

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. IPR2024-001167
U.S. Patent No. 11,738,659

**DECLARATION OF KEVIN C. ALMEROOTH, PH.D.
IN SUPPORT OF PETITION FOR *INTER PARTES* REVIEW OF
U.S. PATENT NO. 11,738,659**

TABLE OF CONTENTS

I.	Introduction.....	1
II.	Qualifications and Background.....	2
III.	Materials Considered	15
IV.	Legal Standards.....	16
	A. Claim Construction.....	16
	B. Anticipation Under 35 U.S.C. § 102.....	17
	C. Obviousness Under 35 U.S.C. § 103	17
	D. Priority Under 35 U.S.C. § 120	21
V.	The '659 patent	24
	A. Overview of the '659 patent	24
	B. Prosecution History of the '659 patent	28
	C. The '659 patent's claims are entitled to an effective filing date of no earlier than October 25, 2013	31
	D. Person of Ordinary Skill in the Art.....	38
VI.	Claim Construction of Terms of the '659 patent	40
VII.	Overview of Prior Art	41
	A. Kleve.....	41
	B. Mikan.....	45
	C. Secondary References.....	51
VIII.	Summary of Opinions on Unpatentability	51
	A. Ground 1: Kleve in view of Hatton renders obvious claims 1 and 3-21 under Section 103.....	52

1.	Motivation to Combine Kleve and Hatton and Reasonable Expectation of Success	53
2.	Independent Claim 1.....	58
3.	Claim 3: “The sub-system of the vehicle of claim 1, wherein the vehicle is configured to receive or securely store information from the server to perform authentication or verification that the coded data received from the mobile device should activate the eKey.”	76
4.	Claim 4: “The sub-system of the vehicle of claim 1, wherein the communications circuitry of the vehicle is configured to receive one or more additional requests from other mobile devices to use the vehicle, each request is associated with coded data generated by the server, such that each coded data is associated with a user account having privileges assigned by an administrator of the vehicle that enables assigning or use of eKeys to use the vehicle.”	78
5.	Claim 5: “The sub-system of the vehicle of claim 1, wherein the wireless communication circuitry is associated with an NFC standard or a radio frequency standard for said local connection between the mobile device and the vehicle.”	81
6.	Claim 6: “The sub-system of the vehicle of claim 1, wherein an application associated with said mobile device is configured to enable sharing of said eKey with a recipient user having a recipient mobile device, the sharing is enabled via a message initiated from said mobile device.”	82
7.	Claim 7: “The sub-system of the vehicle of claim 1, wherein the coded data is processed securely by the mobile device responsive to registering the e-Key to the mobile device, the registering being enabled by an owner of said vehicle or an administrator of said vehicle.”	83

8. Claim 8: “The sub-system of the vehicle of claim 1, wherein a mode of allowed use of the vehicle using the eKey is configured to monitor said use of the vehicle, and said on-board computer is configured to transmit one or more notifications when a violation of a restriction is detected.” 85
9. Claim 9: “The sub-system of the vehicle of claim 1, wherein the tracked use of the vehicle is configured to identify a violation, and the violation is associated with one or more of driving too fast, or driving out of an area, or accelerating too fast, or stopping too fast, or parking too close to a structure or other vehicle, or coming in contact with a structure or another vehicle, or slamming a door of the vehicle, or turning on a radio, or texting while driving, or interfacing with vehicle controls while driving, or two or more thereof.” 86
10. Claim 10: “The sub-system of the vehicle of claim 1, wherein the tracked use of the vehicle is configured to identify a violation, and the violation is associated with exceeding a speed limit, or time limit, or an area limit.” 87
11. Independent Claim 11.....88
12. Claim 12: “The system of a vehicle as recited in claim 11, wherein a server is configured for communication with the application executed by the mobile device, the server is one of a plurality of servers, and one of said servers is associated with a manufacturer of the vehicle.” 93
13. Claim 13 95
14. Claim 14: “The system of a vehicle as recited in claim 11, wherein said on-board computer includes logic for processing encryption operations of said eKey in coordination with logic of said mobile device.” 98
15. Claim 15: “The system of a vehicle as recited in claim 14, wherein said encryption operations use secure public/private key pair encryption operations.” 99

16.	Claim 16: “The system of a vehicle as recited in claim 11, wherein said wireless communication circuitry facilitates one or more of Bluetooth, near field communication (NFC), WiFi, or radio communication.”	101
17.	Claim 17: “The system of a vehicle as recited in claim 11, wherein said eKey is validated and securely bound to the mobile device to prevent unauthorized transfers of the ekey.”.....	101
18.	Independent Claim 18.....	102
19.	Claim 19: “The vehicle of claim 18, wherein the privilege settings being unrestricted for an owner of the vehicle and restricted for a shared user of the vehicle, the shared user of the vehicle receives a shared eKey responsive to said owner of the vehicle causing the shared eKey to be sent for shared use of the vehicle.”	104
20.	Claim 20: “The vehicle of claim 18, wherein the eKey is securely generated on the mobile device, and wherein a server associated with a manufacturer of the vehicle is configured to communicate with the application, the application further being associated with a manufacturer of the vehicle.”.....	106
21.	Claim 21: “The vehicle of claim 18, wherein encryption operations are associated with use of said eKey, and said encryption operations use public/private key pair encryption, and wherein said wireless communication circuitry uses one or more of Bluetooth, or near field communication (NFC), or WiFi, or radio communication.”	106
B.	Ground 2: Klevé in view of Hatton and Sekiyama renders obvious claim 2 under Section 103.....	106
1.	Motivation to Combine Klevé, Hatton, and Sekiyama and Reasonable Expectation of Success.....	107

2.	Claim 2: “The sub-system of the vehicle of claim 1, wherein said privileges function as restrictions that enable access to specific vehicle areas that include one or more of vehicle door operation, or trunk operation.”	110
C.	Ground 3: Mikan anticipates or renders obvious claims 1-3, 5 and 8-10 under Section 102 or Section 103.....	111
1.	Claim 1	112
2.	Claim 2: “The sub-system of the vehicle of claim 1, wherein said privileges function as restrictions that enable access to specific vehicle areas that include one or more of vehicle door operation, or trunk operation.”	122
3.	Claim 3: “The sub-system of the vehicle of claim 1, wherein the vehicle is configured to receive or securely store information from the server to perform authentication or verification that the coded data received from the mobile device should activate the eKey.”.....	123
4.	Claim 5: “The sub-system of the vehicle of claim 1, wherein the wireless communication circuitry is associated with an NFC standard or a radio frequency standard for said local connection between the mobile device and the vehicle.”.....	124
5.	Claim 8: “The sub-system of the vehicle of claim 1, wherein a mode of allowed use of the vehicle using the eKey is configured to monitor said use of the vehicle, and said on-board computer is configured to transmit one or more notifications when a violation of a restriction is detected.”.....	125
6.	Claim 9: “The sub-system of the vehicle of claim 1, wherein the tracked use of the vehicle is configured to identify a violation, and the violation is associated with one or more of driving too fast, or driving out of an area, or accelerating too fast, or stopping too fast, or parking too close to a structure or other vehicle, or coming in contact with a structure or another vehicle, or slamming a door of	

the vehicle, or turning on a radio, or texting while driving, or interfacing with vehicle controls while driving, or two or more thereof.”	126
7. Claim 10: “The sub-system of the vehicle of claim 1, wherein the tracked use of the vehicle is configured to identify a violation, and the violation is associated with exceeding a speed limit, or time limit, or an area limit.”	127
D. Ground 4: Mikan in view of Xiao renders obvious claims 4, 11-18, and 20-21 under Section 103	127
1. Motivation to Combine Mikan and Xiao and Reasonable Expectation of Success.....	128
2. Claim 4: “The sub-system of the vehicle of claim 1, wherein the communications circuitry of the vehicle is configured to receive one or more additional requests from other mobile devices to use the vehicle, each request is associated with coded data generated by the server, such that each coded data is associated with a user account having privileges assigned by an administrator of the vehicle that enables assigning or use of eKeys to use the vehicle.”	131
3. Independent Claim 11.....	137
4. Claim 12: “The system of a vehicle as recited in claim 11, wherein a server is configured for communication with the application executed by the mobile device, the server is one of a plurality of servers, and one of said servers is associated with a manufacturer of the vehicle.”	142
5. Claim 13	144
6. Claim 14: “The system of a vehicle as recited in claim 11, wherein said on-board computer includes logic for processing encryption operations of said eKey in coordination with logic of said mobile device.”	145

