

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

IPR2026-00059
U.S. Patent No. 11,104,245

**DECLARATION OF DR. SAM MALEK IN SUPPORT OF PATENT
OWNER'S 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”).....	12
VI.	BACKGROUND	13
	A. Overview of the ’245 Patent.	13
VII.	CLAIM CONSTRUCTION.....	15
VIII.	OPINIONS	17
	A. Kleve’s matrix barcode does not teach or suggest the “unique access code” of independent claim 1.	17
	B. A POSITA would not have been motivated to combine or modify Kleve in view of Mottla, as proposed, or have a reasonable expectation of success in doing so.....	22
	C. The Zaid Reference.....	29
	D. The Petition does not identify any disclosure from Zaid that meets claim 1’s recited limitations of “coded data from the mobile device for unlocking and use of the vehicle, the coded data from the mobile device including a unique access code received by the mobile device from the server.”	30
	E. Zaid’s “unique increment” disclosures fail to satisfy claim 1[e]-1[f]’s limitations requiring “coded data ... for unlocking and use of the vehicle, the coded data ... including a unique access code received by the mobile device from the server[.]”	32
	F. The Petition does not identify any disclosure from Zaid that teaches or suggests recited limitations of claim 1[g]: “privileges are for the unique access code” and “privileges are set via the server responsive to a restriction set by an administrator of the vehicle, the restriction is associated with a mode of allowed use of the vehicle[.]”	36
	G. I disagree that the combination of Zaid and Mottla renders obvious claim limitation 1[i] because the Petition does not identify any prior	

	art disclosure for the recited limitation “the unique access code functioning for the e-key[.]”	39
H.	I disagree that the combination of Zaid and Mottla renders obvious claim limitation 1[i] because the Petition does not demonstrate why a POSITA would have been motivated to modify Zaid in view of Mottla or that a POSITA would have had a reasonable expectation of success in doing so.....	40
I.	The Petition does not provide any argument for its Ground 1-claim 6 challenge.	42
J.	The Petition does not identify any reference that discloses claim limitation 6[a].	43
K.	Kleve does not disclose a “unique access code generated by the server,” or a “user account having privileges assigned by the administrator,” as recited by claim 3.	46
L.	Zaid does not disclose “each request is associated with a unique access code generated by the server,” as recited by claim 3.....	52
M.	Zaid does not disclose “a user account having respective privileges assigned by the administrator of the vehicle,” as recited by claim 3...	54
N.	The Petition’s Ground 3-claim 15 challenge fails because Zaid does not disclose multiple limitations of the claim.	55
IX.	CONCLUSION	58

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. 11,104,245 (“the ’245 patent”). Specifically, I have been asked to consider the Petition for *Inter Partes* Review numbered IPR2026-00059 (“the Petition”) regarding the ’245 patent, and specifically the Declaration of Dr. Almeroth (EX1004) that accompanies the Petition.

2. In this declaration I provide my independent analysis of the ’245 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 ’245 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 certain references and opinions of Dr. Almeroth with respect to obviousness challenges in the Petition.

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 '245 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 EX2014. That exhibit also includes a list of my publications.

6. I have approximately 26 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 140 peer-reviewed research publications. These publications have been highly cited (more than 12,000 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 clientat 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 '245 patent; the Petition and declaration by Dr. Almeroth ("Almeroth Decl.") (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 '245 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 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 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.

22. 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.

23. 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.

24. 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.

25. 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.

26. 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.

27. 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.

28. 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.

29. 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.

30. 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.

31. 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”)

32. 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 '245 patent is that of cloud-based processing systems.

33. For the purpose of this Declaration, and based on my opinions herein, the time of invention for the '245 patent is April 2011. However, I understand that Dr. Almeroth opines that the time of the invention is October 2013. Any invention data 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, a date of invention in October 2013, or any date in between. My opinions regarding a POSITA apply to a date of invention in October 2013.

34. 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.

35. I understand that Petitioners' expert, Dr. Almeroth, opined that a person of ordinary skill in the art would have "had 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. More education can supplement practical experience and vice versa." EX1004, Almeroth Decl., ¶ 84.

36. 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 '245 Patent.

37. United States Patent Number 11,104,245 (the "'245 patent") is titled "Vehicles and Cloud Systems for Sharing E-Keys to Access and Use Vehicles." EX1001, Face Page. The '245 patent "relates to systems and methods for generating and sharing electronic keys (e-Keys) with users and cloud-based processing systems[.]" EX1001, 1:1-3, 1:59-62.

38. I note that independent claim 1 includes various features and functionality for the recited “unique access code.” EX1001, claim 1. For example, claim 1 recites “communications circuitry of the vehicle is configured to receive coded data from the mobile device for unlocking and use of the vehicle, the coded data from the mobile device including a unique access code received by the mobile device from the server[.]” EX1001, claim 1. Claim 1 also recites “the unique access code functioning for the e-key[.]” EX1001, claim 1. The specification of the ’245 patent describes “[t]he unique generation of access codes enables each electronic key[] to be different for each user and each e-key can be canceled at any time from a device having access to the Internet.” EX1001, 43:49-53. “Each unique e-key, being unique, can be cancelled and eliminated without affecting other issued e-keys.” EX1001, 48:53-59.

39. Independent claim 1 of the ’245 Patent recites:

“A vehicle, comprising,
an on-board computer of the vehicle;
a first system of the vehicle interfaced with the on-board computer of the vehicle for enabling unlocking of the vehicle;
a second system of the vehicle interfaced with the on-board computer of the vehicle for enabling starting of the vehicle for use of the vehicle;
and
communications circuitry of the vehicle interfaced with the on-board computer of the vehicle, the communications circuitry is configured to process program instructions to enable communication with a server and to enable communication with a mobile device;

wherein the communications circuitry of the vehicle is configured to receive coded data from the mobile device for unlocking and use of the vehicle, the coded data from the mobile device including a unique access code received by the mobile device from the server, wherein the unique access code is associated with privileges set via the server responsive to a restriction set by an administrator of the vehicle, the restriction is associated with a mode of allowed use of the vehicle, and privileges are for the unique access code, and a camera of the vehicle is used for capturing video of an area that includes the vehicle during a period of time in which the unique access code is to be active, such that actions taken by a user using an electronic key (e-key) is recorded;

wherein the unique access code functioning for the e-key that is managed via one or more graphical user interface inputs rendered on a screen of the mobile device.”

VII. **CLAIM CONSTRUCTION**

40. I understand that the district court issued a Markman Order on May 14, 2025 for each of U.S. Patent No. 10,407,026 (“the ’026 Patent”), U.S. Patent No. 11,738,659 (“the ’659 Patent”), and U.S. Patent No. 9,365,188 (“the ’188 Patent”) (collectively “related e-key patents”). EX1015. I understand that the district court construed the “electronic key” / “eKey” / “e-key” terms of those related e-key patents as “electronic data that enables one or more functions of the vehicle”:

Term	Disputed Term	The Court’s Construction
1	“electronic key”/ “eKey”/ “e-key” (’026 patent, Claims 1, 2, 6, 13, 15; ’659 Patent, Claims 1, 3, 4, 12, 13, 20; ’188 Patent, Claims 1, 11, 16, 17; ’268 Patent, Claims 10, 18)	“electronic data that enables one or more functions of the vehicle”

EX1015, at 32.

41. I also understand that the district court ordered that the plain and ordinary

meaning of various “privileges” / “conditions of use” terms (EX1015, at 12), as recited in the related e-key patents, specifically excludes “unfettered access.” See EX1015, at 12-13, excerpted below.

From Defendants’ perspective, the dispute centers on whether the “privileges” or “conditions of use” can allow what they call “unfettered access.” They say Plaintiff’s “non-construction of these terms invites the incorrect possibility that mere (unrestricted) access alone might be a privilege within the context of the . . . patents.” Dkt. No. 134 at 5. For support, they cite prosecution-history and IPR statements purportedly distinguishing cited references that allow such access.

The Court agrees with Defendants. The patents use “privileges” and “conditions” similarly, and there appears to be no dispute about what “conditions” are. For example, the specification explains various drivers can each have their own user account, “which provides specific privileges (use capabilities, restrictions, limits, parameters, etc.).” ’026 Patent at 36:46–50. Elsewhere, the patents explain conditions of use “define[] one or more privileges associated to use of the e-key.” *Id.* at 4:65–66; *see also id.* at 6:60–63 (describing “use of the vehicle in accordance with conditions defined in the privilege settings”).

EX1015, at 12. *See also* EX1015, at 13:

Id. (internal citations omitted). Plaintiff then emphasized its prosecution remarks that Zaid did not disclose “a unique access code that includes privilege settings set for additionally limiting types of use of the vehicle.” *Id.* at 17. In other words, Plaintiff equated “unfettered access” with the absence, not presence, of “privileges.” Given that, the Court agrees with Defendants that “privileges for use of the vehicle” cannot simply be “unfettered access” to the vehicle, which is the “plain and ordinary meaning” of these phrases on this record.

42. I am informed that the standard for claim construction of terms within the

claims of the patent is the same as that applied in federal district court litigation. I apply the district court's constructions for these terms, as set forth by the district court in the Markman Order above, in my analysis herein.

