

4. The Virtual Key Is Not Unmoored from Restrictions

Third, PO argues that the virtual key is "operable independent of the agreed-upon rental period." POR 21-26. PO suggests that since Kleve describes processes for the vehicle owner to provide leeway to the temporary user if they are near or exceed the rental period end time, or processes to shut down the virtual key because of vehicle abuse, that means the virtual key is entirely unmoored for the rental period and is usable even ***before*** the rental period begins. *Id.* That is a leap that defies logic. Kleve is clear that the rental period controls the virtual key. *See, e.g.*, EX1005, ¶39, Fig. 6 (generating restrictions before user receives virtual key). That there are optional mechanisms for the owner to extend the rental period end time, or cancel the virtual key ahead of time, in no way requires the system to violate the owner's desires and allow the virtual key to be used before the rental period begins. This of course would render moot the rental period, whose enforcement Kleve teaches is "important[t]." *Id.*, ¶51. Indeed, the very purpose of Kleve's invention is to allow "activat[ion of] a vehicle during a ***prescribed*** rental period." *Id.*, Abstract.

It is, of course, desirable for the vehicle owner to allow the temporary user to extend the rental period for a fee. Kleve also permits the vehicle owner to ***not*** allow an extension and instead "induce remedial actions." EX1005, ¶54. It is also desirable to allow the owner to cancel the virtual key if the temporary user is greatly exceeding the agreed-upon restrictions. Both of these options reduce the risk of vehicle damage or improper usage—and Kleve makes clear they are at the option of the vehicle owner. By no means does this mean that Kleve does not enforce the rental period ***at*** all—Kleve enforces the rental period unless the owner permits otherwise.

Thus, given the flaws in PO's description of Kleve, PO's contention that Kleve does not render obvious the challenged claims must fail.

B. Kleve Discloses a Virtual Key that Includes Privilege Settings

PO argues that Kleve does not disclose that the claimed "privilege settings" are included with a virtual key, and that the privilege settings cannot be part of the coded data associated with a virtual key. The Board already rejected this argument, and PO's mischaracterization of Kleve does not refute Kleve's own teaching that the virtual key is "to enable" vehicle access "during a given rental period." EX1005, ¶39; ID 37. PO largely relies on "step 214," which is an optional step that cannot ***preclude*** rental period enforcement before the rental period begins.

PO first argues that all restrictions are set "at the beginning of the rental term," which would be unnecessary if they were set beforehand. POR 29-33, 42-43, 49-50 (citing step 214). As discussed above, this is incorrect—step 214 does not preclude enforcing the rental period before it begins. EX1005, ¶39 ("The virtual key … enable[s] the keyless drive system … during a given rental period."), Fig. 6 (generating restrictions before user receives virtual key); *see also* EX1005, Figs. 8-9, ¶¶84-85, 89-90 ("load weight" and "amount of miles" restrictions assigned *before* "begin[ning] the keyless vehicle rental authorization process"). PO further argues that Dr. Almeroth "misstate[s] that *Kleve*'s 'user restrictions' are included in the virtual key" because the virtual key is distributed at step 210 of Figure 2, before restrictions may be optionally set at step 214. POR 30. PO concedes that these are ***not*** the same restrictions. It is the rental agreement terms which set out the rental period—which must be enforced. That the owner can set *additional* restrictions at step 214 has no bearing on Petitioners' theory.

PO reiterates its argument about extending the rental period end time, arguing that "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." POR 34-35; *see also id.* 42-43. PO does not explain why the extension of the ***end time*** must be the same step

as the initial setting of the rental period, including its start time—these are different restrictions being enforced at different times. Indeed, Figure 3 describes what PO accuses of "mak[ing] no sense," where the step of initially setting the restriction is different from the step for extending the end time. EX1005, ¶51, Fig. 3 (step 326 implements restrictions, steps 346 to 328 extends the end time).