7.	Claim 15: “The system of a vehicle as recited in claim 14, wherein said encryption operations use secure public/private key pair encryption operations.”	147
8.	Claim 16: “The system of a vehicle as recited in claim 11, wherein said wireless communication circuitry facilitates one or more of Bluetooth, near field communication (NFC), WiFi, or radio communication.”	147
9.	Claim 17: “The system of a vehicle as recited in claim 11, wherein said eKey is validated and securely bound to the mobile device to prevent unauthorized transfers of the ekey.”	148
10.	Independent Claim 18.....	149
11.	Claim 20	150
12.	Claim 21: “The vehicle of claim 18, wherein encryption operations are associated with use of said eKey, and said encryption operations use public/private key pair encryption, and wherein said wireless communication circuitry uses one or more of Bluetooth, or near field communication (NFC), or WiFi, or radio communication.”	150
E.	Ground 5: Mikan in view of Sekiyama renders obvious claims 6 and 7 under Section 103.....	151
1.	Motivation to Combine Mikan and Sekiyama and Reasonable Expectation of Success.....	151
2.	Claim 6: “The sub-system of the vehicle of claim 1, wherein an application associated with said mobile device is configured to enable sharing of said eKey with a recipient user having a recipient mobile device, the sharing is enabled via a message initiated from said mobile device.”	154
3.	Claim 7: “The sub-system of the vehicle of claim 1, wherein the coded data is processed securely by the mobile	

device responsive to registering the e-Key to the mobile device, the registering being enabled by an owner of said vehicle or an administrator of said vehicle.” 155

F.	Ground 6: Mikan in view of Xiao and Sekiyama renders obvious claim 19 under Section 103	157
1.	Claim 19: “The vehicle of claim 18, wherein the privilege settings being unrestricted for an owner of the vehicle and restricted for a shared user of the vehicle, the shared user of the vehicle receives a shared eKey responsive to said owner of the vehicle causing the shared eKey to be sent for shared use of the vehicle.”	158
IX.	Secondary Considerations of Non-obviousness.....	159
X.	Conclusion	162

TABLE OF EXHIBITS

No.	Short Name	Description
1001	'659 patent	U.S. Patent No. 11,738,659 to <i>Penilla</i> et al.
1002	'659 prosecution history	Prosecution File History for U.S. Patent No. 11,738,659.
1003	Almeroth CV	Curriculum Vitae of Dr. Kevin Almeroth.
1004		Intentionally Left Blank
1005	Kleve	U.S. Patent Pub. No. 2014/0129053 to Kleve et al.
1006	Sekiyama	Japanese Laid Open Patent Application Publication No. 2010-126949 to Sekiyama
1007	Mikan	U.S. Patent Pub. No. 2008/0150683 to Mikan et al.
1008	Hatton	U.S. Patent No. 9,002,536 to Hatton
1009	Fukushima	U.S. Patent No. 7,868,736 to Fukushima et al.
1010	Xiao	U.S. Patent No. 8,737,913 to Xiao et al.
1011	'436 application	U.S. Patent Application No. 61/478,436
1012	'729 application	U.S. Patent Application No. 61/745,729
1013	'882 application	U.S. Patent Application No. 13/452,882
1014	'158 application	U.S. Patent Application No. 13/842,158
1015	'638 application	U.S. Patent Application No. 14/063,638
1016	'566 application	U.S. Patent Application No. 15/344,566
1017	'306 application	U.S. Patent Application No. 15/180,306
1018	'442 application	U.S. Patent Application No. 14/303,442

No.	Short Name	Description
1019	'958 application	U.S. Patent Application No. 16/653,958
1020	'241 application	U.S. Patent Application No. 15/854,241
1021	'418 application	U.S. Patent Application No. 15/607,418
1022	'158/'638 application comparison	Text Comparison of U.S. Pat. App. No. 13/842,158 to U.S. Pat. App. No. 14/063,638
1023	Reexamination order	Order Granting Request For Ex Parte Reexamination, Reexamination Control No. 90/019,456, Patent No. 11,738,659 (April 15, 2024)
1024	Docket Control order	Docket Control Order in <i>Emerging Automotive LLC v. Kia Corp.</i> , No. 2:23-CV-00437-JRG (E.D. Tex.) (Feb. 6, 2024)

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. 11,738,659 (the “’659 patent”), and I have been asked to provide my opinions as to the patentability of the claims of the ’659 patent. I understand that the application for the ’659 patent was filed on August 30, 2021, and is the last in a series of continuation applications beginning with U.S. Patent Application No. 14/063,638 (the “’638 application”), having a filing date of October 25, 2013. I understand the ’659 patent and the ’638 application also purport to be continuations-in-part of U.S. applications filed March 15, 2013, and April 22, 2012, respectively, and claim 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 ’659 patent. As discussed herein, it is my opinion that claims 1-21 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 '659 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 1-21 of the '659 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 fast-forward) 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 networking 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, create 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 marketplace. 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 documents listed in the Table of Exhibits included on pages ix-x of this declaration.

IV. Legal Standards

31. In forming my opinions and considering the subject matter of the '659 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, 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.

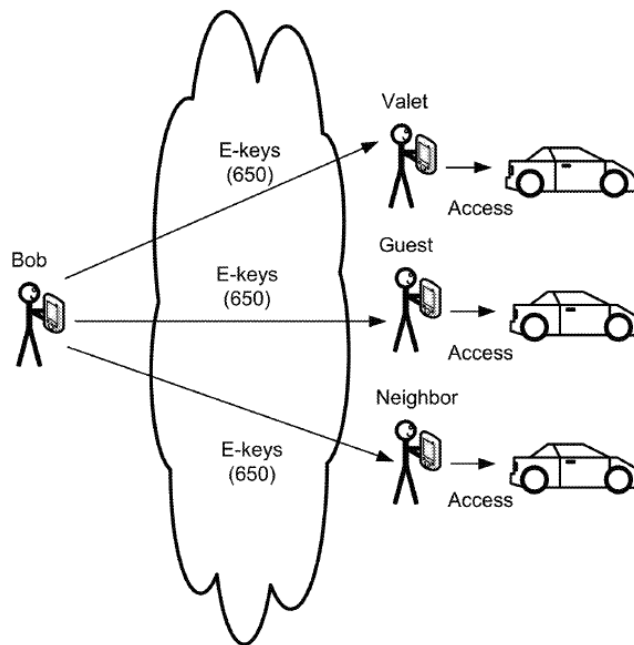
V. The '659 patent

A. Overview of the '659 patent

54. The application that led to the '659 patent was filed on August 30, 2021. It is my opinion that the earliest date to which the challenged claims of the '659 patent can claim priority, as explained in further detail in section V.C, is October 25, 2013. The '659 patent, on its face, references four applications dated earlier than October 25, 2013: 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 '659 patent could claim priority back to any of these dates (which it cannot), my ultimate conclusions as to the invalidity of the '659 patent would not change. To be clear, if the '659 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 '659 patent is entitled to the earliest priority date, the Mikan-based grounds would render the Challenged Claims obvious. In addition, I have been informed that Sekiyama and Xiao are prior art regardless of the '659 patent's priority date.