VIII. OPINIONS

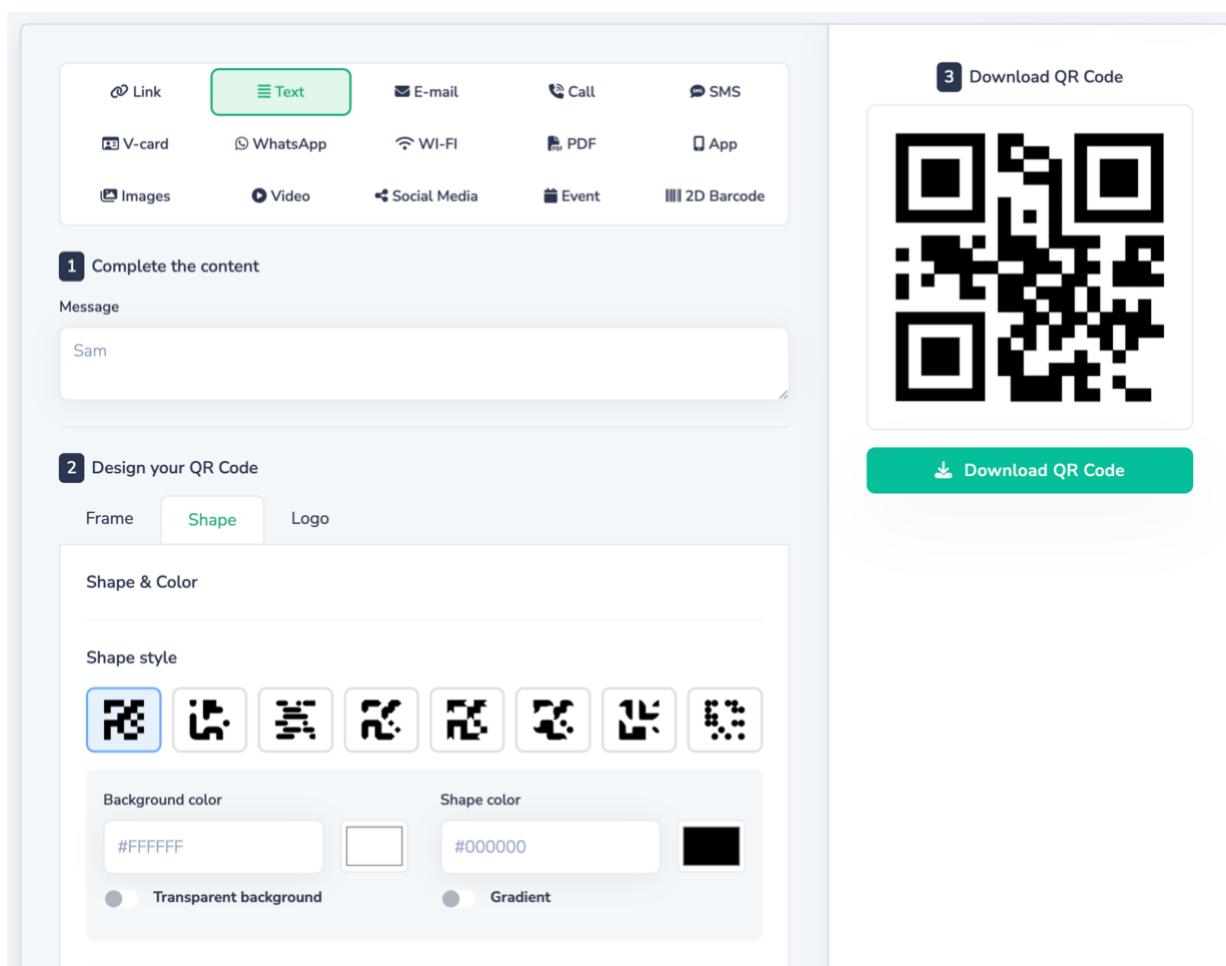
A. Kleve's matrix barcode does not teach or suggest the "unique access code" of independent claim 1.

43. I understand that Dr. Almeroth opines that the "matrix barcode" disclosed in Kleve (EX1005) "encodes a unique access code within the two-dimensional matrix. See Fig.5. It is well known that these 'two-dimensional matrix' codes, or QR codes, essentially encode a unique value that appears to a human as a jumbled two-dimensional matrix barcode." EX1004, Almeroth Decl., ¶ 122. Dr. Almeroth further contends that "the matrix barcode contains or encodes unique information (i.e., a unique access code)[.]" EX1004, Almeroth Decl., ¶ 122. Dr. Almeroth further opines that Kleve discloses this limitation of claim 1 (limitation 1[f]). EX1004, Almeroth Decl., ¶ 122. I disagree with these opinions.

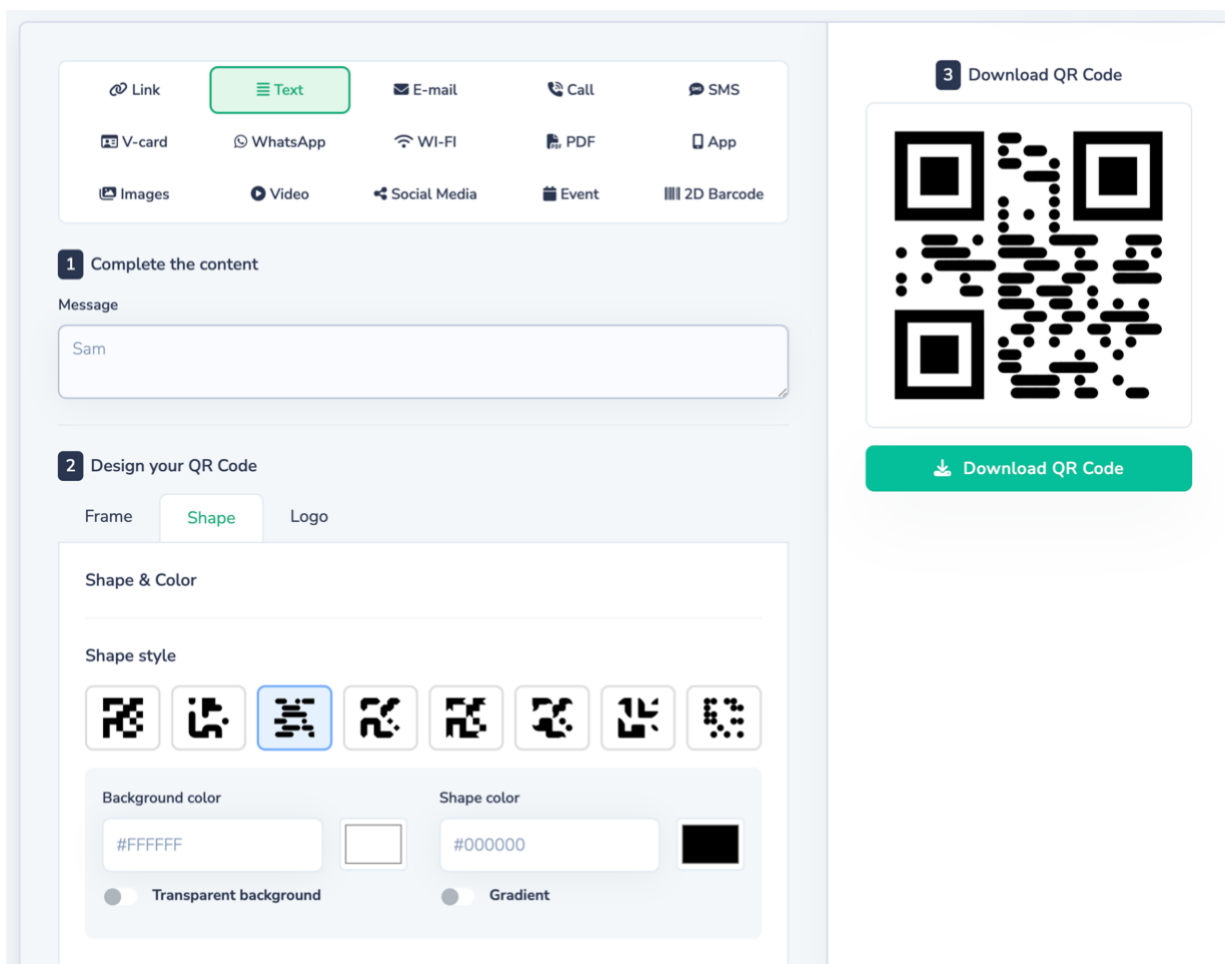
44. A QR (Quick Response) code, also referred to as a matrix barcode, is a two-dimensional barcode that stores information in a grid of typically black and white squares and can be read by imaging devices such as smartphone cameras. EX2012, "How are QR codes generated?", QRcodeKit, *available at* <https://qrcodekit.com/guides/how-are-qr-codes-generated/>. Importantly, a QR code is not inherently nor essentially unique; rather, "a QR code becomes unique only when

the data encoded within it is unique.” EX2012. A QR code may be generated for arbitrary data, regardless of whether that data is unique.

45. Consistent with this understanding, publicly available online services—such as qr.io—allow users to generate QR codes for arbitrary input without any requirement of uniqueness. By way of example, I used the qr.io website to generate a QR code encoding the text “Sam,” which is clearly not a unique name. This demonstrates that QR codes do not, by their nature, encode unique values; any uniqueness derives solely from the semantics of the underlying data and the system in which it is used.



46. Moreover, a QR code is not a unique representation of a given piece of information. For example, using the qr.io service, I altered the visual styling parameters of the QR code (e.g., shape style) and generated a different QR code that nonetheless encodes the same underlying data—namely, my first name. As illustrated here, multiple distinct QR code symbols can encode identical information, further demonstrating that a QR code itself is not inherently unique, even with respect to a specific data value.



47. Dr. Almeroth states “Kleve describes the matrix barcode as a type of

‘unique Temporary User identification’ because, like a fingerprint or photo ID, the matrix barcode contains or encodes unique information (i.e., a unique access code) that is used by the vehicle to ensure that the intended TU is being given access to the vehicle. Kleve, [0069].” EX1004, Almeroth Decl., ¶ 122. However, Kleve at paragraph 69 does not “describe[] the matrix barcode as a type of ‘unique Temporary User identification.’” EX1005, ¶ 69.

48. As shown in paragraph 69 of Kleve, illustrated below, the reference describes a first embodiment in which “the vehicle Owner may generate a virtual key.” EX1005, ¶ 69. I have highlighted this disclosure in **yellow** below. Specifically, the reference discloses: “At step 604, the vehicle Owner may then generate a virtual key based on a password generated by the vehicle Owner that may include a matrix barcode or a code word that the Temporary User may enter/send to the vehicle when ready to begin the rental term.” EX1005, ¶ 69.

49. The reference goes on to disclose a second embodiment, i.e., “[a]nother exemplary embodiment of generating a virtual key[.]” EX1005, ¶ 69. I have highlighted the description of this second embodiment in **light blue**. There, the reference discloses: “Another exemplary embodiment of generating a virtual key may be done by using Temporary User’s credentials including fingerprint recognition, photos of credit cards, photo of forms of ID, facial recognition, voice print recognition, phrase for speech recognition, temporary mobile web login IDs and password, or other type of unique Temporary User identification at step 614.” EX1005, ¶ 69. I note that in

this second embodiment, which describes “unique Temporary User identification,” there is no mention of a “matrix barcode.” EX1005, ¶ 69.