PO further contends that the rental period is enforced through "credentials" disclosed in Figure 5. POR 36. But as discussed above, Kleve discloses that the virtual key is not necessarily the same as the "credential"—the former is sent at step 502 and provides access to the vehicle during the rental period and the latter is sent at step 506 and allows the vehicle to authenticate the temporary user. EX1005, ¶¶62-64. Kleve makes clear that the virtual key must be limited in use to the "[r]ental time," which cannot be enforced by merely sending the credential at the start of the rental period, since the virtual key is sent before the credential and the credential is not checked until after the user enters the vehicle. EX1005, Fig. 5, ¶64. Between the time the virtual key is sent to the temporary user and the time the user unlocks the vehicle and authenticates their credential, there must be a mechanism that prevents the user from using the virtual key before the rental period begins.

PO next argues that other restrictions, such as speed, global position coordinates, load weight restrictions, and permitted uses (*e.g.*, unauthorized cargo or unauthorized trailer tows), cannot be part of coded data included with the virtual key

because they can only be set at optional step 214, after the virtual key is distributed. POR 37-41. As discussed above, this argument is premised on PO's erroneous reading of step 214 as the ***only*** mechanism for setting privilege settings.

PO applies the same erroneous reasoning even to restrictions in embodiments that do not include optional step 214, such as Figure 7. As discussed above, Kleve is clear that Figure 7 monitors restrictions while it "wait[s] for the rental period to start"—indicating that the restrictions can be set prior to the rental period. EX1005, ¶75. To argue that Figure 7 assigns restrictions at the start of the rental period, PO quotes Kleve out of context. Specifically, PO purportedly quotes Kleve as disclosing "performance limitations and restrictions assigned by the Vehicle Owner at the start of the rental period, at step 708." POR 40. In fact, however, the full quote states that Kleve's system "***begins to download*** performance limitations… at step 708." EX1005, ¶75. In the proper context, the clause "at the start of the rental period at step 708" can only reasonably be understood as modifying "download performance limitations." *Id.*, ¶75; Fig. 7A ("Download Geofences or Performance Limits"). In other words, in Figure 7, the VCS downloads pre-assigned privilege settings at the beginning of the rental period—it does not require the vehicle owner to ***assign*** the privilege settings at the beginning of the rental period.

Figure 3, discussed above, similarly discloses pre-assigned restrictions that are implemented (not set) at rental start time. *Id.*, ¶51. Specifically, at step 326 of

Figure 3, "the VCS may implement assigned vehicle control limitations"—*i.e.* restrictions are pre-assigned and then, when the rental period begins, implemented at step 326. This means that the restrictions are set ***before*** the rental period begins.

PO also argues that the rental agreement terms cannot be included in the virtual key and enforced because the rental agreement is not accepted until ***after*** the virtual key is distributed. POR 43-48. PO again conflates the optional with the mandatory. Kleve clearly describes that Figure 5 "illustrates the process after the vehicle Owner and Temporary User ***… have both agreed to the rental agreement***." EX1005, ¶62. Kleve does describe an alternative embodiment where the rental agreement is accepted at the vehicle, but that alternative makes no mention of virtual keys (instead, access to the vehicle is determined by checking the user's identity)—and is again an optional, alternative embodiment. *Id.*, ¶65.

PO finally argues that "the virtual key cannot include any restrictions, let alone any rental agreement restrictions." POR 46-47; EX1048, 16:18-17:16 ("[W]hat Kleve is describing is that the virtual keys … are available prior to the -- prior to the start of the rental period."). Yet Kleve emphasizes ensuring proper enforcement of the agreement, including that the virtual key cannot grant vehicle access until the rental period begins. EX1005, Abstract, ¶¶8, 39, 51. If the virtual key is completely unmoored from any restrictions, then that is highly detrimental to the security of the vehicle. What PO has done is elevate the admittedly optional step

214 into an absolute requirement for setting restrictions, while ignoring all other teachings that state otherwise, resulting in a system that defies common sense and which no POSITA would ever find desirable.

