

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 No. IPR2024-00981
U.S. Patent No. 9,365,188

**DECLARATION OF KEVIN C. ALMEROTH, PH.D.
IN SUPPORT OF PETITION FOR *INTER PARTES* REVIEW OF
U.S. PATENT NO. 9,365,188**

TABLE OF CONTENTS

I.	Introduction	1
II.	Qualifications and Background	2
III.	Materials Considered	15
IV.	Legal Standards	16
A.	Claim Construction	17
B.	Anticipation Under 35 U.S.C. § 102	18
C.	Obviousness Under 35 U.S.C. § 103	18
D.	Priority Under 35 U.S.C. § 120	21
V.	The '188 patent	24
A.	Overview of the '188 patent	24
B.	Prosecution History of the '188 patent	28
C.	The '188 patent's claims are entitled to an effective filing date of no earlier than October 25, 2013	28
D.	Person of Ordinary Skill in the Art	35
VI.	Claim Construction of Terms of the '188 patent	37
VII.	Overview of Prior Art	38
A.	Kleve	38
B.	Zaid	40
VIII.	Summary of Opinions on Unpatentability	44
A.	Ground 1: Kleve renders obvious claims 1-9 and 1120 under Section 103	45
1.	Independent Claim 1	45

2. Claim 2: “The method of claim 1, further comprising, sending a warning notification to the device of the recipient, or the vehicle, or both the device of the recipient, the warning notification identifying the violation of the condition of use.” 65
3. Claim 3: “The method of claim 1, wherein the request to generate the e-key is received from the user account that is one of an administrator of the vehicle, or an owner of the vehicle, or a rental car operator of the vehicle, or a fleet operator for the vehicle, or a user account holder that has the vehicle associated thereto, or a user authorized to request e-keys for the vehicle.” 66
4. Claim 4: “The method of claim 1, further comprising, sending data to one or both of the vehicle and the device of the recipient to notify that the e-key will become disabled due to the violation of the condition.” 66
5. Claim 5: “The method of claim 1, wherein the condition of use is one of a geographic restriction for where the vehicle is allowed to be used, or a speed restriction, or an occupancy restrictions, or a time frame of use, or a time expiration of use, or combinations thereof.” 68
6. Claim 6: “The method of claim 1, wherein the identifying information includes one or more of an email address, a phone number, a text, a message address, a notification, a link, a web address, a social network address, or combinations thereof.” 68
7. Claim 7: “The method of claim 1, wherein receiving use data for use of the vehicle for when the vehicle is used via the e-key includes one or more of a history of where the vehicle has been, or speeds of the vehicle, or events of the vehicle, or multiple violations of the condition of use, or combinations thereof.” 69
8. Claim 8: “The method of claim 1, further comprising, sending messages to one or both of the vehicle and the device of the recipient regarding warnings of when the use

of the vehicle may exceed, has exceeded, or is about to exceed the condition of use.” 69

9. Claim 9: “The method of claim 1, wherein the e-key provides access to at least one of operating functions of the vehicle, or opening the vehicle, or starting the vehicle, or using user interfaces of the vehicle, or turning-off the vehicle, or combinations thereof.”.....70
10. Claim 11 70
11. Claim 12: “The method of claim 1, further comprising, receiving a plurality of requests to generate e-keys for the vehicle from time to time to the recipient or other recipients, such that a plurality of e-keys can be generated for the vehicle and the e-keys that are generated are associated with the user account, and any one of the generated e-keys are removable from being active via the user account, the user account being used for making the requests to generate the e-key or e-keys.” 73
12. Claim 13 76
13. Claim 14: “The method of claim 1, wherein the request to generate the e key for the identified recipient is made using a template having a set of privileges, wherein the template is selectable instead of selecting individual privileges to be associated with the e-key.” 78
14. Claim 15: The method of claim 14, wherein the template is one of a child template, or a teen template, or a spouse template, or a mechanic template, or a valet attendant template, or a friend template, or a quest template, or a custom template.....78
15. Independent Claim 16 79
16. Claim 17: “The method of claim 16, further comprising, receiving, by the server, data from the vehicle being indicative of interface inputs or settings made during use with the e-key, the inputs or settings being examined to

	identify patterns; and learning the patterns, by a process executed by the server, to provide recommendations to the recipient or to an account of the recipient, for settings that should or may be made to the vehicle when using the e-key.”	80
17.	Claim 18	82
18.	Independent Claim 19	83
19.	Claim 20	85
B.	Ground 2: <i>Kleve</i> in view of <i>Sekiyama</i> renders obvious claims 19 and 11-20 under Section 103	86
1.	Motivation to Combine	86
2.	<i>Sekiyama</i> ’s disclosure of 1[a] and 1[b]	88
3.	<i>Sekiyama</i> ’s disclosure of 1[g]	88
C.	Ground 3: <i>Kleve</i> (with or without <i>Sekiyama</i>) in view of <i>Mottla</i> renders obvious claim 10 under Section 103	89
D.	Ground 4: <i>Zaid</i> in view of <i>Harris</i> renders obvious claims 1, 3, 5-7, 9, 11-16, and 18-20 under Section 103	91
1.	Motivation to Combine	92
2.	Claim 1	95
3.	Claim 3: “The method of claim 1, wherein the request to generate the e-key is received from the user account that is one of an administrator of the vehicle, or an owner of the vehicle, or a rental car operator of the vehicle, or a fleet operator for the vehicle, or a user account holder that has the vehicle associated thereto, or a user authorized to request e-keys for the vehicle.”	110
4.	Claim 5: “The method of claim 1, wherein the condition of use is one of a geographic restriction for where the vehicle is allowed to be used, or a speed restriction, or an	

occupancy restrictions, or a time frame of use, or a time expiration of use, or combinations thereof.”.....110

5. Claim 6: “The method of claim 1, wherein the identifying information includes one or more of an email address, a phone number, a text, a message address, a notification, a link, a web address, a social network address, or combinations thereof.” 111
6. Claim 7: “The method of claim 1, wherein receiving use data for use of the vehicle for when the vehicle is used via the e-key includes one or more of a history of where the vehicle has been, or speeds of the vehicle, or events of the vehicle, or multiple violations of the condition of use, or combinations thereof.” 111
7. Claim 9: “The method of claim 1, wherein the e-key provides access to at least one of operating functions of the vehicle, or opening the vehicle, or starting the vehicle, or using user interfaces of the vehicle, or turning-off the vehicle, or combinations thereof.”.....111
8. Claim 11 112
9. Claim 12: “The method of claim 1, further comprising, receiving a plurality of requests to generate e-keys for the vehicle from time to time to the recipient or other recipients, such that a plurality of e-keys can be generated for the vehicle and the e-keys that are generated are associated with the user account, and any one of the generated e-keys are removable from being active via the user account, the user account being used for making the requests to generate the e-key or e-keys.” 113
10. Claim 13 115
11. Claim 14: “The method of claim 1, wherein the request to generate the e key for the identified recipient is made using a template having a set of privileges, wherein the template is selectable instead of selecting individual privileges to be associated with the e-key.” 116

12.	Claim 15: The method of claim 14, wherein the template is one of a child template, or a teen template, or a spouse template, or a mechanic template, or a valet attendant template, or a friend template, or a quest template, or a custom template.....	118
13.	Independent Claim 16.....	119
14.	Claim 18.....	119
15.	Independent Claim 19.....	120
16.	Claim 20.....	122
E.	Ground 5: <i>Zaid</i> and <i>Harris</i> in view of <i>Mottla</i> renders obvious claims 2, 4, 8, and 10 under Section 103.....	122
1.	Motivation to Combine.....	123
2.	Claims 2, 4, and 8.....	125
3.	Claim 10: “The method of claim 1, wherein the e-key enables graphical icons on a screen of the device to be active for enabling use of the vehicle, at least one of the graphical icons on the screen enabling unlocking of the vehicle, or turning on of the vehicle, or locking the vehicle.”.....	126
F.	Ground 6: <i>Zaid</i> and <i>Harris</i> in view of <i>Patenaude</i> render obvious claim 17 under Section 103.....	128
1.	Motivation to Combine.....	128
2.	Claim 17: “The method of claim 16, further comprising, receiving, by the server, data from the vehicle being indicative of interface inputs or settings made during use with the e-key, the inputs or settings being examined to identify patterns; and learning the patterns, by a process executed by the server, to provide recommendations to the recipient or to an account of the recipient, for settings that should or may be made to the vehicle when using the e-key.”.....	131

G.	Ground 7: <i>Kleve</i> in view of <i>Patenaude</i> render obvious claim 17 under Section 103	132
IX.	Secondary Considerations of Non-obviousness.....	133
X.	Conclusion.....	135

I. Introduction

1. I, Kevin C. Almeroth, Ph.D., submit this declaration to state my opinions on the matter described below.

2. I have been retained by Petitioner Kia Corporation (“Petitioner”), as an independent expert in this proceeding before the United States Patent and Trademark Office. Although I am being compensated at my usual and customary rate of \$850 per hour, no part of my compensation depends on the outcome of this proceeding, and I have no other interest in this proceeding.

3. I understand that this proceeding involves U.S. Patent No. 9,365,188 (the “’188 patent”), and I have been asked to provide my opinions as to the patentability of the claims of the ’188 patent. I understand that the application for the ’188 patent was filed on June 12, 2014, and is a continuation application of a U.S. application having a filing date of October 25, 2013. I understand the ’188 patent also purports to be a continuation-in-part of U.S. applications filed March 15, 2013, and April 22, 2012, respectively, and claims priority to two U.S. provisional applications, one filed December 24, 2012, and one filed April 22, 2011. I was also asked to evaluate Patent Owner’s priority claims for the ’188 patent. As discussed herein, it is my opinion that claims 1-20 are entitled to a priority date of no earlier than October 25, 2013.

4. I have been asked to consider the validity of certain claims of the '188 patent based on certain prior art references. I have also been asked to consider the state of the art and prior art available as of October 25, 2013. Based on the prior art discussed in this declaration, it is my opinion that claims 1-20 of the '188 patent are unpatentable for the reasons provided below.

II. Qualifications and Background

5. I believe that I am well qualified to serve as a technical expert in this matter based upon my educational and work experience, and specifically, in the field of vehicle electronics and computing devices. My curriculum vitae ("CV") is submitted as Exhibit 1003.

6. I am currently a Professor Emeritus in the Department of Computer Science at the University of California, Santa Barbara (UCSB). While active at UCSB, I held faculty appointments and was a founding member of the Computer Engineering (CE) Program, Media Arts and Technology (MAT) Program, and the Technology Management Program (TMP). I also served as the Associate Director of the Center for Information Technology and Society (CITS) from 1999 to 2012. I have been a faculty member at UCSB since July 1997.

7. I hold three degrees from the Georgia Institute of Technology: (1) a Bachelor of Science degree in Information and Computer Science (with minors in Economics, Technical Communication, and American Literature) earned in June

1992; (2) a Master of Science degree in Computer Science (with specialization in Networking and Systems) earned in June 1994; and (3) a Doctor of Philosophy (Ph.D.) degree in Computer Science (Dissertation Title: Networking and System Support for the Efficient, Scalable Delivery of Services in Interactive Multimedia System, minor in Telecommunications Public Policy) earned in June 1997. During my education, I have taken a wide variety of courses as demonstrated by my minor. My undergraduate degree also included a number of courses more typical of a degree in electrical engineering including digital logic, signal processing, and telecommunications theory.

8. One of the major concentrations of my research over the past 30+ years has been the delivery of multimedia content and data between computing devices, including various network architectures. In my research, I have studied large-scale content delivery systems, and the use of servers located in a variety of geographic locations to provide scalable delivery to hundreds or thousands of users simultaneously. I have also studied smaller-scale content delivery systems in which content is exchanged between individual computers and portable devices. My work has emphasized the exchange of content more efficiently across computer networks, including the scalable delivery of content to many users, mobile computing, satellite networking, delivering content to mobile devices, and network support for data delivery in wireless networks.

9. In 1992, the initial focus of my research was on the provision of interactive functions (e.g., VCR-style functions like pause, rewind, and fastforward) for near video-on-demand systems in cable systems; in particular, how to aggregate requests for movies at a cable head-end and then how to satisfy a multitude of requests using one audio/video stream broadcast to multiple receivers simultaneously. This research has continually evolved and resulted in the development of techniques to scalably deliver on-demand content, including audio, video, web documents, and other types of data, through the Internet and over other types of networks, including over cable systems, broadband telephone lines, and satellite links.

10. An important component of my research has been investigating the challenges of communicating multimedia content, including video, between computers and across networks including the Internet. Although the early Internet was used mostly for text-based, non-real time applications, the interest in sharing multimedia content, such as video, quickly developed. Multimedia-based applications ranged from downloading content to a device to streaming multimedia content to be instantly used. One of the challenges was that multimedia content is typically larger than text-only content, but there are also opportunities to use different delivery techniques since multimedia content is more resilient to errors. I have worked on a variety of research problems and used a number of systems that

were developed to deliver multimedia content to users. One content-delivery method I have researched is the one-to-many communication facility called “multicast,” first deployed as the Multicast Backbone, a virtual overlay network supporting one-to-many communication. Multicast is one technique that can be used on the Internet to provide streaming media support for complex applications like video-on-demand, distance learning, distributed collaboration, distributed games, and large-scale wireless communication. The delivery of media through multicast often involves using Internet infrastructure, devices and protocols, including protocols for routing and TCP/IP.

11. Starting in 1997, I worked on a project to integrate the streaming media capabilities of the Internet together with the interactivity of the web. I developed a project called the Interactive Multimedia Jukebox (IMJ). Users would visit a web page and select content to view. The content would then be scheduled on one of a number of channels, including delivery to students in Georgia Tech dorms delivered via the campus cable plant. The content of each channel was delivered using multicast communication.

12. In the IMJ, the number of channels varied depending on the capabilities of the server including the available bandwidth of its connection to the Internet. If one of the channels was idle, the requesting user would be able to watch their selection immediately. If all channels were streaming previously selected

content, the user's selection would be queued on the channel with the shortest wait time. In the meantime, the user would see what content was currently playing on other channels, and because of the use of multicast, would be able to join one of the existing channels and watch the content at the point it was currently being transmitted.

13. The IMJ service combined the interactivity of the web with the streaming capabilities of the Internet to create a jukebox-like service. It supported true Video-on-Demand when capacity allowed, but scaled to any number of users based on queuing requested programs. As part of the project, we obtained permission from Turner Broadcasting to transmit cartoons and other short-subject content. We also connected the IMJ into the Georgia Tech campus cable television network so that students in their dorms could use the web to request content and then view that content on one of the campus's public access channels.

14. More recently, I have also studied issues concerning how users choose content, especially when considering the price of that content. My research has examined how dynamic content pricing can be used to control system load. By raising prices when systems start to become overloaded (i.e., when all available resources are fully utilized) and reducing prices when system capacity is readily available, users' capacity to pay as well as their willingness can be used as factors in stabilizing the response time of a system. This capability is particularly useful in

systems where content is downloaded or streamed on-demand to users.

15. As a parallel research theme, starting in 1997, I began researching issues related to wireless devices and sensors. In particular, I was interested in showing how to provide greater communication capability to “lightweight devices,” i.e., small form-factor, resource-constrained (e.g., CPU, memory, networking, and power) devices. Starting in 1998, I published several papers on my work to develop a flexible, lightweight, battery-aware network protocol stack.

16. The lightweight protocols we envisioned were similar in nature to protocols like Bluetooth, Universal Plug and Play (UPnP) and Digital Living Network Alliance (DLNA). From this initial work, I have made wireless networking-including ad hoc, mesh networks and wireless devices-one of the major themes of my research. My work in wireless network spans the protocol stack from applications through to the encoding and exchange of data at the data link and physical layers.

17. At the application layer, even before the large-scale “app stores” were available, my research looked at building, installing, and using apps for a variety of purposes, from network monitoring to support for traditional computer-based applications (e.g., content retrieval) to new applications enabled by ubiquitous, mobile devices. For example, my research has looked at developing applications for virally exchanging and tracking “coupons” through “opportunistic contact”

(i.e., communication with other devices coming into communication range with a user). In many of the courses I have taught there is a project component. Through these projects I have supervised numerous efforts to develop new “apps” for download and use across a variety of mobile platforms.

18. Toward the middle of the protocol stack, my research also looked to build wireless infrastructure support to enable communication among a set of mobile devices unaided by any other kind of network infrastructure. These kinds of networks are useful either in challenged network environments (e.g., when a natural disaster has destroyed existing infrastructure) or when suitable support for network communication never existed. The deployment of such networks (or even the use of traditional network support) are critical to support services like disaster relief, catastrophic event coordination, and emergency services deployment.

19. Yet another theme is monitoring wireless networks, in particular different variants of IEEE 802.11 compliant networks, to (1) understand the operation of the various protocols used in real-world deployments, (2) use these measurements to characterize use of the networks and identify protocol limitations and weaknesses, and (3) propose and evaluate solutions to these problems. I have successfully used monitoring techniques to study wireless data link layer protocol operation and to improve performance by enhancing the operation of such protocols. For wireless protocols, this research includes functions like network

acquisition and channel bonding.

20. Protecting networks, including their operation and content, has been an underlying theme of my research almost since the beginning of my research career. Starting in 2000, I have been involved in several projects that specifically address security, network protection, and firewalls. After significant background work, a team on which I was a member successfully submitted a \$4.3M grant proposal to the Army Research Office (ARO) at the Department of Defense to propose and develop a high-speed intrusion detection system. Key aspects of the system included associating streams of packets and analyzing them for viruses and other malware. Once the grant was awarded, we spent several years developing and meeting the milestones of the project. A number of my students worked on related projects and published papers on topics ranging from intrusion detection to developing advanced techniques to be incorporated into firewalls. I have also used firewalls, including their associated malware detection features, in developing techniques for the classroom to ensure that students are not distracted by online content.

21. Recent work ties some of the various threads of my past research together. I have investigated content delivery in online social networks and proposed reputation management systems in large-scale social networks and marketplaces. On the content delivery side, I have looked at issues of caching and

cache placement, especially when content being shared and the cache has geographical relevance. We were able to show that effective caching strategies can greatly improve performance and reduce deployment costs. Our work on reputation systems showed that reputations have economic value, and as such, creates a motivation to manipulate reputations. In response, we developed a variety of solutions to protect the integrity of reputations in online social networks. The techniques we developed for content delivery and reputation management were particularly relevant in peer-to-peer communication and recommendations for downloadable “apps.”

22. As an important component of my research program, I have been involved in the development of academic research into available technology in the market place. One aspect of this work is my involvement in the Internet Engineering Task Force (IETF). The IETF is a large and open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. I have been involved in various IETF groups including many content delivery-related working groups like the Audio Video Transport (AVT) group, the MBone Deployment (MBONED) group, Source Specific Multicast (SSM) group, the Inter-Domain Multicast Routing (IDMR) group, the Reliable Multicast Transport (RMT) group, the Protocol Independent Multicast (PIM) group, etc. I

have also served as a member of the Multicast Directorate (MADDOGS), which

oversaw the standardization of all things related to multicast in the IETF. Finally, I

was the Chair of the Internet2 Multicast Working Group for seven years.

23. As another important component of my research, I have been involved in the development of academic research into available technology in mobile connections, networks, and protocols in dynamic environments, including moving vehicles. See, e.g.:

- K. Almeroth, K. Obraczka and D. De Lucia, “*A Lightweight Protocol for Interconnecting Heterogeneous Devices in Dynamic Environments*,” IEEE International Conference on Multimedia Computing and Systems (ICMCS), Florence, ITALY, June 1999.
- K. Harras, K. Almeroth and E. Belding, *Delay Tolerant Mobile Networks (DTMNs): Controlled Flooding in Sparse Mobile Networks*,” IFIP Networking Conference, Waterloo, Ontario, CANADA, May 2005.
- C. Holman, K. Harras, and K. Almeroth, “*A Proactive Data Bundling System for Intermittent Mobile Connections*,” IEEE International Conference on Sensor and Ad Hoc Communications and Networks (SECON), Reston, Virginia, USA, September 2006.

- R. Chertov, D. Havey and K. Almeroth, “*MSET: A Mobility Satellite Emulation Testbed*,” IEEE Infocom, San Diego, California, USA, March 2010.

24. My involvement in the research community extends to leadership positions for several academic journals and conferences. I am the co-chair of the Steering Committee for the ACM Network and System Support for Digital Audio and Video (NOSSDAV) workshop and on the Steering Committees for the International Conference on Network Protocols (ICNP), ACM Sigcomm Workshop on Challenged Networks (CHANTS), and IEEE Global Internet (GI) Symposium. I have served or am serving on the Editorial Boards of IEEE/ACM Transactions on Networking, IEEE Transactions on Mobile Computing, IEEE Network, ACM Computers in Entertainment, AACE Journal of Interactive Learning Research (JILR), and ACM Computer Communications Review. I have co-chaired a number of conferences and workshops, including the IEEE International Conference on Network Protocols (ICNP), IEEE Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), International Conference on Communication Systems and Networks (COMSNETS), IFIP/IEEE International Conference on Management of Multimedia Networks and Services (MMNS), the International Workshop On Wireless Network Measurement (WiNMee), ACM Sigcomm Workshop on Challenged Networks (CHANTS), the

Network Group Communication (NGC) workshop, and the Global Internet

Symposium, and I have served on the program committees for numerous conferences.

25. Furthermore, in the courses I taught at UCSB, a significant portion of my curriculum covered aspects of the Internet and network communication, including the physical and data link layers of the Open System Interconnect (OSI) protocol stack, and standardized protocols for communicating across a variety of physical media such as cable systems, telephone lines, wireless, and high-speed Local Area Networks (LANs). The courses I have taught also cover most major topics in Internet communication, including data communication, multimedia encoding, and mobile application design. My research and courses have covered a range of physical infrastructures for delivering content over networks, including cable, Integrated Services Digital Network (ISDN), Ethernet, Asynchronous Transfer Mode (ATM), fiber, and Digital Subscriber Line (DSL). For a complete list of courses I have taught, see my curriculum vitae (CV) (Appendix A).

26. In addition, I co-founded a technology company called Santa Barbara Labs that was working under a sub-contract from the U.S. Air Force to develop very accurate emulation systems for the military's next generation internetwork. Santa Barbara Labs' focus was in developing an emulation platform to test the performance characteristics of the network architecture in the variety of

environments in which it was expected to operate, and, in particular, for network services including IPv6, multicast, Quality of Service (QoS), satellite-based communication, and security. Applications for this emulation program included communication of a variety of multimedia-based services, including video conferencing and video-on-demand.

27. In addition to having co-founded a technology company myself, I have worked for, consulted with, and collaborated with companies for nearly 30 years. These companies range from well-established companies to start-ups and include IBM, Hitachi Telecom, Turner Broadcasting System (TBS), Bell South, Digital Fountain, RealNetworks, Intel Research, Cisco Systems, and Lockheed Martin.

28. Through my graduate education, leadership with CITS, involvement in TMP, role in the development of the Internet infrastructure, and consulting with ISPs, I have gained a strong understanding in the role of the Internet in our society and the challenges of deploying large-scale production networking infrastructure. CITS, since its inception, has looked at the role of the Internet in society, including how the evolution of technology have created communication opportunities and challenges, including, for example through disruptive technologies like P2P. TMP looks to focus on non-purely technical issues, including, for example, state-of-the-art business methods, strategies for successful technology commercialization, new

venture creation, and best practices for fostering innovation. Through my industry collaborations and Internet work, I have developed significant experience in the challenges of deploying, monitoring, managing, and scaling communication infrastructure to support evolving Internet services like streaming media, conferencing, content exchange, social networking, and e-commerce.