[0069] FIG. 6 is an exemplary embodiment of the vehicle rental micro-business distributing and controlling virtual keys using a nomadic device with a vehicle. The vehicle rental micro-business administrative system may consist of a computer system configured to host one or more websites for interaction with a vehicle Owner and Temporary User. In the illustration 600, a server 634 is used to communicate between a vehicle Owner nomadic device 601, a Temporary User nomadic device 611, and a vehicle computing system 621. Using a nomadic device, for example a smart phone, a Temporary User and vehicle Owner may set up user profiles, enter into an agreement and make a payment to initiate the vehicle rental process between the two parties at step 602 and 612. At step 604, the vehicle Owner may then generate a virtual key based on a password generated by the vehicle Owner that may include a matrix barcode or a code word that the Temporary User may enter/send to the vehicle when ready to begin the rental term. Another exemplary embodiment of generating a virtual key may be done by using Temporary User’s credentials including fingerprint recognition, photos of credit cards, photo of forms of ID, facial recognition, voice print recognition, phrase for speech recognition, temporary mobile web login IDs and password, or other type of unique Temporary User identification at step 614. At step 616, the virtual key is generated and sent to the Temporary User. The Owner may deliver a virtual key to the vehicle for recognizing the Temporary User having authorization to enable a keyless drive-away at step 606.

50. As illustrated above, Kleve, at paragraph 69, does not “describe[] the matrix barcode as a type of ‘unique Temporary User identification’ ... like a fingerprint or photo ID[,]” as Dr. Almeroth opines. EX1005, ¶ 69. The embodiment describing “fingerprint recognition, photo of forms of ID, ... or other type of unique Temporary User identification” excludes any mention of a matrix barcode. EX1005, ¶ 69.

51. It is my opinion Kleve’s matrix barcode does not teach or suggest a “unique access code.” It is further my opinion that Dr. Almeroth is incorrect in stating

that “it is well known that these ‘two-dimensional matrix’ codes, or QR codes, essentially encode a unique value.” It is also my opinion that Dr. Almeroth is incorrect in concluding that Kleve’s matrix barcode encodes a “unique access code,” and that Dr. Almeroth is incorrect in stating that Kleve, at paragraph 69 describes “the matrix barcode as a type of ‘unique Temporary User identification’ ... like a fingerprint or photo ID.”

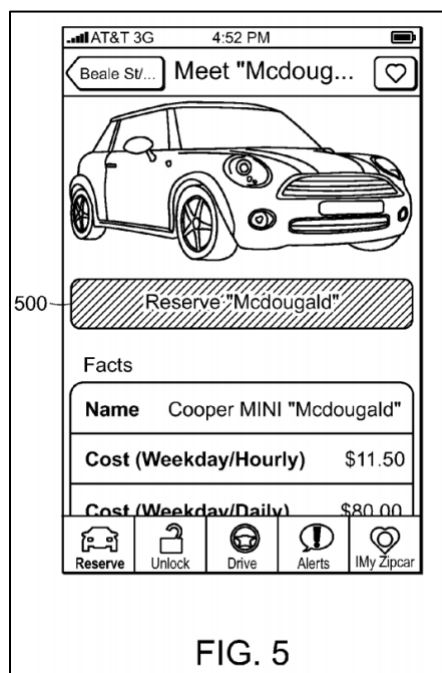
B. A POSITA would not have been motivated to combine or modify Kleve in view of Mottla, as proposed, or have a reasonable expectation of success in doing so.

52. I understand that Dr. Almeroth proposes modifications to Kleve (EX1005) in view of Mottla (EX1006), and Dr. Almeroth further contends that this combination renders obvious the limitations recited by claim 1[i] (EX1004, ¶¶ 129-133), which recites “wherein the unique access code functioning for the e-key that is managed via one or more graphical user interface inputs rendered on a screen of the mobile device.” EX1001, claim 1. However, as I discuss the section above, Dr. Almeroth’s opinion that Kleve discloses a “unique access code” is incorrect. Dr. Almeroth does not opine that Mottla’s disclosures disclose a “unique access code.” (EX1004, ¶¶ 129-133). In my opinion the combination of references therefore fails to render obvious the limitations of claim 1[i], which require “the unique access code functioning for the e-key ...” EX1001, claim 1.

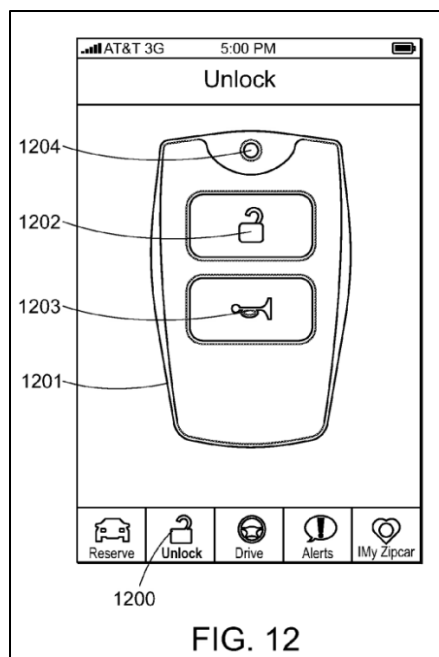
53. I also disagree with Dr. Almeroth’s proposed combination of elements from Kleve and Mottla. Specifically, Dr. Almeroth proposes to combine Kleve’s “user

interface” (EX1005, Figure 9) with Mottla’s Figure 5 (EX1006, Figure 5), which “illustrates a portion of the user interface for displaying information regarding a selected vehicle” (EX1006, ¶ 15) and Mottla’s Figure 12 (EX1006, Figure 12), which “illustrates a portion of the user interface for displaying an icon for unlocking a vehicle or for making a vehicle sound its horn” (EX1006, ¶ 22).

54. I note that Mottla permits its “member” user to browse reservable vehicles using a user interface, allows its “member” user to reserve a vehicle via a user interface, and allows the member to select buttons on a user interface which acts like a “key-fob” and allows the member to unlock and lock the vehicle. EX1006, Figures 5, 12, ¶ 33. Figures 5 and 12 are shown below:

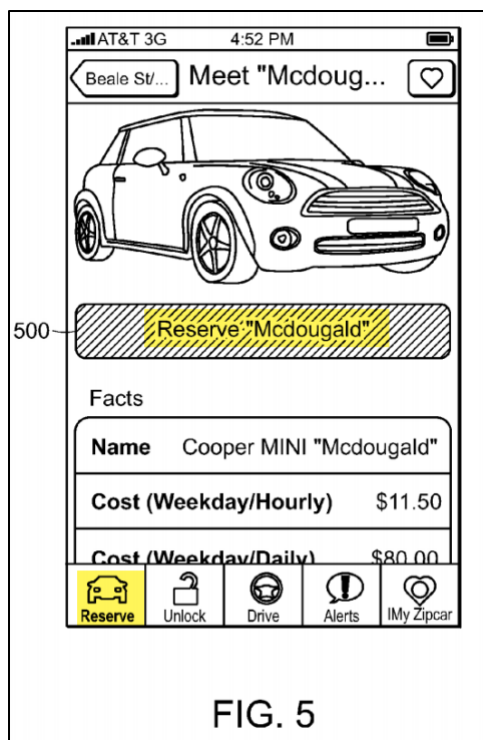


EX1006, Figure 5.



EX1006, Figure 12.

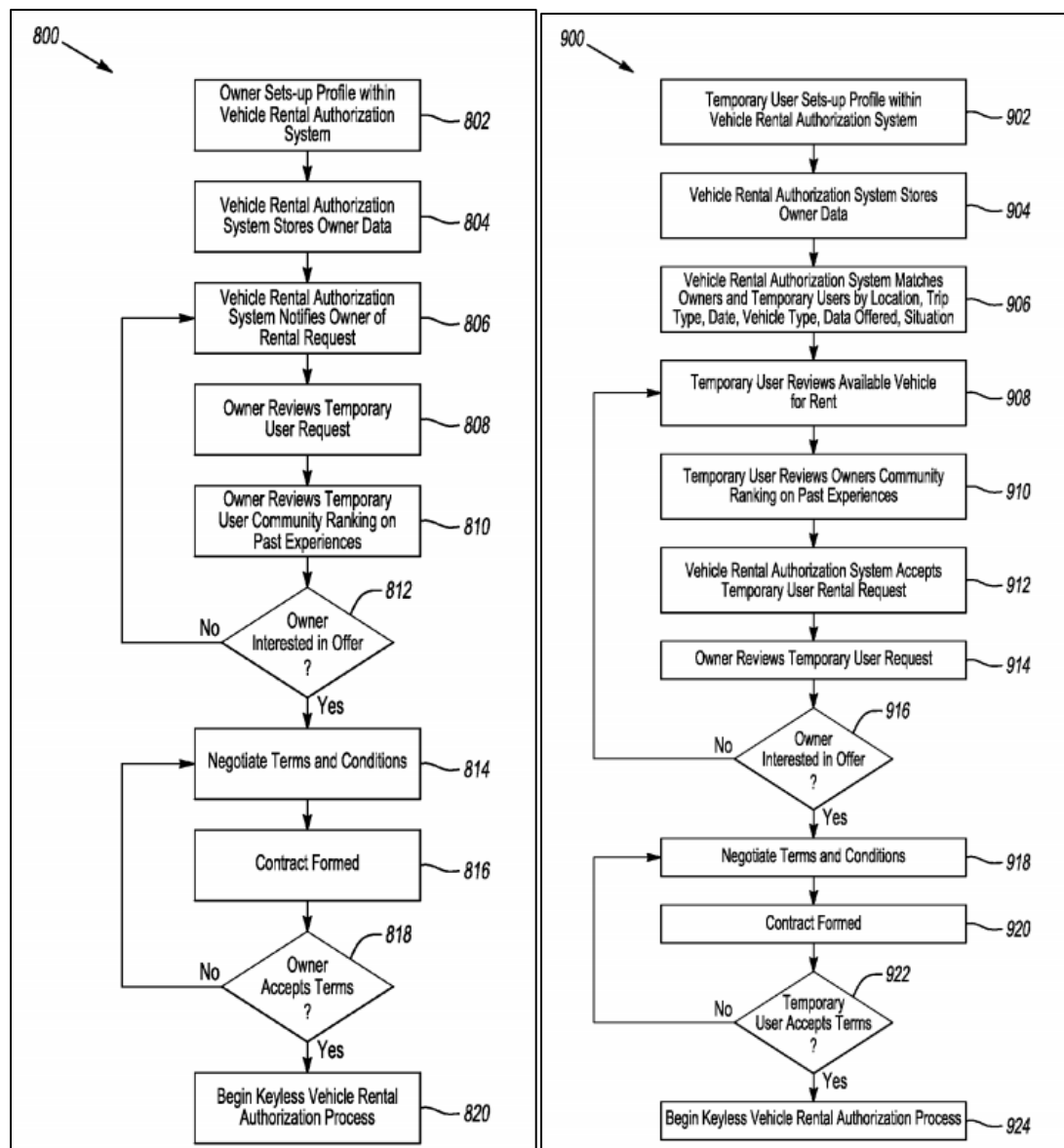
55. Kleve, however, discourages the modifications proposed by Dr. Almeroth. I note that Kleve's system requires the Temporary User to submit a "request" to rent a vehicle, and both the system and the vehicle owner must approve the Temporary User's request to rent the vehicle. EX1005, Figures 8, 9, ¶¶ 83-84, 89. Kleve does not permit its Temporary User the type of direct action taught by Mottla, i.e., to "reserve" a vehicle. EX1006, Figure 5, ¶ 27. Specifically, Mottla teaches the use of graphical user interface inputs which allow a member to "select one or more of the reservable assets" and then to directly reserve that vehicle by selecting the "reserve" button 500 (EX1006, Figure 5, ¶ 27), depicted below:



EX1006, Figure 5.

