

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 11,738,659

**DECLARATION OF DR. SAM MALEK IN SUPPORT OF PATENT
OWNER'S RESPONSE**

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION AND BACKGROUND.....	4
II. QUALIFICATIONS	5
III. MATERIALS CONSIDERED	11
IV. LEGAL PRINCIPLES	11
V. PERSON OF ORDINARY SKILL IN THE ART (“POSITA”).....	16
VI. BACKGROUND	18
A. Overview of the ’659 Patent.	18
B. Prosecution History of the ’659 Patent.....	19
VII. SUMMARY OF KLEVE (EX1005).....	20
VIII. SUMMARY OF HATTON (EX1008)	31
IX. SUMMARY OF MIKAN (EX1007)	32
X. DETAILED ANALYSIS OF PETITION GROUNDS.....	41
A. Each of the Kleve-based grounds (grounds 1-2) fails to establish obviousness of any challenged claim.	41
1. Each of the “restrictions” identified by Petitioners as alleged “privilege settings” included in Kleve’s virtual key are unavailable to be set until after the set up and distribution of the alleged “coded data,” a virtual key, and therefore are not included in the coded data.	41
2. Kleve’s disclosure that a virtual key credential may be “sent to the vehicle configuring the VCS to enable the keyless drive system for the appropriate Temporary User during a given rental period” does not suggest the “rental period” is included in the virtual key itself.	49
3. Dr. Almeroth’s obviousness opinions are contradicted by Kleve’s disclosures.....	52
B. A POSITA would not have combined Kleve and Hatton as proposed.....	54

C.	A POSITA would not have found it obvious to combine Kleve and Hatton as Dr. Almeroth proposes.....	57
D.	The Sekiyama reference does not cure the deficiencies of Kleve/Hatton.	61
XI.	Dr. Almeroth and the Petition fail to show that Mikan, alone or in combination, discloses or suggests a “coded data from the mobile device ... coded data includes privilege settings.”	61
A.	Dr. Almeroth identifies a secure ID as coded data, but the secure ID 407 transmitted by the wireless device to the vehicle does not include any alleged privilege settings.	62
B.	Mikan does not disclose, and in fact discourages, a vehicle receiving any privilege settings from a mobile device.	64
C.	Dr. Almeroth’s opinions are contradicted by Mikan’s solution to retrieve locally stored vehicle operation policies from the vehicle’s local database.	66
XII.	The additional references do not cure the deficiencies of mikan.....	70
XIII.	Dr. Almeroth fails to show that Claim 6 is anticipated or rendered obvious by any reference.	70
XIV.	CONCLUSION	72

I, Dr. Sam Malek, declare under penalty of perjury as follows:

I. INTRODUCTION AND BACKGROUND

1. I have been retained as an expert witness on behalf of Emerging Automotive LLC (“Emerging Auto”) to provide information and assistance regarding U.S. Patent No. 11,738,659 (“the ’659 patent”). Specifically, I have been asked to consider the Petition for Inter Partes Review numbered IPR2024-01167 (“the Petition”) regarding the ’659 patent, and specifically the Declaration of Dr. Almeroth (EX1004) that accompanies the Petition, as well as the Board’s Institution Decision.

2. In this declaration I provide my independent analysis of the ’659 patent in light of the materials cited below and discussed herein and my knowledge and experience in this field during the relevant time frame. I have been asked to consider what one of ordinary skill in the art at the time of the invention of the ’659 patent (a “POSITA,” see Section V below) would have understood from the specification, including scientific and technical knowledge related to the patent. I have also been asked to consider whether certain references anticipate or would have rendered obvious the inventions described in the claims of the ’659 patent.

3. My findings, as explained below, are based on my study, experience, and background in the fields discussed below, informed by my education and my extensive experience in the field of cloud-based processing systems. I have also

relied on my review and analysis of the references identified by Dr. Almeroth, information provided to me, and information that I have independently reviewed. I have personal knowledge of the facts and opinions set forth in this declaration, and, if called upon to do so, I would testify competently thereto.

4. I am being compensated for my independent analysis as an expert with respect to this inter partes review proceeding. My compensation is not contingent in any way on the content of my analysis, the opinions that I offer, or the outcome of this proceeding. I have no financial interest in either Petitioner (Toyota or Kia) or Patent Owner (Emerging Auto) and I have no financial interest in the '659 patent.

II. QUALIFICATIONS

5. My qualifications for forming the opinions given in this declaration are summarized here and are addressed more fully in my curriculum vitae, which was submitted as EX2002. That exhibit also includes a list of my publications.

6. I have approximately 25 years of experience in the general area of computer and software technology in a variety of roles, including as a software engineer, software architect, and programmer at a variety of companies, as well as a researcher and professor at several universities.

7. I am currently a Full Professor of Software Engineering with tenure in the Informatics Department within the School of Information and Computer Sciences at the University of California, Irvine. I am also the Director of the

Software Engineering and Analysis Laboratory (“SEAL”). My general research interests are in the field of software engineering, and to date my focus has spanned the areas of software analysis and testing, mobile computing, architecture and design, and software dependability and security. The underlying theme of my research has been to devise techniques and tools that aid with the construction, analysis, and maintenance of largescale software systems.

8. I received my Ph.D. and M.S. degrees in Computer Science from the University of Southern California and my B.S. degree in Information and Computer Science from the University of California, Irvine. I have received numerous awards for my research contributions, including the Test of Time Award from the Association for Computing Machinery Special Interest Group on Software Engineering (2020), National Science Foundation CAREER award (2013), GMU Emerging Researcher/Scholar/Creator award (2013), and the GMU Computer Science Department Outstanding Faculty Research Award (2011).

9. I have authored over 130 peer-reviewed research publications. These publications have been highly cited (more than 11,000 times according to scholar.google.com). Many of my publications have dealt with the topics that are related to this proceeding, including distributed software systems, cloud computing, client-server architecture, and software settings and configuration. I provide a few examples here.

10. My Ph.D. dissertation resulted in novel algorithms for optimizing the deployment architecture of a distributed software system. The deployment architecture of a distributed software system is the allocation of its software components to its hardware devices. There are many deployments of a software system possible, but some may be superior to others with respect to certain quality of service objectives (e.g., latency, availability, security). One application of my dissertation work was in the context of cloud computing, because in most cloud-based software systems there are many geographically distributed nodes (servers) available for the deployment of software components.

11. I have also worked on techniques to leverage cloud computing for software testing. For instance, in an article titled “A Whitebox Approach for Automated Security Testing of Android Applications on the Cloud,” I showed how the resources in the cloud can be effectively harnessed to facilitate security testing at scale.

12. In another article titled “GLIDE: A Grid-based Lightweight Infrastructure for Data-intensive Environments,” I described the results of my work with colleagues from NASA in the development of a new distributed software system for sharing large amounts of data generated by NASA. This capability was the first of its kind in the realm of Grid Computing, which is a precursor to Cloud Computing.

13. A significant focus of my work has been on computer security, including electronic forms of access control and management of privileges in software systems. For instance, I led a team of researchers in a project sponsored by the Defense Advanced Research Project Agency (DARPA) to develop a novel approach for protecting Android applications from various form of access control attacks. The project resulted in the development of a tool called COVERT. I have published extensively on this work, including a highly cited manuscript that appeared in the IEEE Transactions on Software Engineering in 2015. In another project, I developed DelDroid, which at the time was the first approach for automated determination and enforcement of least privilege architecture in Android. This work was published in the Journal of Systems and Software in 2019.

14. I have received numerous research grants from a variety of organizations, including the National Science Foundation (NSF), Federal Bureau of Investigation (FBI), Air Force Office of Scientific Research, Department of Homeland Security (DHS), National Security Agency (NSA), Defense Advanced Research Projects Agency (DARPA), Office of the Director of National Intelligence, and Army Research Office among others. Software systems and results produced in my research lab have been adopted for use by various organizations in both private (e.g., Boeing, Bosch) and public (e.g., NASA, DHS, FBI) organizations. Many of the above-mentioned projects and software systems involved analysis and design of

client-server software systems deployed on the cloud. For instance, in a project called “RASS: Resilient Autonomic Software Systems” funded by Air Force Office of Scientific Research, I led a team of researchers to develop a new method of automatically adapting Air Force’s software systems to fluctuations in communication networks, thereby making them resilient to network interruptions.

15. I also have several years of experience as a software engineer, software architect, and programmer at a variety of companies, namely the Boeing Company, PricewaterhouseCoopers Consulting (later acquired by International Business Machines (“IBM”) Corporation), FieldCentrix, and Neural Computing Systems Lab. During my tenure in the industry, I gained professional experience in the design, development, and management of largescale software engineering efforts. Among the software systems that I designed and developed were commercial ecommerce and enterprise software systems. Many of the software systems developed in the context of my professional experience were built according to the general client-server architectural style and deployed on the cloud or cloud-like environments. In most of these systems, the server held the state of the distributed application, allowing for that state, such as the preferred user settings, to be transferred to client at runtime.

16. I have taught software engineering and computer science courses on a regular basis at the B.S., M.S., and Ph.D. levels at the universities where I have been

employed. I cover concepts related to cloud computing, distributed software, client-server architectural style, authentication, encryption techniques, access control mechanisms, and protocols for exchange of electronics credentials (e.g., electronic keys, passwords, and tokens) in many of the courses that I teach at the university. Notably, I have regularly taught distributed software engineering courses at UC Irvine and previously at George Mason University (GMU). In these courses, I cover concepts such as the client-server architectural style, cloud computing principles, and server-side storage of user-defined preferences.

17. I have been a frequent speaker at scientific conferences, symposia, workshops, and gatherings of software engineering academics and professionals. I have served as chair, committee member, and reviewer for numerous software engineering journals, magazines, and conferences. I have served on the editorial board of the ACM Transactions on Software Engineering and Methodology, IEEE Transactions on Software Engineering, the ACM Transactions on Autonomous and Adaptive Systems, the Springer Journal of Automated Software Engineering, and the Springer Journal of Computing. I am a member of the Association for Computing Machinery (ACM), ACM Special Interest Group on Software Engineering (SIGSOFT), and the Institute of Electrical and Electronics Engineers (IEEE). I have testified at trial and deposition as an expert witness in numerous cases in the past five years.

III. MATERIALS CONSIDERED

18. In preparing this declaration and forming my opinions, I have considered: the claims, specification, and prosecution history of the '659 patent; the Petition and declaration by Dr. Almeroth (including all materials cited in each); and all materials cited and discussed in this declaration. In addition, I have considered the relevant legal standards, as they have been explained to me by counsel and as I understand them. I have also considered the knowledge and understanding of a person of ordinary skill at the time of the invention of the '659 patent, of which I am familiar. As part of my analysis for this matter, I have also considered my own knowledge and experience, including my work and experience with cloud-based processing systems.

IV. LEGAL PRINCIPLES

19. In forming my opinions here, I have applied the following understanding of certain legal concepts related to anticipation, obviousness, combinations of references, and knowledge of one of ordinary skill in the art. Counsel for Patent Owner has informed me of legal principles that apply in this proceeding.

20. It is my understanding that assessing the validity / patentability of a U.S. patent claim based on a prior art analysis requires two essential steps. First, one must analyze the terms of the patent claims to understand what meaning one of

ordinary skill in the art would give the terms. Second, one may then assess validity by comparing a patent claim to the “prior art.” I understand that the teaching of the prior art is viewed through the eyes of a person of ordinary skill in the art at the time the invention was made. My opinion as to what constitutes a relevant person of ordinary skill in the art is set forth below.

21. I have been informed that in order for a patent claim to be invalid as anticipated by a prior art reference under 35 U.S.C. § 102, each and every element of that patent claim must be found disclosed in that reference, explicitly or inherently, to a person of ordinary skill in the art. Inherent disclosure requires that the claimed element be the only possible option given the other disclosures of the reference, and that it would be so recognized by persons of ordinary skill in the art. I also understand that the missing descriptive material cannot merely be probably or possibly present. If any single element of a claim is not disclosed in the reference, the entire claim is not anticipated. I understand that a prior art reference merely capable of being modified so as to operate in the same manner as the patented device or system does not anticipate. I further understand that obviousness is not inherent anticipation, and that it is insufficient that a missing limitation is so similar to a limitation actually disclosed in the reference that one of ordinary skill in the art would see the substitution as obvious. I also understand that, if it is necessary to reach beyond the boundaries of a single reference to provide missing disclosure of

the claimed invention, the proper ground for asserting invalidity is not anticipation, but obviousness.