29. I am a Member of the Association of Computing Machinery (ACM) and a Fellow of the Institute of Electrical and Electronics Engineers (IEEE).

III. Materials Considered

30. In forming my opinions, I have reviewed the following documents:

Exhibit	Description
1001	U.S. Patent No. 9,365,188 to <i>Penilla</i> et al.
1002	Prosecution File History for U.S. Patent No. 9,365,188.
1003	Declaration of Dr. Almeroth
1004	U.S. Pat. Pub. No. 2014/0129053 (“Kleve”) (prior art under at least §§ 102(a)(2) or pre-AIA § 102(e))
1005	Certified translation of JP2010126949A (“Sekiyama”) (prior art under at least Section §§ 102(a)(1), (2) or pre-AIA § 102(a), (e))
1006	JP 2010126949
1007	Declaration of Herman Kahn
1008	U.S. Pat. Pub. No. 2011/0112969A1 (“Zaid”) (prior art under at least §§ 102(a)(1), (2) or pre-AIA §§ 102(a), 102(b), 102(e))
1009	U.S. Pat. Pub. No. 2011/0312273A1 (“Harris”) (prior art under at least §§

Exhibit	Description
	102(a)(1), (2))
1010	U.S. Pat. Pub. No. 2011/0060480A1 (“Mottla”) (prior art under at least §§ 102(a)(1), (2) or pre-AIA § 102(a), (b), (e))
1011	U.S. Pat. Pub. No. 2006/0136106 (“Patenaude”) (prior art under at least §§ 102(a)(1), (2) or pre-AIA § 102(a), (b),(e))
1012	U.S. Pat. App. No. 61/478,436
1013	U.S. Pat. App. No. 61/745,729
1014	U.S. Pat. App. No. 13/452,882
1015	U.S. Pat. App. No. 13/842,158
1016	U.S. Pat. App. No. 14/063,638
1017	Order Granting Request For Ex Parte Reexamination, Reexamination Control No. 90/019,456, Patent No. 11,738,659 (April 15, 2024)
1018	Text Comparison of U.S. Pat. App. No. 13/842,158 to U.S. Pat. App. No. 14/063,638

IV. Legal Standards

31. In forming my opinions and considering the subject matter of the ’268 patent and its claims in light of the prior art, I am relying on certain legal principles that counsel in this case explained to me. My understanding of these concepts is summarized below.

32. I understand that the claims define the invention. I also understand that an unpatentability analysis is a two-step process. First, the claims of the patent are construed to determine their meaning and scope. Second, after the claims are

construed, the content of the prior art is compared to the construed claims.

33. I understand that a claimed invention is only patentable when it is new, useful, and non-obvious in light of the “prior art.” That is, the invention, as defined by the claims of the patent, must not be anticipated or rendered obvious by the prior art.

A. Claim Construction

34. I understand that the United States Patent and Trademark Office interprets claim terms in an *inter-partes* review proceeding under the same claim construction standard that is used in a United States federal court. I understand that under this standard, the meaning of claim terms is considered from the viewpoint of one of ordinary skill in the art at the time of the alleged invention.

35. I understand that claim terms are generally given their ordinary and customary meaning as understood by one of ordinary skill in the art in light of the specification and the prosecution history pertaining to the patent. I understand, however, that claim terms are generally not limited by the embodiments described in the specification.

36. I understand that in addition to the claims, specification, and prosecution history, other evidence may be considered to ascertain the meaning of claim terms, including textbooks, encyclopedias, articles, and dictionaries. I have been informed that this other evidence is often less significant and less reliable

than the claims, specification, and prosecution history.

B. Anticipation Under 35 U.S.C. § 102

37. I understand that under 35 U.S.C. § 102, a patent claim is invalid if its subject matter was patented or described in a printed publication before the effective filing date of the claimed invention. I have been told that this is referred to as invalidity by anticipation. I have been told that a patent claim is anticipated under § 102 if a single prior art reference discloses all limitations of the claimed invention.

C. Obviousness Under 35 U.S.C. § 103

38. I understand that a patent claim is invalid as obvious if the claimed invention would have been obvious to a person of ordinary skill in the art (“POSITA”) at the time the claimed invention was made. This means that even if all of the elements of the claim cannot be found in a single prior art reference that would anticipate the claim, a person of ordinary skill in the field who knew about all the prior art would have come up with the claimed invention. I understand that in an obviousness determination, the person of ordinary skill in the art is presumed to have knowledge of all material prior art. I understand that whether a claim is obvious is based upon the determination of several factual issues.

39. I understand that obviousness is a determination of law based on underlying determinations of fact. I understand that these factual determinations

include the scope and content of the prior art, the level of ordinary skill in the art, the differences between the claimed invention and the prior art, and secondary considerations of non-obviousness.

40. In considering obviousness, I understand that one must determine the scope and content of the prior art. I understand that, in order to be considered as prior art to a patent being considered, a prior art reference must be reasonably related to the claimed invention of that patent. A reference is reasonably related if it is in the same field as the claimed invention or is from another field to which a person of ordinary skill in the art would look to solve a known problem.

41. I understand that one must determine what differences, if any, existed between the claimed invention and the prior art.

42. I understand that a patent claim composed of several elements is not proved obvious merely by demonstrating that each of its elements was independently known in the prior art. In evaluating whether such a claim would have been obvious, one may consider whether a reason has been identified that would have prompted a person of ordinary skill in the art to combine the elements or concepts from the prior art in the same way as in the claimed invention. There is no single way to define the line between true inventiveness on the one hand (which is patentable) and the application of common sense and ordinary skill to solve a problem on the other hand (which is not patentable). For example, market forces or

other design incentives may be what precipitated a change, rather than true inventiveness.

43. I understand that whether a prior art reference renders a patent claim unpatentable as obvious is determined from the perspective of a person of ordinary skill in the art at the time of the alleged invention. I have been told that there is no requirement that the prior art contain an express suggestion to combine known elements to achieve the claimed invention, but a suggestion to combine known elements to achieve the claimed invention may come from the prior art, as filtered through the knowledge of one skilled in the art. In addition, I have been told that the inferences and creative steps a person of ordinary skill in the art would employ are also relevant to the determination of obviousness.

44. I understand that there is no rigid rule that a reference or combination of references must contain a “teaching, suggestion, or motivation” to combine references. But I also understand that the “teaching, suggestion, or motivation” test can be a useful guide in establishing a rationale for combining elements of the prior art. I have been told that this test poses the question as to whether there is an express or implied teaching, suggestion, or motivation to combine prior art elements in a way that realizes the claimed invention, and that it seeks to counter impermissible hindsight analysis.

45. I understand that one may consider, e.g., whether (1) the change was

merely the predictable result of using prior art elements according to their known functions, or whether it was the result of true inventiveness; (2) there is some teaching or suggestion in the prior art to make the modification or combination of elements claimed in the patent; (3) the claimed innovation applies a known technique that had been used to improve a similar device or method in a similar way; (4) the claimed invention would have been obvious to try, meaning that the claimed innovation was one of a relatively small number of possible approaches to the problem with a reasonable expectation of success by those skilled in the art; (5) the invention merely substituted one known element for another known element in order to obtain predictable results; (6) the invention merely applies a known technique to a known device, method, or product to yield predictable results; or (7) known work in the field may have prompted variations of use of the same inventions in the same or different fields due to market forces or design incentives that would have been predictable to a person of ordinary skill in the art.

46. I understand that any assertion of secondary considerations of non-obviousness must be accompanied by a nexus between the merits of the invention and the evidence offered.

D. Priority Under 35 U.S.C. § 120

47. I understand that the “priority date” or “effective filing date” of a patent is the date on which it is filed, or the date on which an earlier-filed U.S. or

international patent application was filed if the patentee claims the benefit of priority to that earlier-filed application.

48. I understand that in the patent application process, the applicant may keep the originally filed claims, or change the claims between the time the patent application is first filed and the time a patent is issued. An applicant may amend the claims or add new claims. These changes may narrow or broaden the scope of the claims. I understand that a patent application is entitled to the benefit of the filing date of an earlier-filed application only if the disclosure of the earlier application provides support for the claims of the later application as required by the “written description” requirement of 35 U.S.C. § 112. I further understand that for a patent application to have an adequate written description of the invention, it must show the inventor was in possession of the invention at the time the patent application was filed.

49. When determining whether a specification of a patent application contains adequate written description of the claimed invention, I understand that one must make an objective inquiry into the four corners of the specification from the perspective of a POSITA. Further, I understand that the standard for written description is stricter than the standard for determining whether or not a patent claim would have been obvious based on the prior art.

50. In particular, the question for purposes of written description is not

merely whether the claimed invention is an obvious variant of what the specification discloses. Instead, the application itself must describe the invention, and do so in sufficient detail that a POSITA can clearly conclude that the inventor invented the claimed invention as of the date when the application was filed.

51. Similarly, I understand the issue of written description is separate from the question of “enablement” (i.e., whether a specification allows a POSITA to practice the claimed invention without undue experimentation). A specification may adequately enable a claimed invention, yet fail to provide written description support.

52. Finally, I understand that the standard for whether or not a disclosure is sufficient to provide written description support for a claim is different from the standard for whether a disclosure anticipates a claim. To support a claim, the description must be sufficient to convey to a POSITA that the inventors were in possession of the full scope of the claimed subject matter. By contrast, a description anticipates a claim if it discloses even a single species within the scope of the claim. Thus, in the case of “genus” claims covering two or more different species, I understand that there can be situations in which a given disclosure is sufficient to anticipate the claim even though that same disclosure is not adequate to support the claim and entitle the inventors to an earlier priority date.

53. I understand that in order to claim priority to an application through a

chain of applications, every single application in the chain (going back to the particular application on which the inventors want to rely) needs to support the claim as a matter of written description. In other words, each application in the chain must allow a person of ordinary skill in the art to discern that the inventors were in possession of the claimed invention at the time of the application. It is not sufficient under this standard for the disclosure in the specification to render the claimed invention obvious.

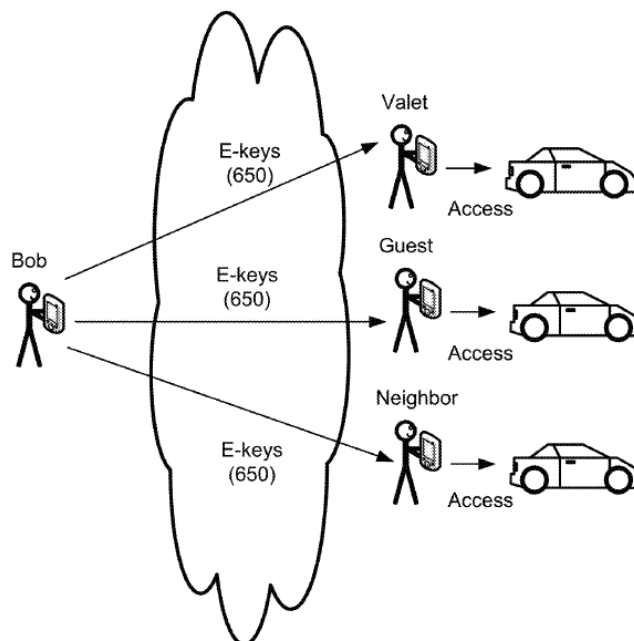
V. The '188 patent

A. Overview of the '188 patent

54. The application that led to the '188 patent was filed on June 12, 2014. It is my opinion that the earliest date to which the challenged claims of the '188 patent can claim priority, as explained in further detail in section V.B, is October 25, 2013. The '188 patent, on its face, references four earlier applications: a provisional application filed April 22, 2011, a provisional application filed December 24, 2012, a non-provisional application filed April 22, 2012, and a non-provisional application filed March 15, 2013. Even if the '188 patent could claim priority back to any of these dates (which it cannot), my ultimate conclusions as to the invalidity of the '188 patent would not change. To be clear, if the '188 patent is not entitled to a priority date earlier than October 25, 2013, then I have been informed that Kleve is prior art and renders obvious the Challenged Claims. But even if the '188 patent is entitled

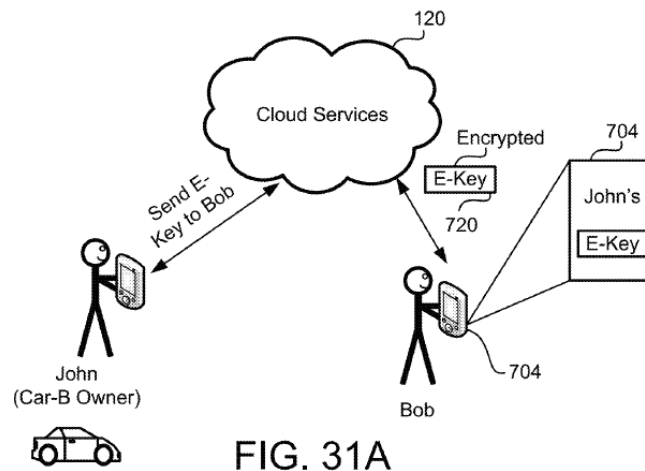
to the earliest priority date, the Zaid-based grounds would render the Challenged Claims obvious. In addition, I have been informed that Sekiyama, Harris, Mottla, and Patenaude are all prior art regardless of the '188 patent's priority date.

55. **The '188 patent** is directed to a system in which a vehicle owner assigns an electronic key to a user for enabling access and use of a shared vehicle by the user. Ex. 1001 at Abstract. For example, in Figure 29, vehicle owner Bob shares electronic keys 650 with users “valet,” “guest,” and “neighbor” for vehicle access. *Id.* at 40:64-66. The specification explains that “[e]ach e-key, in one embodiment, will include a unique access code or substantially unique access code.” '188 patent at 41:12-13. Further, “[t]he unique generation of access codes enables each electronic keyed [sic] to be different for each user and each e-key can expire at any time set by a requesting user.” *Id.* at 41:20-24.



'188 patent, Fig. 29.

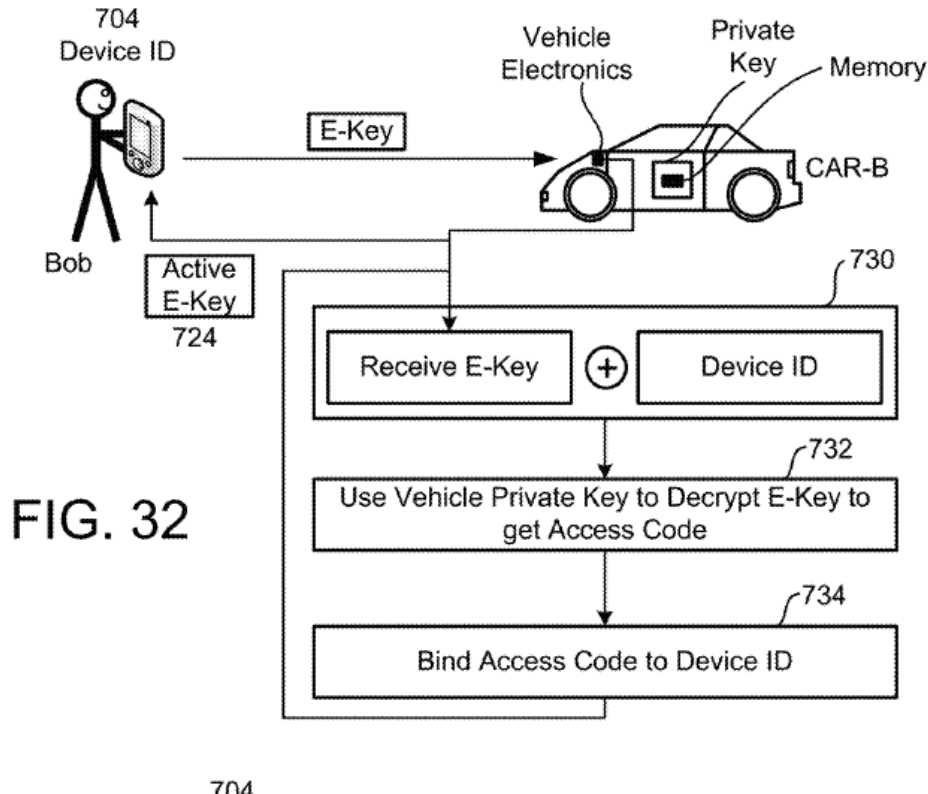
56. In Figure 31A, vehicle owner John utilizes a cloud server 120 to send an encrypted ekey to guest user Bob. In this embodiment, “the server will generate an access code for the vehicle” (*id.* at 42:14), which “will then be encrypted by the server and then sent as encrypted e-keys 722¹ to Bob’s device 704.” *Id.* at 42:16-18.



'188 patent, Fig. 31A.

57. Next, in Figure 32, user Bob “will transfer the encrypted e-keys 720 to the vehicle that belongs to John (car-B). . . At the vehicle, the vehicle will receive the encrypted e-keys and the device ID of Bob’s device 704. The vehicle will hold a private key to unlock and un-encrypt the encrypted e-keys 720.” *Id.* at 42:24-33.

¹ The specification’s reference to “encrypted e-keys 722” is likely a typo and should instead refer to encrypted e-keys 720.



58. Figure 32 further describes a process by which the e-key is associated with the device of the user seeking to utilize the e-key. In step 730, the encrypted ekey is “associated” with the mobile device. *Id.* at 42:38-40. In step 732, “the vehicle private key is used to decrypt the e-keys to get access to an access code.” *Id.* at 42:48-50. And in step 734, “[t]he access code is then sent as activated e-keys 724 back to Bob’s device 704,” allowing Bob’s device to access the vehicle. *Id.*, 42:53-56. The ’188 patent discloses that the unique access code “can be generated by a number generator, and [sic] alphanumeric random generator, in [sic] incremental number generator, or any other generation device that can generate codes that are unique or substantially unique.” *Id.* at 43:25-28.

59. Finally, the specification discloses that the “keys can be assigned to users with various privilege settings” corresponding to the use of a vehicle function for an associated time period. *Id.* at 40:66-67. For example, “electronic keys for each user can be associated with a different expiration time.” *Id.* at 41:9-11; *see also* 48:3-7 (“the privileges can be assigned by selecting . . . time durations[.]”). In the example above, once Bob receives the ekey from the server as John requested, “Bob’s device 704 can now access the vehicle in accordance with the privileges set by John, the owner of the vehicle.” *Id.* at 42:54-56.

B. Prosecution History of the ’188 patent

60. I have reviewed the prosecution history of the application that led to the ’188 patent. Ex. 1002. I note that the examiner did not issue any rejections and allowed the claims over the prior art stating that it did not disclose transmitting the e-key. I am not aware of anything in the prosecution history that changes my opinions expressed in this declaration. To the extent Patent Owner relies on the prosecution history for some point relevant to my opinions, I reserve the right to respond in a future declaration.

C. The ’188 patent’s claims are entitled to an effective filing date of no earlier than October 25, 2013

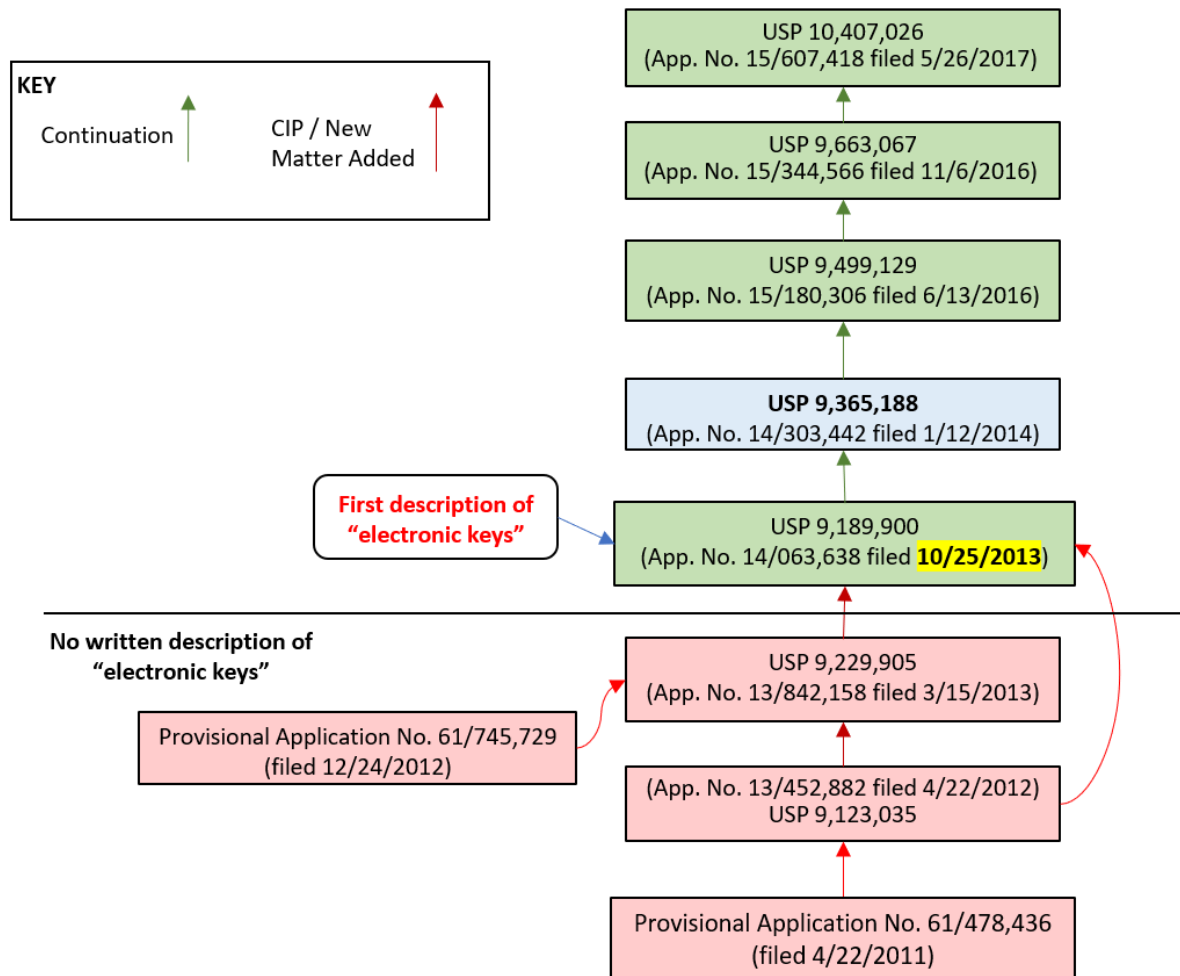
61. The application leading to the ’188 patent claims priority to U.S. Application Nos. 15/344,566 (now U.S. Pat. No. 9,663,067), 15/180,306 (now U.S.

Pat. No. 9,499,129), 14/303,442 (now U.S. Pat. No. 9,365,188), 13/452,882 (now

U.S. Pat. No. 9,123,035), 14/063,638 (“638 Application”) (now U.S. Pat. No.

9,189,900), 13/824,158 (now U.S. Pat. No. 9,229,905) (“158 Application”),

61/478,436, and 61/745,729. See Exs. 1010-1014, 1032-34.