56. Kleve does not allow its “Temporary User” to take this direct reservation action that Mottla’s graphical user interface permits. Instead, Kleve teaches that the Temporary User must “request” to rent the owner’s vehicle, and if Kleve’s system “accepts the request,” then the system will “notify the owner of a rental request.” EX1005, Figures 8, 9, ¶¶ 83-84, 89. At this point, Kleve teaches that the owner is given the opportunity to review the Temporary User’s request, i.e., the nature of the request (“review the requested rental based on what the Temporary User is looking to use the vehicle for,” “when the requested use will be taking place, and where”), as well as review the “Temporary User Community Ranking.” EX1005, Figures 8, 9, ¶¶ 83-84, 89. Kleve teaches that, after this opportunity for the owner to review the request and ranking, it is at step 812 (in Figure 9 shown as “yes”/“no” to step 916) that the owner

must take action to either “decline and wait for the vehicle rental authorization system to notify of any other offers” or “accept the offer.” EX1005, ¶¶ 83-84, 89, Figures 8, 9.



57. Kleve teaches that the Temporary User may submit a “request,” but it is the owner that will either accept or decline that request. EX1005, ¶¶ 83-84, 89, Figures 8, 9. Kleve does not permit the type of direct “reserve” action taught by Mottla.

58. In my opinion, Kleve discourages the type of direct “reserve” action taught by Mottla’s user interface shown in Figure 5. Specifically, Kleve discourages the “reserve” action enabled by the graphical user interface inputs of Mottla’s Figure 5. EX1006, ¶ 27, Figure 5. For at least these reasons, a POSITA would not have been motivated to combine these elements from Kleve and Mottla.

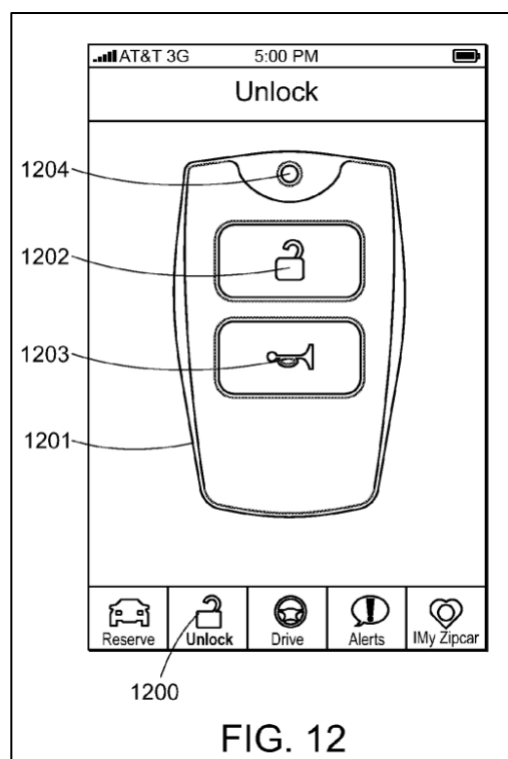
59. I also disagree with Dr. Almeroth’s opinion that a POSITA would have been motivated to modify Kleve’s matrix barcode in view of Mottla’s graphical user interface inputs, shown in Mottla’s Figure 12.

60. I note that Kleve teaches that a “matrix barcode” which itself is passively “used as the virtual key.” EX1005, ¶ 44. Kleve teaches “[o]nce the Temporary User has the matrix barcode scanned by the vehicle, the smart phone may be able to connect with the VCS and be used to enter and enable the vehicle drive away event.”):

[0044] Another exemplary example of the vehicle rental micro-business system may include other enhancements including, but not limited to, matrix barcode (ex. two-dimensional code) used as the virtual key being recognized by the VCS. The smart phone may be used to communicate the matrix barcode information to the vehicle rental micro-business system directly. The system may be able to communicate information from the smart phone to the vehicle notifying the VCS of a virtual key. Once the Temporary User has the matrix barcode scanned by the vehicle, the smart phone may be able to connect with the VCS and be used to enter and enable the vehicle drive away event.

EX1005, ¶ 44.

61. Mottla teaches that a member selects certain buttons on a graphical user interface in order to display a key-fob user interface and then the member selects buttons for unlocking or locking the vehicle on that user interface in order to unlock or lock the vehicle. Mottla teaches, for example, “a member selects a lock icon 1200 that causes the mobile device application to display a user interface with another icon 1201 that has a button 1203 for causing a vehicle 104 to sound its horn, or button or buttons 1202 to lock or unlock the vehicle doors.” EX1006, ¶ 33, Fig. 12:



EX1006, Figure 12.

62. Dr. Almeroth does not explain how the matrix barcode of Kleve would be combined with Mottla or how the two in combination would be expected to function. I note that Kleve’s matrix barcode is a passive mode of communication, without any

buttons to select. As I discuss above, Kleve teaches that the barcode is scanned at the vehicle and that this scanned barcode is used to enter and enable the vehicle drive away event. Mottla, by contrast, teaches that a member must actively select buttons to unlock a door, sound a horn, etc. Dr. Almeroth does not explain how to combine Kleve's matrix barcode with Mottla's graphical user interface inputs, such that the barcode is being managed by some graphical user interface inputs. EX1004, ¶¶ 129-133.

63. It is my opinion that a POSITA would not have been motivated to modify or combine Kleve's matrix barcode in view of Mottla's teachings, as proposed by Dr. Almeroth, and it is further my opinion that a POSITA would not have had a reasonable expectation of success in doing so.

C. The Zaid Reference.

64. United States Publication Number 2011/0112969 by Zaid et al. (EX1008, "Zaid") is titled "Vehicle Access Control Services and Platform."

65. Unlike independent claim 1 of the '245 patent, Zaid does not involve any vehicle that is configured to receive "a unique access code received by the mobile device from the server" or any vehicle that is configured to receive a "unique access code functioning for the e-key." EX1001, claim 1. Zaid does not involve any "privileges set via a server" where the "privileges are for the unique access code," nor any "privileges set via the server responsive to a restriction set by an administrator of the vehicle[.]" *Id.*

66. Zaid describes a "vehicle reservation," which can be made after a

Facebook or other social networking site account holder logs into their account and views an advertisement of this vehicle available for rent. EX1008, ¶ 72. Once the renter makes the reservation, that reservation is relayed as an encrypted message. *Id.*, ¶ 70. Zaid does not suggest that this relayed reservation message is a “unique access code,” or a “unique access code received by the mobile device from the server.” EX1008. Instead, the encryption disclosed by Zaid merely converts the message from one form to another. *Id.*, ¶¶ 125-127.

D. The Petition does not identify any disclosure from Zaid that meets claim 1’s recited limitations of “coded data from the mobile device for unlocking and use of the vehicle, the coded data from the mobile device including a unique access code received by the mobile device from the server.”

67. Petitioners identify Zaid’s “vehicle reservation” as the claim’s recited “coded data” (Pet. 49) and as the alleged “unique access code” that claim 1 requires to be included in “the coded data from the mobile device” and “received by the mobile device from the server,” Petitioners identify a “decrypted vehicle reservation” (Pet. 52). The Petition does not explain how Zaid’s reservation—once encrypted or decrypted—would satisfy the claim’s requirement of “a unique access code.” Pet. 51-52. I have reviewed the Petition’s cited disclosures of Zaid, but Zaid does not teach that its vehicle reservation, encrypted or decrypted, is a “unique access code,” as Petitioners allege. Pet. 51-52; EX1008, Fig. 5, ¶¶ 125-26, 128-130; EX1002, 387.

68. The Petition does not explain how Zaid’s disclosure of encryption “layers,” would meet the limitations of claim 1[e]-[f], which require “coded data ... for

unlocking and use of the vehicle, the coded data from the mobile device including a unique access code received by the mobile device from the server.” EX1001, claim 1. Regardless, it is my opinion that the Petition’s cited disclosures of Zaid do not satisfy claim limitations 1[e]-1[f], as explained further below.

69. At paragraphs 125 and 126, Zaid teaches that the “first layer of encryption can be decrypted using a private key of the wireless communication device” and “the wireless communication device decrypt[s] the first layer of encryption using the public key of the wireless communication device using a locally stored private key of the wireless communication device.” *Id.*, ¶¶ 125-26. Zaid does not teach that this “private key” is a unique access code, but even if the disclosed “private key” were unique, it is my opinion that this “locally stored private key of the wireless communication device” does not meet the recited limitation requiring: “a unique access code received by the mobile device from the server[.]” EX1001, claim 1.

70. Zaid discloses that “the vehicle reservation is further encrypted in a second layer of encryption using a public key of a vehicle access kit that provides access control to the vehicle.” EX1008, ¶ 125. “The second layer of encryption can be decrypted using a private key of the vehicle access kit.” *Id.* ¶¶ 126, 128. Zaid teaches that this “vehicle access kit” is not “the mobile device” recited by claim 1, and I note that Petitioners do not allege that it is (Pet. 51-52); rather, Zaid describes this “vehicle access kit” as a distinct component that is “installed into an existing vehicle” either “during production” or “aftermarket.” EX1008, ¶¶ 85, 86. Again, Zaid does not teach

that its “private key” is “unique,” but whether it is “unique” or not, Zaid shows that the private key for decrypting a second layer of encryption comes from “the vehicle access kit,” and is not “received by the mobile device from the server,” as claim limitation 1[f] requires. EX1001, claim 1. A private key is secret, unlike a public key, which is not secret and is publicly known. However, the fact that a key is secret does not make it unique.

