

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

KIA CORP.,
TOYOTA MOTOR CORP.,
Petitioners,

v.

EMERGING AUTOMOTIVE LLC,
Patent Owner

Case IPR2024-01167
U.S. Patent 11,738,659

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

TABLE OF CONTENTS

I.	Introduction and Background.....	1
II.	Qualifications	2
III.	Materials Considered	8
IV.	Legal Principles.....	8
V.	Person of Ordinary Skill in the Art (“POSITA”)	13
VI.	Background	15
	A. Overview of the ’659 Patent	15
	B. Prosecution History of the ’659 Patent	15
VII.	Summary of Kleve (EX1005)	16
VIII.	Summary of Hatton (EX1008).....	18
IX.	Summary of Mikan (EX1007)	19
X.	Detailed Analysis of Petition Grounds.....	20
	A. Dr. Almeroth fails to demonstrate any reasonable expectation of success for the Kleve/Hatton-based grounds.....	21
	1. Dr. Almeroth fails to demonstrate that Kleve/Hatton teaches or suggests any of the “coded data includes privilege settings” limitations of the independent claims.....	21
	2. Dr. Almeroth fails to demonstrate that Kleve/Hatton teaches “memory” “having program instructions for instructing/controlling unlocking and starting of the vehicle.”	28
	3. A POSITA would not have found it obvious to combine Kleve and Hatton as Dr. Almeroth proposes.....	29
	4. The Sekiyama reference does not cure the deficiencies of Kleve/Hatton.	33
	B. Dr. Almeroth fails to demonstrate any reasonable likelihood of success for the Mikan-based grounds.	33

1.	Mikan fails to teach or suggest any of the “coded data includes privilege settings” limitations of the independent claims.	34
2.	The secondary references do not cure the deficiencies of Mikan.....	38
XI.	Conclusion	38

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.

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

34. For the purpose of this Declaration, and based on my opinions herein, the time of invention for the '659 patent is April 2011. However, I understand that Dr. Almeroth opines that the time of the invention is October 2013. Any invention date from the early-to-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 April 2011 or a date of invention in October 2013.

35. 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.

36. 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 field of access control systems, vehicle electronics, and/or cryptography. Additional education could substitute for professional experience and vice versa." EX1004, Almeroth Dec., ¶ 85.

37. 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

38. 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.* at 1:66-2:2.

39. 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.

40. 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

41. 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.

42. 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.

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

VII. SUMMARY OF KLEVE (EX1005)

44. United States Publication Number 2014/0129053 by Kleve et al. (EX1005, “Kleve”) is titled “Credential Check and Authorization Solution for Personal Vehicle Rental.” Kleve involves a vehicle rental system. In Kleve, a vehicle owner sets up a listing on a car rental platform that allows “Temporary Users”—i.e.,

vehicle renters—to view the information for a vehicle for rent and request to rent the vehicle. EX1005, ¶ 37. As part of the listing, the Owner creates rental agreement forms that must be agreed to before rental. *Id.*, ¶ 38. The Temporary User also sets up a profile and provides “photos of credit cards, photo of forms of ID, facial recognition, voice print recognition, matrix barcode (ex. two-dimensional code), code word or phrase for speech recognition, temporary mobile web login IDS and password, or other types of unique Temporary User identification.” *Id.*

45. A Temporary User may select a vehicle to rent, pay for it, and sign the rental agreement, after which the system provides the Temporary User a “virtual key.” *Id.*, ¶ 39. The virtual key is the Temporary User identification that the user entered into the rental platform. *Id.*, ¶ 63. When a “Temporary User arrives at the vehicle within the scheduled rental time, he or she may enter the virtual key using several methods” such as “scan[ning] their finger with the use of a fingerprint scanner.” *Id.*, ¶ 70. The virtual key is authorized before access is granted. *Id.*, ¶ 70. For example, the vehicle may include a fingerprint reader, voice recognition, barcode reader, password input, etc. to receive the virtual key *Id.*, ¶¶ 63-65. After receipt, “[t]he Temporary User’s virtual key may be authorized several ways including, but not limited to, at the vehicle, communicated back to the vehicle rental authorization server using a telecommunications network, or by having the vehicle Owner verify access using their nomadic device.” *Id.*, ¶ 70.