62. I observe that Application No. 14/063,638 (Ex. 1014) describes itself as a “continuation-in-part” of Application No. 13/842,158 (Ex. 1013) and Application No. 13/452,882 (Ex. 1012). I understand that a continuation-in-part

application repeats all or a substantial part of a prior application's disclosure and adds new subject matter not disclosed in the parent application. Only claims that are adequately disclosed in the parent application receive the benefit of the parent application's filing date, while any claim that recites a feature first introduced in the continuation-in-part application and was not adequately disclosed in the parent application is not entitled to the filing date of the parent application. As illustrated above, the application leading to the '188 patent is related to Application No. 14/063,638 via multiple continuation applications.

63. There are numerous differences between the '638 Application and the '158 Application, which are evident from a computerized comparison of the two. *See* Ex. 1029. Numerous differences also appear between Application No. 13/842,158 and Application No. 13/452,882. *See* Ex. 1038. For example, I observe several new paragraphs and figures describing "e-keys" in the '638 Application that do not appear in either of Application Nos. 13/452,882 or the '158 Application. *Id.* In my opinion, the claim limitations "**receiving, by a server, a request** from a user ... to generate an electronic key (e-key) for an identified recipient to use the vehicle," "**generating, by the server, the e-key** ... with the condition of use of the vehicle," "**transmitting, by the server, the e-key** to the recipient," and "transmitting, by the server, data to the vehicle to **enable use of the vehicle via the e-key**," as required by every claim of the '188 patent, are not found in the earlier applications.

64. The new matter introduced in the '638 Application, is not present in any of the preceding filings. *See* Exs. 1012-1016, Ex. 1018. This new matter is the only basis on which the specification for the '188 patent even arguably conveys to a person of ordinary skill in the art that the inventors had developed a system for requesting, generating, transmitting, and using e-keys.

65. For example, Figures 17 through 35 of the '638 Application (which are the same as Figures 17 through 35 of the '188 patent) and their descriptions were introduced in the '638 Application and discuss in detail the requesting, generating, transmission, and use of e-keys. *See, e.g., id.*, 105 (“FIGS. 17-30B ... describe the use of electronic keys (e-keys) in accordance with several embodiments.”); 122 (“Figure 29 illustrates an example where an owner of the vehicle Bob, is able to assign electronic keys (e-keys) 650 to any number of users.”); *id.* (“Each e-key, in one embodiment, will include a unique access code [which] can be generated by a server ...”); 126 (“FIG. 33 illustrates an example where Bob utilizes his device 704 to activate, open, lock, turn on, unlock, John’s vehicle ... facilitated by the activated e-keys 724, which are used via device 704 ...”); *id.* (“FIG. 31B illustrates ... when a request to send e-keys to a recipient is received [by c]loud services [which] can include identification of the recipient and the privileges defined by the requester for that issuance of e-keys ...”); 128 (“FIG. 35 illustrates an example where a request is sent by John via device 702 to cloud services 120 [which] can generate the unique

access code which is then encrypted in a message and sent as encrypted e-keys 720 to the recipient, Bob, who receives it via device 704. ... The duration that the e-keys will remain active can also be set by the requester.”).

66. As shown below, Figure 35 depicts the requesting, generating, and transmitting of an e-key to Bob’s mobile device.

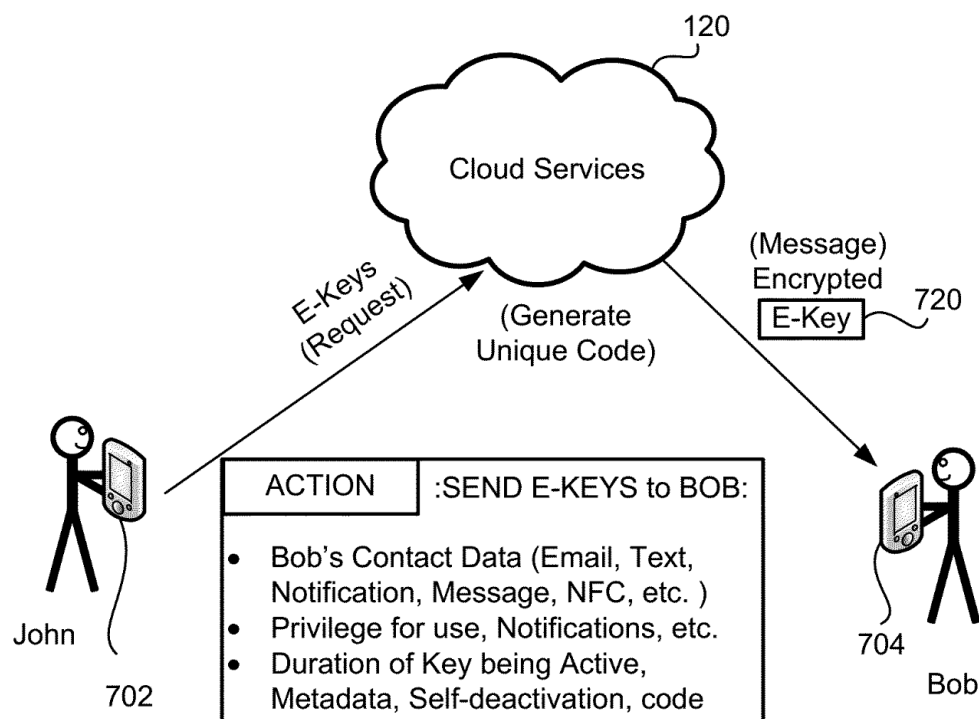


FIG. 35

67. And Figure 33 depicts the use of an e-key by Bob to unlock and start John’s vehicle.

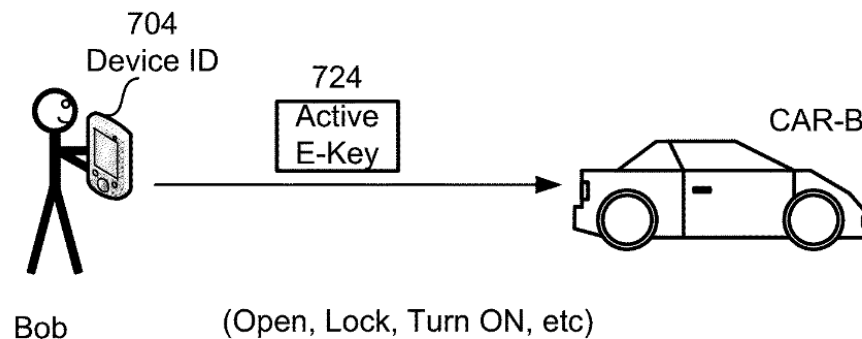


FIG. 33

68. I further understand that Patent Owner relied on new matter introduced by the '638 application, including Figure 31B, throughout prosecution of the '638 application to support claims concerning the “access code.” *See, e.g.*, Ex. 1039, 1.

69. The contrast between the '638 Application and the earlier applications with respect to e-key disclosures is striking. The earlier applications simply do not contain any disclosures relating to electronic keys, much less requesting, generating, transmitting, and using e-keys.

70. Instead, the '158 application is directed to sending vehicle user profiles from a server to a mobile device that define settings for a vehicle, such as radio or comfort settings. Ex. 1015, Abstract. And the '882 application is directed to charging an electric vehicle. Ex. 1014, Abstract; Exs. 1012-13.

71. Although these earlier applications do not discuss e-keys at all, the '158 Application does sporadically disclose remotely accessing and/or starting a car

(including via a mobile device). However, these disclosures do not go into any detail as to how such functionality is accomplished, and certainly do not disclose that it is accomplished by requesting, generating, transmitting, and using an e-key. *See, e.g.*, Ex. 1015 at 42 (“In some embodiments, this allows verification that the user driving the vehicle 200, from the shared network, is the driver that unlocked the vehicle from a remote location (such as a mobile device).”); 28 (“Any vehicle can be abstracted so that any user can log into any vehicle if they have an account that allows access to that vehicle.”); 60-61 (“In one embodiment, the services provided by the electronic systems of a vehicle can include services that access the various components or subsystems of a vehicle, such as door locks, ..., auto-engine start/shut-off remotely via smart devices, ...”).

72. A POSITA in 2013 would in fact understand that remotely accessing/starting a car using a mobile device would not require the use of any e-keys. Instead, the most straightforward way to accomplish such functionality would be for the server to communicate with the vehicle to unlock or start the car, with the mobile device communicating with the server to trigger such functionality. Such systems were well-known by 2013. *See, e.g.*, 1010.

73. Accordingly, in my opinion, the '188 patent's claims are not entitled to a filing date before October 25, 2013. None of the applications prior to this date describe the subject matter of the Challenged Claims including “enabling access to

use the vehicle via one or more electronic keys.” The earliest priority date to which the asserted claims could be entitled is October 25, 2013. Thus, it is my opinion that the applicant was not in possession of the claimed subject matter.

74. I also understand that the Patent Office considered the effective priority date of descendent Patent No. 11,738,659 (the “’659 Patent) in granting Ex-Parte re-examination of the ’659 Patent. *See* Ex. 1017 at 4, fn.1 (“The disclosure of [U.S. Provisional App. No. 61/478,436] however ***appears to lack support*** for several limitations claimed in US Patent 11,738,659 requested for reexamination. These include for example an ‘eKey’, ‘coded data’, ‘unlocking’ or ‘starting’ of the vehicle and ‘privilege settings’.”). My conclusion is consistent with this finding.

75. To the extent Patent Owner argues an earlier priority date, I reserve the right to respond to those opinions.

D. Person of Ordinary Skill in the Art

76. I am informed that patentability must be analyzed from the perspective of “one of ordinary skill in the art” in the same field as the ’188 patent at the time of the invention. As previously discussed, the relevant time of invention is the patent’s priority date, which is no earlier than October 25, 2013. Moreover, I understand that whether or not a patent application provides “written description” support for patent claims must also be assessed from the perspective of a person of ordinary skill in the art.

77. I am also informed that several factors are considered in assessing the level of ordinary skill in the art, including (1) the types of problems encountered in the art; (2) the prior art solutions to those problems; (3) the rapidity with which innovations are made; (4) the sophistication of the technology; and (5) the education level of active workers in the field.

78. The '188 patent claims the benefit of U.S. Provisional Application No. 61/478,436 (Ex. 1010) filed April 22, 2011, U.S. Provisional Application No. 61/745,729 (Ex. 1011) filed December 24, 2012, U.S. Application No. 13/452,882 (Ex. 1012) filed April 22, 2012, and U.S. Application No. 13/842,158 (Ex. 1013) filed March 15, 2013. However, as discussed herein, in my opinion, the challenged claims of the '188 patent are not entitled to a priority date any earlier than October 25, 2013.

79. Regardless of whether the priority date(s) for the challenged claims is October 25, 2013 or April 22, 2011 (or any date in between), a person of ordinary skill in the art pertinent to the '188 patent would have had at least a four-year undergraduate degree in electrical engineering, automotive engineering, or a closely related field and at least two years of experience in the fields of access control systems, vehicle electronics, and/or cryptography. Additional education could substitute for professional experience and vice versa. A person of ordinary skill in the art would also be able to understand and apply the prior art discussed herein.

80. Although I surpass this definition of one of ordinary skill in the art now and at the priority date of the '188 patent, my analysis regarding the '188 patent has been based on the perspective of one ordinary skill in the art as of the priority date of the '188 patent.

81. I am also familiar with the knowledge of the person of ordinary skill in the art as of the priority date of the '188 patent. I am able to opine on how the person of ordinary skill in the art would have understood the disclosure and claims of the '188 patent, the disclosures of the prior art, the motivation to combine the prior art, and what combinations would have been obvious to one of ordinary skill in the art.

82. My conclusions as to the profile of a person of ordinary skill in the art would be the same regardless of the priority date. Moreover, I had or surpassed the level of skill of a person of ordinary skill in the art at all potentially relevant times, including as far back as April 22, 2011.

VI. Claim Construction of Terms of the '188 patent

83. As I discussed above, I have been informed that for purposes of *inter-partes* reviews, 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 have been asked to assume that the claim terms otherwise have their plain and ordinary meaning to a person skilled in the art in light of the specification and the prosecution history.

84. As of this time, I am not aware of any term that requires specific construction for my opinions. To the extent Patent Owner suggests a narrow construction for a term, I reserve the right to respond to those opinions.

VII. Overview of Prior Art

85. Below, I discuss the two primary references I rely on.

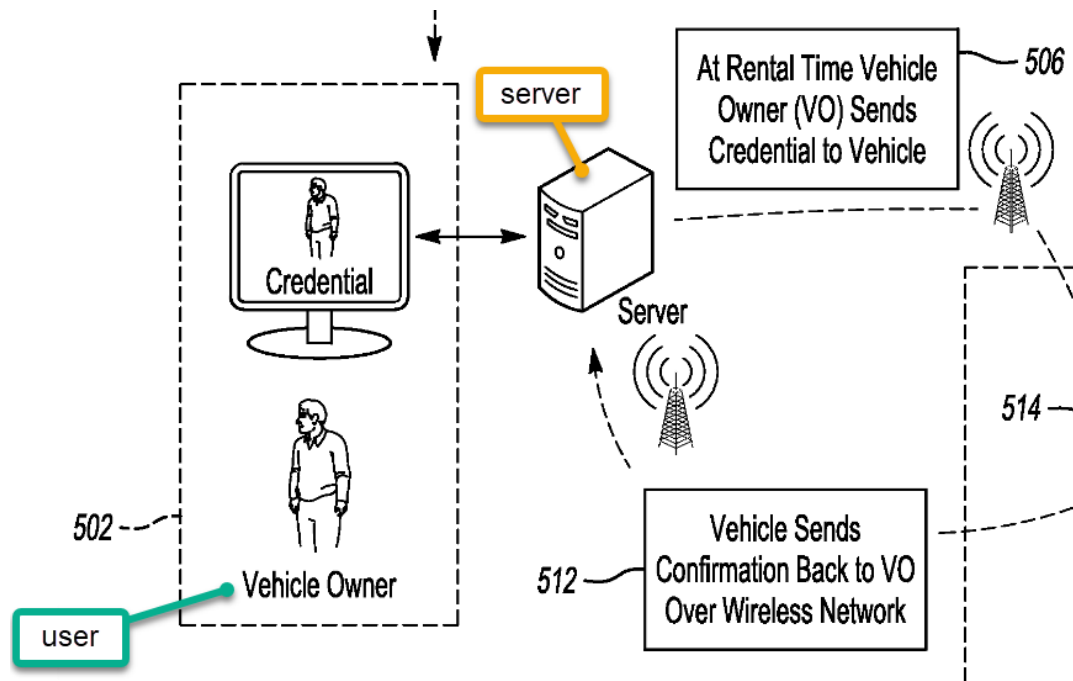
A. Kleve

86. *Kleve* discloses a “vehicle rental micro-business” which “include[s] a website, smart phone application or other nomadic device that an Owner and Temporary User may use to manage their assets and/or user profile.” Ex. 1004 (*Kleve*), ¶ [0035]. The “Owner” is a Vehicle Owner and “may set up a **user profile** using a website ... that is stored in a database,” which includes “the make, model and year of the vehicle available for rent.” *Kleve*, ¶ [0037].

87. A Temporary User likewise “setups their user identity within the website” after which they “may begin to use the vehicle rental services.” *Id.*, ¶ [0047]. Upon selection of a vehicle to rent, “the Temporary User and vehicle Owner agree to terms 316,” and then the agreement “can be signed and payment made through the website.” *Id.*

88. The Temporary User then sends “authorization credentials” to the Vehicle Owner, who enters in that information to the server “to set up a virtual key.” *Id.*, ¶ [0062]. The “virtual key may be sent to the vehicle allowing Temporary User

access to the Owner's vehicle.” *Id.* The Temporary User “may use their virtual key credential to access the vehicle,” and may also use it to “enable the vehicle drive away event.” *Id.*, ¶ [0067], [0044].



89. *Kleve* discloses a number of restrictions that can be associated with the rental agreement, including the “rental period” (¶ [0038]), “speed, global position coordinates, or load weight restrictions” (¶ [0040]), “destination location” (¶ [0051]), “prohibited areas where the owner does not want their vehicle to be used” (¶ [0073]), and “top vehicle speed, limiting the cargo load, and alerting the vehicle owner if the driver enters an area deemed to be prohibited by the owner” (¶ [0075]).

90. The vehicle will monitor usage of the vehicle to determine any violations of such restrictions, and upload such information to the server, including

“GPS data” and “the Temporary User’s behavior during the rental period.” *Id.*, ¶ [0076], [0078]. Such information also includes information about “unauthorized objects or cargo, unauthorized driving behavior, unauthorized driver, and/or an unauthorized trailer tow.” *Id.* at ¶ [0076]; *see also* ¶ [0040] (“[T]he control parameters use restrictions may be monitored and if a restriction exceeds a limit the Temporary User and Owner may be notified.”).

91. If a restriction is violated, the system will notify the both the Temporary User and Owner. *Id.* If the rental period ends, “the monitoring and control system of the vehicle rental micro-business may begin to start its Temporary User vehicle rental exit mode process at step 728.” *Id.*, ¶ [0080]. This exit mode process includes monitoring “vehicle location, fuel level, and additional vehicle diagnostic information.” *Id.* In another example, Kleve discloses that monitoring occurs “for the entire rental period” and if “the rental period is soon to expire,” the system may notify the Temporary User and vehicle Owner. *Id.*, ¶ [0054].

B. Zaid

92. *Zaid* discloses a car sharing system where renters use their mobile devices to find available vehicles, rent them for specified periods of time, and use their mobile devices to unlock and start the shared vehicles. Ex. 1006 (*Zaid*), ¶¶ [0067-69]. During the rental period, a user’s mobile device receives an electronic

key from a server and sends an encrypted vehicle reservation to the vehicle for access and use during the rental period. *Id.*, ¶ [0070].

93. *Zaid* discloses a “vehicle access kit” 102 within **vehicle 100**. The vehicle access component can be added to a commercially available vehicle to permit electronic unlocking and starting of a vehicle from a mobile device and without a physical key. *Zaid*, ¶ [0075]. The vehicle access component receives a vehicle reservation from a user’s **wireless communication device 106**, which can be a smartphone. *Zaid*, ¶¶ [0082, 0135]. The wireless communication device 106 communicates via a **cloud network 114** with a remote central server 110 (**yellow**).

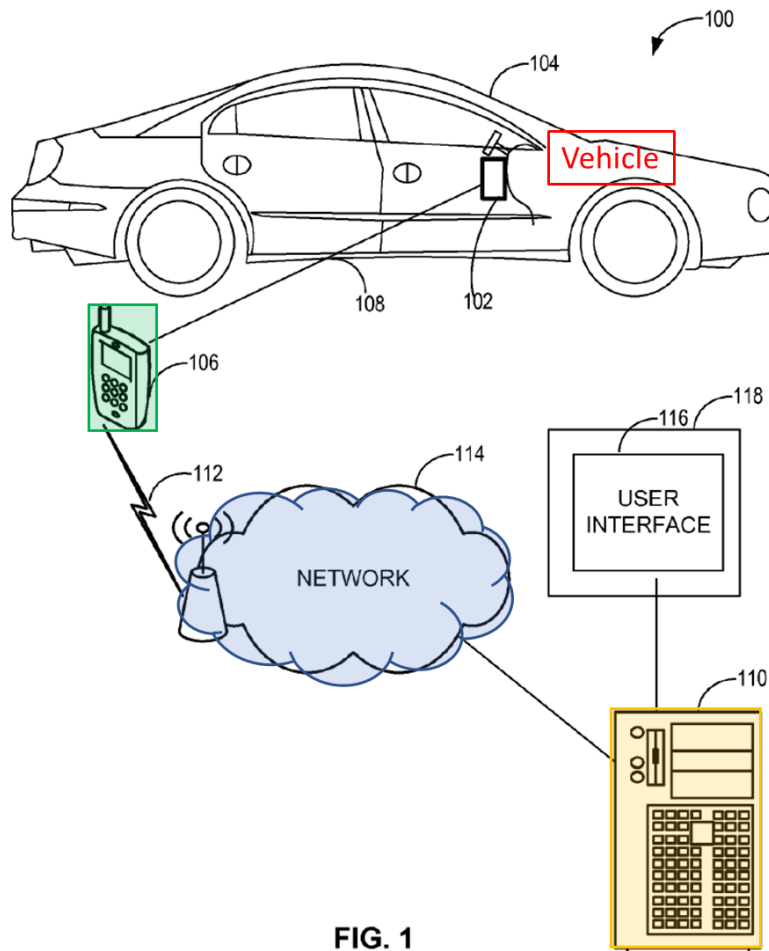


FIG. 1

Zaid, Figure 1 (annotated).

94. *Zaid*'s central server interacts with vehicle access control systems on many vehicles to provide rental options for users across a town or city. *Zaid*, ¶ [0080]. In a typical use case, a customer uses their wireless communication device 106 to search for available vehicles. *Id.*, ¶ [0077]. They make a reservation for a certain vehicle, which is communicated to the central server 110. *Id.*, ¶ [0076]. The central server 110 sends an encrypted vehicle reservation to a vehicle via the wireless communication device 106. *Id.* The vehicle access component 102 then decrypts the

request and, if authentic, permits the user to unlock and start the vehicle, but only for the specific time-period that the user requested and paid for. When the time-period elapses, access is withdrawn and the renter can no longer unlock or start the vehicle. *Id.*, ¶ [0131].

95. *Zaid* discloses that “communications, including vehicle reservation communications, received from the wireless communication device by the vehicle access control system for vehicle access control includes [sic] a unique increment for each message to avoid repeat message attack. In various embodiments, the unique increment is in the form of a counter and/or time stamp that indicate the uniqueness of the message to avoid a repeat message attack.” *Zaid*, ¶ [0081]. Thus, each vehicle reservation is unique.

96. *Zaid*’s vehicle access component can be integrated into a “vehicle access kit,” illustrated in Fig. 2 and shown containing electronic components such as a microprocessor, memory, and a communication interface which can be WiFi or Bluetooth for communicating to a remote server via the user’s mobile device. *Id.*, Fig. 2, ¶ [0087]. A long-range communication function can be added to the communication interface to “act as a backup” in case communication via the user’s mobile phone is unavailable. *Id.*, ¶ [0106].

97. The remaining cited references, *Sekiyama* (Ex. 1005), *Harris* (Ex. 1007), *Mottla* (Ex. 1008), and *Patenaude* (Ex. 1009), demonstrate other well-known

elements of vehicle communication systems present in the art, namely, generating an electronic key at a server (claim 1[b]), requesting an electronic key using identifying information (claim 1[a]), sending notifications to vehicles in the event of a restriction violation (claims 2, 4, and 8), graphical icons for unlocking the vehicle (claim 10), and learning patterns of vehicle settings based on user inputs (claim 17), respectively.