71. It is my opinion that none of the Petition’s relied-upon teachings of Zaid discloses “a unique access code received by the mobile device from the server.” Pet. 51-52. It is further my opinion that Zaid’s “decrypted vehicle reservation” does not meet the recited elements of claim 1[e]-1[f].

E. Zaid’s “unique increment” disclosures fail to satisfy claim 1[e]-1[f]’s limitations requiring “coded data ... for unlocking and use of the vehicle, the coded data ... including a unique access code received by the mobile device from the server[.]”

72. Petitioners rely on Zaid’s disclosure of a unique increment as an alleged “unique access code.” Pet. 52, citing EX1008, ¶ 130. Zaid does not teach that this “unique increment” is included in Zaid’s “vehicle reservation”—the disclosure Petitioners identify as the claim’s recited “coded data” (Pet. 49)—but instead teaches that “each message for exchanging information such as vehicle reservation and updates include a unique increment for each message to avoid repeat message attack.” EX1008, ¶ 130.

73. Zaid discloses “the unique increment is in the form of a counter and/or

time stamp that indicate[s] the uniqueness of the message to avoid a repeat message attack.” *Id.* This “unique increment” renders the message unique, but does not imply that the payload of the message is unique as well.

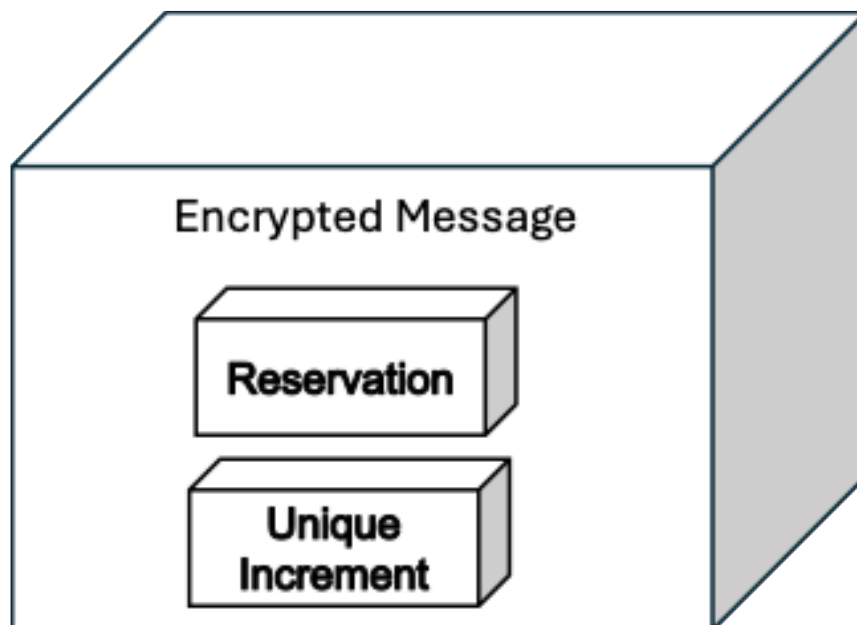
74. A replay, or repeat-message, attack occurs when an attacker who lacks the ability to create valid encrypted messages captures a valid encrypted message and sends it again later in an attempt to reuse its original effect. This is especially important in authentication systems, where an attacker might capture a valid login or authentication message and replay it later to impersonate the user.

75. One common defense is to include a unique value in each encrypted message, such as a nonce, timestamp, counter, or sequence number. The receiver keeps track of the values it has already accepted. If it receives another encrypted message with a value that has already been seen, it can detect that the message is being replayed and reject it.

76. This works because the attacker may be able to copy the original message, but the attacker cannot make the repeated message appear fresh if the unique value has already been used. In this way, uniqueness helps ensure that each valid message can only be accepted once.

77. Zaid discloses including a “unique increment” in a message to prevent replay attacks, also known as repeat attacks. This could prevent duplicate bookings where an attacker obtains a copy of a legitimate booking request and attempts to resend it. Importantly, Zaid discloses including the unique increment in the message, not in the

reservation, which is the payload of the message. The following figure illustrates Zaid's disclosure:



78. Here, the overall encrypted message is unique because it includes a unique increment payload. However, that does not make the message's other payloads, such as the reservation, unique.

79. Whether Zaid's message includes an update, a vehicle reservation, or another form of communication, it is the message itself that has the unique increment, and the message itself that is unique. EX1008, ¶¶ 81, 130. But Petitioners do not point to Zaid's *message* as "coded data" or otherwise allege that the message itself is "for unlocking and use of the vehicle." Pet. 49. Instead, Petitioners identify Zaid's "vehicle reservation" as the recited "coded data" of claim 1 (Pet. 52), but Zaid's reservation does not include a "unique increment," as I explained in the preceding paragraphs 72 to 78. By contrast, the "unique access code" recited by claim limitation 1 is included in

“the coded data,” the “coded data ... for unlocking and use of the vehicle[.]” EX1001, claim 1. Specifically, claim 1 recites “coded data ... for unlocking and use of the vehicle, the coded data ... including a unique access code received by the mobile device from the server.” EX1001, claim 1.

80. A POSITA would understand that Zaid’s disclosures do not teach that Zaid’s “message” including a unique increment is “coded data ... for unlocking and use of the vehicle, the coded data ... including a unique access code,” but is instead teaching that each message includes a unique increment *for message security*, in order “to avoid a repeat message attack,” as I explained in paragraphs 72 to 79 above. EX1008, ¶¶ 81, 130. A POSITA would understand that the “unique increment” of Zaid does not disclose claim 1’s recited “a unique access code.” It is my opinion that Zaid’s message including a “unique increment” does not meet the recited limitations of claim 1: “coded data ... for unlocking and use of the vehicle, the coded data ... including a unique access code[.]”

81. I note that the Petition cites to the prosecution history, at EX1002, 387, in which the Examiner cited to Zaid, paragraph 81. Pet. 52. At paragraph 81, Zaid describes a “unique increment,” which as I explained above, does not disclose the recited “a unique access code” of claim 1. EX1008, ¶ 81. Additionally, at paragraph 81, Zaid teaches “the server update includ[ing] a new private key.” Neither Petitioners nor the Examiner identified Zaid’s “server update” as “coded data ... for unlocking and use of the vehicle,” and a POSITA would not understand from Zaid’s disclosures that the

“server update includes a new private key” discloses the recited limitations of “coded data ... for unlocking and use of the vehicle, the coded data ... including a unique access code[.]” EX1001, claim 1; Pet. 52, citing EX1002, 387; EX1008, ¶ 81.

82. It is my opinion that none of the Petition’s relied-upon teachings of Zaid discloses “the coded data ... including a unique access code a unique access code received by the mobile device from the server.” Pet. 51-53. It is further my opinion that neither Zaid’s disclosures regarding a unique increment nor Zaid’s disclosures regarding the server updates includes a new private key discloses or suggests the recited limitations of claim 1[e]-1[f]: “coded data ... for unlocking and use of the vehicle, the coded data ... including a unique access code[.]” EX1001, claim 1.

F. The Petition does not identify any disclosure from Zaid that teaches or suggests recited limitations of claim 1[g]: “privileges are for the unique access code” and “privileges are set via the server responsive to a restriction set by an administrator of the vehicle, the restriction is associated with a mode of allowed use of the vehicle[.]”

83. Claim limitation 1[g] requires “privileges for the unique access code,” and “privileges are set via the server responsive to a restriction set by an administrator of the vehicle, the restriction is associated with a mode of allowed use of the vehicle[.]” EX1001, claim 1. The Petition does not identify any disclosures that disclose or render obvious these recited limitations of claim 1[g]. Pet. 53-55.

84. Petitioners do not allege that Zaid discloses “privileges for” its “unique increment” or “privileges for” its “server update includes a new private key.” Pet. 53-

55. Either way, Zaid does not disclose any “privileges for” either the “unique increment” or the “server update includes a new private key.” EX1008.

85. As “privileges,” the Petition alleges “Zaid’s privileges that limit (1) vehicle access and (2) use for a period of time” (Pet. 53-54, citing EX1008, ¶ 69), however neither disclosure meets the recited limitations of claim 1[g]. I note first that “vehicle access” is not a “privilege” under the district court’s claim construction order, which is applied to the ’245 patent by Petitioners. Pet. 14. As I showed in paragraphs 40-41 above, there the district court agreed “with Defendants that ‘privileges for use of the vehicle’ cannot simply be ‘unfettered access’ to the vehicle, which is the ‘plain and ordinary meaning’ of these phrases on this record.” EX1015, at 13. Therefore, vehicle “access” is not a “privilege” under the district court’s construction. Pet. 14; EX1015, 12-13.

86. As for the “specified time period” disclosed by Zaid (EX1008, ¶ 69), Zaid does not disclose this specified time period is a “privilege[] set via the server responsive to a restriction set by an administrator of the vehicle,” or any “restriction set by an administrator of the vehicle,” as claim 1[g] requires. EX1008, ¶¶ 69, 72, 77; EX2004, 45; EX1001, claim 1. Zaid does not disclose that an administrator is involved in the reservation’s “specified time period,” nor that the “specified time period” is “set via the server responsive to a restriction set by an administrator[.]” EX1008, ¶¶ 69, 72, 77; EX1001, claim 1. For example, Zaid teaches that a renter can make a reservation, which is “booked through one or more social networking websites, such as

FourSquare® and Facebook®[,]" where "[a] user must first log into the social networking website before he/she can view the advertisement and make [a] reservation." EX1008, ¶ 72. Zaid does not disclose an administrator is involved in setting a "restriction" to which any "specified time period" is set via the server "responsive to" that restriction. *Id.*; EX1001, claim 1.