46. After the Temporary User is verified and his or her owner identity is determined, a vehicle owner “may have access to control usage of the vehicle being rented.” *Id.*, ¶ 40. If the owner does so, the “restrictions assigned by the vehicle owner at the start of the rental period ... [are] download loaded to the VCS,” the vehicle’s computer system. *Id.*, ¶ 75. The vehicle may then be monitored with respect to the restrictions and can be disabled if restrictions are violated. *Id.*, ¶¶ 41-42.

VIII. SUMMARY OF HATTON (EX1008)

47. 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, 13:64-13:9. 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.*, 7-31. If the vehicle authenticates the fob using the security code, it can initiate the command, such as unlocking. *Id.*

48. 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). EX1008, 9:50-63. The purpose of this check is to authenticate the fob to grant access to the vehicle.

49. 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)

50. United States Publication Number 2008/0150683 by Mikan et al. (EX1007, “Mikan”) is titled “Wireless Device as Programmable Vehicle Key.” Mikan discloses synchronizing a “master database” with a local database in a vehicle. EX1007, ¶ 54. Mikan’s master database includes “records representing a vehicle operation policy” for “more than one vehicle.” *Id.* The vehicle operation policy may “indicate to enable, partially enable, or disable a vehicle operation feature.” *Id.*, ¶ 5. Mikan’s local database, which is “resident within vehicle,” also includes “a vehicle operation” policy for the vehicle. *Id.*, ¶ 51. The master database

communicates with the local database so that the local database may “mirror” data in the master database for the vehicle and ensure that the data is consistent. “For example, local database 203 may regularly poll master database 208 to maintain consistent data. In one embodiment, each of local database 203 and master database 208 may communicate an update to the other after a record change.” *Id.*, ¶ 54.

51. When “a user attempt[s] to access or operate [the] vehicle ... the vehicle retrieves a vehicle operation policy by “querying [the] local database.” *Id.*, ¶¶ 71-72.

X. DETAILED ANALYSIS OF PETITION GROUNDS

52. As I describe in detail below, it is my opinion that Dr. Almeroth and the Petition fail to demonstrate any reasonable likelihood of success that any claim of the '659 patent is invalid. Dr. Almeroth presents six grounds. The first set of grounds, 1-2, rely on the Hatton and Kleve references. The second set of grounds, 3-6, rely on the Mikan reference. In my opinion both sets of grounds fail. As an initial matter, a POSITA would not have found it obvious to combine Hatton and Kleve as Dr. Almeroth proposes. Moreover, for both sets of grounds, the references fail to teach elements of the independent claims, including the “coded data includes privilege settings” limitations that were used to distinguish all art presented in prosecution. It is thus my opinion that Dr. Almeroth fails to demonstrate any reasonable likelihood that any challenged claim is anticipated or would have been obvious.

A. Dr. Almeroth fails to demonstrate any reasonable expectation of success for the Kleve/Hatton-based grounds.

53. In my opinion, Dr. Almeroth fails to demonstrate any reasonable likelihood of invalidity for grounds 1 and 2, the Kleve/Hatton-based grounds. In Ground 1, Dr. Almeroth opines that Kleve in view of Hatton would have rendered obvious each independent claim of the '659 patent, claims 1, 11, and 18. I disagree. As an initial matter, a POSITA would not have found it obvious to combine Kleve and Hatton as Dr. Almeroth proposes. Moreover, even if Kleve and Hatton could be combined, the proposed combination nevertheless fails to teach or suggest functionality of each independent claim. While Dr. Almeroth proposes to add Sekiyama in ground 2, Sekiyama does not cure the deficiencies of Kleve and Hatton that I address below, and Dr. Almeroth offers no opinion to the contrary.