VIII. Summary of Opinions on Unpatentability

98. In the analysis that follows, I identify the following combinations of prior art that, in my opinion, anticipate and/or render obvious the '188 patent claims:

Grounds of Unpatentability	
1	<i>Kleve</i> renders obvious claims 1-9, 11-20 under Section 103
2	<i>Kleve</i> and <i>Sekiyama</i> render obvious claims 1-9, 11-20 under Section 103
3	<i>Kleve</i> (with or without <i>Sekiyama</i>) and <i>Mottla</i> render obvious claim 10 under Section 103
4	<i>Zaid</i> and <i>Harris</i> render obvious claims 1, 3, 5-7, 9, 11-16, 18-20 under Section 103
5	<i>Zaid</i> , <i>Harris</i> , and <i>Mottla</i> render obvious claims 2, 4, 8, and 10 under Section 103
6	<i>Zaid</i> , <i>Harris</i> , and <i>Patenaude</i> render obvious claim 17 under Section 103
7	<i>Kleve</i> and <i>Patenaude</i> render obvious claim 17 under Section 103

A. Ground 1: Kleve renders obvious claims 1-9 and 1120 under Section 103

99. A summary of this ground is as follows: *Kleve*'s system allows vehicle rentals between Vehicle Owners and Temporary Users. Through a website account, Vehicle Owners list vehicles to rent, and Temporary Users select a vehicle. They negotiate a rental agreement through the website, including conditions of use like a rental period. Upon agreement, the Temporary User provides identifying information to the Vehicle Owner who submits it to the server to generate a virtual key. The virtual key is sent to the Temporary User's device and the vehicle to allow access and control.

1. Independent Claim 1

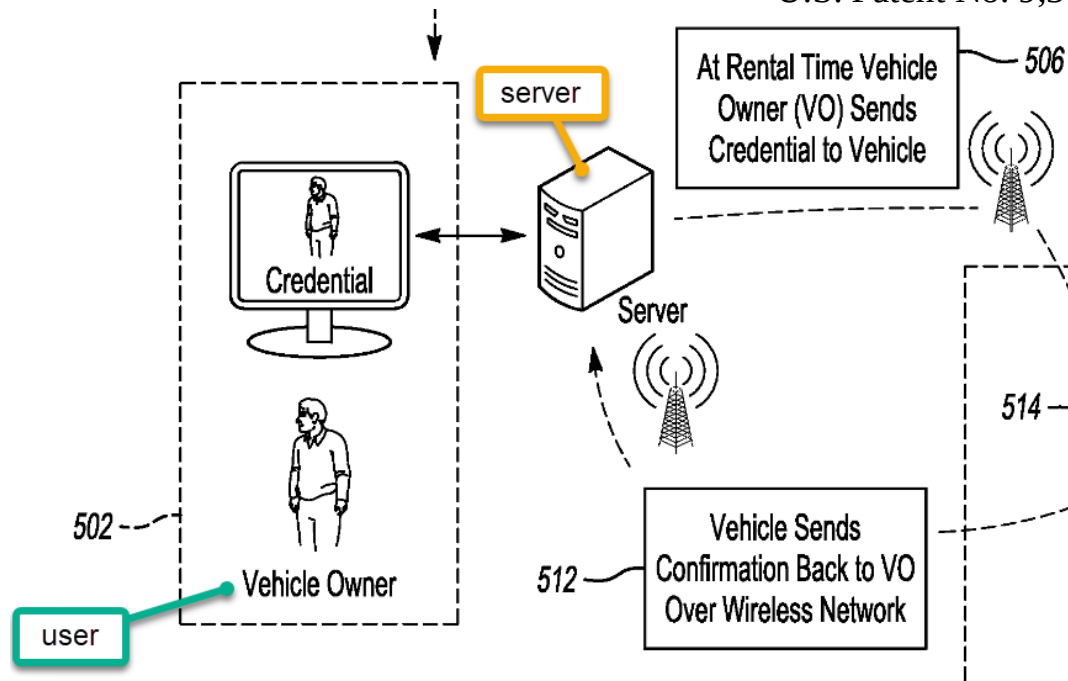
1[pre] / 1[a]: "A method, comprising, receiving, by a server, a request from a user via a user account that has a vehicle associated therewith to generate an electronic key (e-key) for an identified recipient to use the vehicle, the request includes identifying information for enabling sending of the e-key to the recipient via an electronic transmission, the request includes a condition of use of the vehicle as set by the user via the user account"

100. Given the length of this limitation, I divide it into smaller portions. First, I will analyze the limitation "receiving, by a server, a request from a user via a user account that has a vehicle associated therewith to generate an electronic key (e-key) for an identified recipient to use the vehicle." I will also divide up this limitation.

- i. **receiving, by a server, a request from a user via a user account that has a vehicle associated therewith to generate an electronic key (e-key) for an identified recipient to use the vehicle**

101. In my opinion, *Kleve* discloses or renders obvious this limitation. In sum, *Kleve* discloses that a server receives a request from Vehicle Owner (the claimed **user**) via their user profile (**user account**) associated with a vehicle. This request results in the server generating a virtual key (**e-key**) for an identified Temporary User (**identified recipient**) to use the owner's vehicle.

102. *First*, it is my opinion that *Kleve* discloses a “server.” For example, *Kleve* discloses “a vehicle rental micro-business” which comprises a server. *Kleve*, ¶ [0035] (“[T]he exemplary processes may be executed by a ... remote computing system (e.g., ... **a server**).”); ¶ [0036] (“The vehicle rental micro-business 200 may include a website.”); ¶ [0069] (“server 634.”). The below excerpt from Figure 5 depicts the vehicle owner interacting with the server.



103. Second, it is my opinion that *Kleve* discloses a “user account that has a vehicle associated therewith.” *Kleve* discloses that a vehicle owner may create a user profile (**user account**) with the server, and **associate a vehicle** with the profile. Specifically, *Kleve* discloses that the vehicle owner “may set up a **user profile** using a website or a nomadic device communicating with the site that is stored in a database,” which includes “the make, model and year of the vehicle available for rent,” i.e. **a user account that has a vehicle associated therewith**. *Id.*, ¶ [0037].

104. In my opinion, a POSITA would understand that the website and database are part of a server system, because it was known websites were hosted on servers and interacted with database servers. In other words, the various systems

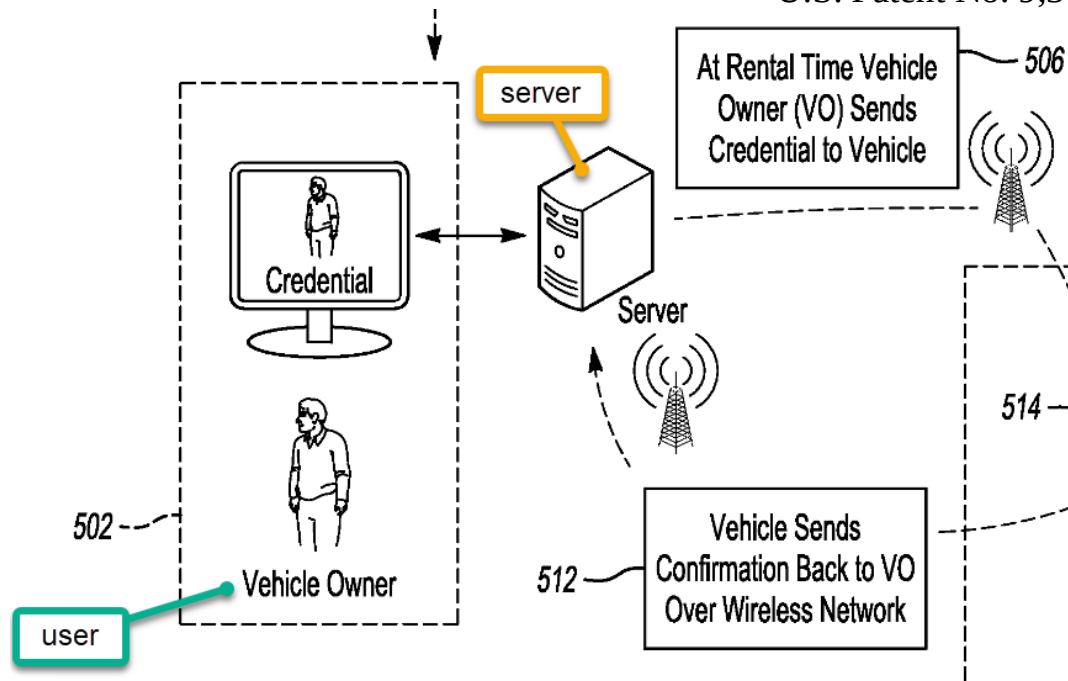
disclosed in *Kleve* for establishing user profiles for renting cars are collectively a **server**.

105. *Third*, in my opinion, *Kleve* discloses an “*identified recipient*.” *Kleve* discloses that a Temporary User can identify himself to create a user profile for browsing and renting a car, making him an ***identified recipient***. *Kleve* states that the “vehicle micro-business 200 may include a process for collecting ***identification*** and payment from Temporary User 204,” including “fill[ing] out a user profile using the website ... to include ... 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.” *Id.*, ¶¶ [0036-0037].

106. *Kleve* discloses that the “Temporary User” uses his user profile to browse available cars on the server and negotiate a rental agreement with the vehicle owner. Specifically, “the Temporary User may begin to use the vehicle rental services” by “brows[ing] the database of available vehicles to rent.” *Id.*, ¶ [0047]. When the Temporary User selects a vehicle, “the Temporary User and vehicle Owner agree to terms 316,” and then the agreement “can be signed and payment made through the website.” *Id.* Thus, *Kleve* discloses that a vehicle owner’s ***user***

account is used to host vehicle information and allow the vehicle owner to come to an agreement with a temporary user for vehicle rental.

107. *Fourth*, in my opinion, Kleve discloses “receiving, by a server, a request from a user via a user account ... to generate an electronic key.” Once there is an agreed rental agreement, the vehicle Owner (**user**) sends a request to the server via their user profile (**user account**) to generate a virtual key, *i.e.* **an electronic key (e-key)**. Specifically, after “the vehicle Owner ... ha[s] already setup a user profile within the database” and after the vehicle Owner and Temporary User have “agreed to the rental agreement,” “[a]t step 502, the vehicle Owner may enter in vehicle authorization credentials based on information received by the Temporary User **to set up a virtual key.**” *Id.*, ¶ [0062]. Kleve further states that such identification is “entered into the server.” *Id.*, ¶ [0063]. The entering of this information is a **request sent by the user** to generate a virtual key. As depicted in Figure 5 (annotated below), step 502 shows the credential is sent to the server via a computer that is communicating with a server (such as via a website).



108. In my opinion, a POSITA would understand that the request for a virtual key is made *via a user account*. *Kleve* states that, in the Figure 5 embodiment, receiving the virtual key is contingent on the vehicle Owner “already set[ting] up a user profile,” i.e. *a user account*. *Id.*, ¶ [0062]. A POSITA would further understand that the server would need to receive the request from a user profile in order to know which vehicle to generate a virtual key and which temporary user to grant the virtual key, since it is the vehicle owner’s user profile for which has information about the vehicle as well as the rental agreement between the vehicle owner and temporary user. *Id.*, ¶¶ [0037-38].

109. It is also my opinion that a POSITA would have found it obvious that the request is made via a user profile (*user account*). By requiring that the request

is made via the Vehicle Owner's profile, that indicates that the Vehicle Owner has authorized the identified Temporary User to receive a virtual key for a specific vehicle. Moreover, because the Temporary User, vehicle, and rental agreement are already associated with the Vehicle Owner's user profile, requests from that user profile can contain all of the necessary information for the server to provide the virtual key. This further provides the well-known benefits of increasing security, reliability and user satisfaction, because requests made from the Vehicle Owner's user profile can be relied on as having been authorized by the actual Vehicle Owner when using conventional, well-known methods for securing a user account (such as requiring strong passwords and 2-factor authentication). Finally, requiring that the Vehicle Owner's user profile request the virtual key would be reasonably expected to succeed as such a configuration was the default and conventional method for users to interact with a server-based reservation system. Such a configuration would have been well-within the capabilities of a POSITA.

110. It is my opinion that a POSITA would further understand that *Kleve* discloses that the server generates the virtual key (***electronic key***). *Kleve* discloses that Temporary User identification is "entered into the server and ***used as a virtual key***, or in addition to the virtual key," which a POSITA would understand to mean the server receives the identification to generate and accompany the virtual key. *Kleve*, ¶ [0063]. *Kleve* further states that the "virtual key may be sent ... to the VCS

[vehicle-based computing system], Temporary User's nomadic device, and/or vehicle Owners nomadic device," thereby indicating that it is the server which generates the virtual key and sends it to those various destinations. *Id.* This is because it would not be necessary for the virtual key to be sent to the Vehicle Owner's device if the Vehicle Owner's device had generated it.

111. I understand that *Kleve* states that the "[V]ehicle Owner may then generate a virtual key." *Id.*, ¶ [0069]. In my opinion, this disclosure is best understood as the Vehicle Owner generating a virtual key by requesting one from the server as I discussed above. In addition, to the extent Patent Owner argues that paragraph 69 should be understood as the Vehicle Owner's device generating the virtual key, I note that this disclosure is stated as optional and does not change the understanding of ¶ [0063] that I discuss above.

112. It is also my opinion that a POSITA would have found it obvious to generate the virtual key at the server (rather than the Vehicle Owner's device). Generating the key requires that the Vehicle Owner enter "authorization credentials" from the Temporary User into the server, and the server stores the Temporary User's user profile that contains recorded copies of those credentials (such as "photos of credit cards, photo of forms of ID," etc.) to confirm the Temporary User's identity. *Kleve*, ¶¶ [0062], [0037]. Thus, a POSITA would be motivated to have the server generate the key since the server (1) maintains the identity of the Vehicle Owner (by

the request being sent via a user account), (2) maintains the identity of the Temporary User (via the authorization credentials), and (3) confirms that they have entered into a rental agreement for a specific vehicle.

113. A POSITA would have known that, by having the server generate the virtual key (instead of the Vehicle Owner's device), this increases security, reliability and user satisfaction since the server can confirm all the necessary information needed before providing the virtual key. The server can confirm that the actual Vehicle Owner authorized the issuance of the virtual key because the request was sent from the Vehicle Owner's user account. The server can further confirm that the actual Temporary User is being issued the virtual key because the server has the identification information from the Temporary User, which it can then match with the saved identification information stored in the server's database. Finally, the server can confirm that the Vehicle Owner and Temporary User have an actual rental agreement. All of these are desirable and indeed necessary steps to ensure that the issuance of virtual keys is done in a secure manner. Issuing an unauthorized virtual key would be disastrous to the Vehicle Owner (and therefore the rental system) because of the cost of vehicles. And because the server is the only one disclosed by *Kleve* as having all the necessary information to authenticate all necessary information, a POSITA would be motivated by convenience and efficiency to have the server generate the virtual keys. Having the server generate

the key would also provide the known benefit of increasing reliability, because it would not require the availability of the Vehicle Owner's personal device—including its ability to access the Internet to communicate with the vehicle and the Temporary Owner's device.

114. In my opinion, having the server generate the virtual key would be reasonably expected to succeed. Because the server receives all the necessary information, the server need only perform the conventional and well-known task of authenticating such information, which would have been well within the knowledge of a POSITA and could have used numerous existing standards and solutions. In addition, *Kleve* discloses and enables authenticating identifying information and generating a virtual key, and thus performing such actions at the server is a mere design choice. I further note that the '188 patent does not purport to advance the state of the art with respect to authentication and instead relies on known standards and solutions.

115. *Fifth*, in my opinion, *Kleve* discloses an “*electronic key (e-key) for an identified recipient to use the vehicle.*” *Kleve* discloses that the virtual key (***electronic key***) allows the recipient to ***use the vehicle.*** For example, *Kleve* discloses that “the Temporary User may use their virtual key credential to ***access the vehicle.***” *Id.*, ¶ [0067]. Once the vehicle is accessed, the user may enter a credential to “verify that the Temporary User has approval to ***use the vehicle.***” *Id.* *Kleve* further states

generally that the virtual key is “used to enter and enable the vehicle **drive away event**.” *Id.*, ¶ [0044].

ii. **the request includes identifying information for enabling sending of the e-key to the recipient via an electronic transmission**

116. In my opinion, *Kleve* discloses that as part of the request, the vehicle owner can include the Temporary User’s identifying information to enable sending of the virtual key (**e-key**) to the Temporary User. *Id.*, ¶¶ [0062-63]. Specifically, the request sent to the server includes “vehicle authorization credentials based on information received by the Temporary User” which is used “to setup a virtual key,” thus **enabling the sending of that key**. *Id.*, ¶ [0062]. Such “authorization credentials” are **identifying information** because it includes “fingerprint recognition of user, photos of credit cards, photo of forms of ID, facial recognition, voice print recognition,” etc. *Id.*, ¶ [0063]. *Kleve* also discloses that the virtual key may be sent to the Temporary User “through an email,” thus indicating that the request includes an email address as **identifying information**. *Id.*, ¶39.

117. *Kleve* further discloses that the virtual key is sent to the temporary user **via an electronic transmission**. *Kleve* states that the virtual key “may be sent in an encrypted message to the ... Temporary User’s **nomadic device**,” which is a wireless device such as a “cell phone, smart phone, PDA, or any other device having **wireless remote network connectivity**.” *Id.*, ¶¶ [0063], [0025]. A POSITA would understand

that an encrypted message sent over a wireless connection is ***an electronic transmission***.

iii. the request includes a condition of use of the vehicle as set by the user via the user account

118. In my opinion, *Kleve* discloses that a vehicle owner may set ***conditions of use of the vehicle*** via the owner's user profile, which are part of the request for generating the virtual key. Specifically, *Kleve* discloses that a vehicle owner and temporary user can, via their website user profiles (***user accounts***), negotiate a rental agreement which includes various restrictions (***conditions of use of the vehicle***). *Id.*, ¶ [0038] ("The Owner and Temporary User may agree to terms and conditions for the rental period ***using the website***."); ¶ [0047] ("The agreement between the Owner and Temporary user can be signed ... ***through the website***."); ¶ [0062] ("vehicle Owner and Temporary User have already setup a user profile within the database and have both agreed to the rental agreement.").

119. *Kleve* describes numerous restrictions that are associated with the rental agreement, including the "rental period" (¶ [0038]), "what can and cannot be transported" (*id.*), "speed, global position coordinates, or load weight restrictions" (¶ [0040]), "destination location" (¶ [0051]), "prohibited areas where the owner does not want their vehicle to be used" (¶ [0073]), and "top vehicle speed, limiting the

cargo load, and alerting the vehicle owner if the driver enters an area deemed to be prohibited by the owner” (¶ [0075]).

120. In my opinion, *Kleve* discloses that such restrictions are sent with the request to generate a virtual key. Specifically, *Kleve* discloses that the virtual key “enable[s] the keyless drive system for the appropriate Temporary User **during a given rental period**,” which indicates that rental agreement restrictions were sent with the request so that the virtual key could be associated with said restrictions. *Id.*, ¶ [0039]; *see also id.* ¶ [0068] (“Once the rental period has expired the virtual key may be reset and cleared from the VCS.”). Moreover, *Kleve* discloses that the virtual key is always generated after the rental agreement. *See, e.g., id.* (“[O]nce the Temporary User selects the vehicle, pays the appropriate amount and signs a consent agreement, then the system may generate a virtual key to distribute to the Temporary User and VCS.”).

121. In my opinion, a POSITA would have understood that the rental agreement restrictions are also sent with the request in order that the generated virtual key can be associated with such restrictions, which allows the restrictions to be monitored and enforced. *See id.*, ¶¶ [0040-43] (describing how the central system monitors and enforces the restrictions).

122. In my opinion, a POSITA would have also considered it obvious to include the restrictions with the virtual key request, because that would provide the

well-known benefits of associating the virtual key with the restrictions such that the central system knows which restrictions must be enforced with which virtual keys. This allows the server to monitor and enforce the restrictions, which as I mentioned above are important aspects of Kleve's system. Moreover, a POSITA would have been motivated by the well-known benefits of monitoring and enforcement, including increased reliability and efficient of the rental system by encouraging and inducing renters to comply with the restrictions or pay a penalty if the restrictions are violated.

123. It is also my opinion that including the restrictions with the virtual key request would have been reasonably expected to succeed by a POSITA. Including such information with the request would have required no more than a conventional implementation well within the skills of a POSITA, as network requests including all manner of different types of information were well-known and easy to implement, especially using publicly-available network APIs. The implementation could simply be, for example, using a network data structure that could hold both the enumerated restrictions and the virtual key request, which would have been trivial for a POSITA.

1[b]: “generating, by the server, the e-key, the e-key being assigned with the condition of use of the vehicle;”

124. In my opinion, *Kleve* discloses or renders obvious this limitation. As I discussed above, *Kleve* discloses or renders obvious a server that generates a virtual key (***e-key***) and assigns to it the rental agreement restrictions (***condition of use of the vehicle***), including the rental period. See, e.g., *Kleve*, ¶ [0063] (“this information to be entered into the server and used as a virtual key, or in addition to the virtual key”); ¶ [0039] (“The virtual key may also be sent to the vehicle configuring the VCS to enable the keyless drive system for the appropriate Temporary User during a given rental period.”).

1[c]: “transmitting, by the server, the e-key to the recipient using the identifying information so that a device of the recipient is implemented to use the e-key;”

125. In my opinion, *Kleve* discloses this limitation. As I discussed above for the limitation “the request includes identifying information for enabling sending of the e-key to the recipient,” *Kleve* discloses ***transmitting, by the server, the e-key to the recipient using the identifying information***, and specifically to the Temporary User’s nomadic device (***device of the recipient***). See, e.g., *Id.*, ¶¶ [0062-63].

126. *Kleve* further discloses that when the Temporary User’s nomadic device receives the virtual key, it can be used to access the vehicle, *i.e.* the device ***is implemented to use the e-key***. For example, *Kleve* discloses that the “virtual key may be sent in an encrypted message to the ... Temporary User’s nomadic device”

and that “the Temporary User may use their virtual key credential to access the vehicle.” *Id.*, ¶¶ [0063], [0067].

1[d]: “transmitting, by the server, data to the vehicle to enable use of the vehicle via the e-key; and”

127. In my opinion, *Kleve* discloses this limitation. *Kleve* discloses that the server transmits a copy of the virtual key ***to the vehicle to allow use of the vehicle via the virtual key*** when presented by the Temporary User. For example, *Kleve* discloses that the “virtual key may be sent to the vehicle allowing Temporary User access to the Owner's vehicle.” *Id.*, ¶¶ [0062], [0059], [0066]-[69]. As I discussed above for the limitation “electronic key (e-key) for an identified recipient to use the vehicle,” *Kleve* discloses that the virtual key enables the Temporary User to access and use the vehicle.

1[e]: “receiving, by the server, use data regarding use of the vehicle for when the vehicle is used via the e-key;”

128. In my opinion, *Kleve* discloses this limitation. *Kleve* discloses that the vehicle monitors the Temporary User's usage of the vehicle and uploads the monitoring data to the server. *Id.*, ¶¶36, 40, 42-43, 52. For example, *Kleve* discloses “continuous ***monitoring*** of the Temporary User's behavior during the rental period [*i.e., when the vehicle is used via the e-key*] may be ***transmitted to the server***” including transmitting “GPS data . . . to the server.” Ex. 1004, ¶76. *Kleve* discloses

monitoring and transmitting to the server the “vehicle speed, acceleration force, wheel speed, breaking, steering, vehicle weight, throttle and pedal position” to determine whether “the Temporary User is using the vehicle under extreme circumstances or if they are driving responsibly.” *Id.*, ¶78.