87. The Petition cites to Zaid's owner updating "various vehicle related information such as vehicle availability and vehicle location"—at paragraph 79—but Zaid does not teach that its disclosures at paragraph 79 are "privileges [] set via the server responsive to a restriction" or "a restriction set by an administrator of the vehicle," as recited by claim 1. Pet. 54, citing EX1008, ¶ 79. Zaid explains that the owner making a "vehicle availability" update is an advertisement or announcement when the vehicle will be available for sharing. *See, e.g.*, EX1008, ¶ 77 ("advertise or announce when the vehicle will be available for sharing"). Zaid further explains that "availability information [is] used by the backend vehicle sharing system to register the vehicle as available for sharing." *Id.*, ¶ 79. By Zaid's teachings, the owner's advertisement or announcement that the vehicle is available for sharing or when the vehicle is available for sharing is not a restriction to which "privileges" are "responsive." *Id.*, ¶¶ 77, 79; EX1001, claim 1. Zaid's availability for sharing can be a year (or more), or months within a year, or weeks within a month, or days within a week, etc. EX1008, ¶¶ 77, 79. Zaid does not disclose "a restriction set by an administrator of the vehicle" for the reservation to which the server sets "privileges"

that are “responsive,” nor does Zaid disclose an owner setting a “reservation period” as asserted in the Petition. Pet. 54-55; EX1008, ¶¶ 72, 77, 79; EX1001, claim 1.

88. The Petition does not explain how Zaid’s “specified time period” for the reservation is allegedly “set via the server responsive to” the identified “availability information,” and Zaid does not disclose that it is. Pet. 54-55; EX1001, claim 1[g]. It is my opinion that the Petition does not provide any disclosure for the claim limitation 1[g].

G. I disagree that the combination of Zaid and Mottla renders obvious claim limitation 1[i] because the Petition does not identify any prior art disclosure for the recited limitation “the unique access code functioning for the e-key[.]”

89. The Petition does not identify a prior art disclosure for the recited limitation of claim 1[i]: “the unique access code functioning for the e-key[.]” EX1001, claim 1. The Petition appears to rely on the Examiner’s findings at EX1002, 124-125 (Pet. 56), however the Examiner cited to Zaid at paragraph 81, referring to an alleged “unique private key” as the claim’s recited “unique access code.” EX1002, 124. As I explained above, e.g., in paragraphs 67 to 82, Zaid does not disclose the recited “unique access code,” and Zaid does not even disclose a “unique private key.” EX1008, ¶ 81. As I showed above, neither Zaid’s “unique increment,” nor its disclosure that “the server update includes a new private key” discloses the recited limitations of claim 1[e]-1[f].

90. As an additional deficiency for claim 1[i], neither the Petition nor the

Examiner's findings (EX1002, 124-25) demonstrates that Zaid's "unique increment" or its "private key" is "functioning for the e-key," which is required by claim 1[i]. Pet. 56-59. It is my opinion that the Petition fails to show any disclosure of "the unique access code functioning for the e-key" as claim 1[i] requires, and the Petition does not allege that Mottla discloses this limitation. *Id.* The Petition relies on Mottla for alleged disclosure of "one or more graphical user interface inputs rendered on a screen of the mobile device." Pet. 56.

H. I disagree that the combination of Zaid and Mottla renders obvious claim limitation 1[i] because the Petition does not demonstrate why a POSITA would have been motivated to modify Zaid in view of Mottla or that a POSITA would have had a reasonable expectation of success in doing so.

91. The Petition contends that a POSITA would have been motivated to use Mottla's system "instead of scanning the virtual key—providing a better user experience while maintaining security." Pet. 58. I disagree with this contention. Zaid does not disclose "scanning the virtual key." EX1008.

92. The Petition also cites to the Examiner's findings, contending that a POSITA would have been motivated to look to Mottla "to conveniently control the vehicle." Pet. 56, citing EX1002, 124-25. I disagree with this conclusion. I note that the Petition states that Zaid's mobile device is used to perform "unlocking requests," i.e., "the vehicle receives a request from a mobile device that unlocks the vehicle[.]" Pet. 49. The Petition does not contend that Zaid's operations for unlocking the vehicle

“[in]conveniently control the vehicle,” and the Petition offers no disclosure from Zaid to otherwise support the notion that a POSITA would be motivated to look to Mottla for alleged improvement as to “convenience.” Pet. 56-59.

93. In Section VIII.B., above, I explained why a POSITA would not have been motivated to modify Kleve in view of Mottla, as Petitioners argue. For example, the Petition failed to show any motivation for a POSITA to add Mottla’s graphical user interface inputs, e.g., for unlocking the vehicle, to Kleve’s matrix barcode. As I explained there, Kleve already teaches that the matrix barcode is used for that very purpose, unlocking the vehicle. Here, too, the Petition does not explain why a POSITA would be motivated to add Mottla’s graphical user interface inputs, e.g., for unlocking the vehicle, to Zaid’s mobile device, since Petitioners argue that Zaid’s mobile device already performs these unlocking requests. *See* Pet. 49 (Petitioners contend: “Zaid discloses ‘the vehicle receives a request from a mobile device that unlocks the vehicle’”). It is my opinion that a POSITA would not be motivated to modify Zaid in view of Mottla, as the Petition alleges.

94. The Petition does not show that a POSITA would have had a reasonable expectation of success in modifying Zaid with Mottla as Petitioners proposed. Pet. 56-59. I note that the Petition relies on the Examiner’s conclusions, and as I discussed above, the Examiner identified Zaid’s “unique increment” and “private key” at paragraph 81 as the alleged “unique access code,” however for the proposed modification of Zaid and Mottla, neither the Examiner nor Petitioners explain how to

combine the cited “unique increment” or “private key” of Zaid (Pet. 56, citing EX1002, 124-25) with Mottla’s graphical user interface inputs, or offer an explanation as to how the proposed combination would function. The Petition provides no basis for concluding that a POSITA would have had a reasonable expectation of success in making the proposed modification.

95. It is my opinion that a POSITA would not have been motivated to modify or combine Zaid in view of Mottla’s teachings, as proposed by Petitioners, and it is further my opinion that a POSITA would not have had a reasonable expectation of success in doing so.

I. The Petition does not provide any argument for its Ground 1-claim 6 challenge.

96. I note that the Petition offers an argument with respect to limitation 6[a] (Pet. 32), but fails to address the remaining limitation (6[b]) reciting: “wherein the e-key has functions enabled via graphical user interfaces of the application of the mobile device.” EX1001, claim 6.

7. Claim 6

6: “The vehicle of claim 1, wherein an application accessed by said mobile device is configured to enable sending instructions to said server to enable sharing said vehicle with the user to enable use of the e-key or another e-key on said vehicle,”

Kleve’s application is accessed by TU’s mobile device. *Kleve*, [0036]. The TU uses the application to “input profile information” “including details about the vehicle he intends to rent.” *Id.* [0086]. This is stored in “the vehicle rental authorization system” so that the owner can be notified about “the requested vehicle rental.” *Id.* [0088]. The application enables sharing the key with the user to enable use of the e-key, because once agreement terms are accepted between VO and TU, “the vehicle rental authorization system may begin the keyless vehicle rental authorization process without [TU] physically meeting the owner.” *Id.*, [0090].

Accordingly, *Kleve* discloses this limitation. Almeroth, ¶¶149-50.

8. Claim 7

97. It is my opinion that the Petition fails to specify where any element of limitation 6[b] is found in any prior art patent or printed publication.

J. The Petition does not identify any reference that discloses claim limitation 6[a].

98. The Petition does not identify any prior art disclosure of an application that is allegedly “configured to enable sending instructions to said server to enable sharing said vehicle with the user to enable use of the e-key[,]” as recited by limitation 6[a]. EX1001, claim 6.

99. For its Ground 1-claim 6 challenge, the Petition identifies *Kleve*’s “application” that is “accessed by TU’s mobile device” (Pet. 32, citing EX1005, at ¶ 36), and alleges that this “application enables sharing the key with the user to enable

use of the e-key” (Pet. 32, citing EX1005, at ¶ 90). However, I note that even if the Kleve reference supported these arguments, the Petition does not address the remaining elements required by claim limitation 6[a].

100. For example, the Petition does not explain how Kleve’s application discloses the recited application “configured to enable sending instructions to said server,” nor does the Petition explain how Kleve’s application discloses the recited application “configured to enable sending instructions to said server to enable sharing said vehicle with the user to enable use of the e-key[.]” Pet. 32; EX1001, claim 6. The Petition cites to Kleve at paragraphs 36, 88 and 90, but these paragraphs do not provide a disclosure of an application “configured to enable sending instructions to said server to enable sharing said vehicle with the user to enable use of the e-key[.]” EX1005, ¶¶ 36, 88, 90. In my opinion, the Petition has not shown that Kleve discloses an application “configured to enable sending instructions to said server to enable sharing said vehicle with the user to enable use of the e-key or another e-key on said vehicle,” as recited by claim 6[a].

101. Additionally, for its Ground 3-claim 6 challenge, the Petition identifies Zaid’s “application” and alleges that “it would have been obvious to a POSITA to implement Zaid’s vehicle reservation application to enable both geolocation [] and requesting use of the vehicle,” but the Petition does not allege that even with these proposed modifications the application would be “configured to enable sending instructions to said server,” or “configured to enable sending instructions to said server

to enable sharing said vehicle with the user to enable use of the e-key,” as claim 6 requires. Pet. 65.

102. For example, at paragraph 77, Zaid teaches that “the “vehicle reservation application or other software function” “enables a vehicle user (e.g., renter and owner) to communicate with backend server(s)” to “advertise or announce” “the location of the vehicle,” “the location of the user,” or “when the vehicle is available for sharing,” and/or “retrieving a list of nearby vehicles available for sharing.” EX1008, ¶ 77. Petitioners do not allege that the application communicating with the backend server to “advertise or announce” locations or availability, or “retrieving a list” is an “application ... configured to enable sending instructions to said server to enable sharing said vehicle with the user to enable use of the e-key or another e-key on said vehicle” (Pet. 64-65), and these teachings from Zaid do not disclose an “application ... configured to enable sending instructions to said server to enable sharing said vehicle with the user to enable use of the e-key or another e-key on said vehicle,” as claim 6 requires. EX1008, ¶ 77. I note that the Petition quotes the words “sharing” and “enable” from paragraph 77, but does not offer any reason to conclude that Zaid’s disclosures therein meet the elements of limitation 6[a]. Pet. 64-65. In my opinion, they do not.

103. The Petition also cites to Zaid’s disclosure that a “reservation is booked by a user at a central server via a user interface displayed on a computing device” (EX1008, ¶ 80) and that it is “booked at the server 110 via a user interface 116” (*id.*, ¶ 125). Pet. 64-65. But here, too, the Petition does not offer any reason to conclude that

Zaid's application is "configured to enable sending instructions to said server to enable sharing said vehicle with the user to enable use of the e-key or another e-key on said vehicle," as claim 6 requires. Pet. 64-65.