55. **The '659 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. '659 patent at Abstract. For example, in Figure 29, vehicle owner Bob

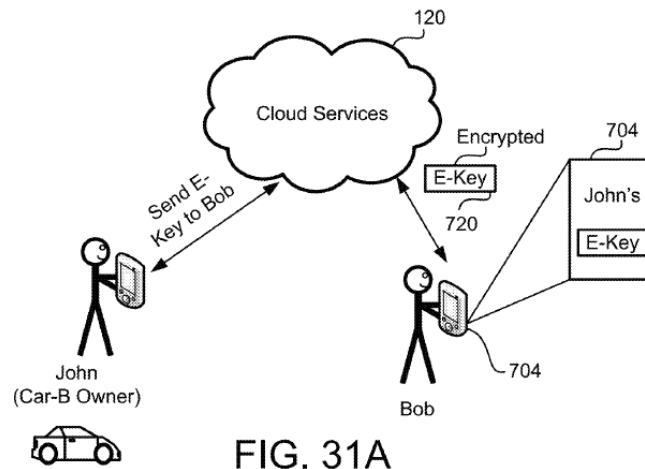
shares electronic keys 650 with users “valet,” “guest,” and “neighbor” for vehicle access. *Id.* at 43:37-39. The specification explains that “[e]ach e-key, in one embodiment, will include a unique access code or substantially unique access code.” *Id.* at 43:52-53. Further, “[t]he unique generation 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 43:60-64.



'659 patent, Fig. 29.

56. In Figure 31A, vehicle owner John utilizes a cloud server 120 to send an encrypted e-key to guest user Bob. In this embodiment, “the server will generate an access code for the vehicle” (*id.* at 44:54-55), which “will then be encrypted by

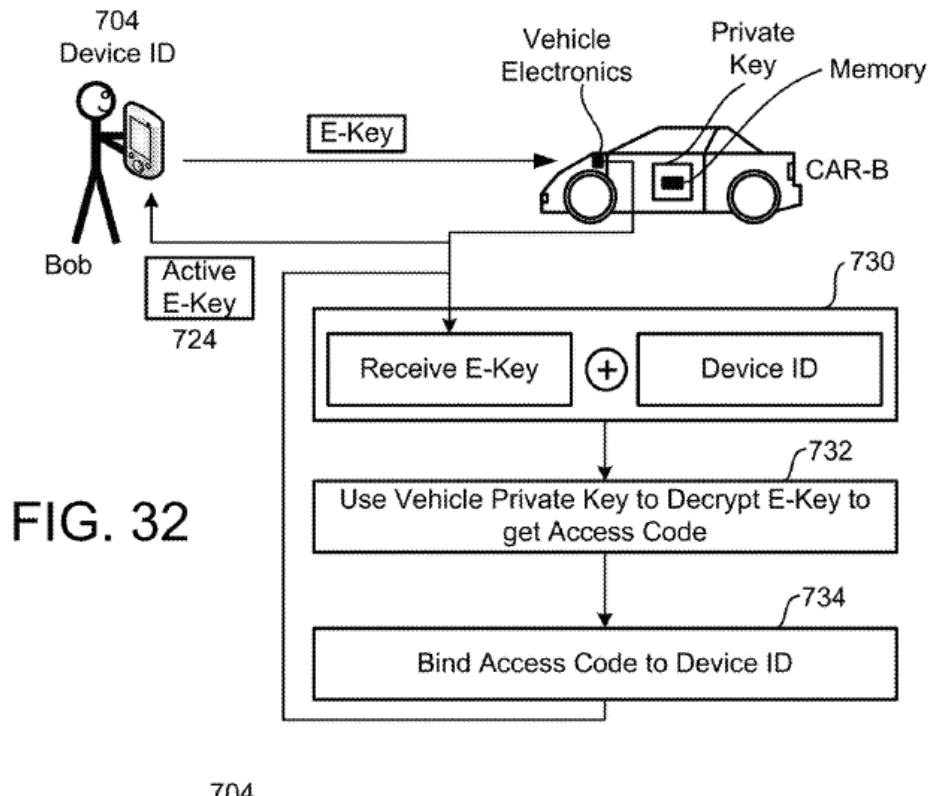
the server and then sent as encrypted e-keys 722¹ to Bob's device 704." *Id.* at 44:55-57.



'659 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 44:63-45:5.

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



'659 patent, Fig. 32.

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 e-key is “associated” with the mobile device. *Id.* at 45:10-12. In step 732, “the vehicle private key is used to decrypt the e-keys to get access to an access code.” *Id.* at 45:20-22. 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.* at 45:25-27.

59. The specification also 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 43:39-40. For example, “electronic keys for each user can be associated with a different expiration time.” *Id.* at 43:50-51; *see also id.* at 50:50-52 (“the privileges can be assigned by selecting . . . time durations[.]”). Other privilege settings may determine the “type of access, speed limits, geographic restrictions, [and] amount of time the e-keys will be valid.” *Id.* at 44:39-48, 45:27-29. In the example above, once Bob receives the e-key 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 45:27-29.

B. Prosecution History of the ’659 patent

60. I have reviewed the prosecution history of the application that led to the ’659 patent. Ex. 1002. I summarize several of the important office actions and amendments below.

61. On August 25, 2022, the Examiner issued a non-final rejection rejecting all claims based on U.S. Patent Pub. 2011/0112969 (“Zaid”), alone or in combination with several other references (U.S. Patent Pub. No. 2011/0060480 (“Mottla”), U.S. Patent Pub. No. 2009/0062971 (“Rottig”)). Ex. 1002 (’659 Prosecution History) at 173-196.

62. On January 6, 2023, the Applicant amended the claims, adding a limitation to each independent claim reciting that “coded data” for the electronic key

includes “privilege settings set for additionally limiting types of use of the vehicle when using the ekey with the vehicle.” *Id.* at 332-338. The Applicant argued that in Zaid’s system, once a vehicle reservation is decrypted, “the use [of the vehicle] is unlimited,” and Zaid’s electronic key is only “used to control the ‘time’ for the reservation and the identification of the vehicle.” *Id.* at 339. The Applicant distinguished this from the “privilege settings set for additionally limiting types of use of the vehicle when using the ekey with the vehicle” added to the claims. *Id.*

63. On February 7, 2023, the Examiner issued a final rejection rejecting all claims based on Zaid in combination with U.S. Patent Pub. No. 2005/0203752 (“Shinada”). *Id.* at 342-368. The Examiner explained that Shinada teaches “restrictions to limit the usage of the vehicle.” *Id.* at 352.