1[f]: “wherein the use data identifies information regarding the use of the vehicle, and the information identifies a violation of the condition of use;”

129. In my opinion, *Kleve* discloses this limitation. *Kleve* discloses that the monitoring data regarding use of the vehicle is used to identify violations of the restrictions in the rental agreement (***condition of use***). For example, *Kleve* discloses that the monitoring data includes ***information regarding use of the vehicle and identifies a violation*** such as “***unauthorized*** objects or cargo, ***unauthorized*** driving behavior, ***unauthorized*** driver, and/or an ***unauthorized*** trailer tow.” *Id.*, ¶ [0076]; see also ¶ [0040] (“[T]he control parameters use restrictions may be monitored and if a restriction exceeds a limit the Temporary User and Owner may be notified.”). The monitoring data (e.g., “vehicle speed, acceleration force, wheel speed, breaking, steering, vehicle weight, throttle and pedal position”) indicates whether “the Temporary User is using the vehicle under extreme circumstances or if they are driving responsibly.” *Id.*, ¶ [0078].

130. *Kleve* explains that, “if a restriction exceeds a limit the Temporary User and Owner may be notified” (*id.*, ¶40), which “allow[s] the Owner continued control

of the vehicle with the use of vehicle **restriction limits** initially set by the Owner at the beginning of the rental term” (*id.*, ¶43). *Id.*, ¶53. Kleve’s “restriction limits” may be based on, e.g., “speed, global position coordinates, or load weight restrictions.” For example, “[i]f the Temporary User enters a restricted area, he may be notified by the system and the vehicle may enter a remedial actions limiting vehicle speed.” *Id.*, ¶41. As a separate example, Kleve also uses the monitoring data to enforce the “end time restriction” by determining if the vehicle is still in use as the end of the rental period. *Id.*, ¶43. For example, *Kleve* discloses that “[i]f the rental period has ended, the monitoring and control system of the vehicle rental micro-business may begin to start its Temporary User vehicle rental exit mode process at step 728.” *Id.*, ¶ [0080]. This exit mode process includes monitoring “vehicle location, fuel level, and additional vehicle diagnostic information.” *Id.* In another example, Kleve discloses that monitoring occurs “for the entire rental period” and if “the rental period is soon to expire,” the system may notify the Temporary User and vehicle Owner. *Id.*, ¶ [0054].

1[g]: “wherein the server processes logic for generating the e-key and processes logic for analyzing the data regarding use of the vehicle when the e-key is used for the vehicle, the server or other servers connected to the server being accessible over the Internet, the vehicle having wireless communication systems for communicating with the server or other servers and for communicating with devices local to the vehicle.”

131. In my opinion, *Kleve* discloses or renders obvious this limitation. Due to the length of this limitation, I will again break it up into smaller parts.

- i. **wherein the server processes logic for generating the e-key and processes logic for analyzing the data regarding use of the vehicle when the e-key is used for the vehicle**

132. As I discussed above, *Kleve* discloses or renders obvious that the server generates the e-key (limitations 1[a] and 1[b]) and analyzes vehicle use data (1[f]).

133. *Kleve* further discloses or renders obvious that such functionality is performed by the server **processing logic**, such as execution of CPU instructions. For example, *Kleve* discloses “a computer readable storage medium for storing instructions that, when executed by a processor is configured to enable a vehicle rental transaction.” *Id.*, ¶ [0009]. A POSITA would have understood and considered it obvious that, the “instructions” refer to **logic processed** in the server for generating an ekey and analyzing data regarding vehicle use.

134. *Kleve* further discloses that the server is a “remote computing system,” which a POSITA would understand to be a conventional computer containing at least a CPU and memory. A POSITA would further understand that a “computing system” performs functions by **logic processing**, that is, executing CPU instructions.

135. A POSITA would also consider it obvious that a “server” or “remote computing system” performs its disclosed functions using **logic processing** because

that was the well-known and conventional means for a computer to perform functions. A POSITA would also find it beneficial to use a general-purpose computer (which uses a CPU to execute instructions) for a server because of the commodification of computer hardware and software, making such systems significantly cheaper and easy to access. A POSITA would have also reasonably expected such logic processing to succeed, because computing systems performing logic processing were conventional, ubiquitous and easy to implement.

ii. the server or other servers connected to the server being accessible over the Internet

136. In my opinion, *Kleve* discloses this limitation. *Kleve* discloses that the server system (including the website and database) are accessible over the Internet. For example, *Kleve* discloses that data to a server is “sent over the internet.” *Id.*, ¶ [0058]. *Kleve* also discloses that the server and the owner or temporary user’s devices can communicate via a “website,” which a POSITA would understand to be hosted on the Internet. *Id.*, ¶¶ [0036], [0030], [0056]. A POSITA would understand or at least consider it obvious that a website accessible by a cell phone would be accessible via the Internet.

iii. the vehicle having wireless communication systems for communicating with the server or other servers and for communicating with devices local to the vehicle.

137. In my opinion, *Kleve* discloses this limitation. *Kleve* discloses that a vehicle owner's vehicle wirelessly communicates with a server as well as a Temporary User's nomadic device (***devices local to the vehicle***). For example, with respect to the server, *Kleve* discloses that the "vehicle computing system located in a vehicle" communicates with "a remote computing system (e.g., and without limitation, a ***server***) connected through [a] ***wireless device***." *Id.*, ¶ [0035]. With respect to ***devices local to the vehicle***, *Kleve* discloses that the vehicle has a "BLUETOOTH transceiver" which "may allow communication with the nomadic device 403" such as "the Temporary User's nomadic device ... using a wireless connection." *Id.*, ¶ [0061]. *Kleve* also discloses that "the Temporary User's nomadic device may be paired with the VCS." *Id.*, ¶ [0072].

2. **Claim 2: "The method of claim 1, further comprising, sending a warning notification to the device of the recipient, or the vehicle, or both the device of the recipient, the warning notification identifying the violation of the condition of use."**

138. In my opinion, *Kleve* discloses this limitation. *Kleve discloses* that when a Temporary User violates a rental agreement restriction (***condition of use***), the system will provide a warning notification to the Temporary User or vehicle. Specifically, *Kleve* discloses that "the control parameters use restrictions may be monitored and if a restriction exceeds a limit ***the Temporary User*** and Owner may be notified," such as "[e]mail notification, text messages or ***an in-vehicle display***

message.” *Id.*, ¶ [0040]. As one example, *Kleve* discloses that, when monitoring the rental period, if “the rental period is soon to expire,” the system may notify the Temporary User and Vehicle Owner. *Id.*, ¶ [0054].

3. **Claim 3: “The method of claim 1, wherein the request to generate the e-key is received from the user account that is one of an administrator of the vehicle, or an owner of the vehicle, or a rental car operator of the vehicle, or a fleet operator for the vehicle, or a user account holder that has the vehicle associated thereto, or a user authorized to request e-keys for the vehicle.”**

139. As I discussed above for limitation 1[a], *Kleve* discloses the limitation “receiving, by a server, a request from a user via a user account ... to generate an electronic key,” and further discloses that the request is made via the vehicle owner’s user profile (*user account of an owner of the vehicle*). See, e.g., *Kleve*, ¶ [0062].

4. **Claim 4: “The method of claim 1, further comprising, sending data to one or both of the vehicle and the device of the recipient to notify that the e-key will become disabled due to the violation of the condition.”**

140. In my opinion, *Kleve* discloses or renders obvious this limitation.

141. *Kleve* discloses that when the rental period is expired (*violation of the condition*), the Temporary User (*recipient*) is notified of such, which will disable the virtual key. Ex. 1003, ¶¶140-41. Specifically, “if a restriction exceeds a limit the Temporary User and Owner may be notified.” Ex. 1004, ¶40. These notifications may be sent “through the website, with an email notification, or on the Owner’s

nomadic device at step 220.” *Id.* Further, “the system may send a message to issue a warning to the Temporary User notifying of unauthorized usage of the vehicle at the display information center, instrument cluster [of the vehicle], and/or other driver display device.” *Id.*, ¶53. Kleve further discloses terminating the virtual key if the vehicle detects usage after the rental period expires, and also providing notification thereof. *Id.*, ¶¶54-55.

142. Kleve also discloses that the system may “warn and induce remedial actions” in response to a violation. *Id.*, ¶54. Remedial actions include “preventing the vehicle from being started [i.e., **disabling the ekey**].” *Id.*, ¶53, 41-42. A POSITA would find it obvious that these warnings would include a notification that of the “remedial action,” as that would provide the known and straightforward benefit of informing the Temporary User of the possible consequences of continuing to violate the rental conditions. A POSITA would understand that such warnings would induce desired behavior, such as slowing down, returning to an agreed geographic area, or returning the vehicle at expiration of the rental period. A POSITA would further reasonably expect such notifications to succeed because providing notifications were conventional and easy to implement, as notifications are already disclosed in Kleve. The only necessary modification would be changing the text of the notification to warn of the impending remedial action – an adjustment well within the abilities of a POSITA.

143. A POSITA would have understood Kleve's "preventing the vehicle from being started" to be implemented by ***disabling the e-key***, since that is the mechanism for starting the vehicle is enabled. Further, a POSITA would have understood that it is preferable to allow the Owner to start the vehicle while preventing the Temporary User. Ex. 1004, ¶45. For example, a vehicle having been "preventing the vehicle from being started" due to a Temporary User traveling outside of the agreed geographic area would need to be retrieved by the owner. As such, a POSITA would understand that "preventing the vehicle from being started" must not disable the vehicle outright, but rather disable only the virtual key associated with the Temporary User.

5. **Claim 5: "The method of claim 1, wherein the condition of use is one of a geographic restriction for where the vehicle is allowed to be used, or a speed restriction, or an occupancy restrictions, or a time frame of use, or a time expiration of use, or combinations thereof."**

144. In my opinion, *Kleve* discloses this limitation. As I discussed above for the limitation "condition of use of the vehicle as set by the user via the user account," the Vehicle Owner and Temporary User may negotiate a set of restrictions, including a "rental period" (***time frame of use / time expiration of use***), "speed" (***speed restriction***), and "global position coordinates" or "prohibited areas" (***geographic restriction***). *Id.*, ¶¶ [0038], [0040], [0051], [0073].

6. **Claim 6: "The method of claim 1, wherein the identifying**

information includes one or more of an email address, a phone number, a text, a message address, a notification, a link, a web address, a social network address, or combinations thereof.”

145. In my opinion, *Kleve* discloses this limitation. As I discussed above for the limitation “the request includes identifying information,” *Kleve* discloses that the request includes *identifying information* such as *an email address*. *Id.*, ¶ [0039].

7. **Claim 7: “The method of claim 1, wherein receiving use data for use of the vehicle for when the vehicle is used via the e-key includes one or more of a history of where the vehicle has been, or speeds of the vehicle, or events of the vehicle, or multiple violations of the condition of use, or combinations thereof.”**

146. In my opinion, *Kleve* discloses this limitation. As I discussed above for limitations 1[e] and 1[f], the received use data includes “GPS data” (*history of where the vehicle has been*), “vehicle speed” (*speeds of the vehicle*), or various “unauthorized” behaviors (*multiple violations of the condition of use*). *Id.*, ¶¶ [0076], [0078].

8. **Claim 8: “The method of claim 1, further comprising, sending messages to one or both of the vehicle and the device of the recipient regarding warnings of when the use of the vehicle may exceed, has exceeded, or is about to exceed the condition of use.”**

147. In my opinion, *Kleve* discloses this limitation. As I discussed above for claim 2, *Kleve* discloses that the system will send a warning to the vehicle or device of the recipient when use of the vehicle has violated a restriction (*exceed the*

condition of use). *Id.*, ¶ [0040] (“the control parameters use restrictions may be monitored and if a restriction exceeds a limit *the Temporary User* and Owner may be notified,” such as “[e]mail notification, text messages or *an in-vehicle display message*.”).

9. **Claim 9: “The method of claim 1, wherein the e-key provides access to at least one of operating functions of the vehicle, or opening the vehicle, or starting the vehicle, or using user interfaces of the vehicle, or turning-off the vehicle, or combinations thereof.”**

148. In my opinion, *Kleve* discloses this limitation. As I discussed above for the limitation “electronic key (e-key) for an identified recipient to use the vehicle,” *Kleve* discloses that the virtual key (*e-key*) allows the Temporary User to “access the vehicle” (*opening the vehicle*) and “enable the vehicle drive away event” (*starting the vehicle*). *Id.*, ¶¶ [0067], [0044].

10. Claim 11

11[a]: “The method of claim 1, wherein the device is one of a smartphone, or a smartwatch, or smart glasses, or a portable device, or a computer, or a digital assistant, or a key fob,”

149. In my opinion, *Kleve* discloses this limitation. As I discussed above, *Kleve* discloses that the Temporary User’s nomadic device which receives the virtual key can be a “*cell phone, smart phone*, PDA, or any other device having wireless remote network connectivity.” *Id.*, ¶¶ [0063], [0025].

11[b]: “and wherein the e-key, once used via the device of the recipient, the e-key cannot be used via another device or sent to another device to enable use of the e-key without receiving new data from the server to reactivate the e-key.”

150. In my opinion, *Kleve* discloses or at least renders obvious this limitation.

151. *Kleve* discloses that once the virtual key is used by the recipient, such as the expiration of the rental period, the “virtual key may terminate,” *i.e.* the key is deactivated and ***cannot be used via another device or sent to another device***. *Kleve*, ¶ [0049].

152. *Kleve* further discloses that the virtual key is specific to the Temporary User, and therefore unique to the Temporary User and his nomadic device. *See, e.g., id.*, ¶ [0062] (“At step 502, the vehicle Owner may enter in vehicle authorization credentials based on information received by the Temporary User to set up a virtual key. The virtual key may be sent to the vehicle allowing Temporary User access to the Owner's vehicle.”). *Kleve* discloses that the virtual key is created after an agreement between Vehicle Owner and Temporary User and then sent “to the vehicle allowing Temporary User access to the Owner’s vehicle.” *Id.*, ¶ [0063]. Thus, the virtual key cannot be used by another device. Because the virtual key is verified by the vehicle by confirming the Temporary User’s credentials, the virtual

key cannot be used ***without receiving new data from the server to reactive the e-key***, specifically, updated credentials reflecting the new device. *Id.*, ¶¶ [0067-68].

153. In the alternative, a POSITA would have found it obvious to restrict the virtual key to a specific device upon first use of the virtual key. A POSITA would be motivated to do this because restriction of the virtual key allows a Temporary User to choose which of their devices that will operate the virtual key, improving flexibility and user experience. Furthermore, restricting the key to a specific device upon first use increases security, as this would prevent the virtual key from being stolen (or rather, prevent its use if it were stolen). In my opinion, a POSITA would further consider it obvious to allow for a Temporary User to transfer the virtual key to a different device, after which it must be reactivated (such as by resending the Temporary User's credentials to authorize the Temporary User). By requiring reactivation, it provides the benefit of flexibility and better user experience (by allowing a Temporary User to use a different device) without decreasing security from potential theft of the virtual key, since the virtual key cannot be used without reauthenticating the Temporary User.

154. A POSITA would have reasonably expected such a modification to succeed because it was well within the skill of an ordinary artisan to restrict a virtual key to a specific device such as by associating the virtual key with the unique

identifier or properties of the specific device and disallowing any usage of the virtual key by any device that does not match the unique identifier or properties.

11. **Claim 12: “The method of claim 1, further comprising, receiving a plurality of requests to generate e-keys for the vehicle from time to time to the recipient or other recipients, such that a plurality of e-keys can be generated for the vehicle and the e-keys that are generated are associated with the user account, and any one of the generated e-keys are removable from being active via the user account, the user account being used for making the requests to generate the e-key or e-keys.”**

155. In my opinion, *Kleve* discloses or renders obvious this limitation.

156. As I discussed above in claim 1, *Kleve* discloses ***requests to generate e-keys for the vehicle*** where the ***e-keys that are generated are associated with the user account***, with the vehicle owner’s user profile (***user account***) ***being used for making the requests to generate the e-key or e-keys***.

157. *Kleve* discloses that ***a plurality*** of virtual keys may be requested. For example, *Kleve* discloses that “the vehicle rental micro-business system may generate and deliver ***virtual keys*** to the Temporary User.” *Id.*, ¶ [0048]. A POSITA would further understand that since the virtual keys are specific to a single Temporary User, the vehicle owner’s user profile must request multiple virtual keys from time to time in order to accommodate multiple Temporary Users, since the users are ***temporary*** users that use the vehicle for a ***rental period***, *i.e.* multiple Temporary Users can rent the vehicle for different rental periods. *See, e.g., id.*, ¶

[0074] (“once the schedule rental is complete the virtual key may be terminated, allowing the vehicle to be secured for either the Owners entry or the **next temporary user scheduled to use the vehicle.**”). As *Kleve* teaches, the virtual key is generated after the Temporary User and vehicle owner sign a rental agreement (*see, e.g. id.*, ¶ [0039]), and thus a POSITA would understand a vehicle owner coming to multiple agreements with multiple Temporary Users results in multiple virtual keys. Indeed, a POSITA would understand it would make little sense to limit a vehicle owner’s user profile to only generating a single virtual key as that would require the vehicle owner to recreate the account every time he wishes to rent out the car. *Kleve* even discloses a process where “the Owner and Temporary User may rate their experience on the website to notify others of their satisfaction each person had during the transaction at step 360,” indicating that the vehicle is intended to be rented out multiple times to multiple temporary users and thus requiring multiple requests for virtual keys. *Id.*, ¶ [0055].

158. In my opinion, *Kleve* further discloses that **any one of the generated e-keys are removable from being active via the user account**, specifically that “once the Temporary User has completed the rental period and returned the vehicle to the appropriate drop off, **the virtual key may terminate** allowing the system to reset any private information stored on the vehicle-based computing system.” *Id.*, ¶ [0049]. A POSITA would understand that the virtual key is terminated, *i.e. removed from*

being active, via the user account because it is the Vehicle Owner's user profile that defines the rental period through the rental agreement and to which the virtual key is associated, and thus upon expiration of the rental period, the virtual key's termination requires removal via the user account.

159. It is also my opinion that a POSITA would have also considered it obvious that ***any one of the generated virtual keys are removable via the user account*** in order to facilitate, for example, cancellations from the Vehicle Owner. A POSITA would be motivated by the well-known benefit of allowing flexibility for either Vehicle Owners to cancel rentals if circumstances call for such. For example, if the vehicle is damaged and needs to be repaired, it would be desirable to allow the vehicle owner to cancel any rental agreement (and therefore associated virtual keys) until the vehicle can be repaired or a replacement obtained. A POSITA would have reasonably expected such a modification to succeed because it would simply involve providing a mechanism for cancellation of rentals, such as a button within an app that sent a request to the server for cancellation—a simple change well-within the abilities of a POSITA. No additional hardware would be required to make such a change, and Kleve already discloses much of the necessary software, e.g., a “Smartphone application” (*id.*, ¶ [0047]) in communication with a “server” (*id.*, ¶ [0057]) to “enable a Temporary User keyless access and drive away capabilities” (*id.*) via a virtual key. Providing the ability to disable (or “remove”) the virtual key

via the application would be an obvious extension of the disclosed ability to generate the virtual key.

12. Claim 13

13[a]: “The method of claim 1, further comprising, receiving data indicative that the device having the e-key remains within a communication distance of the vehicle during use of the e-key; and”

160. In my opinion, *Kleve* discloses this limitation. *Kleve* discloses that the vehicle has a “BLUETOOTH transceiver” to communicate with “the Temporary User’s nomadic device” during use of the virtual key. *Id.*, ¶ [0061]. A POSITA would understand that the Bluetooth connection requires that the device be within communication distance of the vehicle. *See id.*, Abstract (“A vehicle computing system includes a processor programmed and configured to establish communication with a wireless device ***brought into proximity of a vehicle.***”). Thus, the vehicle is always receiving data indicative of the Temporary User’s device being within communication distance of the vehicle.

13[b]: “sending data to disable the e-key and prevent use of the vehicle after a period of time when the data indicates that the device is not within the communication distance of the vehicle for which the e-key is to be used or is used; and”

161. In my opinion, *Kleve* discloses this limitation. *Kleve* discloses that the virtual key is terminated after the Temporary User has “returned the vehicle to the

appropriate drop off.” *Id.*, ¶ [0055]. A POSITA would understand that detecting that the Temporary User has performed the drop off requires determining that the Temporary User is no longer in proximity to the vehicle, because if the user is still in proximity (such as in the vehicle or unloading their belongings), then it would be unsafe and undesirable to lock the vehicle. By walking away, the Temporary User has confirmed that they have given up possession of the vehicle. In my opinion, a POSITA would thus consider it obvious to perform proximity detection by sending data indicating that the device is not within, for example, Bluetooth communication distance of the vehicle. This could be easily achieved by sending to the server an indication that the Temporary User’s device is no longer connected to Bluetooth, after which the server can terminate the virtual key per the drop off procedure. Alternatively, it also would have been obvious to track the Temporary User’s device location to determine proximity to the vehicle. A POSITA would be motivated to perform proximity detection to allow for easy drop off procedures that does not require the Temporary User to do anything beyond park the vehicle and walk away. This would improve the user experience.

13[c]: “sending a notification or a report, or a log to an administrator of the vehicle to report activity of use of the vehicle in association with use of the e-key.”

162. As I discussed above for limitation 1[e], *Kleve* discloses that the Temporary User's use of the vehicle with the virtual key is monitored to ensure compliance with the restrictions in the rental agreement.

13. **Claim 14: “The method of claim 1, wherein the request to generate the e key for the identified recipient is made using a template having a set of privileges, wherein the template is selectable instead of selecting individual privileges to be associated with the e-key.”**

163. In my opinion, *Kleve* discloses this limitation. As I discussed above for limitation 1[a], *Kleve* discloses a request to generate a virtual key is made using a rental agreement. *Id.*, ¶ [0047]. *Kleve* further discloses that the rental agreement can be made ***using a selectable template having a set of privileges associated with the virtual key***. For example, *Kleve* discloses a “standard rental agreement form” or “a custom form based on the type of use the Temporary User is requesting to use the vehicle for.” *Id.*, ¶ [0038]. A POSITA would understand that a “standard rental agreement form” is a ***template having a set of privileges***, such as maximum vehicle speed, restricted vehicle location, use for a specified time period or other standard usage for a vehicle, such as “mov[ing] furniture.” *Id.*

14. **Claim 15: The method of claim 14, wherein the template is one of a child template, or a teen template, or a spouse template, or a mechanic template, or a valet attendant**

template, or a friend template, or a quest template, or a custom template.

164. As discussed above for claim 14, Kleve discloses a “standard rental agreement form” or “a **custom form** based on the type of use the Temporary User is requesting to use the vehicle for.” *Id.*, ¶ [0038]. A POSITA would understand that the custom form is at least a **custom template** in the various scenarios in which it is described.

15. Independent Claim 16

165. I note that limitations 16[pre] through 16[f] are identical to limitations 1[pre] through 1[f], respectively. Moreover, limitation 16[h] is identical to claim 9. Thus, Kleve discloses or renders obvious those limitations from claim 16 for the same reasons I explained above. I discuss limitation 16[g] below.