22. I understand that a claim is invalid as obvious under 35 U.S.C. § 103 if the differences between the claimed subject matter and the prior art are such that the subject matter as a whole would have been obvious at the time of the invention to a person having ordinary skill in the art.

23. I understand that a person of ordinary skill in the art provides a reference point from which the prior art and the claimed invention should be viewed. This reference point prevents one from using his or her own insight or hindsight in deciding whether a claim is obvious.

24. I have been informed that the following factors are used to determine whether or not the claimed subject matter would have been obvious: (i) the scope and content of the prior art; (ii) the differences between the prior art and the claimed invention; (iii) the level of ordinary skill in the field of the invention; and (iv) any relevant objective considerations of non-obviousness, such as commercial success, long-felt but unresolved needs, failure of others, etc.

25. I also understand that in considering the scope and content of the prior art, references must be reasonably related (i.e., analogous) to the claimed invention of that patent. I understand that the test for determining whether a prior art reference constitutes analogous art to the claimed invention is (1) whether the reference is from

the same field of endeavor, regardless of the problem addressed and, (2) if the reference is not within the field of the inventor's endeavor, whether the reference is still reasonably pertinent to the particular problem the inventor is trying to solve.

26. I understand that a party asserting obviousness based on a combination of prior art references must demonstrate that one of ordinary skill in the art would have been motivated to combine the teachings of those references to achieve the claimed invention and that the skilled artisan would have had a reasonable expectation of success in doing so. It is my understanding that it is not enough to show that one skilled in the art could combine elements of multiple references, but instead there must be some reason that would have prompted a person of ordinary skill in the art to combine the elements in the way the claimed invention does. I understand that there must be some reasoned explanation as to why one of ordinary skill in the art would combine the references. The reason cannot come from hindsight.

27. I understand that in considering whether a claimed invention is obvious, one may but is not required to find obviousness if at the time of the claimed invention there was a reason that would have prompted a person having ordinary skill in the field of the invention to combine the known elements in a way the claimed invention does, taking into account such factors as: (1) whether the claimed invention was merely the predictable result of using prior art elements according to their known

function(s); (2) whether the claimed invention provides an obvious solution to a known problem in the relevant field; (3) whether the prior art teaches or suggests the desirability of combining elements claimed in the invention; (4) whether the prior art teaches away from combining elements in the claimed invention; (5) whether it would have been obvious to try the combinations of elements, such as when there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions; and (6) whether the change resulted more from design incentives or other market forces. To find it rendered the invention obvious, the prior art must provide a reasonable expectation of success. Obvious to try is not sufficient in unpredictable technologies.

28. I understand that each claim must be evaluated separately for obviousness, and that it is improper to use hindsight. I understand that the disclosures in a patent or a prior art reference are viewed from the perspective of a person of ordinary skill in the art at the time of the invention. The obviousness analysis by a person of ordinary skill in the art must consider only what was known at the time of the invention.

29. It is my further understanding that obviousness cannot be based on a hindsight combination of components selected from one or more prior art references. I also understand that an invention would not have been obvious simply because all of the elements of the invention may have been known separately in the prior art.

30. I understand that a combination of disclosures or references would not have been obvious if the alleged modification(s) to be made to the reference(s) would have been inconsistent with the reference's stated goals or would have rendered the combination inoperable for its intended purpose. I further understand that for something to have been obvious, the party asserting obviousness must explain why a POSITA would have selected components or features for combination in the manner claimed.

31. I have been informed that a prior art reference must be considered in its entirety, i.e. as a whole, including portions that would lead away from the claimed invention.

32. I understand that with respect to claim construction, the proper construction is considered in the context of, and must be consistent with, the specification and that the claim language should be read in light of the specification and file history as it would be interpreted by one of ordinary skill in the art.

V. PERSON OF ORDINARY SKILL IN THE ART ("POSITA")

33. Counsel for Patent Owner has informed me that a person of ordinary skill in the art is a hypothetical person who is presumed to have known the relevant art at the time of the invention. The '659 patent properly claims priority to the Provisional application No. 61/745,729 application, which was filed on December 24, 2012. As shown on its face, the '659 patent claims priority to "Provisional

application No. 61,745,729.” ’659 patent face page items 45 and 60; *see also id.* at 1:7-62.

34. For the purpose of this Declaration, and based on my opinions herein, the time of invention for the ’659 patent is December 2012. However, I understand that Dr. Almeroth opines that the time of the invention is October 2013. Any invention date from the early 2010s to the mid-2010s would not alter my opinion regarding a person of ordinary skill in the art. Thus my opinion regarding a POSITA applies to either a date of invention in December 2012 or a date of invention in October 2013.

35. In my opinion, the relevant field of art for the ’659 patent is that of cloud-based processing systems.

36. I have been informed by counsel for Patent Owner that the person of ordinary skill is generally familiar with the type of problems encountered in the field and the prior art solutions to those problems and possesses an ordinary level of creativity.

37. I understand that Petitioners’ expert, Dr. Almeroth, opined that a person of ordinary skill in the art would have had at least a four-year undergraduate degree in electrical engineering, automotive engineering, or a closely related field and at least two years of experience in the fields of access control systems, vehicle

electronics, and/or cryptography. Additional education could substitute for professional experience and vice versa.” EX1004, Almeroth Decl., ¶ 85.

38. For purposes of this declaration, I apply Dr. Almeroth’s definition. However, I note that the opinions I set forth below are applicable under any reasonable definition of a POSITA. I also note that I qualify as a POSITA under Dr. Almeroth’s proposed definition.

VI. BACKGROUND

A. Overview of the ’659 Patent.

39. United States Patent Number 11,738,659 (the “’659 patent”) is titled Vehicles and Cloud Systems for Sharing E-Keys to Access and Use Vehicles. EX1001, Face Page. The ’659 patent “relates to systems and methods for generating and sharing electronic keys (e-Keys) with users and cloud-based processing systems.” *Id.*, 1:66-2:2.

40. In embodiments, a vehicle owner or administrator may request an electronic key, or eKey, for personal use or to share an e-key with “any number of users.” *Id.*, 43:37-40. The eKey may be associated with privilege settings for the users. *Id.*, claim 1. As such, each eKey may be unique, allowing eKeys for “the same vehicle, but assigned to different devices/people with different privileges.” *Id.*, 46:12-22.

41. As described in the ’659 patent, a mobile device may be configured to

use an e-key to unlock or start a vehicle. *Id.*, 52:25-27. The vehicle “receive[s] coded data from the mobile device when using the eKey,” and the “coded data includes privilege settings associated with the eKey.” *Id.*, 52:29-36.

B. Prosecution History of the '659 Patent

42. After submitting the application that issued as the '659 patent, the Examiner issued an office action alleging that the claims were anticipated by Zaid or obvious over Zaid in view of Mottla. EX1002, 178, 189. In response, the applicants amended the claim to recite that “the coded data including privilege settings set for additionally limiting types of use of the vehicle when using the ekey with the vehicle.” *Id.*, 333, 336. As the applicants explained, the purported “coded data” in the Zaid reference included a “type of counter or time stamp” in its messages to “avoid repeat message attacks”; however, that counter or time stamp in Zaid does not include “privilege settings set for additionally limiting types of use of the vehicle when using the ekey with the vehicle.” *Id.*, 339.

43. The Examiner withdrew the rejections and issued new rejections based on Zaid in view of Shinada. *Id.*, 349. The applicants explained that Shinada also did not teach “coded data including privilege settings.” *Id.*, 511-512. The applicants explained that any restrictions in Shinada were set at the time of renting, and not part of the coded data associated with the ekey. *Id.*, 511.

44. The Examiner withdrew the second rejection and issued a notice of allowance. *Id.*, 515.

VII. SUMMARY OF KLEVE (EX1005)

45. Kleve discloses a system for a credential check and authorization solution for personal vehicle rental. EX1005, title. Kleve's system allows the parties to negotiate terms of a rental agreement, sign a rental contract, input identifying information for the Temporary User that is used as a credential virtual key, and at the beginning of the rental term, the Vehicle Owner has the option to set user restrictions which the vehicle's vehicle based computing system ("VCS") will use to monitor and control the usage of the vehicle. EX1005, ¶¶ 40-43, 51, 75.

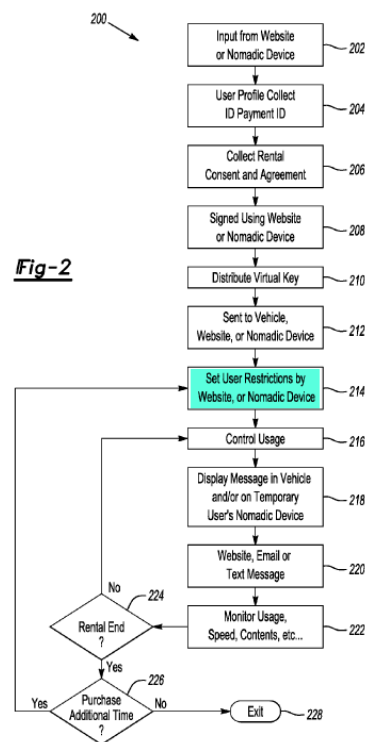
46. Kleve generally discloses that the Owner and Temporary User will agree to terms and sign a rental agreement before a virtual key is distributed (e.g., Figure 2, ¶ 62), however Kleve's system also discloses that the virtual key may be already be distributed to the Temporary User, and the Temporary User does not "agree to rental terms" until they have already entered the vehicle. *Id.*, ¶ 65 (using vehicle hardware to agree to terms). Whether the rental agreement is formed before the virtual key is set up or distributed or the Temporary User agrees to terms at the vehicle after the virtual key has been created and distributed, Kleve does not teach or suggest that the rental agreement terms are included in the set up of a virtual key or the virtual key itself. EX1005. Kleve does not teach or suggest that any rental

agreement terms are included as any privilege setting in the set up or distribution of a virtual key. Kleve teaches that the virtual key may be encrypted as a message or matrix barcode, however regardless of the form of the virtual key and regardless of whether it is encrypted, the virtual key does not include any privilege setting.

47. Kleve teaches a different solution for controlling vehicle usage. Kleve's system allows the Owner "control of the vehicle with the use of vehicle restrictions limits initially set by the Owner at the beginning of the rental term." *Id.*, ¶¶ 43, 75 ("the system may begin to download performance limitations and restrictions assigned by the vehicle owner at the start of the rental period"), Figs. 2, 7A. "At the beginning of the rental term," the vehicle owner may set restrictions that can include the very same restrictions the parties had agreed to as part of the rental agreement, i.e., to "enforce compliance with the rental agreement terms," and the owner may set additional user restrictions for monitoring and control, such as speed, wherein those restrictions will be monitored and controlled by the vehicle's VCS. *Id.*, ¶¶ 40-41, 43, 51, 75. By this solution, the Owner can enforce compliance with specific rental agreement terms, by inputting, for example, load weight restrictions, as well as set additional user restrictions that are not necessarily agreed or contemplated in the rental agreement. *Id.*

48. Kleve's Figure 2, below, shows step 214, which is when the Owner first has access to control usage of the vehicle being rented by the user by inputting "user

restrictions.” *Id.*, Fig. 2, *Id.*, ¶¶ 40, 43 (“restriction limits initially set by the Owner at the beginning of the rental term”). “At step 214, the Owner may have access to control usage of the vehicle being rented by the Temporary User. The Owner may set user restrictions by use of the website or nomadic device. The restrictions may be based on ... the owner’s selection of parameters including ... speed, global position coordinates, or load weight restrictions.” *Id.*, ¶ 40.