64. On May 9, 2023, the Applicant again amended the claims, adding to each independent claim a limitation that “wireless communication circuitry” is used “for enabling local connection with a mobile device, the mobile device is configured to use the eKey for said unlocking and said starting of the vehicle,” and further amending the claims to recite that the coded data is received by the “wireless communications circuitry ... when using the eKey” and “is associated to the eKey for use by the mobile device.” *Id.* at 503-510. Responding to the Examiner’s rejection based on Shinada, the Applicant argued that “Shinada’s teachings are not

related to what is claimed” because “Shinada is not teaching an electronic key that can be used by a mobile device,” and Shinada’s “restriction is defined under the car rental contract ... set at the time of renting.” *Id.* at 511-512. The Applicant argued that Shinada did not teach that “the coded data is associated to the eKey for use by the mobile device, and the coded data includes privilege settings associated with the eKey for limiting types of use of the vehicle when using the eKey with the vehicle.” *Id.* The Applicant did not specifically address the Examiner’s combination of Zaid and Shinada, which relied on Zaid for the teaching of an electronic key system where a mobile device is used as the electronic key. Specifically, the Applicant did not provide any reason why a POSITA would not or could not have combined Zaid and Shinada by applying Shinada’s restrictions on use to Zaid’s electronic key system in order to arrive at the claims. *See id.*

65. The Applicant also argued that the combination of Zaid and Shinada does not teach “communications circuitry includ[ing] wireless communications circuitry for enabling local connection with a mobile device, and the mobile device is configured to use the eKey for said unlocking and said starting of the vehicle.” *Id.* at 504-10, 512. But the Applicant did not discuss the specific portions of Zaid that were cited by the Examiner, and describe a “wireless communication device” that

allows “opening the vehicle door, and/or allowing engine to be turned on by user.”

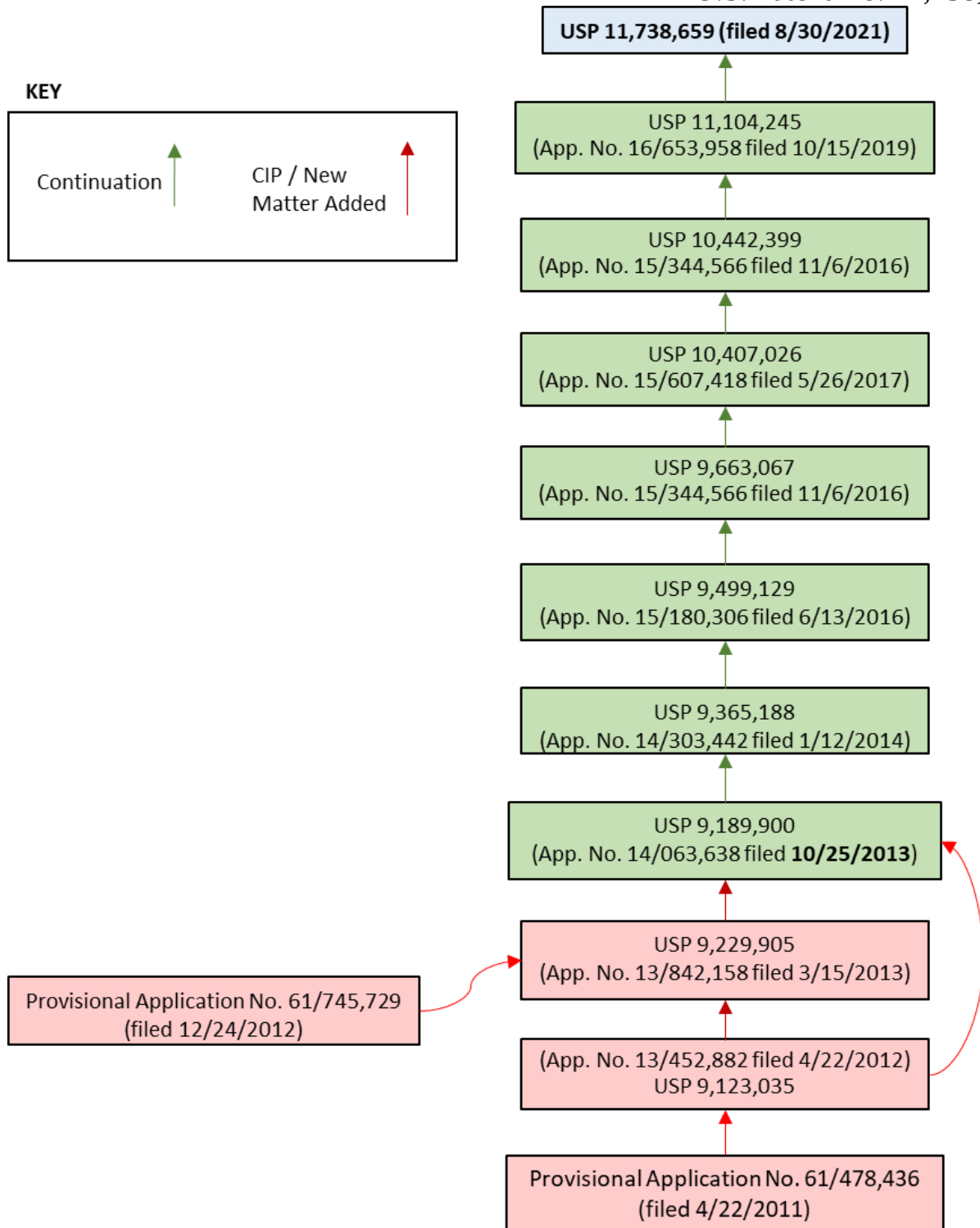
Id. at 350 (quoting Zaid).

66. On June 26, 2023, the Examiner allowed the claims based on the May 9, 2023 amendment. *Id.* at 519-522.

67. I am not aware of anything else in the prosecution history that impacts 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 '659 patent's claims are entitled to an effective filing date of no earlier than October 25, 2013

68. The application leading to the '659 patent claims priority to U.S. Application Nos. 16/653,958 (now U.S. Pat. No. 11,104,245), 15/854,241 (now U.S. Pat. No. 10,442,399), 15/607,418 (now U.S. Pat. No. 10,407,026), 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), 14/063,638 (now U.S. Pat. No. 9,189,900), 13/824,158 (now U.S. Pat. No. 9,229,905) (“'158 Application”), 13/452,882 (now U.S. Pat. No. 9,123,035) ('882 application), 61/478,436, and 61/745,729. *See* Exs. 1011-1021. The chart below summarizes the relationships between the different applications.



69. I observe that the '638 application (Ex. 1015) describes itself as a

“continuation-in-part” of the ’158 application (Ex. 1014) and the ’882 application (Ex. 1013). 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 ’659 patent is related to the ’638 application via multiple continuation applications.

70. There are numerous differences between the ’638 application and the ’158 application, which are evident from a computerized comparison of the two. See Ex. 1022. For example, I observe several new paragraphs and figures describing “e-keys” in the ’638 application that do not appear in either the ’158 application or the ’882 application. *Id.* In my opinion, the claim limitations reciting “**processing**” or “**communicating**” “**an electronic key (eKey)**”; “**us[ing] the eKey** for said unlocking and said starting of the vehicle”; and “**receiv[ing] ... coded data** includ[ing] privilege settings set for limiting types of use of the vehicle when **using the vehicle via the eKey,**” as required by every claim of the ’659 patent, are not found in the earlier applications.

71. The new matter introduced in the '638 application, is not present in any of the preceding filings. *See* Exs. 1011-1015, Ex. 1022. This new matter is the only basis on which the specification for the '659 patent even arguably conveys to a person of ordinary skill in the art that the inventors had developed a system for processing, using, and receiving eKeys and associated coded data.

72. For example, Figures 17 through 35 of the '638 application (which are the same as Figures 17 through 35 of the '659 patent) and their descriptions were introduced in the '638 application and discuss in detail the processing, communicating, and use of e-keys and associated data. *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.”).

73. As shown below, Figure 35 depicts the processing and communicating of an e-key and coded data to Bob’s mobile device.