C. Kleve Renders Obvious Including Privilege Settings in Coded Data Associated With a Virtual Key

Dr. Almeroth opined it would be obvious to include restrictions as coded data associated with the virtual key. EX1004, ¶¶110-113; Pet. 12-14. Dr. Almeroth opined that doing so would "increase[] security, efficiency, and [provide a] better user experience," including by "ensuring that only the intended recipient … may access and use the electronic key" and "prevent[ing] a Temporary User from tampering with the electronic key or otherwise circumventing restrictions and limits on the use of the electronic key." EX1004, ¶¶110-111.

PO argues that Kleve already "provides this benefit" because "restrictions used to control and monitor vehicle usage" are only set "*after* the virtual key has already been created and distributed. POR 51. But PO's argument again rests on the false premise that optional step 214 is the ***only means*** for setting privilege settings, which contradicts Kleve's other disclosures, including the embodiments illustrated in Figures 3, 5, 6, and 7. At least the rental start time ***must*** be included with the virtual key to accomplish Kleve's goal of establishing and enforcing a rental period. *See, e.g.*, EX1005, ¶¶39, 51, 54; EX1048, 16:18-17:16. A POSITA would

thus be motivated to include that information as part of the coded data for the reasons identified by Dr. Almeroth. EX1004, ¶¶110-111.

PO also argues that including privilege settings as part of the virtual key contradicts Kleve's disclosure that "*only the vehicle owner* may set user restrictions that the vehicle will monitor and/or control." POR 52-54. But ***who*** sets the privilege settings and ***how*** the privilege settings are communicated are entirely separate. For example, the rental start time must be included with the virtual key to enforce the rental period, but the ***vehicle owner*** determines the rental period. As Dr. Almeroth explains, the fact the Kleve intends that only the vehicle owner can set privilege settings only reinforces the need to include the privilege settings as part of the coded data, so that such settings cannot be modified or added to the virtual key by a temporary user after the virtual key has been distributed. EX1004, ¶111.

D. PO's Arguments on Motivation to Combine Are Misplaced

PO argues that a POSITA would not combine Kleve with Hatton because Hatton uses encryption for "authentication" and not for "confidentiality," and Hatton assigns encrypted data during manufacturing. POR 54-57. The Board already rejected this argument. ID 41; *see also* EX1008, 9:50-63.

PO raises an improper "bodily incorporation" argument. *See Uber Techs., Inc. v. X One, Inc.*, 957 F.3d 1334, 1341 (Fed. Cir. 2020) ("whether one prior art reference can be incorporated into another is 'basically irrelevant.'"). Obviousness

does not require implementing precisely the same encryption scheme taught by Hatton in Kleve's system; the inquiry "focuses on what the combined teachings would have suggested." *In re Mouttet*, 686 F.3d 1322, 1330 (Fed. Cir. 2012). Hatton's disclosure of using encryption to prevent unauthorized access, in view of Kleve, would have suggested using encryption to also prevent a temporary user from circumventing restrictions assigned to a virtual key. EX1004, ¶¶111.

In addition, the Petition relies on ***Kleve's*** disclosures regarding encryption, which PO does not challenge. Pet. 19-20. Kleve discloses using coded data (*e.g.*, a "matrix barcode"), EX1005, ¶¶44-45, 71, and sending a virtual key "in an encrypted message," *id.*, ¶63. Hatton adds the use of well-known wireless communication protocols (*e.g.*, Bluetooth, WiFi) and transmitting encrypted data via a mobile device. Pet. 19-20; EX1008, 7:49-60. PO does not address these arguments in the Petition and does not explain why a POSITA would not apply Kleve's existing encryption techniques to wireless communication protocols as disclosed by Hatton to facilitate secure transmission via a temporary user's mobile device. *See* EX1004, ¶¶111-112.