49. Kleve’s system allows the Owner access to set restrictions initially at step 214. *Id.*, ¶¶ 40, 43, Fig. 2. At step 210, the system distributes a virtual key. *Id.*, Fig. 2. Before the “Owner may have access to control usage of the vehicle being

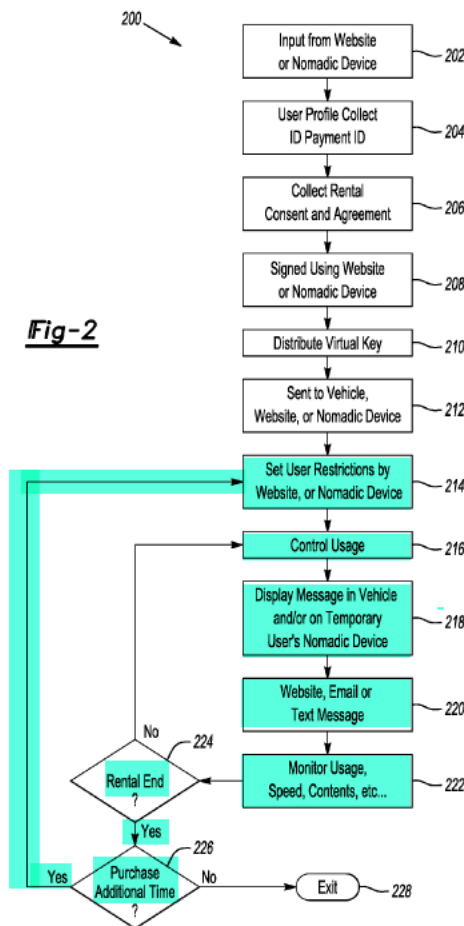
rented by the Temporary User,” i.e., to “set user restrictions” at step 214, the virtual key has already been created and distributed. *Id.*, ¶¶ 40, 43, Fig. 2.

50. Kleve explains that its solution allows only the Owner to set user restrictions that will be monitored and controlled by the vehicle’s VCS, because “[c]ontrolling usage to enforce compliance with 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.*, ¶¶ 51, 40-43, 75. I note that it would not be necessary for Kleve to have this solution to “enforce compliance with rental agreement terms” if the rental agreement terms were already included as “privilege settings” in Kleve’s “set up” or distribution of the virtual key. *Id.*

51. Kleve teaches that the very same restrictions that the parties had agreed to in the rental agreement, such as “load weight restrictions” (*id.*, ¶¶ 84-85, 89-90), must be input by the Owner as a “user restriction” at step 214, in order to “enforce” and “control” the agreed-upon “load weight restrictions” (*id.*, ¶¶ 40, 51) (“owner may set user restrictions” e.g., “load weight restrictions”).

52. As another example, “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 (*id.*, ¶ 40), even if the rental period was already agreed-to by the parties in their rental agreement (*id.*, ¶¶ 38-39). “At step 226, if the Temporary User decides that he may need to purchase additional rental time, the system may update the new rental

period end time restriction and continue to monitor usage of the vehicle.” *Id.*, ¶¶ 43, 54; *see id.*, Fig. 2. Figure 2 illustrates that the system will return to step 214, to “update the new rental period end time restriction” and the system will continue to monitor the vehicle usage, at steps 216, 218, 220, and 222. *Id.*



Id., Fig. 2 (annot.).

53. It would not be necessary for Kleve to require a discrete operation for the Owner 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 the rental

agreement restrictions were already included as “privilege settings” in Kleve’s “set up” or distribution of the virtual key, at step 210. *Id.*, ¶¶ 84-85, 89-90, 40, 51.

54. Kleve’s system provides several examples in which the virtual key is not only operable during the agreed-upon rental period. That is, the virtual key may be operable outside of the agreed-upon rental period, e.g., via a rental end time update, and the virtual key may be terminated before the agreed-upon rental period and after the end of the agreed-upon rental period.

55. Kleve’s system teaches a vehicle rental “exit mode process,” which involves several steps, including “terminating the virtual key” (*id.*, ¶ 80), and that “exit mode process” may be initiated before or after the agreed-upon rental period expiration (*id.*, ¶¶ 43, 53-55, 79-80).

56. For example, 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. *Id.*, ¶ 53, Fig. 3B. Then the system will “save any enhancement information” and “terminate [the] virtual key.” *Id.*, Fig 3B. In this example, the virtual key is terminated based on the user restriction violation, irrespective of whether an agreed-to rental period has ended. *Id.*

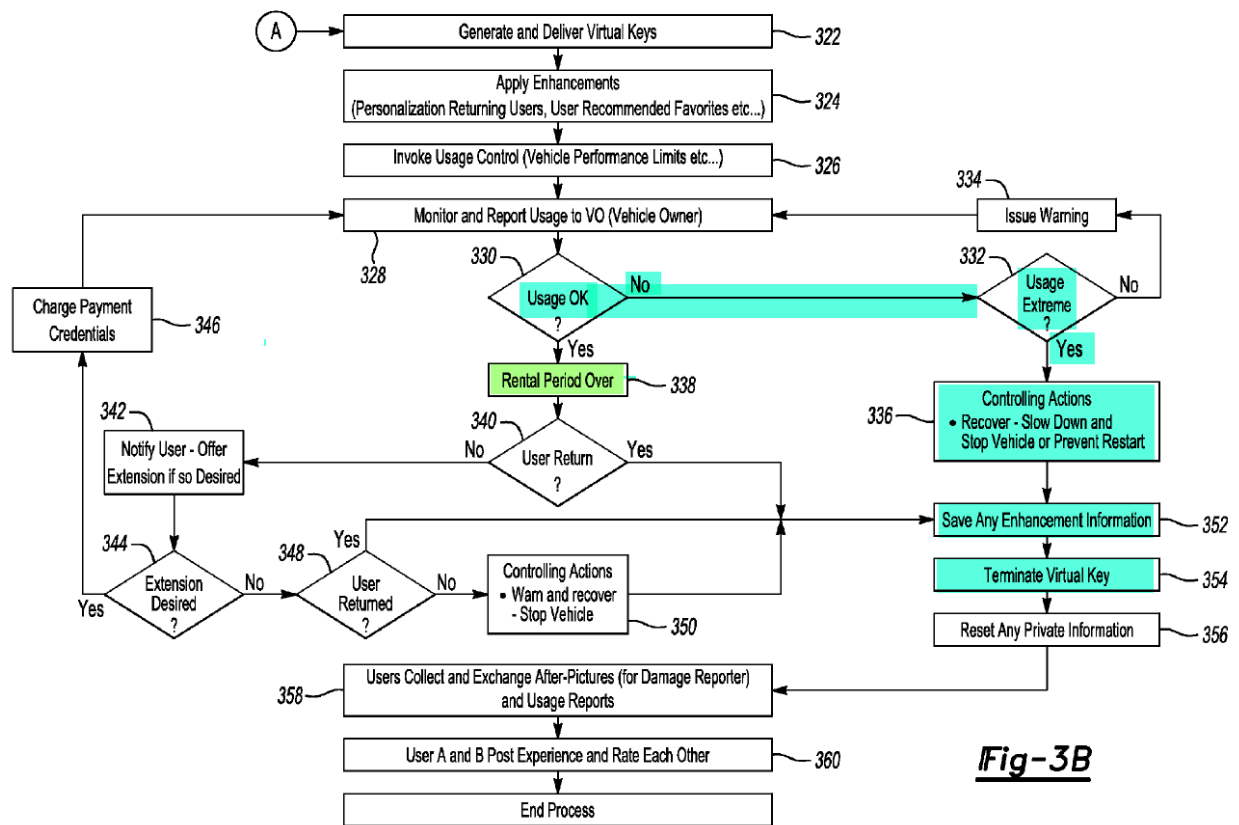


Fig-3B

Id., Fig. 3B.

57. Kleve also teaches that if an accident is detected and the vehicle's condition is unsafe to drive, the virtual key will terminate, regardless of the "rental end" time. *Id.*, ¶¶ 79-80, 53, Fig. 7B.

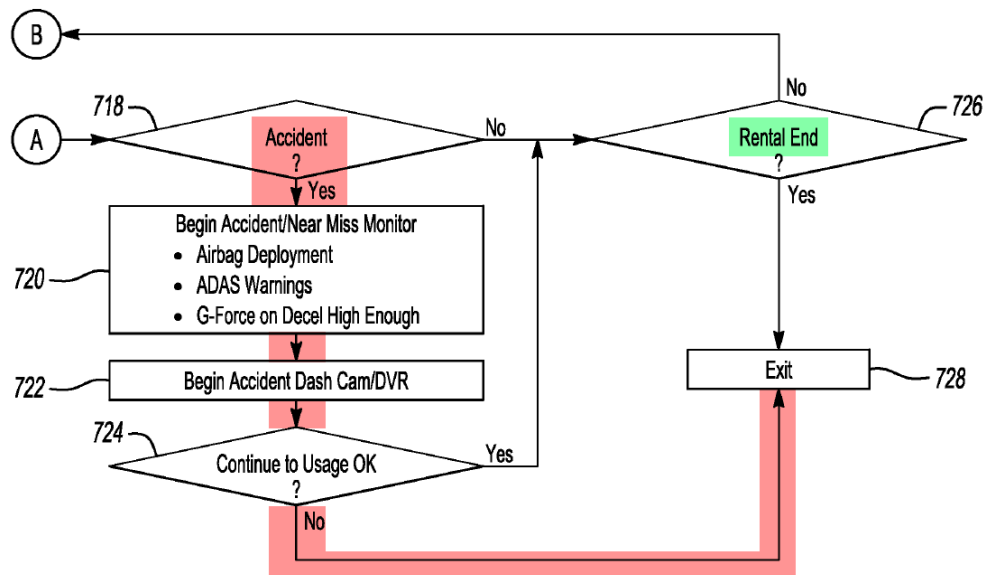
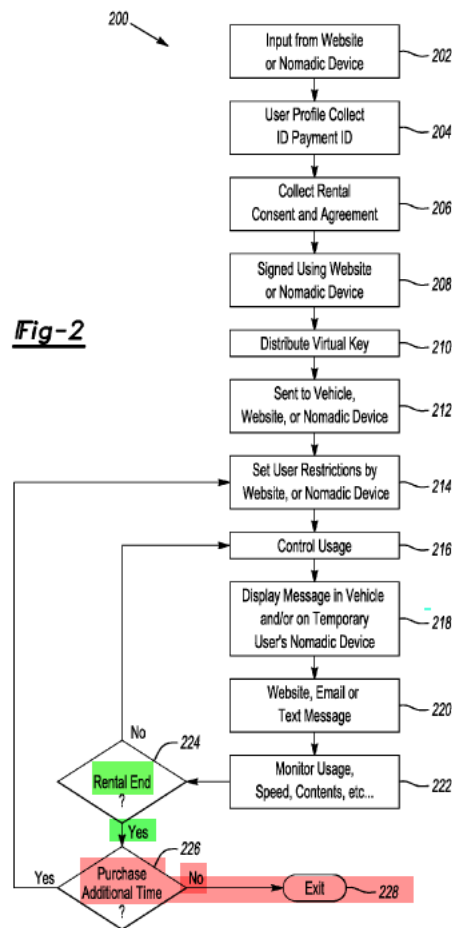


Fig-7B

Id., Fig. 7B.

58. Kleve teaches additional examples where the virtual key is operable after the rental term has ended and will not be terminated until the vehicle rental exit process, which is after the rental period is over. *E.g., id.*, ¶ 54. 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,” at step 228. *Id.*, ¶ 43, Fig. 2.

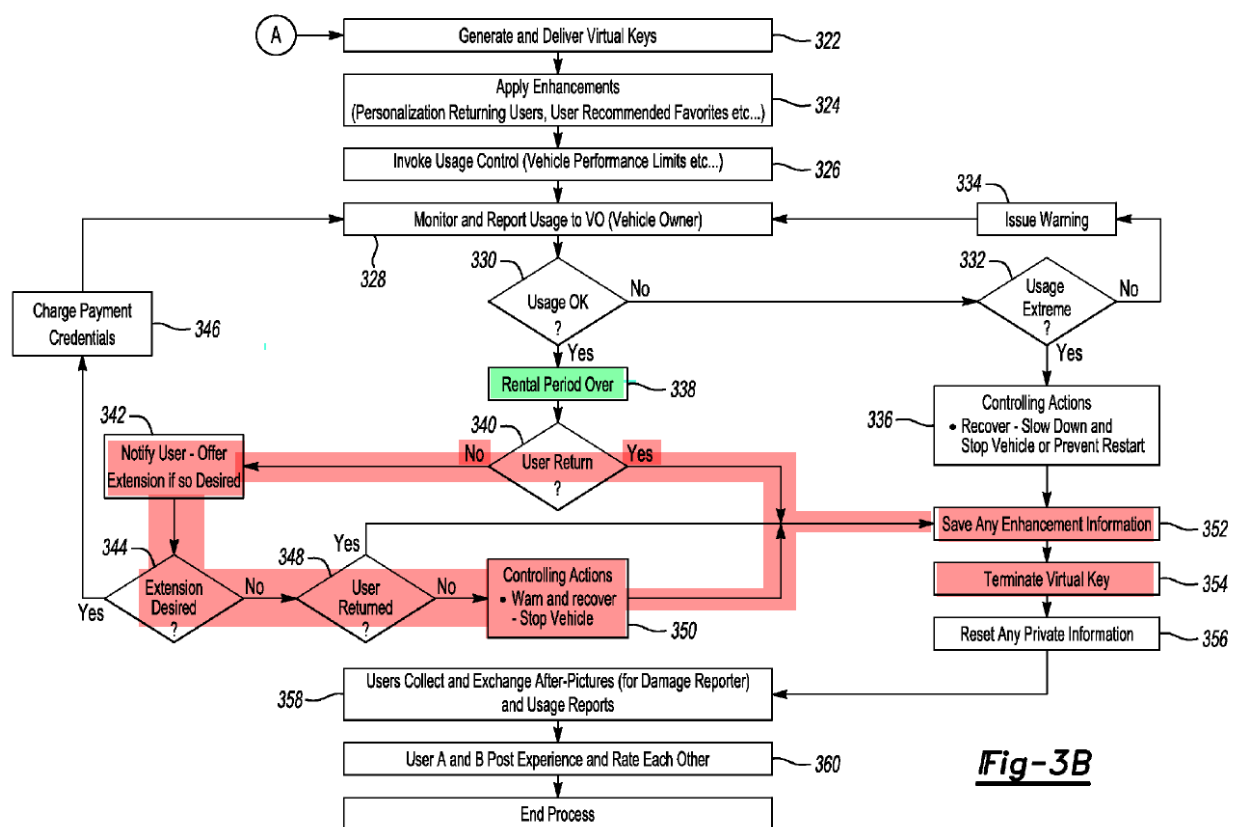


Id., Fig. 2.