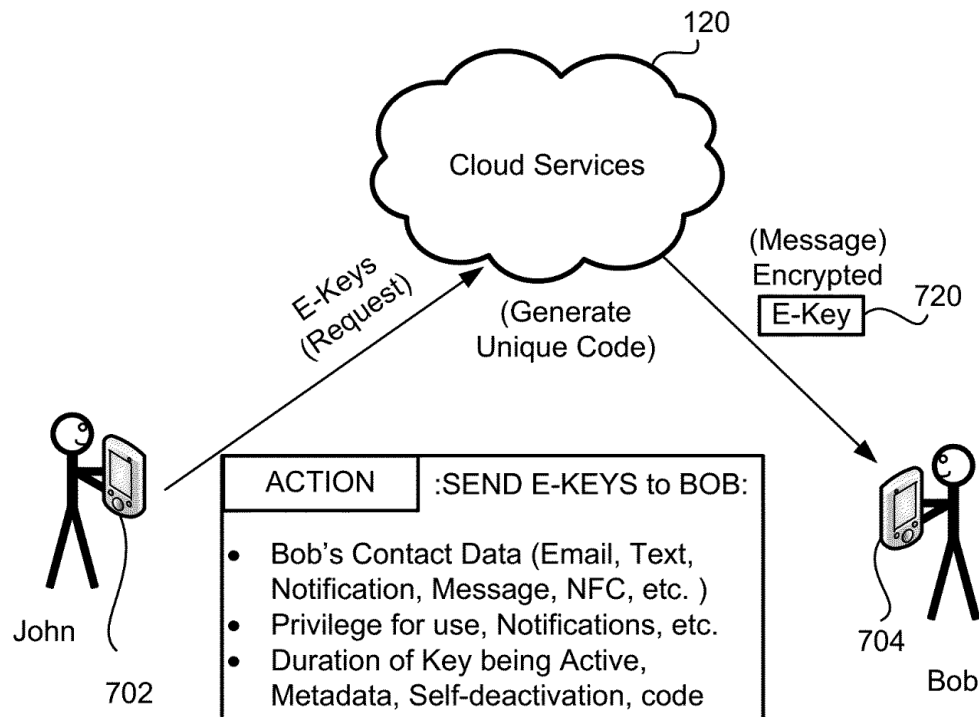


FIG. 35

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

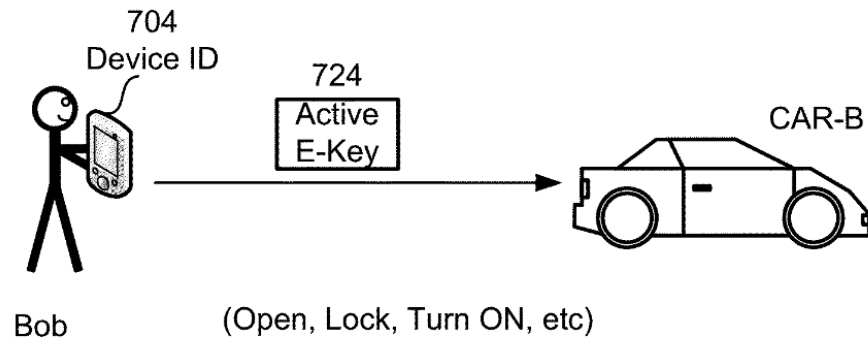


FIG. 33

75. 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.

76. 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. 1014, Abstract. And the '882 application is directed to charging an electric vehicle. Ex. 1013, Abstract; Exs. 1011-12.

77. 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. 1014 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, ...”).

78. 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.

79. Accordingly, in my opinion, the '659 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, as described above. 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.

80. I also understand that the Patent Office considered the effective priority date of the '659 patent in granting *ex parte* reexamination of the '659 patent. See Ex. 1023 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.

81. 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

82. 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 '659 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.

83. 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.

84. The '659 patent claims the benefit of U.S. Provisional Application No. 61/478,436 (Ex. 1011) filed April 22, 2011, U.S. Provisional Application No. 61/745,729 (Ex. 1012) filed December 24, 2012, U.S. Application No. 13/452,882 (Ex. 1013) filed April 22, 2012, and U.S. Application No. 13/842,158 (Ex. 1014) filed March 15, 2013. However, as discussed herein, in my opinion, the Challenged Claims of the '659 patent are not entitled to a priority date any earlier than October 25, 2013.

85. 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 '659 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.

86. Although I surpass this definition of one of ordinary skill in the art now and at the priority date of the '659 patent, my analysis regarding the '659 patent has been based on the perspective of one ordinary skill in the art as of the priority date of the '659 patent.

87. I am also familiar with the knowledge of the person of ordinary skill in the art as of the priority date of the '659 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 '659 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.

88. 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 '659 patent

89. 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.

90. 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

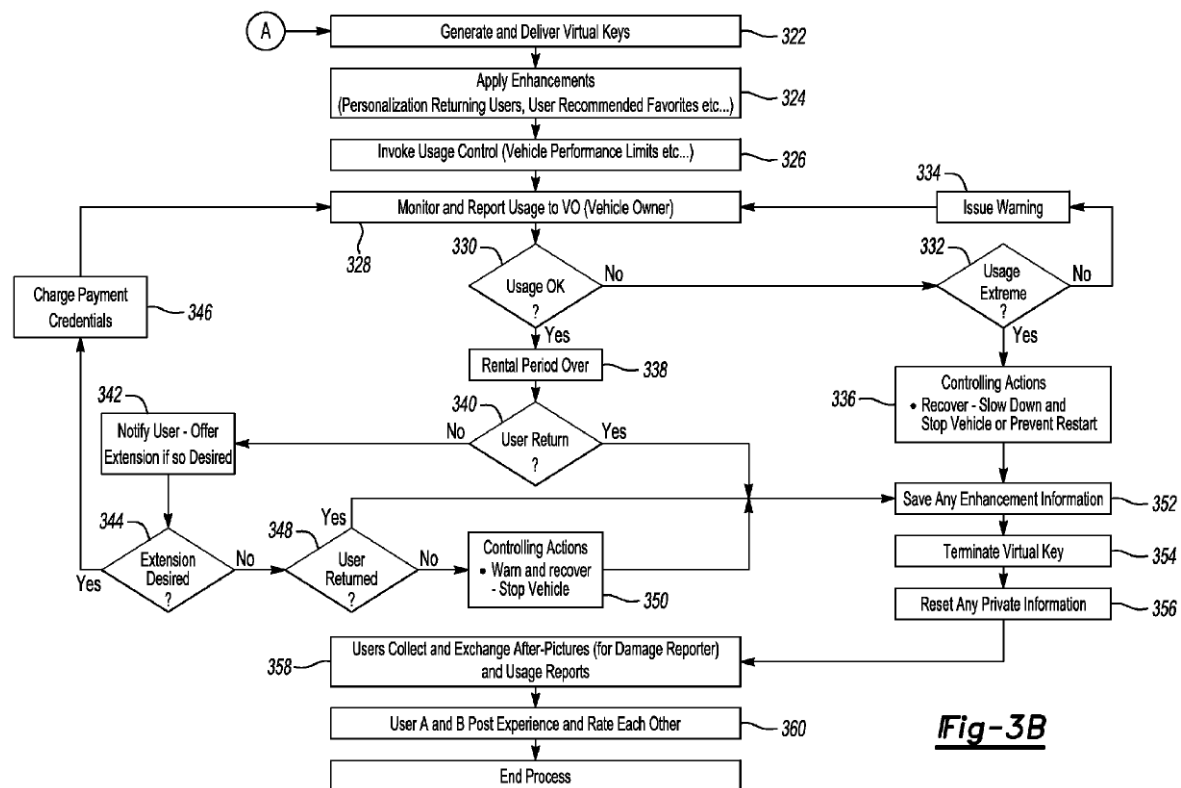
91. Below, I discuss the two primary references I rely on.