1. Dr. Almeroth fails to demonstrate that Kleve/Hatton teaches or suggests any of the “coded data includes privilege settings” limitations of the independent claims.

54. In my opinion, Dr. Almeroth fails to demonstrate that the proposed combination of Kleve and Hatton would have taught or suggested the following elements of the independent claims:

- “the coded data includes privilege settings associated with the eKey for limiting types of use of the vehicle” Claim 1[e];
- “the coded data includes privilege settings set for limiting types of use of the vehicle when using the vehicle” Claim 11[e]; and

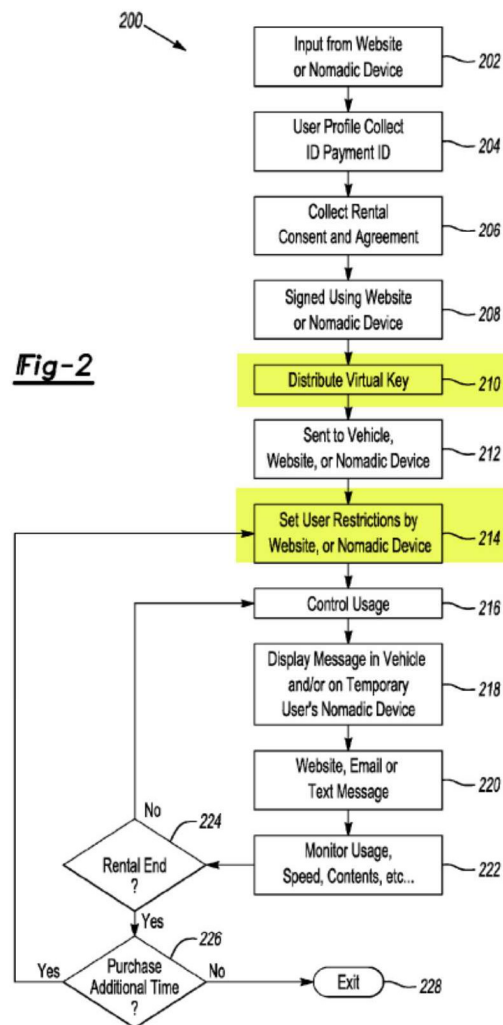
- “the coded data includes privilege settings for use of the vehicle when using the eKey” Claim 18[e].

55. For these claim limitations, Dr. Almeroth turns to Kleve’s “virtual key,” such as a “matrix barcode (ex. two-dimension code),” as the alleged coded data, opining that the “virtual key includes restrictions on the types of use of the vehicle.” EX1004, ¶¶ 138-139, 166, 190. Dr. Almeroth goes on to opine that the “restrictions” include “speed, global position coordinates, or load weight restrictions,” as mentioned in paragraph 40 of Kleve. *Id.* However, Dr. Almeroth is incorrect, as Kleve does not disclose its “virtual key” as including these restrictions. In my opinion, Kleve’s “virtual key” cannot include restrictions because the virtual key is distributed to the Temporary User before rental time and Kleve discloses that any “restrictions” are downloaded directly to the vehicle after the rental start time. *Id.*, ¶¶ 75, 40. That restrictions are downloaded after the rental start time is also illustrated in figure 7 of Kleve. This makes sense because a POSITA would understand that Temporary Users are not authenticated until they attempt to access the rental vehicle at rental time, which then allows the Owner to determine whether restrictions should be set for the authenticated Temporary User. *See id.*, ¶¶ 70-71 (authenticating Temporary User identity for access).

56. Nothing in Kleve discloses that the “virtual key” includes restrictions as Dr. Almeroth opines. Indeed, Dr. Almeroth relies on Kleve at paragraphs 44 and

63 as disclosing the “virtual key” and on a separate disclosure, paragraph 40, as disclosing “restrictions.” EX1004, ¶¶ 138-139. However, paragraph 40 makes no mention of including the “restrictions” in Kleve’s “virtual key.” Thus Dr. Almeroth’s theory fails.