59. As shown above at step 228, if no additional time is purchased, the system will proceed with a “vehicle exit mode process” after the rental period has ended. *Id.* Similarly, in the above example where an accident is detected by the VCS, but the vehicle is deemed safe to drive, the system will proceed with a “vehicle exit mode process” after the rental period has ended. *Id.*, ¶ 80 (“if the rental period has

ended, the monitoring and control system of the vehicle rental micro-business may begin to start its Temporary User vehicle rental exit mode process.”).

60. For example, 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.

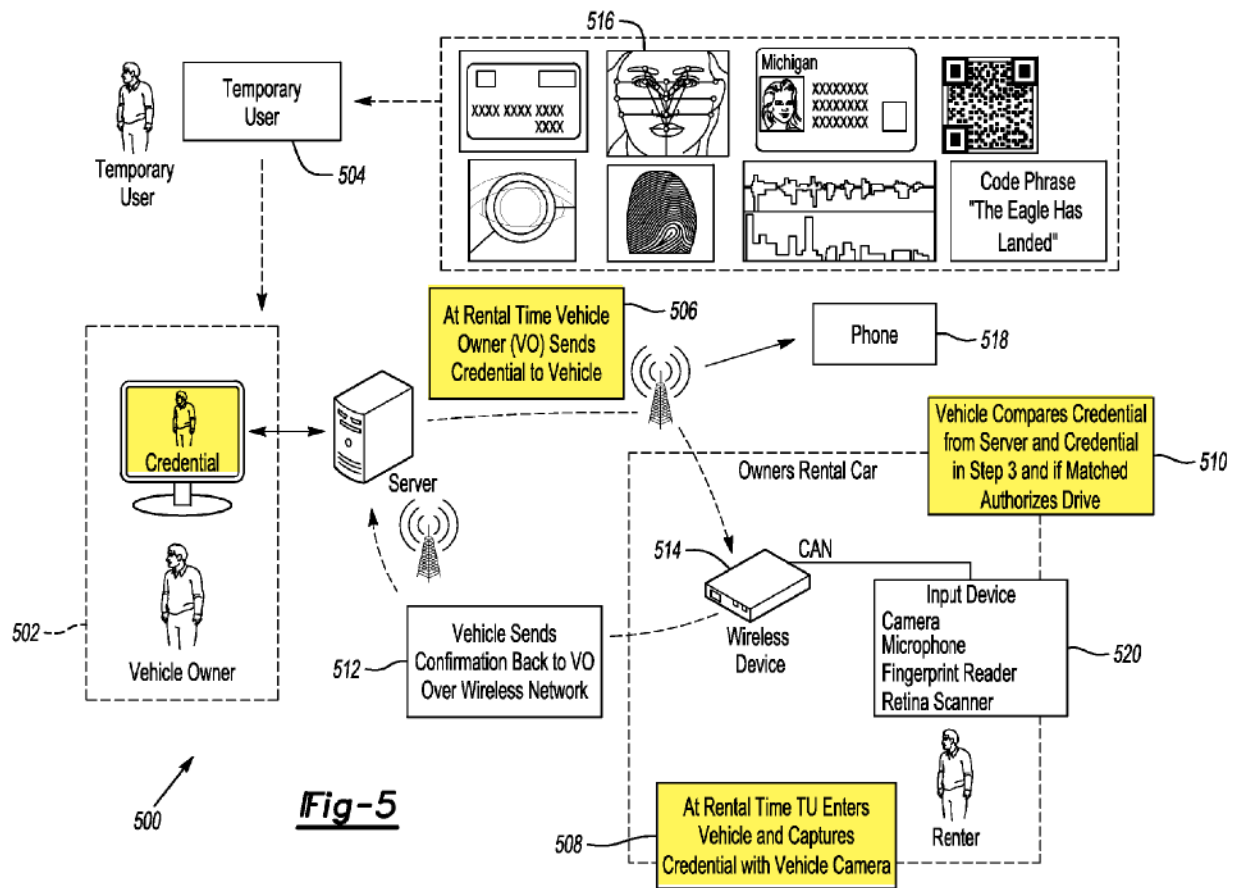


Id., Fig. 3B.

61. As another example, if “the rental period has expired,” but the Temporary User has not yet returned the vehicle, and the rental period end time is not extended, “the system may transmit controlling action to warn and induce

remedial actions at step 350.” *Id.*, ¶ 54, Fig. 3B. After terminating the virtual key at step 354, the system will reset any private information stored on the VCS at step 356. *Id.*, ¶¶ 80, 49, Fig. 3B.

62. I also note that Kleve’s disclosures regarding the set up of a virtual key do not involve the input or inclusion of any privilege settings, regardless of the form of the virtual key and regardless of whether it is encrypted. Kleve teaches that “to set up a virtual key,” the Vehicle Owner enters a vehicle authorization credential or “unique Temporary User identification” (*id.*, Fig. 5: 504, 516), which was received from the Temporary User (*id.*, ¶ 62, Fig. 5). Kleve instructs that the Vehicle Owner sends this same “credential” to the vehicle, e.g., via a server, and the Temporary User will provide this same credential to the vehicle, e.g., captured via camera, microphone, etc. *Id.*, Fig. 5. As shown in Figure 5 below, the vehicle compares the credential from the Owner and the credential captured from the Temporary User to authorize the Temporary User’s drive. *Id.*, Fig. 5, step 510.



Id., Fig. 5.

VIII. SUMMARY OF HATTON (EX1008)

63. United States Patent 9,002,536 to Hatton (EX1008, “Hatton”) is titled “Key Fob Security Copy to a Mobile Phone.” Hatton discloses that a “vehicle key,” such as a fob, may be embedded with security codes during the manufacturing process and/or at a vehicle dealership. EX1008, 13:64-14:9. Those security codes allow the fob to communicate with a vehicle to control its function, e.g., unlocking/locking the doors. *Id.* Specifically, a user may press a button on the fob,

which transmits the security codes to the vehicle and a command. *Id.*, 14:7-31. If the vehicle authenticates the fob using the security code, it can initiate the command, such as unlocking. *Id.*

64. Hatton discloses passive 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 the security codes sent from the fob are checked against the encrypted data in a PEPS look up table that is stored on the vehicle computing system (VCS). *Id.*, 9:50-63. The purpose of this check is to authenticate the fob to grant access to the vehicle.

65. Hatton teaches a mobile device that receives security keys from the fob and stores them, allowing the mobile device to send the security codes and commands to the car to initiate commands, such as locking/unlocking. *Id.*, Abstract, 14:49-15:36. Once the mobile device receives the security codes from the fob, it may then perform the functionality of the fob. *Id.*, 31-36. Specifically, the mobile device transmits security codes to the PEPS controller to authenticate the device. *Id.*, 17:29-36. After authenticated, the mobile device may transmit commands, such as locking or unlock. *Id.*, 17:36-46.

IX. SUMMARY OF MIKAN (EX1007)

66. United States Publication Number 2008/0150682 by Mikan et al. (EX1007, “Mikan”) is titled “Wireless Device as Programmable Vehicle Key.

Mikan discloses a wireless vehicle security system, in which an electronic key may be embedded in a traditional metal key, a phone, or a personal digital assistant. EX1007, Abstract, ¶ 50. In Figure 2, shown below, Mikan's system includes keys 205A-C, which may communicate directly with the vehicle's control unit 202, 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 vehicle 201, also shown below in Figure 2, includes both the vehicle control unit 202, as well as a local database 203. *Id.*, ¶¶ 50-51, 54. Mikan's master database 208 is part of the system's wireless network 207, and Mikan teaches that the master database 208 communicates with the vehicle's control unit 202. *Id.*

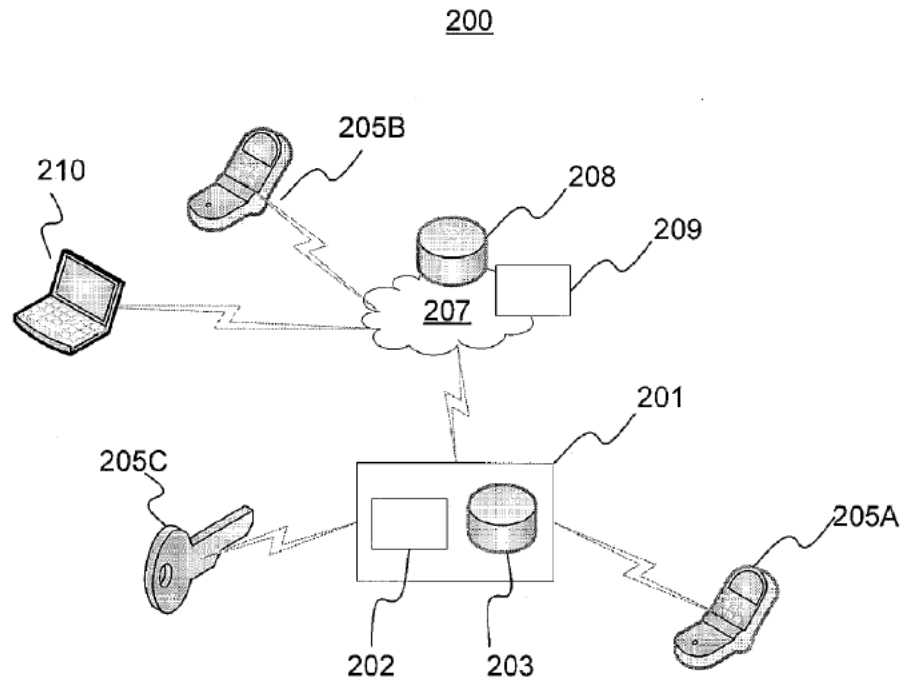


FIG. 2

Id., Fig. 2.

67. Mikan also describes “a vehicle operation policy,” which may “indicate to enable, partially enable, or disable a vehicle operation feature.” *Id.*, ¶¶ 5, 57. This vehicle operation policy 311 may be stored in the master database 208, on the wireless network 207, and after the master database syncs with the vehicle (e.g., Fig. 5, step 502), the vehicle’s local database 203 stores the vehicle operation policy 311 records for that vehicle. *Id.*, ¶¶ 58-59, 72, 81, Figs. 3A-3B.