104. It is my opinion that the Petition fails to show that Zaid's application is "configured to enable sending instructions to said server," even with the modifications "to enable both geolocation [] and requesting use of the vehicle," as proposed, and further fails to show that Zaid's application is "configured to enable sending instructions to said server to enable sharing said vehicle with the user to enable use of the e-key or another e-key on said vehicle," as claim 6 requires.

105. I note that the Petition does not contend that Mottla discloses this limitation of claim 6. Pet. 64-66. Therefore, even if the Petition's combination of Zaid and Mottla were proper, the Petition still fails to demonstrate that any reference discloses or renders obvious claim 6.

K. Kleve does not disclose a "unique access code generated by the server," or a "user account having privileges assigned by the administrator," as recited by claim 3.

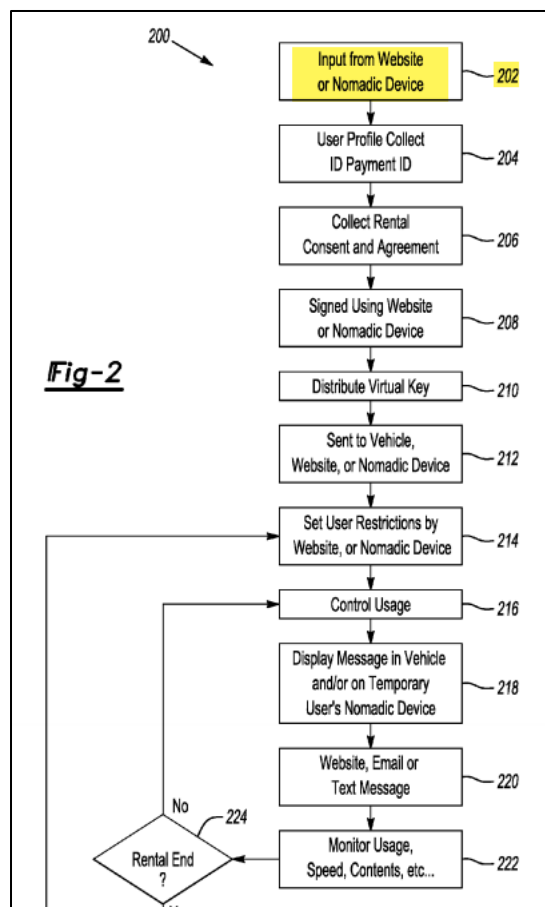
106. The Petition contends that "[e]ach of Kleve's requests is associated with a unique access code embedded in a virtual key that can be expressed as a matrix barcode" (Pet. 27), however, as I explained in paragraphs 43 to 51 above, Kleve does not disclose a "unique access code embedded in a virtual key that can be expressed as a matrix barcode," as the Petitioners allege.

107. The Petition's challenge to claim 3 also fails for another reason: Kleve's

matrix barcode is not “a unique access code generated by the server” as claim 3 requires. EX1001, claim 3. Kleve teaches that its matrix barcode is part of the temporary user’s user profile, and this “user profile” or “user identity” is one that Kleve requires the Temporary User to complete before the temporary user can use the vehicle rental service. EX1005, ¶¶ 37, 47 (“After a Temporary User set[s] up[] their user identity within the website” that “the Temporary User may begin to use the vehicle rental services.”). For example, “[a]t step 202,” Kleve teaches that the “Temporary User may set up a user profile using a website or nomadic device” “to include a ... matrix barcode”:

[0037] At step 202, the Owner and Temporary User may set up a user profile using a website or a nomadic device communicating with the site that is stored in a database. The Owner may set up a user profile by inputting information into the website or nomadic device including, but not limited to the make, model and year of the vehicle available for rent. The Temporary User may also fill out a user profile using the website or nomadic device to include, but not limited to, 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 to validate and pay for the rental service at step 204.

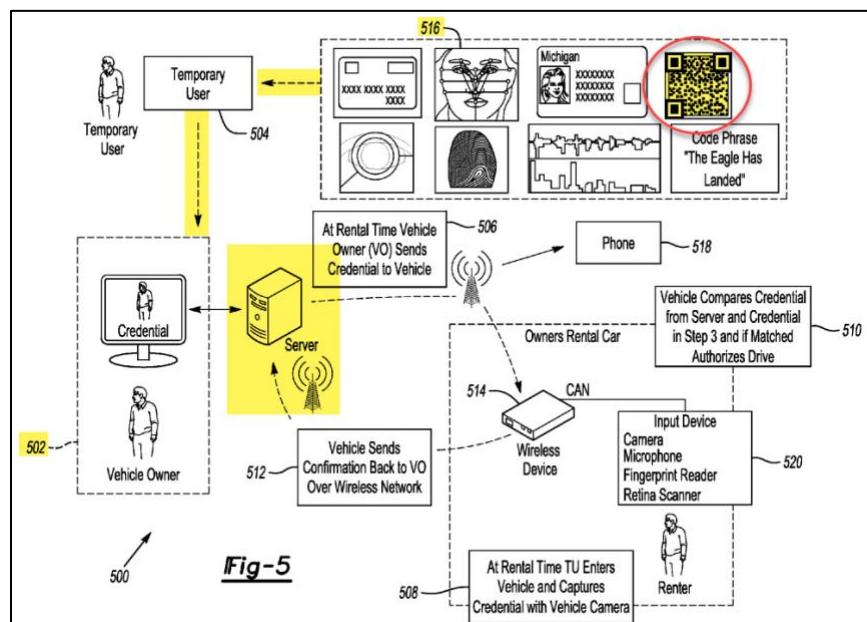
EX1005, ¶ 37; *see id.*, Fig. 2:



108. Kleve, at Figure 2 and paragraph 37, shows a matrix barcode is part of the temporary user’s user profile, that the user profile is set up at step 202, and step 202 occurs before step 210: “distribute virtual key.” *Id.*

109. Kleve also teaches that before a vehicle owner may “set up a virtual key,” the Temporary User has “already setup a user profile within the database.” *Id.*, ¶ 62. Therefore, the “user profile”—taught by Kleve “to include...a matrix barcode”—has already been setup before the owner may “set up a virtual key.” *Id.*; and see *id.*, ¶ 37. Additionally, Figure 5 shows that Kleve’s matrix barcode is not “generated by the server,” as Petitioners allege. EX1005, Fig. 5. Instead, the “Temporary User’s information for vehicle authorization **516**”—which “may include ... matrix barcode”—

exists before the owner may “set up a virtual key.” EX1005, ¶¶ 62-63, Fig. 5:



110. The Petition cites to Kleve at paragraph 69 to support its challenge to claim 3. However, as I explained in paragraphs 47 to 51, at paragraph 69, Kleve distinguishes between two “exemplary embodiment[s]” of “generating a virtual key”: in the first embodiment, Kleve does not teach that a server is involved in generating the virtual key, instead only “the vehicle owner may generate a virtual key” using a “vehicle owner nomadic device” to generate a virtual key “based on a password that may include a matrix barcode.” *Id.*, ¶ 69, Fig. 6. Next, Kleve teaches “another exemplary embodiment of generating a virtual key,” at step 616, which excludes the matrix barcode that Kleve had included in the first embodiment. *Id.* As shown below, neither embodiment discloses a server generating any matrix barcode. *Id.*:

[0069] FIG. 6 is an exemplary embodiment of the vehicle rental micro-business distributing and controlling virtual keys using a nomadic device with a vehicle. The vehicle rental micro-business administrative system may consist of a computer system configured to host one or more websites for interaction with a vehicle Owner and Temporary User. In the illustration 600, a server 634 is used to communicate between a vehicle Owner nomadic device 601, a Temporary User nomadic device 611, and a vehicle computing system 621. Using a nomadic device, for example a smart phone, a Temporary User and vehicle Owner may set up user profiles, enter into an agreement and make a payment to initiate the vehicle rental process between the two parties at step 602 and 612. At step 604, the vehicle Owner may then generate a virtual key based on a password generated by the vehicle Owner that may include a matrix barcode or a code word that the Temporary User may enter/send to the vehicle when ready to begin the rental term. Another exemplary embodiment of generating a virtual key may be done by using Temporary User's credentials including fingerprint recognition, photos of credit cards, photo of forms of ID, facial recognition, voice print recognition, phrase for speech recognition, temporary mobile web login IDs and password, or other type of unique Temporary User identification at step 614. At step 616, the virtual key is generated and sent to the Temporary User. The Owner may deliver a virtual key to the vehicle for recognizing the Temporary User having authorization to enable a keyless drive-away at step 606.

EX1005, Fig. 6:

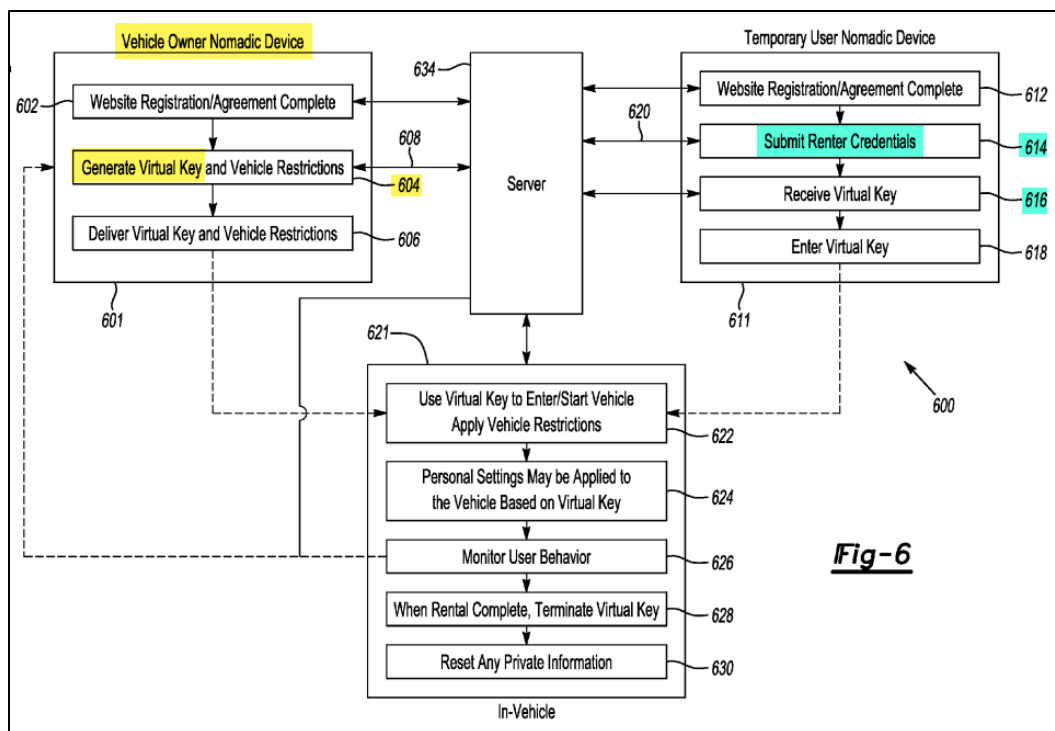


Fig-6

111. The Petition also cites Kleve’s disclosure of an “authorization code,” but the Petition does not provide any argument as to why this authorization code supports its challenge to claim 3. For example, the Petition argues that “[e]ach of Kleve’s requests is associated with a unique access code embedded in a virtual key that can be expressed as a matrix barcode.” Pet. 27. However, as I explained in paragraphs 43 to 51 above, Kleve does not disclose a unique access code embedded in a matrix barcode. Additionally, Kleve’s authorization code is not “embedded in a virtual key,” instead, Kleve teaches that its “authorization code” is a code that is (1) manually “typed in a touchscreen” to “authorize” an authorized user, and (2) is distinct from Kleve’s “matrix barcode.” EX1005, ¶ 59. It is my opinion that the Petition fails to show that Kleve discloses the elements of claim 3.