57. Indeed, a POSITA would understand from paragraph 40—and Kleve as a whole—that Kleve teaches to not include the “restrictions” in the “virtual key.” A POSITA would understand that Kleve teaches to “set user restrictions” after the virtual key is distributed and after the step in which the virtual key is “sent to vehicle, website or nomadic device.” EX1005, Figure 2, ¶¶ 39-40. Moreover, while a Temporary User may “initiate[] the rental event” before the rental period, the system waits until “rental time start” to “begin to download ... restrictions assigned by the vehicle owner at the start of the rental period.” *Id.*, ¶ 75. As such, none of the “restrictions” would, or even could, be included in the virtual key. *Id.* Kleve instructs that it is only “[a]t step 214 [that] 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.” *Id.*, ¶ 40. Step 214, Kleve explains, occurs after “step 210 – distribute virtual key,” and therefore the restrictions could not be included in the “virtual key,” as Dr. Almeroth contends.



EX1005, Figure 2 (highlighting step 210 – showing the distribution of a virtual key—and step 214 – showing ability to “set user restrictions” after virtual key’s distribution). While Kleve’s “virtual key” is distributed before the rental period beings, Kleve again makes clear at paragraphs 39-40, that an “Owner” may set user restrictions” for “the vehicle being rented,” meaning that restrictions are not set until rental time. Kleve makes this clear again in paragraph 75, by disclosing that while a Temporary User may “intitiate[] the rental event” before the rental period, the

system waits until “rental time start” to “begin to download ... restrictions assigned by the vehicle owner at the start of the rental period.” *Id.*, ¶ 75. Thus, not only does Kleve not teach or suggest that its “virtual key” includes “restrictions,” it is clear from Kleve that the restrictions are not and cannot be included in the “virtual key.”

58. Dr. Almeroth also opines 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. However, 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.

59. 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.

60. In Kleve, the “restrictions” are not sent to the Temporary User (a renter of a vehicle) or a Temporary User’s device. Instead, information for the reservation, including any restrictions, is sent from a server to the vehicle, at the direction of the vehicle owner. EX1005, ¶¶ 39 (sending virtual key to the VCS [vehicle computing system] “to enable the keyless drive system for the appropriate Temporary User during a given rental period”), 62 (similar); 66 (sending Temporary User’s information for credential verification to the vehicle computer system); ¶ 75 (the system downloads restrictions to the vehicle’s VCS). Thus, Kleve discloses providing any “restrictions” to the car’s VCS from the server—not via the “virtual key.”

61. 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. *See* 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 cannot modify the restrictions.

62. 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 renter restrictions when the server must be in communication with the vehicle and can send the restrictions to the vehicle without sending to the Temporary User's device—a more secure and efficient process.

2. Dr. Almeroth fails to demonstrate that Kleve/Hatton teaches “memory” “having program instructions for instructing/controlling unlocking and starting of the vehicle.”

63. In my opinion, Dr. Almeroth fails to demonstrate that the proposed combination of Kleve and Hatton would have taught or suggested the following elements of the independent claims:

- “memory ... having program instructions for instructing unlocking and starting of the vehicle” Claim 1[a];
- “memory ... having program instructions for controlling unlocking and starting of the vehicle” Claim 11[a]; and
- “memory ... having program instructions for controlling unlocking and starting of the vehicle” Claim 18[a].