68. Mikan teaches that 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.” *Id.*, ¶ 58, Fig. 3A. The master database also stores a policy set of vehicle operation policies 311, and “mapping 312,” which relates individual keys from the records of the key set 310 with specific vehicle operation policies 311. *Id.*

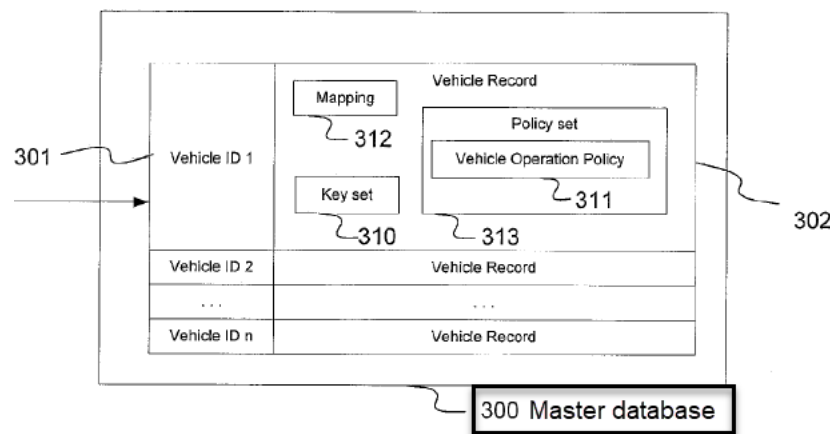


FIG. 3A

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

69. Mikan teaches that the vehicle 201 includes a local database that stores a “vehicle ID,” which corresponds to a specific vehicle ID record on the master database. *Id.*, ¶¶ 59-60. The vehicle’s local database also stores a key set 310, and a policy set of vehicle operation policies 311, with access control rules 317 for associated vehicle operations. *Id.*

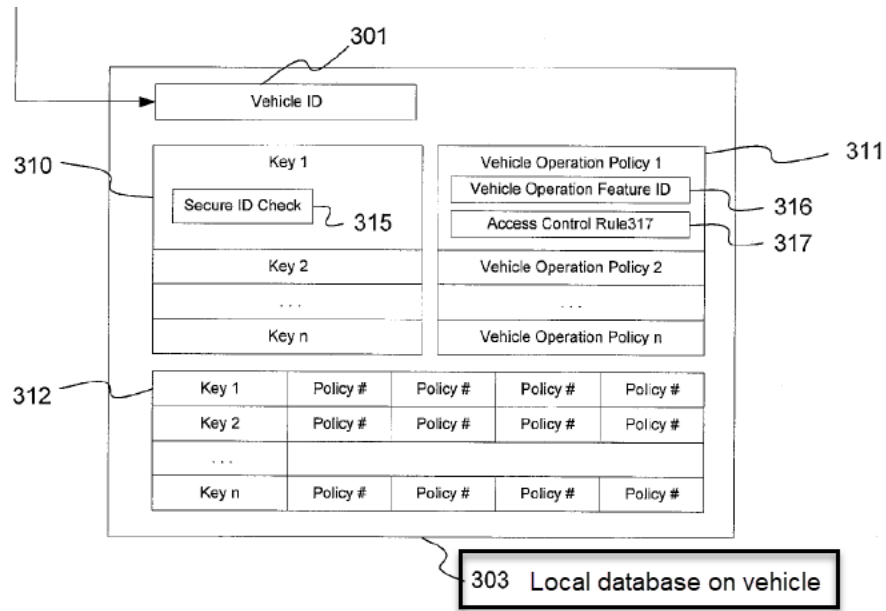


FIG. 3B

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

70. The vehicle’s local database includes “mapping 312,” which relates a vehicle operation policy 311 to a specific key in the key set stored on the vehicle. *Id.*, ¶ 61. Mikan provides an example showing that mapping 312 can indicate whether a particular key in the key set is related to a vehicle operation policy 311 that enables all vehicle operation features. *Id.* As another example, Mikan teaches that mapping 312 relates a second key to a vehicle operation policy 311 that restricts the key holder’s access to certain vehicle operation features via access control rules 317, for example, by restricting access to the glove box or trunk. *Id.*

71. As I indicated above, the vehicle’s local database 203 may be synchronized with records in the master database. *Id.*, ¶ 69, Fig. 5. Mikan teaches

that this synchronization allows the data in the master database and vehicle's local database to be kept consistent and updated, including any vehicle operation policy records. *Id.*, ¶¶ 54, 68-69.

72. Mikan teaches that this synchronization occurs before the vehicle 201 detects and authentication of a key (e.g. keys 205A-C). At the time a key is detected and authenticated, Mikan teaches that the vehicle's control unit 202 retrieves from the local database 203 the vehicle operation policy 311 records, and any corresponding vehicle operation feature ID 316 and access control rule 317, which pertain to that detected key. *Id.*; *id.*, Fig. 5. As I detail further in the paragraphs below, the vehicle uses its "mapping 312" to relate the detected key to stored vehicle operation policy 311 records. *Id.*, ¶ 61.

73. Mikan teaches that a wireless device is detected and authenticated as a key using secure identifiers. That is, the vehicle local database includes a "secure ID check 315" associated with each key in the key set 205A-C and this secure ID check 315 may be used in a "challenge-handshake authentication protocol (CHAP)" to authenticate a user's key. *Id.*, ¶¶ 59, 70-71.

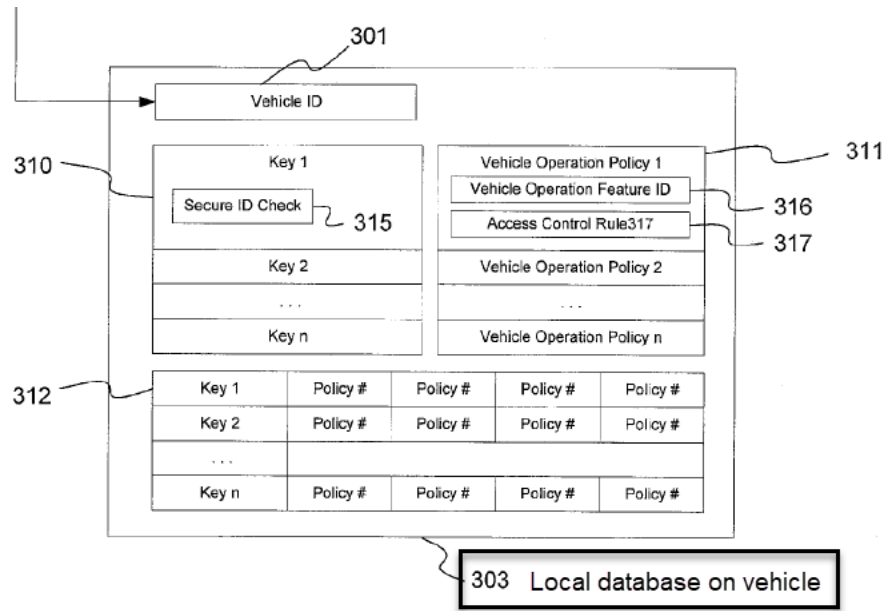


FIG. 3B

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

74. Mikan teaches that a user with a wireless device may approach the vehicle 201, and the vehicle detects that device by receiving a secure ID 407 (also “secure key identifier 407”) from the wireless device. *Id.*, ¶ 70, Fig. 5. The vehicle uses this secure ID 407 to authenticate the user’s wireless device as a key to access the vehicle, for example, in the “challenge-handshake authentication protocol (CHAP),” which I noted above. *Id.*, ¶¶ 60, 70. The wireless device stores its secure key identifier 407 in memory, as illustrated in Figure 4 below. *Id.*, ¶ 70, Fig. 4.

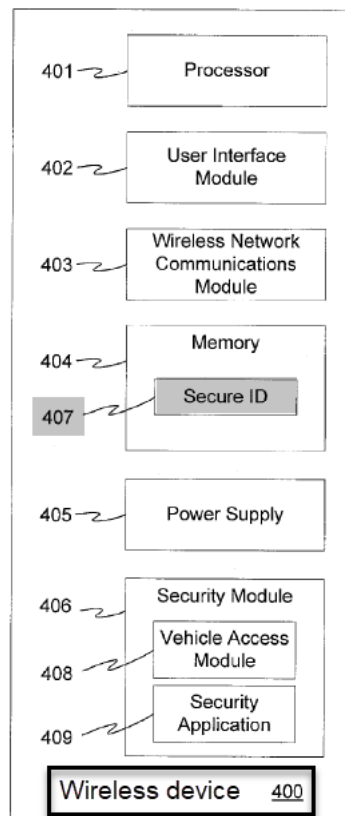
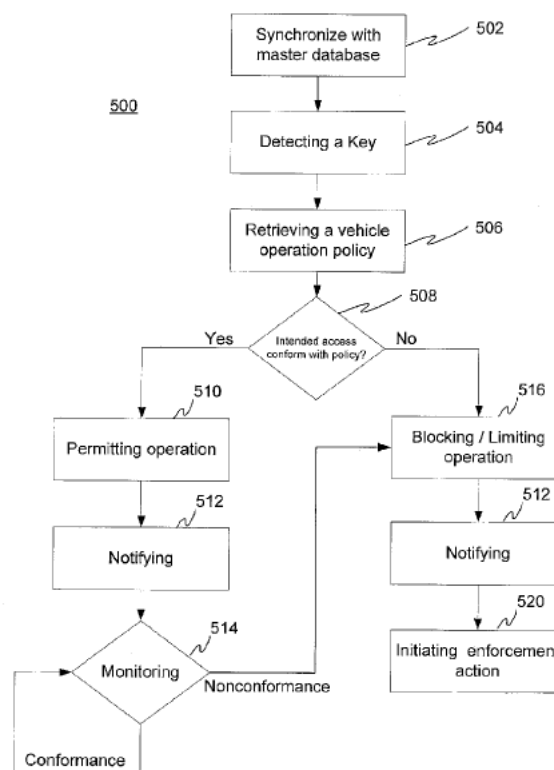


FIG. 4

Id., Fig. 4 (annot.).

75. Mikan does not disclose or teach that the vehicle receives any vehicle operation policy or access control rule from the wireless device. As I described above, Mikan’s system uses the wireless device’s secure ID 407 to authenticate the wireless device as a key. *Id.*, ¶ 65. After this authentication, Mikan teaches that the vehicle control unit 202 “retrieves” a vehicle operation policy from the vehicle’s local database 203. *Id.*, ¶ 72, Fig. 5. Mikan offers no teaching or suggestion that the wireless device’s secure ID 407 signal, sent to the vehicle for authentication,

includes any vehicle operation policy. *Id.*, ¶¶ 72-74, 65. I note that the vehicle control unit 202's "retriev[al]" of the vehicle operation policy 311 from the vehicle's local database 203 for the authenticated key would be unnecessary were the vehicle operation policy 311 already included in the secure ID 407 that had already been transmitted from the wireless device to the vehicle.



Id., Fig. 5.

76. I also note that the vehicle database's mapping 312 relates any locally stored vehicle operation policy 311 that may be in effect with relation to the authenticated key. *Id.*, ¶¶ 71-72. This mapping 312 function would be unnecessary

were the vehicle operation policy 311 already included in the secure ID 407 that had already been transmitted from the wireless device to the vehicle.

X. DETAILED ANALYSIS OF PETITION GROUNDS

77. As I describe in detail below, it is my opinion that Dr. Almeroth and the Petition fail to demonstrate that any claim of the '659 patent is invalid.

A. Each of the Kleve-based grounds (grounds 1-2) fails to establish obviousness of any challenged claim.

78. The independent claims require “communications circuitry of the vehicle is configured to receive coded data from the mobile device when using the eKey ... the coded data includes privilege settings set for limiting types of use of the vehicle when using the vehicle via the eKey.” EX1001, claim 1[d-e], 11[d-e], claim 18[d-e].

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

79. It is my opinion Kleve does not teach or suggest “the vehicle is configured to receive coded data from the mobile device when using the eKey ... the coded data includes privilege settings set for limiting types of use of the vehicle when using the vehicle via the eKey,” as required by the claims. As the alleged “privilege settings,” Petitioners and Dr. Almeroth identify a number of “restrictions,” but Kleve makes clear that none of these “restrictions” is available as

a restriction to monitor or control vehicle usage until after the set up and distribution of the virtual key. Pet. 20-21 (citing EX1005, ¶¶ 40, 83, 76); EX1004, ¶¶ 138-140 (same). Whether represented as an encrypted message or a matrix barcode, Kleve's virtual key does not include any of the "restrictions" alleged as the recited "privilege settings." Instead, Kleve teaches a solution that gives the Owner "control of the vehicle with the use of vehicle restriction limits initially set by the Owner at the beginning of the rental term." EX1005, ¶¶ 43, 75.