16[g]: “wherein the transmitted e-key is encrypted and configured for decryption to enable use of the vehicle using the e-key;”

166. In my opinion, *Kleve* discloses or renders obvious this limitation. *Kleve* discloses that the virtual key (**e-key**) “may be sent in an **encrypted message**.” *Id.*, ¶ [0063]. A POSITA would have understood that an encrypted message is **configured for decryption** because the message could not be readable without decryption. For example, *Kleve* discloses that the virtual key could be a “matrix barcode (ex. two-dimensional code)” to be scanned by the vehicle. *Id.*, ¶ [0044]. A POSITA would

understand that encrypting the matrix barcode would render it unusable as a barcode, and thus would need to be decrypted after receipt. A POSITA would have also considered it obvious to decrypt the encrypted message since encryption-decryption mechanisms were very well-known and implementation of such was well-within the skill of a POSITA, and would have reasonably expected such to succeed.

167. As I discussed in limitation 1[a], the virtual key (*e-key*) enables use of the vehicle.

16. Claim 17: “The method of claim 16, further comprising, receiving, by the server, data from the vehicle being indicative of interface inputs or settings made during use with the e-key, the inputs or settings being examined to identify patterns; and learning the patterns, by a process executed by the server, to provide recommendations to the recipient or to an account of the recipient, for settings that should or may be made to the vehicle when using the e-key.”

168. In my opinion, *Kleve* discloses or renders obvious this limitation. I discuss this limitation in parts due to its length.

receiving, by the server, data from the vehicle being indicative of interface inputs or settings made during use with the e-key

169. In my opinion, *Kleve* discloses this limitation. *Kleve* discloses that the vehicle may “monitor the Temporary User’s utilization of the vehicle including ... vehicle location.” *Id.*, ¶ [0073]. This location data is “transmitted to the server.” *Id.*, ¶ [0076].

170. *Kleve* further discloses that “frequent destinations” are a vehicle “setting[.]” *Id.*, ¶ [0050]. Thus, a POSITA would understand that a location in the form of frequent destinations is *indicative of settings made during use with the e-key*.

the inputs or settings being examined to identify patterns; and learning the patterns, by a process executed by the server

171. In my opinion, *Kleve* renders obvious this limitation. Specifically, *Kleve* discloses that the server can provide “stored frequent destinations sent to the [vehicle].” *Id.*, ¶ [0050]. In my opinion, a POSITA would have considered it obvious for the server to identify patterns in the vehicle location data to learn frequent destinations. A POSITA would have been motivated to provide such a feature because of the well-known benefits of providing all car rental users the convenience of having the most frequent destinations available when renting a car. A POSITA would have reasonably expected such a modification to succeed because learning the most frequent destinations is well within the skill of an ordinary artisan, as it would merely involve determining which locations were visited the most based on the GPS location data.

to provide recommendations to the recipient or to an account of the recipient, for settings that should or may be made to the vehicle when using the e-key

172. In my opinion, *Kleve* discloses this limitation. *Kleve* discloses that a Temporary User may have “vehicle preset settings applied when renting a vehicle” such as “stored frequent destinations.” *Id.*, ¶ [0050]. As discussed above, it would have been obvious to learn such frequent destinations from the data sent to the server. A POSITA would understand that “frequent destinations” are a ***recommendation to the recipient*** for destinations the recipient may want to visit again.

17. Claim 18

18[a]: “The method of claim 1, wherein the condition of use defines one or more privileges associated to use of the e-key, and further comprising,”

173. As I discussed above for the limitation “the request includes a condition of use of the vehicle,” *Kleve* discloses privileges associated with the virtual key (***e-key***), such as a rental period. *See, e.g., id.*, ¶¶ [0038]-[0042].

18[b]: receiving a request from the device of the recipient to expand use, or remove a privilege, or add a privilege of the condition of use.

174. In my opinion, *Kleve* discloses this limitation. *Kleve* discloses that the Temporary User (***recipient***) may request extending the rental period through the user’s device. For example, *Kleve* discloses that if the “rental period may expire soon, ... the system may allow the Temporary User to purchase additional rental time ... with the use of ... a nomadic device [*i.e. device of the recipient*].” *Id.*, ¶43.

18. Independent Claim 19

175. I note that limitations 19[pre] through 19[f] are identical to limitation 1[pre] through 1[f], respectively. I also note that limitation 19[h] is identical to claim 9. Thus, *Kleve* discloses or renders obvious those limitations for the same reasons I discussed above.

19[g]: “wherein the e-key received at the device of the recipient includes data to inform the recipient of a level of monitoring that is to occur of the vehicle when the e-key is used for the vehicle, wherein a log is made to save the use of vehicle to a cloud storage, or storage of the vehicle or both, the log including one or more of driving data that took place, or where the vehicle was driven, or speeds of the vehicle, or damage of the vehicle, or radio stations listened to, or conversations had, or images of drivers during specific times, or combinations to two or more thereof;”

176. In my opinion, *Kleve* discloses or renders obvious this limitation. I discuss this limitation in parts given its length.

i. wherein the e-key received at the device of the recipient includes data to inform the recipient of a level of monitoring that is to occur of the vehicle when the e-key is used for the vehicle

177. As I discussed above for limitation 1[e], *Kleve* discloses monitoring various uses of the vehicle. In my opinion, a POSITA would have considered it obvious to include with the virtual key (*e-key*) a notification to the Temporary User (*recipient*) about the *level of monitoring* that will occur. Indeed, a POSITA would understand that such level of monitoring will be disclosed in the rental agreement

between the Vehicle Owner and Temporary User, not least because local privacy laws may require such monitoring to be disclosed in advance. In any case, a POSITA would have considered it obvious to inform the Temporary User of such monitoring because it will encourage the Temporary User to use the vehicle within the agreed-upon restrictions. A POSITA would also have a reasonable expectation of success since such notifications could be implemented using well-known, conventional systems such as those provided by Apple and Google to provide push notifications to iOS and Android devices.

- ii. **wherein a log is made to save the use of vehicle to a cloud storage, or storage of the vehicle or both, the log including one or more of driving data that took place, or where the vehicle was driven, or speeds of the vehicle, or damage of the vehicle, or radio stations listened to, or conversations had, or images of drivers during specific times, or combinations to two or more thereof**

178. In my opinion, *Kleve* discloses this limitation. As I discussed above for limitations 1[e] and 1[f], *Kleve* discloses monitoring and uploading data that includes ***where the vehicle was driven*** and ***speeds of the vehicle***. See, e.g., *id.*, ¶¶ [0076], [0078], [0080]. *Kleve* further discloses that such data is ***saved to a cloud storage or the vehicle***. For example, the data is “transmitted to either the server ... or saved on a storage device for later download.” *Id.*, ¶ [0078]. In addition, because the “Vehicle Owner may review monitored data at a given time throughout the rental period,” a

POSITA would understand that the data is saved on the server (**cloud storage**) for review by the Vehicle Owner. *Id.*

19. Claim 20

20[a]: “The method of claim 19, wherein a plurality of e-keys for the vehicle are producible, the plurality of e-keys can co-exist, and wherein,”

179. As I discussed above for claim 12, *Kleve* discloses or renders obvious generating a plurality of virtual keys (**e-keys**) that can co-exist, such as generating virtual keys for different Temporary Users for different rental periods.

20[b]: “only one e-key is associated with active use of the vehicle at one time; or a particular e-key in use with the vehicle can be swapped for another e-key having access to the vehicle, such that each e-key has the same or different privileges or conditions of use; or a priority order of e-keys is defined, such that higher level priority e-keys are placed in use over lower priority e-keys.”

180. In my opinion, *Kleve* discloses this limitation. *Kleve* discloses that a virtual key is only active for the specified rental period. *See, e.g., id.*, ¶ [0039] (“The virtual key may also be sent to the vehicle configuring the VCS to enable the keyless drive system for the appropriate Temporary User **during a given rental period.**”); ¶ [0049] (“Once the Temporary User has **completed the rental period** and returned the vehicle to the appropriate drop off, **the virtual key may terminate** allowing the system to reset any private information stored on the vehicle-based computing

system.”). Thus, when there are multiple virtual keys for different rental periods, only one virtual key is active at one time.

B. Ground 2: *Kleve* in view of *Sekiyama* renders obvious claims 19 and 11-20 under Section 103

181. In my opinion, *Kleve* in view of *Sekiyama* provides an alternative ground for rendering obvious claims 1-20. In particular, *Sekiyama* discloses a server generating an e-key, and a POSITA would have found it obvious to incorporate this teaching into *Kleve*, thereby providing an alternative basis for rendering obvious limitations 1[a] and 1[b] (and their counterparts in claims 16 and 19).

1. Motivation to Combine

182. In my opinion, a POSITA would have been motivated to combine *Kleve* with *Sekiyama*’s teaching of a server that generates an e-key to unlock and start a vehicle. *See Sekiyama*, ¶¶ (0018), (0026). Specifically, although as discussed above it would have been obvious in view of *Kleve* alone that *Kleve* uses its server to generate a virtual key, it also would have been obvious in view of *Sekiyama* for *Kleve*’s server to generate a virtual key.

183. A POSITA would have been motivated for *Kleve*’s server to generate a virtual key in view of *Sekiyama*. A POSITA would have understood the well-known benefits of centralizing the generation of virtual keys, including an increase in security and reliability. In *Kleve*, generating the key requires that the vehicle owner

enter “authorization credentials” from the Temporary User, and it is the server which stores the Temporary User’s user profile that contains copies of those credentials (such as “photos of credit cards, photo of forms of ID,” etc.) to confirm the Temporary User’s identity. *Kleve*, ¶¶ [0062], [0037]. Thus, a POSITA would be motivated to have the server generate the key since it is the server which can confirm the identity of the Vehicle Owner (by the request being sent via a user account), confirm the identity of the temporary user (via the authorization credentials), and confirm that they have entered into a rental agreement for a specific vehicle. A POSITA would have known that, by having the server generate the virtual key, this increases security and reliability since the server can confirm all the necessary information needed before providing the virtual key.

184. It is my opinion that a POSITA would have reasonably expected the combination to succeed. Having *Kleve*’s server generate a key would have been well-within the capabilities of a POSITA. Since *Kleve* already discloses a mechanism for generating a key and discloses that the server transmits the key to the Temporary User and vehicle, there would be a reasonable expectation of success for having the server perform that mechanism.

185. In my opinion, *Kleve*, *Sekiyama* and the ’188 patent are all directed to the same field of endeavor, the field of electronic key systems. See Ex. 1001, Abstract (“One method includes receiving a request to generate electronic key (e-

key) for an identified recipient to use a vehicle.”); *Kleve*, ¶ [0048] (“The virtual key may allow a Temporary User temporary granted access to the Owner's vehicle. The granted access allowed by the virtual key may permit entry of the vehicle; grant a keyless drive-away of a vehicle, and/or both.”); *Sekiyama*, ¶ (0026) (“the electronic key (key information) outputted from the center server 20.”).

2. *Sekiyama*’s disclosure of 1[a] and 1[b]

186. In my opinion, *Sekiyama* discloses a server that generates an electronic key for unlocking and starting a car upon. For example, *Sekiyama* states that “the electronic key (key information) outputted from the center server 20.” *Id.*, ¶ (0026). This key can control “locking and unlocking of the door lock” and “permission for engine start.” *Id.*, ¶ (0018).

187. As discussed above, it would have been obvious to incorporate this functionality into *Kleve*.

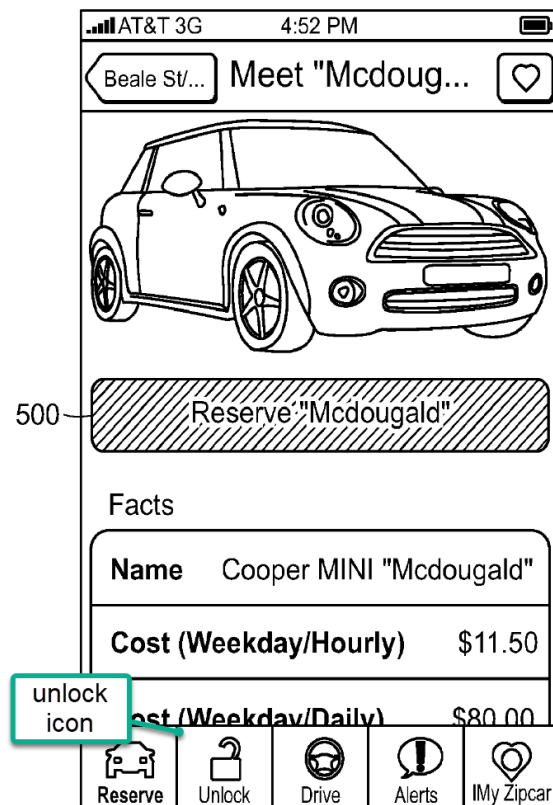
3. *Sekiyama*’s disclosure of 1[g]

188. *Sekiyama* also discloses the server processes logic for analyzing the data regarding use of the vehicle when the e-key is used for the vehicle. *Id.*, ¶ (0021-23) (“In the server 20 ... there is ... a vehicle status monitoring unit 22 [which] acquires information related to the vehicle status of the vehicle 40 based on signals outputted from the vehicle 40.”)

189. It would also be obvious to include such a monitoring unit in Kleve to perform the logic processing of Kleve's usage monitoring.

C. Ground 3: *Kleve* (with or without Sekiyama) in view of *Mottla* renders obvious claim 10 under Section 103

190. In my opinion, *Kleve* (optionally combined with *Sekiyama*) in view of *Mottla* provides an alternative ground for rendering obvious claim 10. Claim 10 requires a “the e-key enables graphical icons on a screen of the device to be active for enabling use of the vehicle, at least one of the graphical icons on the screen enabling unlocking of the vehicle.” At a minimum, this functionality is disclosed by *Mottla*, which describes a graphical user interface with “an unlock icon” for remotely “unlock[ing] the vehicle doors.” *Mottla*, ¶ [0033]; Fig. 5.



191. In my opinion, it would have been obvious to incorporate *Mottla's* unlock icon into *Kleve*, and to enable the use of this icon with *Kleve's* virtual key. A POSITA would be motivated by the benefits of a user-friendly GUI, as providing an unlock button activated by the e-key allows the user better and easier control over vehicle access, and using an unlock icon (instead of text) is easier to comprehend and is more user-friendly. A POSITA would have been motivated to allow the Temporary User control of locking/unlocking via an icon instead of only unlocking the vehicle upon scanning of the virtual key—that would allow a Temporary User to use the unlock icon after the virtual key has been scanned and authorized, providing a better user experience while maintaining security. A POSITA would

have a reasonable expectation of success because GUI icons were standard and implementation was within the capabilities of a POSITA.

192. My opinions likewise apply if *Kleve* is combined with *Sekiyama*'s teachings of e-keys generated by a server, as discussed above. Implementing an unlock icon because of the desire for a user-friendly GUI would equally apply if *Sekiyama* is combined with *Kleve*.

193. As I discussed above, *Kleve* and the '188 patent are in the same field of endeavor of electronic key systems. In my opinion, *Mottla* is as well. *Mottla*, Abstract; Ex. 1001, Abstract; *Kleve*, ¶ [0048].

D. Ground 4: *Zaid* in view of *Harris* renders obvious claims 1, 3, 5-7, 9, 11-16, and 18-20 under Section 103

194. I summarize this ground as follows: As with *Kleve*, *Zaid* similarly discloses a rental system where a vehicle owner can list the availability of his or her vehicle for renters (who have identified themselves by signing into a social media account) to choose. When the vehicle owner accepts a renter's request for a vehicle, the server generates an electronic key by encrypting the vehicle request and sending it to the user's device, which is used to access and turn on the vehicle. *Zaid* further discloses that the vehicle monitors the renter's usage to ensure usage is within the conditions of the vehicle reservation, such as the length of reservation.

195. To the extent Patent Owner argues that *Zaid* does not explicitly disclose that the request for an electronic key contains the renter's identifying information, or that the encrypted vehicle reservation is not an electronic key, it is my opinion that such limitations were taught in *Harris*, and it would have been obvious to combine *Zaid* with *Harris*.

1. Motivation to Combine

196. In my opinion, a POSITA would have been motivated to modify *Zaid*'s Internet-based rental car system with *Harris*'s teachings of the generation of electronic keys following authentication of a user.

197. *Harris* teaches a system where a server distributes electronic keys for accessing and starting cars. *Harris*, ¶¶ [0038-41]. In particular, a user (including a non-owner temporary user like a valet) "identifies themselves to a server," and after "[t]he server recognizes the credentials," it "allows the user to get a new key" which can be used to "start the vehicle." *Id.*, ¶ [0040]. This key can be "a code" such as "a 2048 byte number" which "can be downloaded." *Id.*, ¶¶ [0033], [0037]. The server generates keys by using a "unique seed in the server." *Id.*, ¶ [0038].

198. In my opinion, a POSITA would have been motivated to incorporate these teachings into *Zaid*'s system because of the well-known benefits of those teachings, including increased security, efficiency, and better user experience. A POSITA would have understood that by requiring a user to properly identify and

authenticate themselves prior to receiving a key, this increases security of the system by better ensuring the user is who they say they are. Since the key is used for access and starting vehicles, which are valuable assets and frequent targets of theft, a POSITA would understand the importance of ensuring any recipient of a key is properly identified and authenticated as someone with permission to receive such a key. In addition, such authentication provides a better user experience for the vehicle owner, including greater peace of mind.

199. Furthermore, a POSITA would also have been aware of the known benefits of using a code-based electronic key as disclosed in *Harris*. As *Harris* explains, a code-based key is used to “match[] to one or may codes within the automobile” only after which a car “can be accessed; and the engine can be started.” *Harris*, ¶ [0033]. A POSITA would have known that the matching of a code, even a code as long as a 2048 byte number, requires less time and processing power than the decryption of a vehicle reservation as taught in *Zaid*. This allows for quicker access to a vehicle and therefore a better user experience.

200. In view of the above motivations and teachings, a POSITA would have enhanced *Zaid*’s system to include a renter’s identifying information with an e-key request so that the server can authenticate and ensure the identity of the renter. A POSITA would have further modified *Zaid*’s system to, in response to a request, generate a key code as taught in *Harris* to be accompanied with the encrypted

reservation when sent to the renter's device. A POSITA would have further enhanced *Zaid*'s system for the server to provide the key code to the rental vehicle. Thus, access to the vehicle can be granted upon matching the key code—during which the reservation can also be decrypted to determine the conditions of use for the vehicle. Alternatively, as taught in *Harris*, the key code itself can embed the conditions of use, such as a key being “limited in time and usable for only 3 to 15 minutes” or “one ride.” *Harris*, ¶¶ [0039-40]. Such teachings further establish the suitability of combining *Zaid* with *Harris*, since *Zaid* similarly discloses “a specified time period” as a condition of use of the vehicle. *Zaid*, ¶ [0069].

201. In my opinion, a POSITA would have reasonably expected this combination to succeed. Providing identifying information to a server in order to authenticate a user had long been used in the industry and implementing such functionality would have been within the capabilities of a POSITA. As a result, and for the reasons stated above, all of the above modifications were easy to implement and well-within the capabilities of a POSITA using conventional techniques.

202. In my opinion, *Zaid*, *Harris* and the '188 patent are all directed to the same field of endeavor, the field of electronic key systems. See Ex. 1001, Abstract (“One method includes receiving a request to generate electronic key (e-key) for an identified recipient to use a vehicle.”); *Zaid*, Abstract (“[A] vehicle reservation from a wireless communication device is received, the vehicle reservation is

authenticated, and access to the vehicle is provided after authenticating the vehicle reservation.”); *Harris*, ¶ [0033] (“In an embodiment, the key is a code on a non-volatile device such as a USB key 105. The code on that key is verified by the automobile to allow starting or other access to the vehicle.”).

2. Claim 1

1[pre] / 1[a]: “A method, comprising, receiving, by a server, a request from a user via a user account that has a vehicle associated therewith to generate an electronic key (e-key) for an identified recipient to use the vehicle, the request includes identifying information for enabling sending of the e-key to the recipient via an electronic transmission, the request includes a condition of use of the vehicle as set by the user via the user account”

203. Again, given the length of this limitation, I divide it into smaller portions. First, I will analyze the limitation “receiving, by a server, a request from a user via a user account that has a vehicle associated therewith to generate an electronic key (e-key) for an identified recipient to use the vehicle.” I will also divide up this limitation.

i. receiving, by a server, a request from a user via a user account that has a vehicle associated therewith to generate an electronic key (e-key) for an identified recipient to use the vehicle

204. In my opinion, *Zaid* discloses or renders obvious in view of *Harris* this limitation. *Zaid* discloses or renders obvious a vehicle owner (***user***) that can use a ***user account*** (such as through facebook) to facilitate a vehicle rental reservation that

causes the server to generate an encrypted reservation (**e-key**) to allow an identified user (**identified recipient**) to use the owner's vehicle.

205. First, it is my opinion that *Zaid* discloses a “server.” For example, *Zaid* discloses that “the received vehicle reservation is booked at a central **server** via a user interface displayed on a computing device.” *Zaid*, ¶ [0072]. It is through this central server that the rental user's device will receive an encrypted reservation (**e-key**). See, e.g., *id.*, ¶ [0125].

206. Second, it is my opinion that *Zaid* discloses a “user account that has a vehicle associated therewith.” *Zaid* discloses that a vehicle owner can list a vehicle for rental on the vehicle reservation application. *Zaid*, ¶ [0077] (“[A] vehicle reservation application ... that enables a vehicle ... owner ... to communicate with backend server(s) ... to ... advertise or announce when the vehicle will be available for sharing.”). In my opinion, a POSITA would understand that the listing of the vehicle is associated with a user account belonging to the vehicle owner. *Zaid* already discloses that the vehicle reservation application can be accessed “through one or more social networking websites, such as FourSquare® and Facebook®,” where the “user must first log into the social networking website.” *Zaid*, ¶ [0072]. A POSITA would understand that the vehicle owner would likewise access the vehicle reservation application via such an account in order for the application to be able to associate a vehicle with the correct person in order to, for example, allow the

owner to “update the server(s) (e.g., online vehicle reservation system) of various vehicle related information such as vehicle availability and vehicle location.” *Id.*, ¶ [0079]. A POSITA would further understand that such an account would also be required to facilitate rental payments or confirm insurance.

207. Alternatively, in my opinion, a POSITA would consider it obvious to allow a vehicle owner to access the vehicle rental application through a user account (such as a Facebook account as already disclosed in *Zaid*) in order to associate their vehicle with the account. This would provide the known benefit of increasing security and improving the vehicle owner experience. For example, allowing a vehicle owner to create an account would provide a mechanism for the application to confirm the identity of the vehicle owner, confirm the ownership status of the vehicle, and confirm the presence of insurance. It would also improve the user experience for the vehicle owner, allowing the vehicle owner to, for example, receive payment for the rental as well as provide a centralized storage of vehicle information and history, allowing the vehicle owner to more easily make their vehicle available for rental at any time. In addition, a POSITA would have a reasonable expectation of success because *Zaid*’s system already supports user accounts (such as through Facebook) and implementation would simply be a matter of requiring a vehicle owner use a user account before offering vehicles for rental.

208. *Third*, it is my opinion that *Zaid* discloses or renders obvious in view of *Harris* the limitation “*identified recipient*.” *Zaid* discloses that the rental user is an ***identified recipient*** by identifying him or herself when accessing the “central server” “through one or more social networking websites, such as FourSquare® and Facebook®,” where the “user must first log into the social networking website before he/she can view the advertisement and make reservation.” *Zaid*, ¶ [0072]. A POSITA would understand that by logging in through a social networking website, the user has identified him or herself and is therefore an ***identified recipient***.