A. Kleve

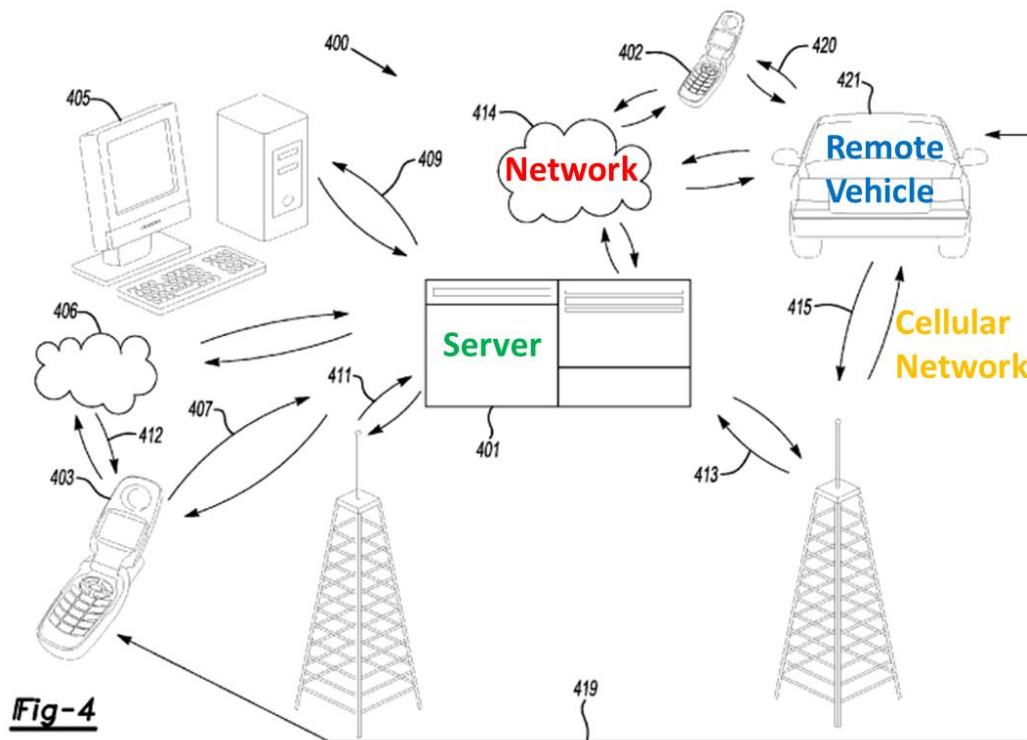
92. Kleve discloses a “vehicle rental micro-business” which “include[s] a website, smart phone application or other nomadic device that an Owner and Temporary User may use to manage their assets and/or user profile.” Ex. 1005 (Kleve) at ¶ [0035]. The “Owner” is a Vehicle Owner and “may set up a *user profile* using a website ... that is stored in a database,” which includes “the make, model and year of the vehicle available for rent.” *Id.* at ¶ [0037].

93. A Temporary User likewise “setups their user identity within the website” after which they “may begin to use the vehicle rental services.” *Id.* at ¶ [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.*

94. 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.* at ¶ [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.* at ¶ [0067], [0044]. Figure 3B illustrates the process by which virtual keys are generated, delivered to the Temporary User, and used to access the vehicle.



95. Kleve's vehicle manages virtual keys using a "vehicle computing system" in communication with a "server." *Id.* at ¶ 0035. Communication with the server may be direct, using built-in wireless capabilities in the vehicle, or indirect, via a Bluetooth connection to the user's mobile device. *Id.* at ¶¶ [0057], [0060]. The two alternative communication paths are illustrated in Figure 4.



96. 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]).

97. 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.* at ¶ [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.”).

98. 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.* at ¶ [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.* at ¶ [0054].

B. Mikan

99. Mikan discloses “wireless devices for providing secure operation of a vehicle.” Ex. 1007 (Mikan) at Abstract. Mikan’s system supports multiple types of keys, including “electronic keys” that are “embedded in a wireless device such as a cellular telephone or Personal Digital Assistant.” *Id.* at Abstract, ¶ [0050]. When the key is detected by the vehicle, “a vehicle operation policy associated with the key is retrieved, and operation of the vehicle consistent with the vehicle operation policy is permitted. *Id.* “The vehicle operation policy may include an access control rule that may indicate to enable, partially enable, or disable a vehicle operation feature.” *Id.*

100. A high level diagram of Mikan’s system is illustrated in Figure 2, reproduced below.

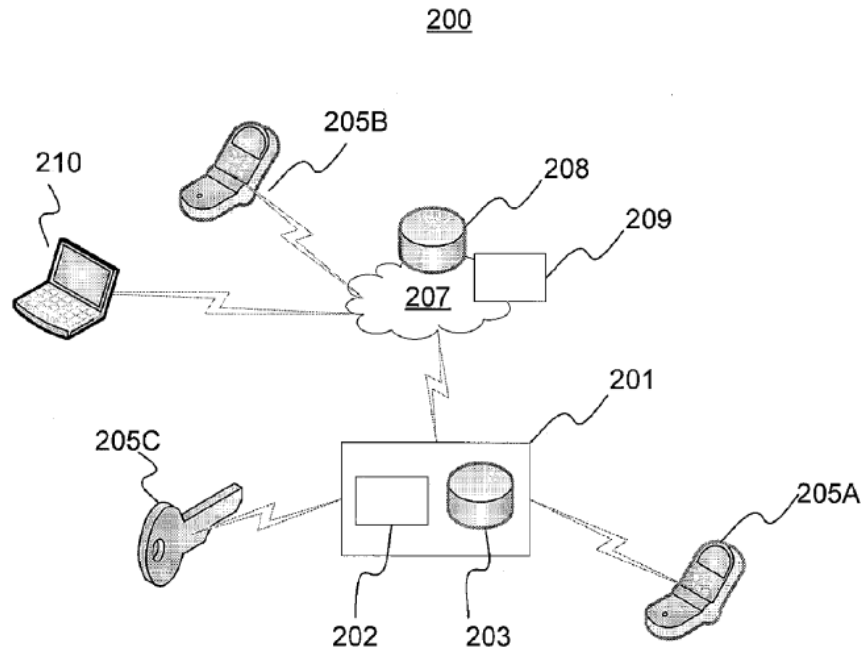


FIG. 2

101. Mikan's vehicle includes a "control unit 202 ... in communication with wireless network 207." *Id.* at ¶ [0052]. Wireless communications from the vehicle may make use of various standard wireless communication protocols, including cellular communication protocols (such as GSM, GPRS, EDGE, and W-CDMA), IEEE 802.11 WiFi, and Bluetooth. *Id.* at ¶¶ [0052], [0067]. "Control unit 202 may interface with vehicle 201" and "control vehicle functions and ... sense operation of vehicle 201." *Id.* at ¶ [0053]. The control unit uses the interface with the vehicle to

perform functions such as “lock[ing] and unlock[ing] the vehicle doors” or “sens[ing] vehicle speed and the status of the ignition.” *Id.*

102. Mikan’s vehicle can interface with a “wireless device 400 equipped for use as a key 205A-C within wireless vehicle security system 200.” *Id.* at ¶ [0062]. The wireless device includes a “security application 409 and vehicle access module 408.” *Id.* at ¶ [0067]. The vehicle access module “may communicate with vehicle 201 to send [a] secure identifier 407 to vehicle 201.” *Id.* The secure identifier may be “a digital signature associated with wireless device 400,” or “a digital signature associated with a key 205A-C.” *Id.* at ¶¶ [0059], [0065]. The security application “may include software relating to the management of secure identifiers 407,” and “may perform cryptographic functions related to the secure identifier, an authentication process, or cryptographic key generation.” *Id.* at ¶ [0067].