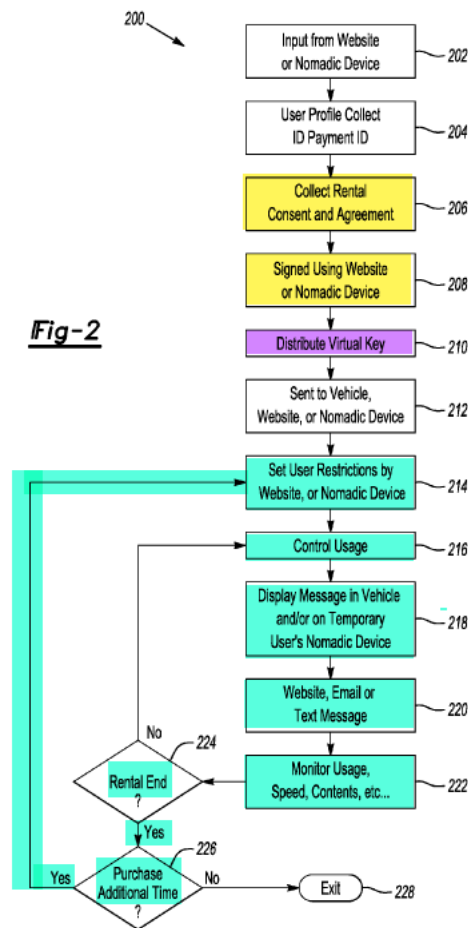
80. To set up a virtual key, Kleve discloses that "the Vehicle Owner may enter in vehicle authorization credentials based on information received by the Temporary User to set up a virtual key." EX1005, ¶ 62. Kleve teaches that the "distribution" of this virtual key credential occurs at step 210. EX1005, ¶¶ 62, 39, Fig. 2.

81. As the "restrictions" allegedly "sent with the request to generate a virtual key," the Board's Institution Decision identifies "a rental period restriction." IPR2024-01167, Paper 14 at 37-38 (citing EX1005, ¶¶ 38-39 and EX1004, ¶¶ 119-120). I disagree with this statement. At paragraph 38, Kleve 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; EX1005, ¶ 38). As I discuss above in Section

VII, none of the rental agreement terms, including any “rental period” described in paragraph 38, is disclosed or suggested to be included as a restriction when the virtual key is created or distributed. *Id.* I also note that there is no mention in paragraph 38 of any “virtual key.” *Id.* At paragraph 38, Kleve describes the Vehicle Owner and Temporary User formulating a rental agreement, at steps 206 and 208, and those steps precede the distribution of the virtual key (step 210). *Id.*; *id.*, Fig. 2. Kleve teaches that user restrictions for monitoring and controlling vehicle usage are “initially set at ... the beginning of the rental term.” EX1005, ¶¶ 43, 75 (“restrictions assigned ... at the start of the rental period”).

82. As I detailed above in my summary of Kleve, the reference teaches a specific solution “to enforce compliance with rental agreement terms,” which dictates that the Vehicle Owner must input as “user restrictions” at the beginning of the rental term. EX1005, ¶¶ 40-43, 51. And based on those restrictions, and the control parameters set to enforce those restrictions, the vehicle’s VCS will monitor vehicle usage and undertake remedial actions according to violations of those restrictions, e.g. “extreme usage.” *Id.* As I discussed above, it would be unnecessary for the Vehicle Owner to input—at the beginning of the rental term—user restrictions “to enforce compliance with rental agreement terms,” were those rental agreement terms already “privilege settings” included in the creation of the virtual key.

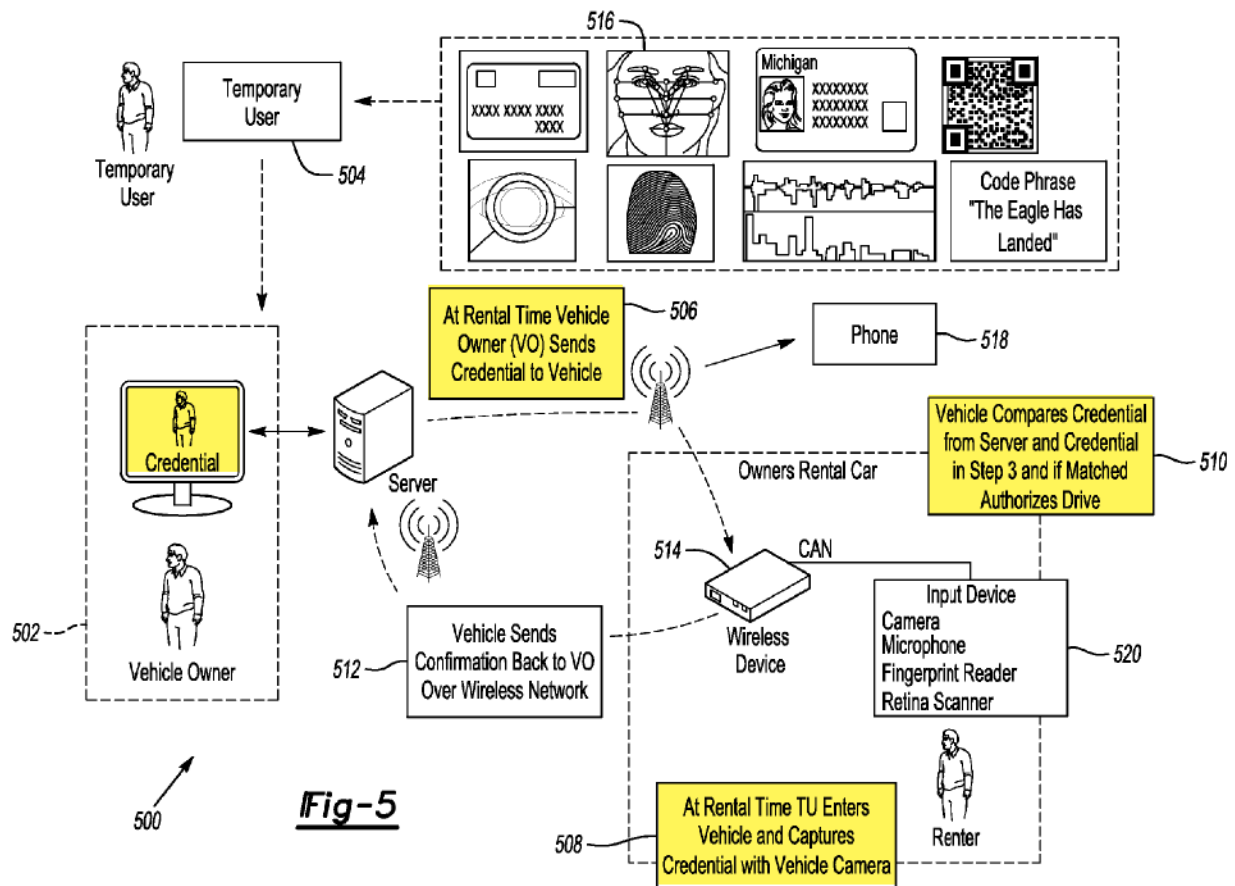
83. Also, as I describe above in Section VII, Kleve describes a solution to “enforce” any “rental end time restriction” which does not involve including any rental agreement terms, such as “rental period,” in the set up or distribution of the virtual key. EX1005, ¶ 43, Fig. 2. Regardless of what “rental period” may have been agreed to by the parties in their rental agreement, Kleve teaches that “rental period end time” is a “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.” *Id.*, ¶ 43, Fig. 2. If “rental period” was somehow included in the virtual key, at step 210 (or even earlier), it would make no sense for Kleve to update only step 214, in order to “update the new rental period end time restriction,” at step 226 → 214 (Figure 2), but not at step 210 or steps 206 or 208. EX1005, ¶ 43, Fig. 2.



Id., Fig. 2 (annot.).

84. I also note that Kleve teaches that the Owner sends the authorization “credential” to the vehicle “at Rental Time.” *Id.*, ¶ 66, Fig. 5. In this way, Kleve’s solution ensures that “the scheduled rental period of time begins” according to the agreed-upon rental period. *Id.*, ¶¶ 66, 62, Fig. 5. Kleve further teaches that “[a]t 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. If the “rental time” was somehow included in the creation or distribution of the virtual key, it would be unnecessary that the “Vehicle (VO) Owner sends [the] credential to [the] vehicle” (*id.*, Fig. 5, ¶ 66) “at rental time,” i.e., “[w]hen the scheduled rental period of time begins” (*id.*, ¶ 66, Fig. 5).



Id., Fig. 5 (annot.).

85. Dr. Almeroth additionally identifies Kleve’s description of “speed, global position coordinates, or load weight restrictions,” at paragraph 40, as alleged “restrictions” included in its virtual key. EX1003, ¶ 139. I disagree with this opinion.

At paragraph 40, Kleve describes steps 214, 216, 218 and 220. EX1005, ¶ 40. Kleve teaches that each of these steps proceed after the set up and distribution of the virtual key. *Id.*, ¶ 40, Fig. 2.

86. I note that at paragraph 40, Kleve describes step 214 as the first step in which “the Owner may have access to control usage of the vehicle being rented by the Temporary User,” Kleve describes how “the Owner may set user restrictions” for controlling usage of those restrictions, and Kleve teaches when those restrictions may be “initially set”—“at the beginning of the rental term,” but not at any time prior. *Id.*, ¶¶ 40-43.

87. Dr. Almeroth also opines 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 authorized trailer tow.” EX1003, ¶¶ 139 (EX1005, ¶¶ 83, 76). I disagree with this opinion. Kleve does not teach or suggest that the virtual key may be “configured” for any use, restriction, or rental request. At paragraph 83, cited by Dr. Almeroth, Kleve teaches that a Vehicle Owner may review the rental request submitted by a Temporary User. EX1005, ¶ 83. That rental request may include information such as “what the Temporary User is looking to use the vehicle for (e.g., without limitation, for towing, hauling, or errands), when the requested use will be taking place, and where.” *Id.* Kleve teaches that the Vehicle Owner may either accept or

decline the rental request. *Id.*, ¶ 84. If the Vehicle Owner accepts the rental request, the parties may negotiate the terms and conditions of the rental period. *Id.* Kleve’s description of submitting, reviewing and accepting / rejecting a Temporary User’s proposed rental request does not mention or suggest the involvement of any virtual key, let alone allowing the Temporary User’s stated demands from their “rental request” to be included as any privilege settings in a virtual key. *Id.*, ¶¶ 82-83.

88. As I described in Section VII, above, Kleve’s solution to “control the vehicle with the use of vehicle restriction limits” provides the Vehicle Owner—not the Temporary User—the option to set user restrictions “at the beginning of the rental term.” *Id.*, ¶ 43. Because the virtual key has already been created and distributed before the Owner may set any user restrictions, these restrictions cannot be sent or included as an alleged “privilege setting” in the creation or distribution of that virtual key. *Id.*, ¶¶ 51, 43, Fig. 2; EX1001, claims 1[d-e], 11[d-e], 18[d-e].

89. I also disagree with Dr. Almeroth’s opinion that the virtual key is “configured to monitor for unauthorized cargo or an unauthorized trailer tow” simply because Kleve’s system may monitor restrictions related to unauthorized cargo or unauthorized trailer tow. EX1003, ¶¶ 139 (citing EX1005, ¶ 76). Instead, the cited disclosure from 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. Based on restrictions that are “assigned by the Owner at

the start of the rental period,” this monitoring may include “unauthorized objects or cargo, unauthorized driving behavior, unauthorized driver, and/or an unauthorized trailer tow.” *Id.* Kleve teaches that these restrictions, and the control parameters on which they are based, “enforce compliance with the rental agreement terms,” as well as monitor and control any other user restrictions set by the Vehicle Owner, but they are initially set at the beginning of the rental term, which is after the virtual key has been created and distributed. *Id.*, ¶¶ 51, 43, 75 (“restrictions assigned by the Vehicle Owner at the start of the rental period”), Figs. 2, 7A.

90. As I discussed in Section VII, above, it would not be necessary for Kleve’s system to require the Vehicle Owner to input any “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 (¶¶ 84., ¶¶ 84, 89, 38)—were already included as “privilege settings” in the creation and distribution of a virtual key, at step 210.

91. It is my opinion that none of the alleged “restrictions” identified by Petitioners and Dr. Almeroth is included in a virtual key or included within any alleged coded data, “the encrypted data associated with the virtual key.” Pet. 21 (citing EX1005, ¶¶ 40, 83, 76); EX1003, ¶¶ 139-140 (same).

2. Kleve’s disclosure that a virtual key credential may be “sent to the vehicle configuring the VCS to enable the keyless drive system for the appropriate Temporary User during a given

rental period” does not suggest the “rental period” is included in the virtual key itself.

92. It is my opinion that Kleve’s disclosure that a virtual key credential may be “sent to the vehicle configuring the VCS to enable the keyless drive system for the appropriate Temporary User during a given rental period” does not teach or suggest the “rental period” is included in the virtual key. *See* EX1005, ¶ 39. Instead, as I discussed in Section VII, 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.