209. In addition, *Harris* discloses this limitation, because it teaches that “the user identifies themselves to a server” after which “[t]he server recognizes the credentials ... and allows the user to get a new key.” *Harris*, ¶ [0040]. As I discussed above, a POSITA would have been motivated to incorporate this teaching into *Zaid* by requiring the renter to identify themselves by providing credentials. Thus, *Zaid* in view of *Harris* renders obvious this limitation.

210. *Fourth*, in my opinion, *Zaid* discloses or renders obvious “*receiving, by a server, a request from a user via a user account ... to generate an electronic key*.” *Zaid* discloses that the server receives a vehicle reservation (***request***) which results in generating an encrypted reservation (***electronic key***). Specifically, *Zaid* states that a “vehicle reservation is booked by a user at a ***central server***,” after which “the central server encrypts the message containing the vehicle reservation.” *Zaid*, ¶

[0125]. A POSITA would understand that the vehicle reservation request is sent to the server from the owner's user account. It is the owner who advertises when the vehicle is available for reservation, and it is the owner who has "control over the type of user the owner is lending/sharing/renting vehicle to." *Id.*, ¶¶ [0072], [0077]. Thus, *Zaid* discloses it is the owner who decides whether or not a reservation will go forward—a POSITA would therefore understand that the reservation request to the server comes from the owner through the owner's account.

211. Alternatively, a POSITA would have found it obvious that the reservation request is sent by the owner through the owner's account. Since both the renter and the owner accounts are involved in making the reservation, whether the reservation request is sent by the renter or the owner is a mere design choice—the system can handle the request regardless of the source.

212. Moreover, a POSITA would have been aware of the known benefits of having the owner account send the request, because that allows the owner greater control over which renters are allowed to reserve the vehicle, giving effect to *Zaid*'s teachings that "a tracking mechanism can be established to track group member driving history and reputation and allow the vehicle owner to have better control over the type of user the owner is lending/sharing/renting vehicle to." *Id.*, ¶ [0172]. Since the owner is also the one bearing the risk of vehicle loss, it would be advantageous to have the owner send the request to ensure that the owner has truly

consented to the reservation. A POSITA would have a reasonable expectation of success in having the owner's account send the request, because that is a mere design choice using conventional networking APIs and coding practices well within the capabilities of a POSITA.

213. *Fifth*, in my opinion, *Zaid* discloses or renders obvious in view of *Harris* an “*electronic key (e-key) for an identified recipient to use the vehicle.*” *Zaid* discloses that the encrypted reservation is an **electronic key** that is sent to the recipient to allow **use of the vehicle**. Specifically, *Zaid* teaches that “the central server encrypts the message containing the vehicle reservation” and then it is “communicated to a wireless communication device of the user [*i.e. identified recipient*].” *Id.*, ¶¶ [0125-26]. The reservation is used to grant “vehicle access” to the recipient, which includes “opening the vehicle door, and/or allowing engine to be turned on by the user,” *i.e. use of the vehicle*. *Id.*, ¶ [0129].

214. In addition, *Zaid* in view of *Harris* renders obvious this limitation. *Harris* teaches the generating of a “key” in the form of a “code” such as “a 2048 byte number,” where “[i]f the code on the key matches to one or many codes within the automobile, then the car systems can be accessed; and the engine can be started.” *Harris*, ¶ [0033]. This key is generated by a server after a user authenticates themselves. *Id.*, ¶ [0040]. As I discussed above, a POSITA would have been motivated to combine this teaching with *Zaid* by generating a code in addition to

encrypting the reservation, both of which are sent to the renter's device for gaining access to the vehicle.

ii. the request includes identifying information for enabling sending of the e-key to the recipient via an electronic transmission

215. In my opinion, *Zaid* discloses or renders obvious in view of *Harris* this limitation. *Zaid* discloses that the reservation requests includes ***identifying information about the recipient***, such as information about their social networking account in order to allow the vehicle owner to track the user's "driving history and reputation." *Zaid*, ¶ [0072]. Such information enables sending of the e-key to the recipient because it "allow[s] the vehicle owner to have better control over the type of user the owner is lending/sharing/renting vehicle to." *Id.*

216. In addition, the reservation request contains a reservation which a POSITA would understand to have ***identifying information about the recipient*** because the reservation is made using the recipient's account. *See, e.g., id.*, ¶ [0072] ("[T]he received vehicle reservation is booked ... through one or more social networking websites."). This allows the encrypted reservation to be routed to the renter's device.

217. Alternatively, as I discussed above, *Harris* teaches that a user sends to a server identifying credentials, *i.e.* "the user identifies themselves to a server" and "[t]he server recognizes the credentials." *Harris*, ¶ [0040]. As I discussed above, a

POSITA would have been motivated to combine these teachings with *Zaid* such that a renter provides identifying credentials following acceptance of a vehicle reservation, with such credentials being included in the key generation request such that the server can authenticate the renter.

218. Furthermore, *Zaid* teaches that the encrypted reservation is sent as an ***electronic transmission***. *Zaid* teaches that “the central server encrypts the message containing the vehicle reservation” and then “communicated to a wireless communication device of the user [*i.e. identified recipient*].” *Zaid*, ¶¶ [0125-26]. Since the communication is encrypted and sent over a wireless network, a POSITA would understand that it is an ***electronic transmission***.

iii. the request includes a condition of use of the vehicle as set by the user via the user account

219. In my opinion, *Zaid* discloses this limitation. *Zaid* states that the reservation request “includes a reservation for a specified time period,” which is ***a condition of use of the vehicle***. *Id.*, ¶ [0069]. This condition is ***set by the user via the user account*** such as when the owner “announces ***when the vehicle is available for sharing***,” which sets limits on the specific time period for reserving the vehicle. *Id.*, ¶ [0077].

1[b]: “generating, by the server, the e-key, the e-key being assigned with the condition of use of the vehicle;”

220. In my opinion, *Zaid* discloses or renders obvious in view of *Harris* this limitation. As I discussed above, *Zaid* discloses or renders obvious that the server generates an encrypted reservation (***e-key***) and assigns it to a rental period restriction (***condition of use of the vehicle***). *Id.*, ¶ [0069]. In addition, *Harris* discloses generating a key in the form of a code, including a embedding a condition of use such as a period of time. *Harris*, ¶¶ [0033], [0039] (“one ride”), [0040] (“The new key may be limited in time.”). As discussed above, it would have been obvious to incorporate this teaching into *Zaid* by including the key code with the encrypted reservation.

1[c]: “transmitting, by the server, the e-key to the recipient using the identifying information so that a device of the recipient is implemented to use the e-key;”

221. In my opinion, *Zaid* discloses or renders obvious in view of *Harris* this limitation. As I discussed above for the limitation “the request includes identifying information for enabling sending of the e-key to the recipient,” *Zaid* discloses ***transmitting, by the server, the e-key to the recipient using the identifying information***, and specifically to the renter’s device (***device of the recipient***).

222. As I also discussed above, *Zaid* further discloses that when the renter’s device receives the encrypted reservation (***e-key***), it can be used to access the vehicle, *i.e.* the device ***is implemented to use the e-key***. *Zaid*, ¶ [0129]. And it is my opinion,

as I stated above in the motivation to combine section, that it would have been obvious to also include *Harris*'s key code with the encrypted reservation.

1[d]: “transmitting, by the server, data to the vehicle to enable use of the vehicle via the e-key; and”

223. In my opinion, *Zaid* discloses or renders obvious (alone or in view of *Harris*) this limitation. *Zaid* discloses that the server transmits a decryption key to the vehicle to decrypt the encrypted reservation (*e-key*) which ***enables use of the vehicle via the e-key***. Specifically, *Zaid* discloses that “the vehicle access control system ... is configured to receive a ***server update***” which “includes a new ***private key***.” *Id.*, ¶ [0081]. This private key is used to decrypt the encrypted reservation, which “verif[ies] the authenticity of the wireless communication device is the intended device,” thereby enabling use of the vehicle. *See, e.g., id.*, ¶ [0128]. *Harris* further discloses transmitting a key code to the vehicle such that it can be matched with the key code of the user's device, and as I discussed above, it would be obvious to combine this teaching with *Zaid*. *Harris*, ¶33.

224. If Patent Owner argues that the combination only teaches a vehicle that does not receive the update from the server but instead from the renter's device, then my opinion is that a POSITA would have found it obvious to have the server directly transmit the server update to the vehicle. Indeed, *Zaid* expressly discloses an embodiment where “the vehicle access kit additionally includes a long-range mobile

communication radio/interface, such as GSM radio, which can be used for **wireless communication to a vehicle reservation or sharing system.**” *Zaid*, ¶ [0106]. *Zaid* discloses that such wireless communication replaces the communication via the user’s device. *Id.* A POSITA would have found it obvious to combine these embodiments in *Zaid* such that the “server update” is sent directly to the vehicle using this wireless connection. Specifically, in my opinion, it would have been obvious to a person of ordinary skill in the art in 2013 to combine *Zaid*’s method of communicating the vehicle reservation to the vehicle via the wireless communication device with *Zaid*’s method of updating the private key at the vehicle via an update transmitted from the server directly to the vehicle, in which case the short-range wireless link and the long-range mobile communication radio would together constitute the claimed communications circuitry. In such a combination, the server would maintain control over the reservation authentication process and has added flexibility to use the wireless communication device to route data to the vehicle. As *Zaid* notes, “cellular and satellite communication service fees can be expensive,” *Zaid*, ¶ [0016], so by including both direct-to-server communications alongside communications that rely on the user’s separately-paid-for mobile device, the vehicle designer optimizes connectivity while minimizing cost. Reliability and redundancy would have been important considerations in the design of a vehicle-based system since vehicles have access to different levels of connectivity based on

their changing location. Reliability is improved since direct-to-server communication does not rely on the user's mobile device to connect, avoiding the possibility of power or service interruptions from the mobile device. A POSITA would be further motivated to make this combination because it would be advantageous to allow the vehicle to receive server updates without requiring proximity to a renter's device. This would ensure that the vehicle will have the most recent server updates, as the timing of when a renter's device will be in proximity of the vehicle is unpredictable.

225. This combination would have been nothing more than an obvious design choice, since providing multiple pathways for communication with the vehicle would have provided added reliability and redundancy, improving the user experience. A person of ordinary skill in the art would have had a reasonable expectation of success in the combination given that, as the '026 patent acknowledges, communications between a vehicle and a server, whether or not using an intervening mobile device were well established and common place by 2013. *See* Ex. 1001, 1:47-49, *Zaid* [0106]. A person of ordinary skill at the relevant time would have easily combined *Zaid*'s server update method with *Zaid*'s method of conveying a reservation to the vehicle via the wireless communication device. Accordingly, a person of ordinary skill in the art at the relevant time would have been motivated to

make this combination to improve communication reliability with the vehicle rental system. See *Zaid*, ¶ [0130]).

1[e]: “receiving, by the server, use data regarding use of the vehicle for when the vehicle is used via the e-key;”

226. In my opinion, *Zaid* discloses this limitation. *Zaid* discloses that, when the renter is operating the vehicle, the server receives “control information” such as “location information” and “vehicle usage information” including “e.g., speed/acceleration, pedal position, air intake, altitude, temperature.” *Zaid*, ¶¶ [0130], [0098]; see also ¶¶ [0095] (“monitoring acceleration of the vehicle during one or more reservations to provide vehicle usage data”), [0099] (“the vehicle usage data and other information are communicated back to the central server.”). Such information is *use data regarding use of the vehicle*.

1[f]: “wherein the use data identifies information regarding the use of the vehicle, and the information identifies a violation of the condition of use;”

227. In my opinion, *Zaid* discloses this limitation. *Zaid* discloses that the received “control information” *identifies information regarding the use of the vehicle*, such as “location information” and “vehicle usage information.” *Id.*, ¶ [0130]. *Zaid* further discloses that “vehicle access is withdrawn when the vehicle reservation becomes invalid.” Ex. 1008, ¶131. Because, as a POSITA would have understood, vehicle use and access must not be revoked while the vehicle is in use

(e.g., to prevent collision), Kleve discloses that “a time-out period elapses before vehicle access is withdrawn.” *Id.*, ¶131. Additionally, it would have been obvious to a POSITA to extend this teaching to preventing withdraw of vehicle access or use whenever the vehicle is in use, even if the Temporary User has violated the time period condition of use. This would prevent the vehicle from being deactivated while, e.g., the Temporary User is travelling on the highway, which could otherwise cause an accident. As described above, Zaid’s system already receives and monitors use data indicative of whether the vehicle is currently traveling (e.g., speed/acceleration). Adding such a safety check to identify whether the Temporary User is still operating the vehicle after the rental period (i.e., a violation of the condition of use) thus would have been a clear and straightforward design choice requiring no additional hardware. Such a safety check could be implemented in software by a simple “if” statement - well within the abilities of a POSITA.

1[g]: “wherein the server processes logic for generating the e-key and processes logic for analyzing the data regarding use of the vehicle when the e-key is used for the vehicle, the server or other servers connected to the server being accessible over the Internet, the vehicle having wireless communication systems for communicating with the server or other servers and for communicating with devices local to the vehicle.”

228. In my opinion, *Zaid* discloses or renders obvious this limitation. Due to the length of this limitation, I will again break it up into smaller parts.

- i. **wherein the server processes logic for generating the e-key and processes logic for analyzing the data regarding use of the vehicle when the e-key is used for the vehicle**

229. In my opinion, *Zaid* discloses this limitation. As discussed above, *Zaid* discloses or renders obvious that the server generates the e-key and analyzes vehicle use data. A POSITA would have understood and considered it obvious that, in order to perform these functions, the server ***processes logic*** related to those functions, such as execution of CPU instructions. *Zaid* discloses that its teachings “can be implemented in numerous ways, including ***as a process*** ... such as a ***processor configured to execute instructions***.” *Id.*, ¶ [0013]. A POSITA would have understood and considered it obvious that, the “instructions” refer to ***logic processed*** in the server for generating an ekey and analyzing data regarding vehicle use.

- ii. **the server or other servers connected to the server being accessible over the Internet**

230. In my opinion, *Zaid* discloses this limitation. *Zaid* discloses that the server communicates over “the Internet and/or a wireless network, such as cellular network.” *Id.*, ¶ [0126].

- iii. **the vehicle having wireless communication systems for communicating with the server or other servers and for communicating with devices local to the vehicle.**

231. In my opinion, *Zaid* discloses or renders obvious this limitation. *Zaid* discloses that “the vehicle access kit additionally includes a long-range mobile

communication radio/interface, such as GSM radio, which can be used for wireless communication to a vehicle reservation or sharing system (e.g., as another and/or backup network communication channel),” *i.e. a server*. *Id.*, ¶ [0106]. As I discussed above, a POSITA would have found it obvious to combine this embodiment with the other embodiments taught in *Zaid*. *Zaid* further teaches that the vehicle communicates with a renter’s device in proximity. *Id.*, ¶ [0099] (“[N]earby wireless communication device that has established wireless connection via for example a short-range wireless link with the vehicle access kit.”).

3. **Claim 3: “The method of claim 1, wherein the request to generate the e-key is received from the user account that is one of an administrator of the vehicle, or an owner of the vehicle, or a rental car operator of the vehicle, or a fleet operator for the vehicle, or a user account holder that has the vehicle associated thereto, or a user authorized to request e-keys for the vehicle.”**

232. As I discussed above for limitation 1[a], *Zaid* discloses or renders obvious the limitation “receiving, by a server, a request from a user via a user account ... to generate an electronic key,” and further discloses or renders obvious that the request is made via the vehicle owner’s user profile (*user account of an owner of the vehicle*). *See, e.g., Id.*, ¶ [0077].

4. **Claim 5: “The method of claim 1, wherein the condition of use is one of a geographic restriction for where the vehicle is allowed to be used, or a speed restriction, or an occupancy restrictions, or a time frame of use, or a time expiration of use, or combinations thereof.”**

233. As I discussed above for the limitation “condition of use of the vehicle as set by the user via the user account,” *Zaid* discloses that the vehicle reservation can set a condition of use “for a specified time period” and “reservation time slot” (*time frame of use / time expiration of use*). *Id.*, ¶ [0069].

5. **Claim 6: “The method of claim 1, wherein the identifying information includes one or more of an email address, a phone number, a text, a message address, a notification, a link, a web address, a social network address, or combinations thereof.”**

234. As I discussed above for the limitation “the request includes identifying information,” *Zaid* discloses that the request includes *identifying information* such as a facebook account, *i.e. a social network address*. *Id.*, ¶ [0072].

6. **Claim 7: “The method of claim 1, wherein receiving use data for use of the vehicle for when the vehicle is used via the e-key includes one or more of a history of where the vehicle has been, or speeds of the vehicle, or events of the vehicle, or multiple violations of the condition of use, or combinations thereof.”**

235. As I discussed above for limitations 1[e] and 1[f], the received use data includes “location information” (*where the vehicle has been*), “accident information” (*events of the vehicle*), or “acceleration” (*speeds of the vehicle*). *Id.*, ¶¶ [0130], [0095].

7. **Claim 9: “The method of claim 1, wherein the e-key provides access to at least one of operating functions of the vehicle, or opening the vehicle, or starting the vehicle, or using user interfaces of the vehicle, or turning-off the**

vehicle, or combinations thereof.”

236. As I discussed above for the limitation “electronic key (e-key) for an identified recipient to use the vehicle,” Zaid and Harris disclose that the e-key allows *opening the vehicle* and *starting the vehicle*.

8. Claim 11

11[a]: “The method of claim 1, wherein the device is one of a smartphone, or a smartwatch, or smart glasses, or a portable device, or a computer, or a digital assistant, or a key fob,”

237. In my opinion, *Zaid* discloses this limitation. *Zaid* discloses a “wireless communication device” can be a “smart phone, mobile handset, PDA, smartbook, netbook, and laptop.” *Id.*, ¶ [0073].

11[b]: “and wherein the e-key, once used via the device of the recipient, the e-key cannot be used via another device or sent to another device to enable use of the e-key without receiving new data from the server to reactivate the e-key.”

238. In my opinion, *Zaid* discloses this limitation. *Zaid* discloses that the encrypted reservation (*e-key*) is encrypted “using a public key of the wireless communication device ... and is decrypted by the wireless communication device using a private key of the wireless communication device.” *Id.*, ¶ [0099]. In my opinion, a POSITA would understand that since the decryption key is a “private key” of the renter’s device, only the renter’s device can decrypt the reservation and thus only the renter’s device can use the e-key. The e-key could only be used by another

device if encrypted by that other device's public key, *i.e. receiving new data from the server to reactivate the e-key.*

9. **Claim 12: “The method of claim 1, further comprising, receiving a plurality of requests to generate e-keys for the vehicle from time to time to the recipient or other recipients, such that a plurality of e-keys can be generated for the vehicle and the e-keys that are generated are associated with the user account, and any one of the generated e-keys are removable from being active via the user account, the user account being used for making the requests to generate the e-key or e-keys.”**

239. In my opinion, *Zaid* discloses this limitation. As I discussed above, *Zaid* discloses or renders obvious ***requests to generate e-keys for the vehicle*** where the ***e-keys that are generated are associated with the user account***, with the vehicle owner's user profile (***user account***) ***being used for making the requests to generate the e-key or e-keys.***

240. *Zaid* further discloses that a ***plurality*** of e-keys may be requested from ***time to time***. For example, *Zaid* discloses that a reservation includes “a specified time period” and “reservation time slot.” *Zaid*, ¶ [0069]. A POSITA would have understood that a vehicle owner's user profile can request multiple encrypted reservations (e-keys) because multiple temporary users can rent the vehicle for different rental periods.

241. *Zaid* further discloses that ***any one of the generated e-keys are removable from being active via the user account***, specifically that “a time-out

period elapses before vehicle access is withdrawn when the vehicle reservation ***becomes invalid.***” *Id.*, ¶ [0131]. A POSITA would understand that the deactivation of keys is done via the owner’s account, because as discussed above, the vehicle reservation (including time-out period) was sent to the server using the owner’s account, and so later deactivation occurs via the same user account transmission. A POSITA would also consider it obvious to deactivate a user account by request of the owner to facilitate cancellation by the owner, as discussed in Ground 1, as such reasons apply to Zaid given its similarities to Kleve in disclosing a vehicle rental/sharing system. Specifically, a POSITA would be motivated by the well-known benefit of allowing flexibility for either Vehicle Owners to cancel rentals if circumstances call for such. For example, if the vehicle is damaged and needs to be repaired, it would be desirable to allow the vehicle owner to cancel any rental agreement (and therefore associated virtual keys) until the vehicle can be repaired or a replacement obtained. A POSITA would have reasonably expected such a modification to succeed because it would simply involve providing a mechanism for cancellation of rentals, such as a button within an app that sent a request to the server for cancellation—a simple change well-within the abilities of a POSITA. No additional hardware would be required to make such a change, and Zaid already discloses much of the necessary software, e.g., an “iPhone or Droid application” (*id.*, ¶ [0077]) in communication with a “backend server” (*id.*) to book a “vehicle

reservation” and enable “unlocking the vehicle door and/or allowing for starting of the vehicle engine” (*id.* ¶ [0089]) via an ekey. Providing the ability to disable (or “remove”) the virtual key via the application would be an obvious extension of the disclosed ability to generate the virtual key.

10. Claim 13

13[a]: “The method of claim 1, further comprising, receiving data indicative that the device having the e-key remains within a communication distance of the vehicle during use of the e-key; and”

13[b]: “sending data to disable the e-key and prevent use of the vehicle after a period of time when the data indicates that the device is not within the communication distance of the vehicle for which the e-key is to be used or is used; and”

242. In my opinion, *Zaid* discloses these limitations. *Zaid* discloses that “the vehicle reservation becomes invalid [***sending data to disable the e-key and prevent use of the vehicle after a period of time***] when the wireless communication device is removed from the ***communication range*** of the vehicle access control system, for example when the wireless communication device is removed from physical or wireless communication with the vehicle wireless communication device.” *Id.*, ¶ [0131]. This is performed by “the vehicle access control system periodically communicates with the wireless communication device to verify that the authentic wireless communication device is in communication with the vehicle access control

system by verifying the symmetric key of the wireless communication device,” *i.e.* ***receiving data indicative that the device remains within a communication distance of the vehicle.*** *Id.*

13[c]: “sending a notification or a report, or a log to an administrator of the vehicle to report activity of use of the vehicle in association with use of the e-key.”

243. As discussed above for limitation 1[e], *Zaid* discloses that the renter’s use of the vehicle is monitored to ensure compliance with the conditions of the vehicle reservation.

11. Claim 14: “The method of claim 1, wherein the request to generate the e key for the identified recipient is made using a template having a set of privileges, wherein the template is selectable instead of selecting individual privileges to be associated with the e-key.”

244. In my opinion, *Zaid* discloses or renders obvious this limitation. *Zaid* discloses two types of users: a “vehicle owner” and a “user,” each being a ***selectable template*** with different privileges for (1) accessing the vehicle during a specified time period and (2) using the vehicle during a specified time period. *Id.*, ¶¶ [0069], [0072], claims 5-6. The vehicle owner can reserve “an ***unlimited time period*** for access to the vehicle.” *Id.*, ¶ [0069]. The users can make only temporary reservations, and *Zaid* discloses that “the vehicle reservation ***becomes invalid at the end of the vehicle reservation period.***” *Zaid*, ¶ [0131]. The vehicle owner is thus one template,

and the user is a different template, each defining distinct privileges for use of the vehicle.