112. It is my opinion that the Petition’s challenge to claim 3 fails for yet

another reason: the Petition does not show any disclosure of “a user account having respective privileges assigned by the administrator of the vehicle[.]” Pet. 27; EX1001, claim 3. I note that the Petition cites to “a user account, the Temporary User,” and further states “the unique access code is associated with the rental period, which provides the respective privileges assigned by the Vehicle Owner, the vehicle administrator.” Pet. 27. But the Petition fails to allege any connection between the cited “account” and the alleged “privileges.” *Id.* Neither the underlying disclosures of Kleve, cited to by the Petition, nor even the Petition’s characterizations of those disclosures, teaches or suggests “a user account having respective privileges assigned by the administrator[.]” as claim 3 requires.

L. Zaid does not disclose “each request is associated with a unique access code generated by the server,” as recited by claim 3.

113. For its challenge to claim 3 in Ground 3, the Petition relies on its argument from claim limitation 1[e], arguing: “[a]s in 1[e], each vehicle reservation in Zaid is associated with an encrypted unique access code generated by the server ...” Pet. 61. However, as I explained above, at paragraphs 67 to 71, Zaid’s vehicle reservation, either encrypted or decrypted, does not disclose claim limitation 1[e]’s recited “a unique access code.”

114. As an additional deficiency, the reservation identified by the Petition is not a “unique access code generated by *the* server”—*the* same server identified for claim 1. EX1001, claim 3. For claim 1, the Petition identified Zaid’s “central server” (Pet. 48),

but for claim 3[b], Petitioners point to a reservation “booked through one or more social networking websites, such as FourSquare® and Facebook®[,]” where “[a] user must first log into the social networking website before he/she can view the advertisement and make [a] reservation.” EX1008, ¶72; Pet. 61 (citing *id.*). Zaid provides no disclosure that its “central server” (“*the* server” the Petition identified for claim 1) generates a “unique access code” in its disclosures regarding a renter “mak[ing]” a reservation through FourSquare® or Facebook®, and I note that Petitioners do not argue that Zaid’s “central server” does so. Pet. 61; EX1008, ¶72; EX1001, claim 3.

115. The Petition cites to Zaid’s other functions performed by its “central server,” for example, Zaid’s server encrypts a message containing a vehicle reservation (Pet. 61, citing EX1008, ¶ 128) and its server “communicates the vehicle reservation to a wireless communication device” (Pet. 61, citing EX1008, ¶ 126). However, as I explained above, at paragraphs 67 to 71, the encryption disclosed by Zaid merely converts the message from one form to another, and Zaid’s mere communication of the reservation is not disclosing the generation of “a unique access code.” EX1008, ¶¶ 125-127. In any event, it is the Petition that draws a clear distinction between the function of “generating the access code,” encrypting it in a message, and sending it as encrypted e-keys. Pet. 49 (citing EX1001, 46:32-35) (“[c]loud services 120 can generate the unique access code which *is then encrypted* in a message and sent as encrypted e-keys...”) (emphasis in Petition).

116. In my opinion, the Petition fails to show that Zaid discloses a “unique access code generated by the server,” as claim 3 requires.

M. Zaid does not disclose “a user account having respective privileges assigned by the administrator of the vehicle,” as recited by claim 3.

117. For the limitation of claim 3 requiring “a user account having respective privileges assigned by the administrator of the vehicle,” the Petition identifies Zaid’s disclosure of a Facebook® account or similar social networking account. Pet. 61 (citing EX1008, ¶ 72). However, at paragraph 72, Zaid teaches that a prospective vehicle renter can log into Facebook® or a similar social networking site, view an ad for a vehicle placed by a vehicle owner, and if interested, the renter can click on that ad and make a reservation. EX1008, ¶ 72; EX2004, 45. It is my opinion that Zaid’s disclosure of a Facebook® account or similar social networking account is not a “user account having respective privileges assigned by the administrator of the vehicle,” as claim 3 requires.

118. Zaid teaches that a vehicle owner can advertise their vehicle on social networking sites, like Facebook®, but Zaid makes clear that it is the prospective renter, and not an “administrator of the vehicle,” that “must first log into the social networking website before he/she can view the advertisement and make [a] reservation.” EX1008, ¶ 72; EX2004, 45. Zaid does not disclose the renter’s Facebook® or other social networking account as “having privileges assigned by the administrator of the vehicle.”
Id.

119. With respect to Petitioners' argument that the reservation made by the renter is "time-limited," this does not disclose "a user account having privileges assigned by the administrator of the vehicle," as claim 3 recites. Pet. 60-61. Zaid does not teach that the vehicle owner or "administrator" "assigns" such a "privilege" to a renter's Facebook® or other social networking account. EX1008, ¶ 72. Zaid teaches that it is only the renter that "make[s]" the reservation and that the reservation itself may be "for a specified time period." EX1008, ¶¶ 72, 69. Moreover, claim 3 requires "a user account having privileges assigned by the administrator of the vehicle," not the reservation, as Petitioners allege. EX1001, claim 3; Pet. 60-62.

N. The Petition's Ground 3-claim 15 challenge fails because Zaid does not disclose multiple limitations of the claim.

120. It is my opinion that the Petition's Ground 3-claim 15 challenge fails because the Petition does not show that Zaid's "server is part of a cloud processing system," as claim 15 requires. The Petition's relied-upon disclosures do not mention or show that Zaid's server is part of any cloud processing system. Pet. 71-73 (citing EX1008, Fig. 1). Zaid's Figure 1, described at paragraphs 75 and 76, shows "[t]he wireless communication device is connected to a data network 114 via a long-range communication link 112," and the "vehicle reservation is received by the wireless communication device 106 from a central server 110 sitting on a data network 114 via a long-range wireless communication link 112 or a wired link (not shown)." EX1008, ¶¶ 75-76. But Zaid does not teach that this "data network 114" is a cloud processing

system, and Petitioners do not allege that this “data network 114” functions as “a cloud processing system.” *Id.*; Pet. 71-73.

121. It is my opinion that the Petition’s Ground 3-claim 15 challenge also fails because Zaid does not disclose a cloud processing system that “is configured to manage user accounts and manage use of said e-key,” as claim 15 requires. For this limitation, the Petition identifies “a cloud processing system is managing the user social media accounts” such as Facebook® and Foursquare® (Pet. 72), but Zaid does not disclose any such cloud processing system managing these user social media accounts, as Petitioners allege. As I explained above, Zaid teaches that a prospective vehicle renter can log into their own Facebook® or a similar social networking site, view an ad for a vehicle and, if interested, the renter can click on that ad and make a reservation. EX1008, ¶ 72. However, there is an additional deficiency with the Petition’s challenge. Claim 15 requires that the same “cloud processing system is configured to manage user accounts *and manage use of said e-key*,” but the Petition does not identify any cloud processing system that “is configured to” both “manage user accounts and manage use of said e-key,” as claim 15 recites. Pet. 71-73; EX1001, claim 15. I note that the Petition does not contend that the alleged cloud processing system managing Facebook®, Foursquare® and similar social networking accounts is also “configured to” manage *the e-key of claim 1*. *Id.*; EX1001, claim 15 (“...manage use of *said e-key*”). The Petition’s challenge to claim 15 fails for this reason as well.

122. It is my opinion that the Petition’s Ground 3-claim 15 challenge also fails

because Petitioners do not contend, and Zaid does not show, that Zaid's server is "part of" the same "the cloud processing system" that "is configured to manage user accounts and manage use of said e-key," as recited by claim 15. EX1001, claim 15. For its challenge to claim 15, the Petition cites to functions of Zaid's server (Pet. 71-72, citing server functions at ¶¶125-26, 129-30), and further cites to Zaid's disclosure of a renter making a reservation by logging into their own Facebook® or a similar social networking site (Pet. 72, citing EX1008, ¶72), but the Petition does not establish that Zaid's server is "part of" the identified "*the* cloud processing system [] managing the user social media accounts." Pet. 72.

123. Therefore, whether or not "Zaid's server is part of a cloud processing system," as alleged (Pet. 73), and whether or not Zaid discloses a "cloud processing system is managing user accounts," Zaid's server is still not part of the same "*the* cloud processing system [that] is managing the user social media accounts" for Facebook®, Foursquare®, and similar social networking accounts. Pet. 72 (citing EX1008, ¶72). Zaid does not disclose that its "server is part of a cloud processing system and the cloud processing system is configured to manage user accounts and manage use of said e-key," as claim 15 requires. Also, the Petition does not allege that a POSITA would be motivated to make such a modification to include Zaid's server in the alleged cloud processing system "managing the user social media accounts," nor explain what motivation a POSITA would have to make that modification to Zaid's system. Pet. 71-73; EX1004, ¶¶ 285-287. It is my opinion that the Petition's challenge to claim 15 fails

for this reason as well.

IX. CONCLUSION

120. 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.

121. 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 12th day of June, 2026, at Irvine, California

A handwritten signature in dark ink, appearing to read "Sam Malek", with a stylized, flowing script.

Dr. Sam Malek