93. For example, as I noted in Section VII above, rental agreement terms may be agreed to after the virtual key has been created and distributed, and after the Temporary User has used the virtual key to access the vehicle to “agree to rental terms” in the vehicle. *Id.*, ¶ 65. Agreed-to rental agreement terms, such as the “rental period” cannot be a “privilege setting” included in the creation or distribution of the virtual key if the Temporary User already had and used the virtual key before agreeing to rental terms. *Id.*, ¶¶ 65, 67.

94. Additionally, I note that Kleve is not suggesting that the virtual key itself enforces compliance with rental agreement terms where Kleve instructs that the Temporary User may “agree to rental terms” after the virtual key has already been created, after the virtual key has already been distributed to the Temporary

User, and after the virtual key has already been used by the Temporary User to access the Owner's vehicle. *Id.*; *id.*, ¶¶ 43, 51, 75, Fig. 7A.

95. Instead, Kleve's system will monitor and control usage—that is, enforce compliance with rental agreement terms—according to the “vehicle restriction limits initially set by the Owner at the beginning of the rental term.” *Id.*

96. I disagree with the statement that Kleve's virtual key is “always generated after the rental agreement.” Paper 14 at 38. As I discussed above, Kleve teaches that a virtual key may be created and distributed to the Temporary User, and used by the Temporary User to access the vehicle before the Temporary User agrees to rental terms. EX1005, ¶¶ 65, 67; Pet. 10-11.

97. I also described in Section VII, above, Kleve's teaching that the Vehicle Owner send the virtual key credential “at rental time.” *E.g.*, EX1005, Fig. 5. This would be unnecessary were the “rental period” itself already included as a privilege setting in the creation or distribution of a virtual key. *Id.*, Fig. 5, ¶¶ 48, 66-67.

98. Kleve's virtual key is not only operable during the agreed-to rental period because, as I discussed in Section VII above, Kleve provides several examples in which the VCS's monitoring and control of the Owner's set use restrictions may terminate a virtual key either before or after an agreed-to rental period, and extend a rental end time by updating a rental end time restriction. These examples include, for instance, (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), and (3) the virtual key is terminated *after* the agreed upon rental period has expired (*id.*, ¶¶ 43, 53-55, 79-80). Additionally, I note that 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 the beginning of a rental term, of a “rental period end time restriction” at step 214. *Id.*, ¶ 43, Fig. 2.

3. Dr. Almeroth’s obviousness opinions are contradicted by Kleve’s disclosures.

99. I disagree with Dr. Almeroth’s opinion 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. Kleve’s system already achieves this benefit, but in a more secure manner than the modification proposed by Dr. Almeroth: 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. 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, but those restrictions are not transmitted to the Temporary User. *Id.*, ¶¶ 40-43, Fig. 2.

100. Dr. Almeroth fails to offer any benefit that would be achieved by modifying Kleve to include restrictions with its virtual key in addition to Kleve’s existing solution to control usage according to restrictions initially set by the Owner at the beginning of the rental term. EX1004, ¶ 140.

101. Dr. Almeroth also fails to explain how his proposed modification to Kleve’s virtual key, to include restrictions from the parties’ agreed-upon rental agreement, would ensure the Owner retains the full discretion and control over vehicle usage, which is already taught by Kleve’s solution. *See id.*

102. I also disagree with Dr. Almeroth’s proposed modification to include restrictions, such as rental agreement terms, in Kleve’s virtual key because such a modification would ignore Kleve’s intent and rationale to have the Vehicle Owner, but only the Vehicle Owner, set restrictions that will be monitored and controlled by the vehicle’s VCS.

103. By contrast to Kleve’s teachings that both the Vehicle Owner and the Temporary User may negotiate and agree to the terms of the rental agreement (EX1005, ¶¶ 38, 84, 89), Kleve is consistent in teaching that only the Vehicle Owner may utilize the control the “monitoring” and “control usage” features of Kleve’s

system by inputting user restrictions (*id.*, ¶¶ 40-41, 51, Figs. 2, 7A). *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”). For example, Kleve teaches that “performance limits *chosen by the VO [Vehicle Owner]*” (*id.*, Fig. 7A) (emphasis added) are 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). Also as I discussed in Section VII above, Kleve provides a rationale for this design, explaining, “[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.*, ¶ 51. Kleve discloses 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.

B. A POSITA would not have combined Kleve and Hatton as proposed.

104. I disagree with Dr. Almeroth’s opinion that it would have been obvious to “include the restrictions ... as part of the coded data associated with a virtual key ... as part of the encrypted data described in Hatton.” EX1004, ¶ 140. It is also my opinion that it would not have been obvious to a POSITA to modify Kleve in view of Hatton as Petitioners and Dr. Almeroth propose.

105. I note that Dr. Almeroth does not opine that Hatton discloses any “restrictions” included in its “encrypted data.” *Id.* And Hatton does not. *See* EX1008, 7:33-56 (cited by Dr. Almeroth). As Hatton does not teach including restrictions in any encrypted data, combining Kleve in view of Hatton to include encrypted data in Kleve’s system would not cure Kleve’s failures. That is, modifying Kleve’s “virtual key” to encrypt it would not modify the key to include “restrictions.” Neither reference, alone or in combination, teaches the functionality that was added during prosecution and relied upon to overcome all art-based rejections. *See* Section VI.B, above.

106. While Dr. Almeroth opines that it would have been obvious to encrypt data, including restrictions, on the mobile device, Dr. Almeroth never opines why it would have been obvious to include restrictions on a mobile device to begin with, a feature that is not taught by Kleve or Hatton. *See* EX1004, ¶¶ 111, 140. Dr. Almeroth opines that “a POSITA would have been motivated to include data identifying restrictions ... as part of the encrypted data transmitted with the electronic key ... so that the Temporary User cannot modify those restrictions at his or her mobile device.” *Id.*, ¶ 140. However, in my opinion, Dr. Almeroth’s explanation actually demonstrates why it would not have been obvious to modify Kleve to include “restrictions” as part of Kleve’s “virtual key” because including the restrictions on the Temporary User’s device leads to an additional point of security vulnerability

and would provide a Temporary User an opportunity to modify his or her own device to tamper with security restrictions.

107. In Kleve, the “restrictions” are not sent to the Temporary User (a renter of a vehicle) or a Temporary User’s device. Instead, the Vehicle Owner inputs user restrictions, at the beginning of the rental term, and the VCS of the vehicle downloads those restrictions after the Temporary User has already initiated the rental period. EX1005, ¶ 43, 75, Fig. 7A. Thus, Kleve discloses providing any “restrictions” to the vehicle’s VCS from the server, not via the “virtual key.

108. While Dr. Almeroth provides no sufficient reason why a POSITA would have modified Kleve to instead send the “restrictions” to the Temporary User’s device and then include them in every request to unlock the vehicle, a POSITA would understand that making such a modification (not taught by either reference) would be undesirable. By sending restrictions to the Temporary User’s device, the Temporary User would have an opportunity to “modify those restrictions at his or her mobile device and circumvent the restrictions”—the reason Dr. Almeroth proposed to do so. EX1004, ¶ 140. A POSITA would understand Kleve to already avoid the problems that Dr. Almeroth identified: as the restrictions are not sent to the Temporary User in Kleve, the Temporary User has no opportunity to “modify those restrictions at his or her mobile device and circumvent the restrictions.” *Id.*

109. Moreover, this explanation of how Kleve works from the previous paragraph again demonstrates that it would not have been obvious to provide “restrictions” to a Temporary User’s device. Kleve discloses that the vehicle verifies the Temporary User’s virtual key (e.g., facial features or barcode) by “communicating with the server to compare the credential and verify Temporary User’s access.” EX1005, ¶ 68. As such, Kleve’s vehicle must be in communication with the server to operate. In my opinion, Dr. Almeroth fails to identify any sufficient reason to modify Kleve’s server of a rental system to provide a render with “restrictions,” when the server must be in communication with the vehicle and can send the restrictions to the vehicle without sending any to the Temporary User’s device—a more secure and efficient process.

C. A POSITA would not have found it obvious to combine Kleve and Hatton as Dr. Almeroth proposes.

110. I disagree that a POSITA would have found it obvious to combine Kleve and Hatton as Dr. Almeroth proposes.

111. Dr. Almeroth proposes to combine Kleve with Hatton’s teachings of generating keys and communicating encrypted data. EX1004, ¶ 109. I disagree.

112. I note that Dr. Almeroth’s “Overview of Prior Art” section does not provide an overview of Hatton, other than generally opining, without citation or explanation, that it teaches functionality of certain claim elements. EX1004, ¶ 105.

Similarly, in his “Motivation to Combine” section, Dr. Almeroth generally opines that Hatton teaches “encrypted data,” but again without citation or reference to the disclosure of Hatton to which he is referring. *Id.*, ¶¶ 109-115.

113. Dr. Almeroth opines that Hatton’s teachings of communicating encrypted data increases “security, efficiency, and better user experience.” EX1004, ¶¶ 109-112. I disagree that the proposed combination would provide any of these benefits. With respect to security, Dr. Almeroth opines that a POSITA would realize that encrypted data “prevents a Temporary User from tampering with the electronic key or otherwise circumventing restrictions and limits on the use of the electronic key (for example, by circumventing restrictions on use set by the Vehicle Owner, or by re-distributing the key to additional unauthorized third parties).” EX1004, ¶ 111. As an initial matter, a POSITA would not be motivated to make this combination to overcome the problem of Temporary User tampering and, indeed, it would allow a Temporary User an opportunity to tamper, as I described in Section X.B., above. Regardless, the benefit Dr. Almeroth is associating with encrypted data is when encryption is used for the purpose of confidentiality, not for the purpose of authentication. Hatton teaches encrypted data being used for the purpose of authentication.

114. While Hatton teaches encrypting data, a POSITA would understand that Hatton’s encryption is for authentication, not confidentiality. By way of

background, in computer science, authentication is the process of verifying the identity of an entity before granting access to a resource, while confidentiality is a distinct concept involving the protection of information from unauthorized access or disclosure. Hatton's encrypted data is used for authentication, not confidentiality. Hatton discloses passive 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 the encrypted data sent from the key/mobile device is checked against the encrypted data in a PEPS look up table that is stored on the vehicle computing system (VCS). EX1008, 9:50-63. The purpose of this check is to authenticate the key/mobile device to grant access to the vehicle. Thus, Dr. Almeroth is mistaken in his understanding of Hatton and the disclosures it contains. Furthermore, Kleve already teaches authentication: as I discussed above, Kleve teaches a comparison of the "virtual key" (e.g., facial features) to authenticate a user. E.g., EX1005, ¶ 70. A POSITA thus would have no reason to add Hatton's authentication to Kleve, which also compares the received data for authentication.

115. Second, Dr. Almeroth incorrectly contends Hatton teaches generating encrypted data at a mobile device. EX. 1004, ¶ 112. There is no disclosure of any encrypted data being generated by a mobile device in Hatton. Hatton discloses passive entry passive start (PEPS) and passive anti-theft security (PATs) controllers for access control, neither of which involves generation of encrypted data. As Hatton

describes, all the encrypted data used in PEPS and PATS are assigned at the time the vehicle is manufactured. EX1008, 8:24-36, 14:7-18. Hatton does not describe a mobile device generating encrypted data. Hatton only discloses changing the designation of key status between primary and secondary. EX1008, tables 1 and 2, 8:24-36. Relying on his flawed understanding of Hatton, Dr. Almeroth opines that based on the disclosures in Hatton a POSITA would have been motivated to modify Kleve to generate encrypted data containing restrictions on the use of a rental vehicle. EX 1004, ¶ 140. Under Dr. Almeroth's combination theory, for each car rental agreement in Kleve, a new key with encrypted data containing restrictions on the use of the vehicle needs to be generated. However, Hatton does not disclose generating any encrypted data. Instead, Hatton teaches the encrypted data is assigned to the vehicle by the manufacturer when it is manufactured. In my opinion, Hatton would not have taught a POSITA how to generate encrypted data containing restrictions on the use of a rental vehicle in the context of Kleve.

116. Dr. Almeroth is also incorrect that encryption would improve the efficiency and user experience. It is generally known that encrypted communication is substantially less efficient than unencrypted communication, because encrypted communication requires the encryption and decryption of data, both of which are computationally expensive operations.