III. GROUND 3: MIKAN

As the Board correctly concluded in its institution decision, Mikan "at least suggests a vehicle receiving coded data" corresponding to electronic keys, which are "linked to vehicle operation policies." ID 47; EX1007, ¶¶50, 60-61, 72, 76-77. At

a minimum, Mikan renders obvious including the vehicle operation policy as part of the coded data for the electronic key. EX1005, ¶¶221-222. As it did in its preliminary response, which the Board rejected, PO relies on Mikan's local and master database. These teachings, however, do not preclude sending the vehicle operation policy to the wireless device. And Mikan itself acknowledges disadvantages in relying exclusively on the master database to provide virtual key information to the vehicle.

A. PO Relies on Exemplary Embodiments as Limiting

PO provides and relies on a "summary" of Mikan that treats exemplary embodiments where vehicle operation policies ***may be*** synchronized from a master database to a local database as limiting disclosures to argue that vehicle operation policies ***cannot*** be part of the coded data embedded in the wireless device acting as a virtual key. POR 58-73. PO misinterprets Mikan's disclosures on this point.

Mikan discloses exemplary embodiments where vehicle operation policies "may" be synchronized between the master database and local database. EX1007, ¶¶69 ("[L]ocal database 203 ***may*** synchronize with master database 208."), 84 (similar). In addition to the permissive term "may," Mikan also describes both embodiments as "example[s]" only. *Id.*, ¶¶68, 79. Mikan does not preclude including the vehicle operation policy with the associated electronic key in a wireless device, or sending the vehicle operation policy as coded data using the wireless

device. To the contrary, Mikan discloses that an electronic key may be "embedded in a wireless device." *Id.*, ¶50. Mikan also discloses that information associated with the electronic key, such as a secure ID, is stored as coded data in the wireless device. *Id.*, ¶¶54 (describing "secure ID check 315 associated with a key 205A-C"), 65 (discussing storing an encrypted "secure identifier" at the wireless device). A POSITA would have understood that Mikan at least suggests that other information associated with the electronic key, such as the vehicle operation policy, may also be stored at the wireless device. *Id.*, ¶5 (describing "vehicle operation policy associated with the key"); EX1004, ¶¶220-222.

PO argues Mikan's vehicle "***receives only*** a secure ID 407 from the mobile device." POR 66, 76. But Mikan never states that the secure ID is the ***only*** information sent from the wireless device to the vehicle. Similarly, PO argues that the vehicle operation policy may only be retrieved from the master database or the vehicle's local database and need never be retrieved from the mobile device. POR 65-66, 69-73. Again, however, the vehicle operation policy is synchronized between the master and local databases in exemplary embodiments only. And where the vehicle operation policy is ***not*** provided by the master database, Mikan does not disclose that the vehicle's local database can ***independently*** generate an electronic key or associated vehicle operation policy. Accordingly, they must initially be

provided to the vehicle's local database through different means, *.e.g.*, via the wireless device.

B. Mikan Renders Obvious Providing the Vehicle Operation Policy as Coded Data

Even if Petitioner's characterization of Mikan's disclosures is adopted (it should not be), Dr. Almeroth explains that it would have been obvious to include the vehicle operation policy as coded data stored in and sent by the wireless device. Pet. 45; EX1004, ¶¶221-222.

PO argues that Mikan "discourages" sending the vehicle operation policy via the mobile device because it discloses an alternative solution, *i.e.*, synchronizing the master and local databases. POR 73-75, 77-79. But this argument is legally flawed because "mere disclosure of alternative designs does not teach away." *Mouttet*, 686 F.3d at 1334.

PO also argues if the vehicle operation policy were sent from the wireless device, the "mapping" between keys and vehicle operation policies, and retrieving the vehicle operation policy from the vehicle's local database, would both be unnecessary. POR 74-75. But Mikan discloses that each vehicle may be associated with multiple keys. EX1007, ¶50. Thus, Mikan's vehicle would still need to associate each vehicle operation policy with a key. Further, even if the vehicle operation policy is ***initially*** provided by mobile device, the vehicle may

subsequently retrieve the policy from its local database, so it need not be transmitted with ***every*** access request.