103. Mikan’s vehicle also includes a “local database 203” that “may include any number of records, where each record represents a vehicle operation policy [that] relate[s] to vehicle operation features and keys 205A-C.” *Id.*, ¶ [0051]. The local database is in communication with a “master database 208,” which also “include[s] any number of records representing a vehicle operation policy, and ... may include any number of vehicle operation policies relating to more than one vehicle.” *Id.*, ¶ [0054]. The “local database 203 may mirror some of the data in

master database 208 such that records within each database are consistent,” and “local database 203 and master database 208 may communicate an update to the other after a record change.” *Id.* The contents of the master and local database in one embodiment are illustrated in Figures 3A and 3B (respectively), reproduced below.

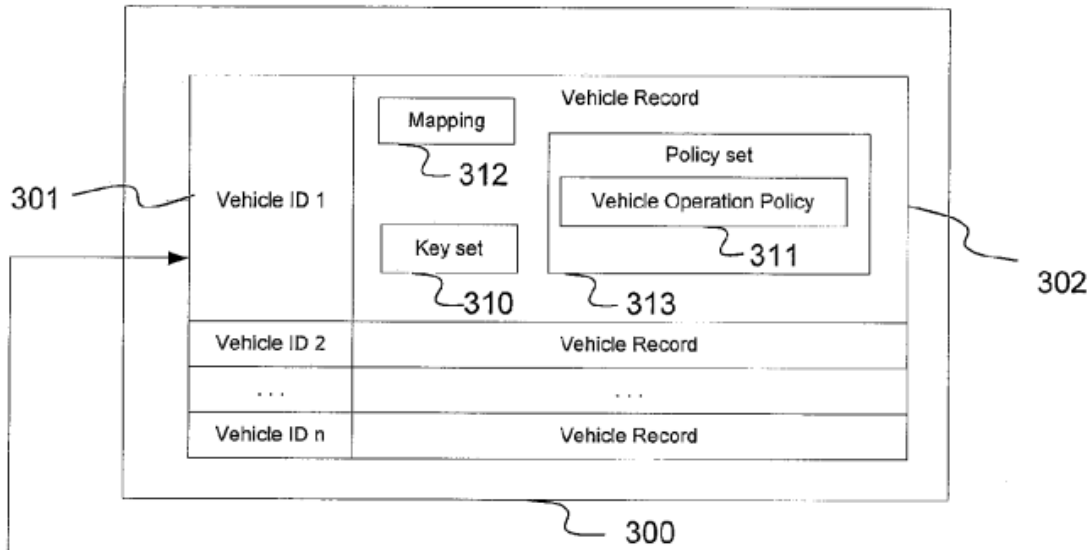


FIG. 3A

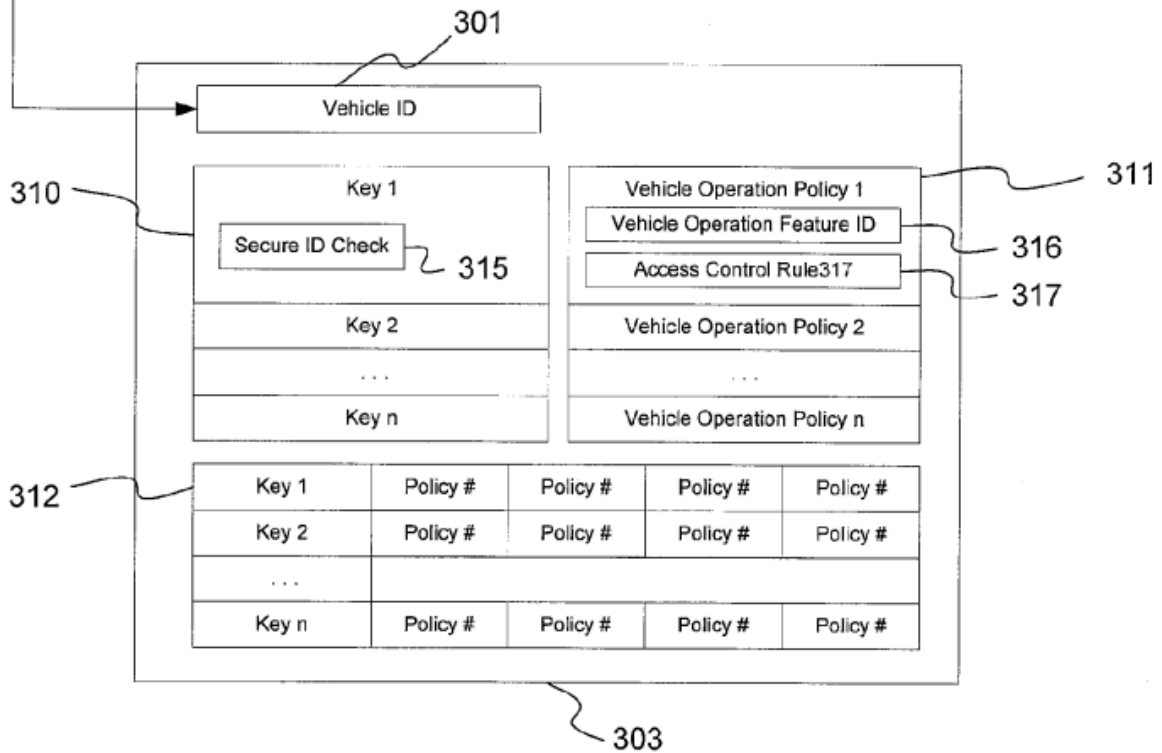


FIG. 3B

104. Mikan's "vehicle operation policy" includes "feature ID 316 and a related access control rule 317," which may be used to "support various vehicle operation features such as unlocking a door, opening a trunk, opening a glove box, engaging an ignition, directing the vehicle from a one [sic] location to another geographic location and accelerating the vehicle." *Id.* at ¶ [0060]. Mikan's databases "link vehicle operation policy 311 and keys 205A-C." *Id.* at ¶ [0061]; *see also id.* at ¶ [0072]. The control unit checks that an "access request is consistent with [a] retrieved vehicle operation policy 311," and when "the access request is inconsistent with the ... retrieved vehicle operation policy 311, then ... control unit 202 may block and/or limit the operation of the vehicle." *Id.* at ¶ [0074]. For example, "the control unit 202 may monitor the status of a particular vehicle operation feature and confirm[] its conformance with vehicle operation policy 311 associated with the key 205A-C that is currently in use. *Id.* at ¶ [0076]. The monitoring may include, for example, "check[ing] the speed of vehicle 201" when "vehicle operation policy 311 includes setting a maximum speed for the operation of vehicle 201," and "[i]f vehicle 201's speed exceeds that defined by policy 311, notification and/or enforcement action may be taken." *Id.*

C. Secondary References

105. The remaining cited references, Sekiyama (Ex. 1006), Hatton (Ex. 1008), and Xiao (Ex. 1010), demonstrate other well-known elements of vehicle communication systems present in the art, namely, communicating encrypted data between the vehicle and a mobile device using conventional radio communication protocols such as Bluetooth, NFC, and WiFi (claims 1[d], 3, 5, 11[d], 16, 18[d], 21), using an electronic key to restrict access to the door locks and trunk of a vehicle (claim 2), associating electronic keys and privileges with user accounts or profiles (claims 4, 11-21), sharing electronic keys with authorized users (claims 6, 19), registration of electronic keys (claim 7), servers and software applications associated with a vehicle manufacturer (claims 12, 13, 20), and binding an electronic key to a mobile device (claim 17).