64. In my opinion, Dr. Almeroth fails to demonstrate the alleged memory has program instructions for instructing or controlling unlocking and starting of the vehicle. Here, Dr. Almeroth states that there are instructions that “enable a vehicle rental transaction by “activat[ing] the vehicle during a prescribed rental period” and “enabling keyless drive away.” EX1004, ¶ 123 (citing EX1005, ¶ 9). However, a POSITA would understand that merely “activating” a vehicle is not “instructions for unlocking and starting the vehicle” or “instructions for controlling unlocking and starting of the vehicle.” Instead, a POSITA would understand “activating” a vehicle to mean making the vehicle operative, such as setting a flag to indicate that a particular rental agreement is in effect. Indeed, Kleve discloses that a vehicle is

active “during a prescribed rental period.” Kleve, Abstract. A POSITA would thus not understand instructions to “activate” a vehicle to be instructions for starting and unlocking of the vehicle. While Dr. Almeroth opines that Kleve’s “virtual key may be used ‘to unlock and drive,’” he identifies no instructions in the alleged memory that does so, and no instructions at all.

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

65. I disagree that a POSITA would have found it obvious to combine Kleve and Hatton as Dr. Almeroth proposes. Dr. Almeroth proposes to combine Kleve with Hatton’s teachings of generating keys and communicating encrypted data. EX1004, ¶ 109. I disagree.

66. 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.

67. 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 IX.A.1. 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.

68. 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.

69. 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.

70. 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.

71. 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.

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

72. 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.

73. It is my opinion that there is no reasonable expectation of success that any challenged claim would have been obvious under grounds 1 and 2.

B. Dr. Almeroth fails to demonstrate any reasonable likelihood of success for the Mikan-based grounds.

74. In my opinion, Dr. Almeroth fails to show any reasonable likelihood of success for grounds 3-6, the Mikan-based grounds. In Ground 3, Dr. Almeroth opines that Mikan alone anticipates or would have rendered obvious independent claim 1 of the '659 patent. For the remaining independent claims, 11 and 18, Dr. Almeroth proposes to combine Xiao with Mikan in ground 4. I disagree that Mikan or Mikan and Xiao would have rendered obvious any independent claim. Indeed, Mikan fails to teach or suggest functionality of each independent claim, and Dr. Almeroth offers no opinion that these failures are cured by Xiao or any other secondary reference identified in grounds 4-6.

1. Mikan fails to teach or suggest any of the “coded data includes privilege settings” limitations of the independent claims.

75. As with the references distinguished in prosecution and the proposed combination of Kleve and Hatton, it is my opinion that Mikan likewise fails to teach or suggest the following elements of the independent claims:

- “receiv[ing] coded data from the mobile device” and “the coded data includes privilege settings associated with the eKey for limiting types of use of the vehicle” Claim 1[d]/[e];
- “receiv[ing] coded data from the mobile device” and “the coded data includes privilege settings set for limiting types of use of the vehicle when using the vehicle” Claim 11[d]/[e]; and
- “receiv[ing] coded data from the mobile device” and “the coded data includes privilege settings for use of the vehicle when using the eKey” Claim 18[d]/[e].

76. Dr. Almeroth relies on Mikan’s “vehicle operation policy” as the alleged “privilege settings.” EX1004, ¶ 220. However, Mikan does not disclose that any vehicle operation policy is included in the alleged “coded data” or received as coded data from a mobile device, or from a mobile device at all. In my opinion, a POSITA would understand that a major purpose of Mikan was to receive vehicle operation policies not from the alleged mobile device, but from a remote “master database 208.” *See* EX1007, Fig. 2.

77. Mikan describes a vehicle having a “local database 203” that is “resident within vehicle 201,” and a “master database 208” that is remote from the vehicle and has “vehicle operation policies relating to more than one vehicle.” EX1007, ¶¶ 51, 54. Mikan’s master database “communicate[s] with local database” for synchronization of the vehicle operation policy for the vehicle of the local database. *Id.* ¶ 54. “For example, local database 2014 may regularly poll master database 208 to maintain consistent data.” *Id.* Both the local and master databases include a vehicle ID, a key set for the vehicle, and vehicle operation policies. *Id.*, ¶¶ 58-59. If the master database is updated, the local database synchronizes with the master database. *Id.*, ¶ 69. For example, the “[c]ontrol unit 202 [of the vehicle] or local database 2013 may initiate the synchronization to pull updated data from master database 208” or the master database may push data to the vehicle. *Id.* “The synchronization may be a partial or complete refresh of the data.” *Id.* When a user accesses a vehicle, e.g., using a “metal key,” a vehicle operation policy is retrieved by “querying local database 203.” *Id.*, ¶¶ 70, 72. A POSITA would thus understand that Dr. Almeroth’s alleged “privilege settings,” a vehicle operation policy, is not included in any coded data “from the mobile device.” Instead, Mikan’s alleged privilege settings are provided to the vehicle by synchronization with the master database. Mikan therefore does not disclose this limitation as Dr. Almeroth incorrectly opines.