Finally, Mikan identifies a problem in relying on the master database for vehicle operation policies that is solved by the proposed combination. Mikan acknowledges that "synchronization data" may not be communicated when the vehicle is "out of range of [the] wireless network." EX1007, ¶85; *see also* EX1048, 48:16-18 (PO's expert admitting same). Providing the vehicle operation policy through the mobile device allows the vehicle to receive this information even when it cannot communicate with the master database. *See* EX1004, ¶274. Further, PO's concerns about security and tampering (POR 78) are resolved by including the vehicle operation policy as ***coded*** data. EX1004, ¶221. In any event, merely identifying potential disadvantages to a combination "does not necessarily obviate motivation to combine." *Medichem, S.A. v. Rolabo, S.L.*, 437 F.3d 1157, 1165 (Fed. Cir. 2006).

IV. THE DEPENDENT CLAIMS ARE OBVIOUS

PO argues that claim 6 is not obvious because Kleve gives the Vehicle Owner "full control over usage of their vehicle." POR 79-80. But in the proposed combination, a temporary user is only permitted to share the virtual key ***with other authorized users***. Pet. 25-26. PO does not explain why this is inconsistent with Kleve, and does not challenge the motivation to combine identified by Dr. Almeroth.

EX1004, ¶155. Nor does PO explain why Kleve's disclosure of an ***optional*** credential check (*see* POR 80) undermines the benefit of allowing authorized temporary users to share virtual keys.

PO separately argues that Mikan and Sekiyama do not render claim 6 obvious because Mikan's mobile devices only contain a "secure ID" and not an electronic key. POR 80. To the contrary, Mikan expressly teaches that electronic keys—not just a secure ID—may be "embedded" in a wireless device. EX1007, ¶¶5, 50, 70. PO also argues that Mikan's coded data does not include privilege settings (POR 81), which is addressed above in connection with claim 1.

PO also argues the Petition does not claim that any reference discloses the limitations of a server and mobile device application associated with a manufacturer of the vehicle for claims 12, 13, and 20. But the Petition expressly cites to evidence that these limitations are disclosed or rendered obvious, which PO does not address. Pet. 31 (Kleve is a Ford patent, *i.e.*, a vehicle manufacturer), 32 (Hatton discloses application developed by manufacturer), 59 (Xiao discloses server associated with "automobile company"), 60 (electronic key application developed by vehicle manufacturer was well known).

V. CONCLUSION

For these reasons, all challenged claims are unpatentable.

Date: July 30, 2025

Respectfully submitted,

By: /s/ *James M. Glass*
James M. Glass

Counsel for Petitioner Kia

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITATION, TYPEFACE REQUIREMENTS, AND TYPE STYLE REQUIREMENTS

1. This Petition complies with the type-volume limitation of 5,600 words, comprising 5,595 words, as counted using the Microsoft Word software that was used to prepare this paper, excluding the parts exempted by 37 C.F.R. § 42.24(a).

2. This Petition complies with the general format requirements of 37 C.F.R. § 42.6(a) and has been prepared using Microsoft® Word 2016 in 14-point Times New Roman.

Date: July 30, 2025

By: */s/ James M. Glass*

James M. Glass
QUINN EMANUEL URQUHART & SULLIVAN, LLP
295 5th Avenue, 9th Floor
New York, NY 10016
Tel: (212) 849-7000
Fax: (212) 849-7100

Counsel for Petitioner Kia

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on July 30, 2025, true and correct copies of the foregoing document and supporting materials were served in its entirety on the Patent Owner at the following email addresses:

jtice@bdiplaw.com
ahand@bdiplaw.com
bentzminger@bdiplaw.com
BDIP_EmergingAuto@bdiplaw.com

Date: July 30, 2025

By: */s/ James M. Glass*

James Glass
QUINN EMANUEL URQUHART
& SULLIVAN, LLP
295 5th Avenue, 9th Floor
New York, NY 10016
Tel: (212) 849-7000
Fax: (212) 849-7100

Counsel for Petitioner Kia