117. Lastly, Dr. Almeroth provides no reason why an encrypted

communication would improve the user experience. Quite the contrary, a POSITA would have understood that because encrypted communication can result in a slower system, encrypted communication is likely to negatively impact the user experience.

D. The Sekiyama reference does not cure the deficiencies of Kleve/Hatton.

118. For Ground 2, Dr. Almeroth proposes adding the Sekiyama reference to the Kleve/Hatton combination. However, Dr. Almeroth only proposes doing so as related to dependent claim 2. Sekiyama does not cure any deficiencies of Kleve/Hatton discussed above, and Dr. Almeroth offers no opinion to the contrary.

119. It is my opinion that neither Kleve, nor Kleve in combination, would have rendered obvious any challenged claim.

XI. DR. ALMEROOTH AND THE PETITION FAIL TO SHOW THAT MIKAN, ALONE OR IN COMBINATION, DISCLOSES OR SUGGESTS A “CODED DATA FROM THE MOBILE DEVICE ... CODED DATA INCLUDES PRIVILEGE SETTINGS.”

120. In my opinion, Dr. Almeroth does not demonstrate that a POSITA would have understood Mikan, alone or in combination, to disclose or suggest a vehicle configured to receive “coded data from the mobile device ... the coded data includes privilege settings,” as recited by the independent claims. EX1001, claims 1[d-e], 11[d-e], 18[d-e].

A. Dr. Almeroth identifies a secure ID as coded data, but the secure ID 407 transmitted by the wireless device to the vehicle does not include any alleged privilege settings.

121. Dr. Almeroth identifies Mikan's vehicle operation policies as the recited "privilege settings," however Mikan discloses that vehicle operation policy 311 may be stored in the master database and local database, and after synchronization between the two databases, and authentication of wireless device as a key, the vehicle control unit 202 retrieves the vehicle operation policy 311 from its own local database. I note that neither the master database or local database is in or part of Mikan's wireless device, nor does Mikan ever disclose or suggest that the wireless device sends any vehicle operation policy to any vehicle. *E.g.*, EX1007, ¶¶ 59, 64, 71-72, Figs. 3A-3B, 4-5. Therefore, whether or not the wireless device's secure ID 407 is "coded data," it does not include any vehicle operation policy sent to the vehicle. In fact, Mikan's vehicle never receives any privilege settings from a mobile device.

122. Mikan teaches that when a wireless device is used as a key (e.g., key 205A-C), the vehicle does not ever receive any coded data with privilege settings from any mobile device. Instead, Mikan teaches that it is the vehicle itself that retrieves vehicle operation policy 311 from its local database, then may temporarily store or cache those records in the vehicle control unit 202 during the user's operation of the vehicle. *Id.*, ¶ 72. Mikan teaches that before a wireless device is

even authenticated as a key, the vehicle's local database 203 synchronizes with the master database. *Id.*, ¶ 69, Fig. 5 (step 502). Therefore, any vehicle operation policy changes are regularly communicated to a vehicle as part of the synchronization process. *Id.* Then, the vehicle detects and authenticates the user's wireless device, using the "secure ID 407" from the wireless device and the "secure ID check 315" from the vehicle. *Id.*, ¶ 70, Fig. 5 (step 504). The vehicle control unit 202 then retrieves any applicable vehicle operation policy 311 record by querying the vehicle's local database 203. *Id.*, ¶ 72, Fig. 5 (step 506). 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.

123. Mikan teaches that whether the vehicle operation policy 311 is 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 nonetheless remain in the vehicle, and never are, nor need to be, "received" from any mobile device. *Id.*, ¶¶ 59, 64, 71-72, Figs. 3A-3B, 4-5.

124. Maintaining the vehicle operation policy 311 local to the vehicle, Mikan then processes any access request from a user according to the vehicle's locally stored vehicle operation policy. For example, after the master database and local database have synchronized (Fig. 5, step 502), a user may approach the vehicle 201, the vehicle detects the secure ID 407 of the wireless device (step 504) and user

sends a user request, or access request, to unlock a vehicle door. *Id.*, ¶¶ 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, below. *Id.*, ¶ 74. Alternatively, 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.*

125. To perform these comparison functions, Mikan teaches that the vehicle always compares each user access request with the vehicle operation policy 311 “retrieved” from the vehicle’s local database. *Id.*, ¶¶ 72-74.

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

126. As I discussed in Section IX, above, 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 in each database. *Id.*, ¶¶ 59, 61, 81, Figs. 3A-B.

127. When a vehicle synchronizes its vehicle operation policy 311 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, thereby providing that vehicle with the vehicle operation policy 311 records that relate to the key set of that vehicle ID. *Id.*, ¶¶ 81, 84, Fig. 3A. Also, when a vehicle detects a wireless device using its secure ID 407, and authenticates that device as a key 205A-C, the “mapping 312” of the vehicle’s local database determines the relationship between any locally stored vehicle operation policy to that detected and authenticated key. *Id.*, ¶¶ 59, 61. I note that this mapping 312 function would not be needed by the vehicle if there were any vehicle operation policies, i.e., any alleged “privilege settings,” in the secure ID 407 that the wireless device already transmitted to the vehicle.

128. I also note that if the vehicle operation policy were included in any data sent by the mobile device to the vehicle, the vehicle itself would not need to perform the operations of (1) “retriev[ing]” the vehicle operation policy 311 at step 506 by “querying the local database 203,” (2) performing the “mapping” to determine the relationship between a given key from the database’s “key set” with vehicle operation policy records retrieved from the database’s “policy set,” or (3) performing the comparison functions between the “retrieved vehicle operation policy 311” and each user access request. *Id.*, ¶¶ 72-74, 60-61, Fig. 5. Accordingly, it is my opinion that neither the wireless device itself, nor the secure ID 407 stored in the wireless device, ever transmits any vehicle operation policy to the vehicle.

C. Dr. Almeroth’s opinions are contradicted by Mikan’s solution to retrieve locally stored vehicle operation policies from the vehicle’s local database.

129. I disagree with Dr. Almeroth’s opinion 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. As I discussed in Section XI.A-B, above, Mikan does not disclose or suggest any vehicle that receives any “coded data includes privilege settings,” nor does the vehicle “receive coded data from the mobile device” that includes privilege settings. EX1001, claim 1[d-e], 11[d-e], and 18[d-e]. Mikan’s system teaches that the master database synchronizes with the vehicle’s local database, so that when a vehicle detects and authenticates a key, the vehicle can retrieve its locally stored vehicle operation policies for that key. EX1007, ¶¶ 59, 61, 72. Specifically, the vehicle uses its locally stored mapping 312 to relate any key in its locally stored key set to its locally stored vehicle operation policies. *Id.*

130. I disagree with Dr. Almeroth’s conclusion that “[t]he wireless device operating as an electronic key be used to unlock and start a vehicle. For example, Mikan discloses that each electronic key has an associated ‘vehicle operation policy.’” EX1004, ¶ 217 (citing EX1007, ¶ 52). However, I reviewed paragraph 52 and it does not support this statement. Paragraph 52 describes the communication connections involving the vehicle’s control unit 202. EX1007, ¶ 52. I also disagree because Mikan teaches 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.*, ¶¶ 59-60, 72. In this way, the vehicle itself uses the identifier received from the detected wireless device to determine 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.*, ¶¶ 71-72; 60-61

131. I also disagree with Dr. Almeroth’s statement that a POSITA would have been motivated “to encrypt or otherwise encode the vehicle operation policy for transmission so that users cannot tamper with the vehicle operation policies and associated access control rules.” EX1004, ¶ 221. But Mikan does not disclose any such transmission. Indeed, by retrieving the vehicle operation policy 311 records from its local database 203, the vehicle need not rely on the “transmission” of any vehicle operation policy from the wireless device.

132. I also disagree with Dr. Almeroth’s proposed modification of Mikan “to transmit the vehicle operation policy” “either as part of or in addition to Mikan’s secure identifier.” EX1004, ¶¶ 221-222. It would not make sense to make such a modification, since doing so would render Mikan’s local database and its synchronization with the master database superfluous. The point of having a local database and synchronizing it with the master database in Mikan is to then use it for retrieving the vehicle operation policy. Mikan discloses an efficient solution, where vehicle operation policy changes are communicated to a vehicle as part of the

synchronization process. Therefore, each policy change is communicated only once. A POSITA would not have modified Mikan as proposed by Dr. Almeroth because they would have realized it would make the system less efficient. In the modified system, the vehicle operation policy would need to be sent every time the wireless device is used to enter the vehicle, even if there has been no change to the vehicle operation policy.

133. I also disagree with Dr. Almeroth's *proposed motivation* "to transmit the vehicle operation policy" "either as part of or in addition to Mikan's secure identifier," since Dr. Almeroth's proposed modification actually renders the vehicle operation policy records *more* vulnerable to "tampering" by the user, not less. EX1004, ¶¶ 221-222. Mikan teaches that the wireless device does not transmit to the vehicle any vehicle operation policy that limits the types of use of the vehicle when the vehicle is accessed using the electronic key. By modifying Mikan to not only include such vehicle operation policy records in the user's wireless device itself, but also to have the user transmit the vehicle operation policies via the wireless device, would inject *additional security vulnerabilities* into Mikan's system. As I discussed in Section X.C., above, Dr. Almeroth's concern about tampering and unauthorized access actually demonstrates why it would not have been obvious to modify Mikan to include vehicle operation policies as part of Mikan's "secure ID 407" because including the vehicle operation policies on the wireless device and having that device

transmit those policies leads to an additional point of security vulnerability and would provide a wireless device user an opportunity to modify his or her own device to tamper with privilege settings.

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

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

XII. THE ADDITIONAL REFERENCES DO NOT CURE THE DEFICIENCIES OF MIKAN.

136. For grounds 4-6, Dr. Almeroth proposes adding different references in combination with Mikan. However, Dr. Almeroth only proposes doing so as related to different limitations of the independent claims than those discussed above, or as related to dependent claims of the '659 patent. The added references do not cure any deficiencies of Mikan discussed above, and Dr. Almeroth offers no opinion to the contrary.

XIII. DR. ALMEROOTH FAILS TO SHOW THAT CLAIM 6 IS ANTICIPATED OR RENDERED OBVIOUS BY ANY REFERENCE.

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

138. I disagree with Dr. Almeroth's opinion that it would have been obvious that the smartphone application of Kleve "may also be used to enable multiple authorized temporary users to share virtual keys with each other." In fact, Kleve teaches the opposite. As I discussed in Section V, above, Kleve teaches specific features to allow the Vehicle Owner, and the Vehicle Owner alone, full control over the usage of their vehicle, "as this may be the only vehicle the Owner possesses."

EX1005, ¶ 51. Kleve highlights the Vehicle Owner’s ability to exercise complete control over their asset, e.g. disclosing a solution by which the Owner can set user restrictions, which will be monitored and controlled by the vehicle’s VCS, thereby providing the Owner with notifications of the vehicle’s usage and any violations of set user restrictions. Kleve also teaches that even after a virtual key is distributed to the Temporary User, the Vehicle Owner sends the “credential” to the vehicle “at rental time,” and, “at rental time,” the Temporary User inputs their “credential” at the vehicle. *Id.*, Fig. 5, ¶ 66. That is, the vehicle must compare and confirm a “match” between these two credentials before authorizing the Temporary User’s drive. *Id.*

139. It is my opinion that Kleve discourages any suggestion that a Temporary User—whose own vehicle use will be specifically monitored and controlled by the Vehicle Owner’s actions—can share an eKey for the vehicle with some other user. 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.*

140. I also disagree that Mikan teaches a “plurality of electronic keys may be incorporated into mobile devices for use with a vehicle.” Pet. 65. Instead, each wireless device includes its own “secure ID 407,” and it is this “secure ID 407” that is transmitted to the vehicle for authentication. EX1007, ¶ 65. Because Mikan’s secure ID 407 does not include any privilege settings, as I discussed in Section XI

above, the Petition's proposed combination with Sekiyama does not cure Mikan's failure to disclose or suggest coded data from the mobile device that includes privilege settings. Therefore, any sharing of the key, as proposed in this combination, would nonetheless lack the requisite privilege settings included in coded data.

XIV. **CONCLUSION**

141. This declaration reflects my opinions as currently held. However, my analysis may continue such that I may consider additional information that may result in additional observations.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Executed this 23rd day of April, 2025, at Irvine, California .

A handwritten signature in dark ink, appearing to read "Sam Malek", is written over a horizontal line.

Dr. Sam Malek