245. A POSITA would have understood that *Zaid*'s "vehicle rental application" would distinguish vehicle owners from shared users for the purpose of generating either a vehicle owner "reservation request" (which can be unlimited by time) or a user "reservation request" (limited by time) while the reservation was being booked at the central server. *Zaid* discloses that "for the vehicle owner," "the reservation includes an unlimited time period for access to the vehicle." Thus, a POSITA would have understood that the "time slot" is automatically assigned an unlimited duration period based on the owner "template."

246. Further, it would have been obvious to a POSITA at the relevant time to incorporate templates defining the privileges for use of the vehicle into *Zaid*'s application. This would have been nothing more than an obvious design choice. A POSITA at the relevant time would have easily implemented *Zaid*'s time slot assignments as templates distinguishing vehicle owners from non-owner users, and a POSITA at the relevant time would have been motivated to make this combination to automate portions of the reservation requests process for improving ease of use, as would have been readily apparent from applying common sense. *Id.*, ¶ [0085].

247. *Zaid*'s time slot assignments are also consistent with the broadly described "templates" recited in the '188 patent specification. *See, e.g.*, Ex. 1001,

48:7-8 (“A template can have certain *predefined privileges* that match the assignment of the e-keys.”). Similarly, *Zaid*’s “owner” selection has the predetermined privilege of “unlimited access.”

12. Claim 15: The method of claim 14, wherein the template is one of a child template, or a teen template, or a spouse template, or a mechanic template, or a valet attendant template, or a friend template, or a quest template, or a custom template.

248. In my opinion, *Zaid* discloses this limitation. As I discussed above for claim 14, *Zaid* discloses or renders obvious renter and owner templates, which a POSITA would understand to be a ***custom template*** because they are customized for the renter or owner—*e.g.* the owner template is a ***custom template*** because it is customized to give the vehicle owner “unlimited time period for access to vehicle.” *Id.*, ¶ [0069] In addition, *Zaid* discloses that reservations can be “shared among members of a ... family,” which a POSITA would understand to be ***child or spouse templates*** because a POSITA would understand or consider it obvious that a reservation authorized to be shared among a single family (including children and spouses) will be a template with information and privileges directed to sharing a reservation among a single family. *Zaid*, ¶ [0070]. For example, the reservation template would include authentication information for the children and spouses, or age confirmations for the children. The reservation template would only grant the

privilege of vehicle access during the rental period if the child or spouse can be authenticated and can be verified as someone capable of driving.

13. Independent Claim 16

249. I note that limitations 16[pre] through 16[f] are identical to limitations 1[pre] through 1[f], respectively. Moreover, limitation 16[h] is identical to claim 9. Thus, *Zaid* discloses or renders obvious in view of *Harris* those limitations from claim 16 for the same reasons I explained above. I discuss limitation 16[g] below.

16[g]: “wherein the transmitted e-key is encrypted and configured for decryption to enable use of the vehicle using the e-key;”

250. In my opinion, *Zaid* discloses this limitation. As I discussed above, *Zaid* discloses an encrypted reservation as an *e-key*. *Zaid* further discloses that the e-key is decrypted by the vehicle to enable use of the vehicle. *Id.*, ¶ [0128].

14. Claim 18

18[a]: “The method of claim 1, wherein the condition of use defines one or more privileges associated to use of the e-key, and further comprising,”

251. As I discussed above for the limitation “the request includes a condition of use of the vehicle,” *Zaid* discloses conditions associated with the encrypted reservation (*e-key*), such as a rental time period and time slot. *See, e.g., Id.*, ¶ [0069].

18[b]: receiving a request from the device of the recipient to expand use, or remove a privilege, or add a privilege of the condition of use.

252. In my opinion, *Zaid* discloses this limitation. *Zaid* discloses that the renter's device can ***request removal of a privilege***, specifically invalidating the reservation, by removing the device "from the communication range of the vehicle access control system." *Id.*, ¶ [0131].

15. Independent Claim 19

253. I note that limitations 19[pre] through 19[f] are identical to limitation 1[pre] through 1[f], respectively. I also note that limitation 19[h] is identical to claim 9. Thus, *Zaid* discloses or renders obvious in view of *Harris* those limitations for the same reasons I discussed above.

19[g]: "wherein the e-key received at the device of the recipient includes data to inform the recipient of a level of monitoring that is to occur of the vehicle when the e-key is used for the vehicle, wherein a log is made to save the use of vehicle to a cloud storage, or storage of the vehicle or both, the log including one or more of driving data that took place, or where the vehicle was driven, or speeds of the vehicle, or damage of the vehicle, or radio stations listened to, or conversations had, or images of drivers during specific times, or combinations to two or more thereof;"

254. In my opinion, *Zaid* discloses or renders obvious this limitation. I discuss this limitation in parts given its length.

- i. **wherein the e-key received at the device of the recipient includes data to inform the recipient of a level of monitoring that is to occur of the vehicle when the e-key is used for the vehicle**

255. In my opinion, *Zaid* discloses or renders obvious this limitation. As I discussed above, *Zaid* discloses monitoring various uses of the vehicle. A POSITA would have considered it obvious to include with the encrypted reservation (***e-key***) a notification to the renter (***recipient***) about the ***level of monitoring*** that will occur. Indeed, a POSITA would understand that such level of monitoring will be disclosed in the reservation agreement between the owner and renter, not least because local privacy laws may require such monitoring to be disclosed in advance. In any case, a POSITA would have considered it obvious to inform the renter of such monitoring because it will encourage the renter to use the vehicle within the agreed-upon restrictions.

- ii. **wherein a log is made to save the use of vehicle to a cloud storage, or storage of the vehicle or both, the log including one or more of driving data that took place, or where the vehicle was driven, or speeds of the vehicle, or damage of the vehicle, or radio stations listened to, or conversations had, or images of drivers during specific times, or combinations to two or more thereof**

256. In my opinion, *Zaid* discloses this limitation. As I discussed above for limitations 1[e] and 1[f], *Zaid* discloses monitoring and uploading data that includes ***where the vehicle was driven*** and ***speeds of the vehicle***. *Id.*, ¶¶ [0095], [0130]. *Zaid* further discloses that such data is ***saved to a cloud storage or the vehicle***, i.e. “sent to a central server.” *Id.*

16. Claim 20

20[a]: “The method of claim 19, wherein a plurality of e-keys for the vehicle are producible, the plurality of e-keys can co-exist, and wherein,”

257. As I discussed above for claim 12, *Zaid* discloses or renders obvious generating a plurality of virtual keys (*e-keys*) that can co-exist, such as generating virtual keys for different renters for different time periods and time slots.

20[b]: “only one e-key is associated with active use of the vehicle at one time; or a particular e-key in use with the vehicle can be swapped for another e-key having access to the vehicle, such that each e-key has the same or different privileges or conditions of use; or a priority order of e-keys is defined, such that higher level priority e-keys are placed in use over lower priority e-keys.”

258. In my opinion, *Zaid* discloses this limitation. *Zaid* discloses that a virtual key is only active for the specified time period. *See, e.g., Id.*, ¶ [0131] (“[T]he vehicle reservation becomes invalid at the end of the vehicle reservation period.”). Thus, when there are multiple virtual keys for different rental periods, only one virtual key is active at one time.

E. Ground 5: *Zaid* and *Harris* in view of *Mottla* renders obvious claims 2, 4, 8, and 10 under Section 103

259. *Mottla* is a patent application filed by Zipcar and described a system for renting a car using an app. *Mottla* discloses that the vehicle sends usage data to a server, and that the server can send a notification to the renter’s device indicating

violations of the rental agreement, including exceeding the time period of the agreement. As I discuss below, a POSITA would have found it obvious to combine *Zaid* with *Mottla* to provide notifications.

1. Motivation to Combine

260. In my opinion, a POSITA would have been motivated to modify *Zaid*'s rental car system with *Mottla*'s teachings of notifying the renter that conditions of use are or are about to be exceeded.

261. *Mottla* teaches "push notification[s] sent by the reservation server" to a user's "mobile device." *Mottla*, ¶ [0037]. Such messages "can be used to report gasoline levels, alert the member about reservation start and end times, ... confirm reservations, and to provide billing and payment information." *Id.*, ¶ [0038]. *Mottla* also discloses an app that has a GUI with unlock icons that allow a user to unlock a vehicle. *Id.*, ¶ [0033].

262. In my opinion, a POSITA would have been motivated to incorporate these teachings into *Zaid*'s system because of the well-known benefits of providing push notifications to customers and a user-friendly GUI. By the time of the patent in 2013, smartphones had become ubiquitous, and smartphones such as iPhones or Android devices provided apps that were expected to have functional, user-friendly GUIs and also to receive notifications from service providers of important events and alerts.

263. A POSITA would have known the benefits of such notifications, especially in a rental car system, as it would keep the renter apprised of important events and notifications. For example, a POSITA would understand that informing a renter that the rental period is about to expire or has expired would help renters ensure that they do not exceed the rental period. This would reduce the risk that the vehicle will be unavailable for a subsequent renter, thereby increasing user satisfaction and efficiency. A POSITA would have also known the benefits of a functional GUI, including an icon for unlocking a vehicle that is activated by an e-key. This would provide the user more control over access to the vehicle while maintaining security, as it is the encrypted reservation that allows a renter to gain access to the vehicle. It would also be preferable to provide unlocking on demand via an unlock icon rather than always unlocking the vehicle when the device is in proximity to the vehicle, because it gives better control.

264. A POSITA would have reasonably expected this combination to succeed. Providing push notifications and icons in an app's GUI been used in the industry and implementing such functionality would have been within the capabilities of a POSITA.

265. In my opinion, *Zaid*, *Mottla*, and the '188 patent are all directed to mobile device-driven rental vehicle systems. Ex. 1001, ("In still another embodiment, allowing the user's smart phone or portable electronics to sync with an

EV, users of rental cars.”); *Zaid*, Abstract (“[A] vehicle reservation from a wireless communication device is received, the vehicle reservation is authenticated, and access to the vehicle is provided after authenticating the vehicle reservation.”); *Mottla*, Abstract (“Methods, systems, and devices for reserving a reservable asset using a mobile device.”).

2. Claims 2, 4, and 8

266. Claims 2, 4, and 8 each recite sending a notification to the recipient’s device “identifying the violation of the condition of use” (claim 2), “notify[ing] that the e-key will become disabled due to the violation of the condition” (claim 4), and “warnings of when the use of the vehicle may exceed, has exceeded, or is about to exceed the condition of use” (claim 8).

267. In my opinion, the combination of *Zaid* and *Mottla* discloses these limitations. Specifically, as discussed above, *Zaid* describes a “reservation time period” as a condition of use for the vehicle. *Mottla* teaches “push notification[s] sent by the reservation server” to a user’s “mobile device.” Ex. 1010, ¶37. Such messages “alert the member about reservation start and end times.” *Id.*, ¶38.

268. A POSITA would have considered it obvious to combine *Zaid*’s vehicle rental system with *Mottla*’s method of sending the notification after the end time in order to properly warn the renter to induce return of the car. In such a combined system, following identification of the violation of the time period condition of use,

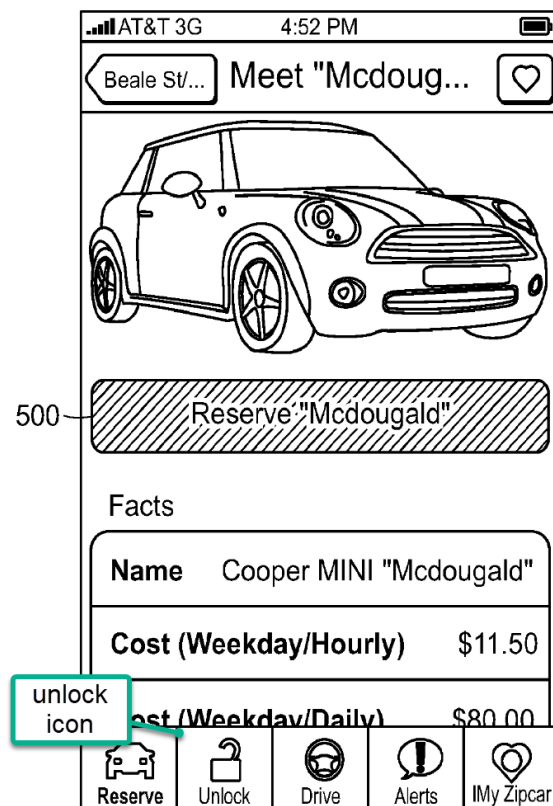
Zaid's server would send a push notification to the Temporary User and the vehicle instructing the Temporary User to terminate use and return the vehicle. This would encourage prompt return of the vehicle and help prevent lengthy overstay.

269. In addition, because Zaid discloses that “the vehicle reservation [**e-key**] becomes invalid at the end of the vehicle reservation period” (Ex. 1008, ¶131), a warning about the expiration is also a warning that the reservation (e-key) is invalid (disabled). If PO argues that the notification must recite “invalid,” it would have been obvious to inform the renter of the consequence of violating the rental period, to encourage timely return of the vehicle. There would be a reasonable expectation of success in providing such a notification due to conventional and well-known systems for providing push notifications, as discussed above. *Id.*

3. Claim 10: “The method of claim 1, wherein the e-key enables graphical icons on a screen of the device to be active for enabling use of the vehicle, at least one of the graphical icons on the screen enabling unlocking of the vehicle, or turning on of the vehicle, or locking the vehicle.”

270. In my opinion, *Zaid* in view of *Mottla* renders obvious this limitation. *Mottla* discloses an application GUI with “an unlock icon 1200” which “unlock[s] the vehicle doors.” *Mottla*, ¶ [0033]. As discussed above, it was obvious to incorporate this icon into *Zaid*, specifically on the renter's device to allow for locking and unlocking capabilities (enabled by an e-key) via a convenient GUI on the device.

271. For example, the functionality of claim 10 is disclosed by *Mottla*, which describes a graphical user interface with “an unlock icon” for remotely “unlock[ing] the vehicle doors.” *Mottla*, ¶ [0033]; Fig. 5.



272. It would have been obvious to incorporate *Mottla*’s unlock icon into *Zaid*, and to enable the use of this icon with *Zaid*’s ekey. A POSITA would be motivated by the benefits of a user-friendly GUI, as providing an unlock button activated by the e-key allows the user better and easier control over vehicle access, and using an unlock icon (instead of text) is easier to comprehend and is more user-friendly. A POSITA would have been motivated to allow the Temporary User control of locking/unlocking via an icon instead of only unlocking the vehicle upon

scanning of the virtual key—that would allow a Temporary User to use the unlock icon after the virtual key has been scanned and authorized, providing a better user experience while maintaining security. A POSITA would have a reasonable expectation of success because GUI icons were standard and implementation was within the capabilities of a POSITA.

273. As I discussed above, Zaid, Mottla, and the '188 patent are in the same field of endeavor of electronic key systems. *Mottla*, Abstract; Ex. 1001, Abstract.

F. Ground 6: Zaid and Harris in view of Patenaude render obvious claim 17 under Section 103

274. *Patenaude* discloses a method for determining a user vehicle entertainment selection profile and automatically activating entertainment units based on monitoring of a user's entertainment selections. As I explain below, it was obvious to incorporate these teachings into *Zaid*.

1. Motivation to Combine

275. In my opinion, it would have been obvious to a person of ordinary skill in the art to combine *Zaid* with *Patenaude*, which teaches a user entertainment selection profile, to reach the limitations of claim 17.

276. *Patenaude* discloses a method for monitoring entertainment selections at a telematics unit, determining a user entertainment selection profile based on that monitoring, and automatically activating entertainment units based on that

monitoring. *Patenaude*, Abstract. *Patenaude* endeavors to “determine and predict entertainment selections,” in particular, by learning a user’s preferences and developing an “entertainment selection profile” for that user which can be stored remotely via a telematics unit in the vehicle. *Id.*, ¶¶ [0001], [0024].

277. It would have been obvious to a person of ordinary skill in the art at the relevant time to combine the features of *Patenaude* with the vehicle of *Zaid*, such that *Zaid*’s electronics and communications circuitry perform *Patenaude*’s method of pattern learning and setting recommendations. Incorporating a pattern learning system to make recommendations based on inputs would have been an obvious functionality to incorporate into a system for sharing vehicles since users may not know how to utilize the interface of a vehicle they are renting or sharing for the first time and/or their favorites may not be stored in it. A system that learns user’s preferred settings such as disclosed in *Patenaude* can recommend those settings automatically to a user who accesses one of *Zaid*’s shared vehicles for the first time.

278. A POSITA would have been motivated to make this combination to provide an additional functionality to *Zaid*’s vehicle sharing service. For example, *Zaid* already recognizes the benefit of “allow[ing] media providers to stream music to the car via the vehicle access kit.” *Zaid*, ¶ [0118]. Implementing *Patenaude*’s method for learning and suggesting entertainment selections with *Zaid*’s vehicle would be a natural improvement since users of *Zaid*’s shared vehicles may be

unfamiliar with the interface and could benefit from automatic suggestions based on past vehicle use stored with their user profile. *See also* Ex. 1018, 13 (“OEMs can extend the in-vehicle communications technologies to allow increased functionality and consumer value with applications that improve the vehicle ownership experience. Enabling the vehicle for m-commerce, remote door lock/unlock, heater on/off, diagnostics, horn sounding and vehicle alarm notification are examples of applications that OEMs can use to differentiate themselves in the marketplace.”), 13 (“Figure 7 lists other data applications that can be provided to the user such as door unlock, sounding the horn, vehicle alarm notification, and web browsing. Other examples include the ability to lock the vehicles doors, flash the lights, turn on the heated seats, start the car (regulations permitting), ***configure user settings (e.g., seat position, radio channel settings, mirror position, etc.)***, transfer data, transfer vehicle information (e.g., mileage, location, error codes, fuel levels, tire pressure, etc.), traffic information and server based navigation.”).

279. In my opinion, a person of ordinary skill in the art would have had a reasonable expectation of success in the combination since *Zaid*’s shared vehicle already includes all necessary hardware for *Patenaude*’s entertainment suggestion system, e.g., wireless communication, local processor and memory, centralized server, music streaming functionality, and typical vehicle audio components. *See Zaid*, ¶ [0085]. The combination would involve *Zaid*’s electronics receiving

Patenaude's "entertainment unit factor" from entertainment units and then performing Patenaude's pattern learning and setting recommendations. The functions of *Patenaude's* telematics unit could easily be performed on *Zaid's* electronics and communications circuitry. The only modification would need to be done in software such that *Zaid's* a user is provided suggestions based on past vehicle use stored in their profile.

280. In my opinion, *Patenaude* is analogous art to the '188 patent and *Zaid* at least because it is reasonably pertinent to the problem faced by the '188 patent inventor (i.e., utilizing remote connectivity to provide added functionality and improve user experience). For example, *Patenaude* describes efforts to overcome limitations in prior systems that could not utilize the telematics services to provide enhanced experiences via predicted entertainment selections. *Patenaude*, ¶¶ [0002-5]. Similar efforts are described throughout the '188 Patent. *See, e.g.*, Ex. 1001, 1:48-50, 4:25-36, 8:19-23.

2. **Claim 17: "The method of claim 16, further comprising, receiving, by the server, data from the vehicle being indicative of interface inputs or settings made during use with the e-key, the inputs or settings being examined to identify patterns; and learning the patterns, by a process executed by the server, to provide recommendations to the recipient or to an account of the recipient, for settings that**

should or may be made to the vehicle when using the e-key.”

281. In my opinion, *Zaid* in view of *Patenaude* renders obvious this limitation.

282. *Patenaude* describes a “telematics unit 120” that communicates with “entertainment units 1356, 136 and 137” such that “data is transmitted ... to the telematics unit 120” “upon power-up of the entertainment units 135, 136 and 137.” *Patenaude*, ¶¶ [0038], [0042-43]. *Patenaude*’s “data” includes “an entertainment unit factor” which is interface input data. *Id.* Specifically, the “entertainment unit factor” includes radio inputs. *Id.*, ¶ [0052].

283. As described above, it would have been obvious to combine the feature of *Patenaude*, including receiving interface input data by the electronics, with the vehicle of *Zaid*.

G. Ground 7: *Kleve* in view of *Patenaude* render obvious claim 17 under Section 103

284. In my opinion, it also would have been obvious to combine *Patenaude* (which as I discussed in Ground 6 above, discloses claim 17) with *Kleve*.

285. In my opinion, it would have been obvious to combine *Kleve*’s rental car system with *Patenaude* for similar reasons I gave above for Ground 6 where I discuss *Zaid* combined with *Patenaude*. For example, learning preferences adds additional functionality to *Kleve*’s rental service in the same way it adds

functionality to *Zaid*'s car sharing service. All of the reasons I mentioned above for combining *Patenaude* with *Zaid* apply equally to *Kleve* given that they disclose similar systems.

286. In my opinion, a POSITA would have had a reasonable expectation of success for similar reasons I mentioned above in Ground 6 since, like *Zaid*, *Kleve* includes all the necessary hardware for *Patenaude*'s system, including wireless communication, computing systems, and vehicle settings. Implementation would simply require adding software to receive *Patenaude*'s data and perform its algorithms

287. In my opinion, as I have discussed above in Ground 2 and Ground 6, both *Kleve* and *Patenaude* are analogous art to the '188 patent.

IX. Secondary Considerations of Non-obviousness

288. I am not aware of any secondary considerations, or so-called "objective indicia of non-obviousness" for the challenged claims.

289. Secondary considerations could include things like commercial success of a product due to the merits of the claimed invention; a long felt need for the solution provided by the claimed invention; unsuccessful attempts by others to find the solution provided by the claimed invention; copying of the claimed invention by others; unexpected and superior results from the claimed invention; acceptance by others of the claimed invention as shown by praise from others in

the field or from the licensing of the claimed invention; teaching away from the conventional wisdom in the art at the time of the invention; independent invention of the claimed invention by others before or at about the same time as the named inventor thought of it; and other evidence tending to show obviousness.

290. Patent Owner has not identified any such secondary considerations, and I am not independently aware of any. For example, Patent Owner has no commercial products embodying the '188 patent that I am aware of. Additionally, as discussed throughout, the claimed features reflect predictable results of combining known elements according to their known functions, and thus, there are no unexpected and superior results from the claimed invention. Also, there are no licenses of the '188 patent of which I am aware.

291. Further, even if Patent Owner were to assert that secondary considerations exist, given the strong reasons that the challenged claims are obvious in light, including the motivations to combine the references set forth above, I do not believe any such secondary considerations would rise to the level of overcoming the invalidity opinions I have expressed.

292. I understand that Patent Owner may address the issue of secondary considerations more fully in the future. I reserve the right to respond to any specific bases for such secondary considerations that Patent Owner may identify.

X. Conclusion

293. For the reasons set forth above, I believe claims 1-20 of the '188 patent are unpatentable in view of the prior art. In signing this declaration, I understand that the declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I acknowledge that I may be subject to cross-examination in this case and that cross-examination will take place within the United States. If cross-examination is required of me, I will appear for cross-examination within the United States during the time allotted for cross-examination.

294. I declare that all statements made herein of my knowledge are true, that all statements made on information and belief are believed to be true, and 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.

Dated: May 29, 2024

By: Kevin C Almeroth
Kevin C. Almeroth, Ph.D.