78. Dr. Almeroth opines that it “would have been obvious to a POSITA to transmit the vehicle operation policy as additional coded data, either as part of or in addition to Mikan’s secure identifier.” EX1004, ¶¶ 221-222. While he goes on to describe the benefits of encrypting data, generally, he never provides a reason why a POSITA would have modified Mikan to have the *mobile phone* perform synchronization between the two databases. Dr. Almeroth did not provide any reason to make this modification to account for Mikan’s failures. While not discussed by Dr. Almeroth, I understand that Petitioners state that a benefit of making this drastic change to Mikan would be to “prevent a secondary user from tampering with the use restrictions.” Pet., 45. I disagree. Under Mikan’s unmodified disclosures, the master database communicates to the vehicle without using any secondary user as an intermediary. But adding an intermediary at the secondary user’s device, it would allow the secondary user access to the data, and an unnecessary point of security vulnerability, as it would allow a secondary user an opportunity to modify data on the device.

79. Moreover, in my opinion a POSITA would not have found it obvious to do so. As an initial matter, if a POSITA wanted the benefits of encrypted transmissions, the POSITA would have understood to simply encrypt the transmissions between the local and master databases rather than recreating Mikan’s

system. A POSITA would have recognized that Mikan's mobile phone was not required to send encrypted information.

80. Further, a POSITA would have been highly discouraged from modifying Mikan to have the mobile device send vehicle operation policies to the vehicle. Mikan teaches that the local database may “regularly poll master database to maintain consistent data” or that the master database communicates an update to the local database after a record change. EX1007, ¶ 54. Thus, Mikan places emphasis on keeping timely and accurate data in the local database. By providing database updates via a mobile device, instead of communication between the two databases, there can be no consistent polling or timely updates—instead, data could only be sent in the event the mobile device was in contact with the car.

81. Moreover, a POSITA would have recognized that sending the vehicle operation policies from the server to the vehicle through an intermediary (i.e., mobile phone) would be inefficient. First, adding a phone as an intermediary in the communication between vehicle and server would slow down the exchange of vehicle operation policies because the policies would need to hop over an additional device in the network before reaching their destination. Furthermore, under Dr. Almeroth's modified version of Mikan, entire vehicle operation policies are sent to the vehicle every time an alleged electronic key is used to lock, unlock, or start the vehicle. It is very unlikely for vehicle operation policies to change that frequently,

resulting in unnecessary transmission of policies to the vehicle. Mikan recognizes the importance of minimizing bandwidth usage through selective synchronization of updated/relevant data between local and master database. EX1007, ¶ 69. A POSITA would have realized Mikan's synchronization of local database with master database is more efficient than the modified version of Mikan proposed by Dr. Almeroth, since it only results in vehicle operation policies being sent when they are changed or determined to be relevant.

82. It is my opinion that ground 3 presents no reasonable likelihood of success.

2. The secondary references do not cure the deficiencies of Mikan.

83. While Dr. Almeroth attempts to rely on various secondary references in grounds 4-6, those references do not cure the deficiencies of Mikan that I identified above, and Dr. Almeroth offers no opinion to the contrary. Thus, there is no reasonable likelihood of success for any Mikan-based ground.

XI. CONCLUSION

84. 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.

85. 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 30th day of October, 2024, at Irvine, California.



Dr. Sam Malek