VIII. Summary of Opinions on Unpatentability

106. In the analysis that follows, I identify the following combinations of prior art that, in my opinion, anticipate and/or render obvious the '659 patent claims:

Grounds of Unpatentability	
1	Kleve and Hatton render obvious claims 1 and 3-21 under Section 103
2	Kleve, Hatton, and Sekiyama render obvious claim 2 under Section 103
3	Mikan anticipates or renders obvious claims 1-3, 5, and 8-10 under

	Section 102 or Section 103
4	Mikan and Xiao render obvious claims 4, 11-18, and 20-21 under Section 103
5	Mikan and Sekiyama render obvious claims 6-7 under Section 103
6	Mikan, Xiao, and Sekiyama render obvious claim 19 under Section 103

A. Ground 1: Kleve in view of Hatton renders obvious claims 1 and 3-21 under Section 103

107. A summary of this ground is as follows: Kleve discloses a vehicle rental system that 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, such as the permitted types of use (for example, to run errands, or to tow or haul cargo). Upon agreement, a virtual key is sent to the vehicle and to the Temporary User's device, allowing the Temporary User to unlock and start the vehicle. The virtual key includes the restrictions on use set by the Vehicle Owner, allowing the vehicle to monitor use by the Temporary User, and if a restriction is exceeded, the Vehicle Owner is notified.

108. Hatton is another Ford patent (like Kleve) that describes an electronic key system the same or substantially the same as that described in Kleve. Hatton describes generating a virtual key at the Vehicle Owner's mobile device, and

transmitting encrypted data associated with the virtual key over radio communications (such as Bluetooth, WiFi, or NFC) in order to authenticate the virtual key and use it to unlock and drive the vehicle. A POSITA would have found it obvious to incorporate these teachings into Kleve to render obvious limitations 1[d], 11[d], and 18[d], and claims 3, 5, 13, 16, 17, 20, and 21.

1. Motivation to Combine Kleve and Hatton and Reasonable Expectation of Success

109. In my opinion, a POSITA would have been motivated to combine Kleve's vehicle rental system with Hatton's teachings relating to generating electronic keys at a mobile device, and communicating encrypted data associated with an electronic key using radio communication protocols.

110. In my opinion, a POSITA would have been motivated to apply Hatton's teachings regarding the communication of encrypted data over radio communications because of the well-known benefits of those teachings, including increased security, efficiency, and better user experience. Conventional radio communication protocols, such as Bluetooth, NFC, and WiFi, are not inherently secure, and messages sent wirelessly using those protocols may also be detected and read by third parties who are not the intended recipients of those messages. In the context of an electronic key system for a vehicle, those third parties could use an unencrypted transmission of electronic key data to gain unauthorized access to the

vehicle. A POSITA would have understood that using encrypted data for communication of electronic keys would increase the security of the system by ensuring that only the intended recipient (*i.e.*, the authorized temporary user or the vehicle) may access and use the electronic key.

111. A POSITA would have also understood that storing and transmitting electronic key information using encrypted data has an additional benefit: it prevents a Temporary User from tampering with the electronic key or otherwise circumventing restrictions and limits on the use of the electronic key (for example, by circumventing restrictions on use set by the Vehicle Owner, or by re-distributing the key to additional, unauthorized third parties). In order to make full use of these benefits, a POSITA would have been motivated to include data identifying restrictions on a Temporary User's use of the vehicle as part of the encrypted data transmitted with the electronic key or as part of the electronic key, so that the Temporary User cannot modify those restrictions at his or her mobile device. A POSITA would also have been motivated to bind the electronic key to the Temporary User's mobile device, so that the Temporary User cannot distribute copies of the electronic key to unauthorized third parties. For example, a POSITA would know how to associate an electronic key with an identifier unique to the mobile device, so

that other mobile devices cannot use the same electronic key without the Vehicle Owner's permission.

112. A POSITA would also have been motivated to enable the Vehicle Owners and Temporary Users in Kleve's vehicle rental system to be able to securely generate and securely communicate encrypted data associated with electronic keys using their mobile devices. These additional features would have made it easier and simpler to use electronic keys in Kleve's system, both for Vehicle Owners and Temporary Users, without sacrificing the security of the system or the Vehicle Owner's ability to limit access and use of the vehicle. For example, by allowing the Vehicle Owner to generate electronic keys on his or her mobile device, and transmit the generated keys directly using encrypted communications, a Vehicle Owner would be able to distribute and activate an electronic key without the need to first communicate it to a server—for example, if the Vehicle Owner and Temporary User are in a location with poor connectivity to cellular networks and the internet. A Temporary User would similarly be able to share the electronic key with other users authorized by the Vehicle Owner (for example, members of a family or travel group who are all authorized to use the vehicle during a rental period). Encrypted wireless communication of the electronic key using radio communication protocols (such as Bluetooth or WiFi) would also enable a Temporary User to authenticate and use the

virtual key with nothing more than his or her mobile device, forgoing the need for additional specialized hardware in the vehicle to recognize and validate the Temporary User, or other cumbersome authentication steps or protocols.

113. In my opinion, a POSITA would have also been especially motivated to look to Hatton specifically for teachings that may be used to improve Kleve's system because both references are assigned to Ford, and both references describe similar electronic key systems in a vehicle, with virtually identical hardware configurations. For example, both Kleve's and Hatton's systems are based on a hardware architecture within the vehicle referred to as a "vehicle computing system" (VCS), and reference the same Ford system (the "SYNC" system) and corresponding top-level block diagram describing the architecture of the system. *See* Kleve at ¶ [0021] ("FIG. 1 illustrates an example block topology for a vehicle based computing system 1 (VCS) for a vehicle 31. An example of such a vehicle-based computing system 1 is the SYNC system manufactured by THE FORD MOTOR COMPANY."), Fig. 1; Hatton at 2:54-58 (same), Fig. 1. Both Kleve and Hatton also describe how their respective systems may be used in the context of a "vehicle rental" business. Kleve at ¶ [0036] ("In the illustrative embodiment as shown in FIG. 2 is an overview of the several steps that may contribute to the process of a vehicle rental micro-business integrated with a VCS."); Hatton at 17:54-60 ("An example

of a temporary user accessing a vehicle may include, but is not limited to, the vehicle rental business.”).

114. In my opinion, a POSITA would also have reasonably expected this combination to succeed. Mobile devices included support for encrypted wireless communications for years before the ’659 patent, and implementing such functionality in Kleve’s system would have been within the capabilities of a POSITA. In fact, Kleve’s vehicle already includes radio communication capabilities (such as Bluetooth or WiFi) that are used to receive encrypted communications from a server. *See* Kleve at ¶ [0061]. Enabling the vehicle to use those same protocols to receive encrypted messages from another device, such as a mobile device, would have required nothing more than a routine application of conventional and well-known radio communication technologies. A POSITA would also have been capable of implementing conventional, well-known encryption techniques (such as public-key encryption techniques) for use within the vehicle and the mobile device, including to generate new electronic keys and to associate or bind an electronic key to a mobile device.

115. In my opinion, Kleve, Hatton, and the ’659 patent are all directed to the same field of endeavor, the field of electronic key systems. *See* ’659 patent at Abstract (“A vehicle configured to communicate with a server of a cloud system to

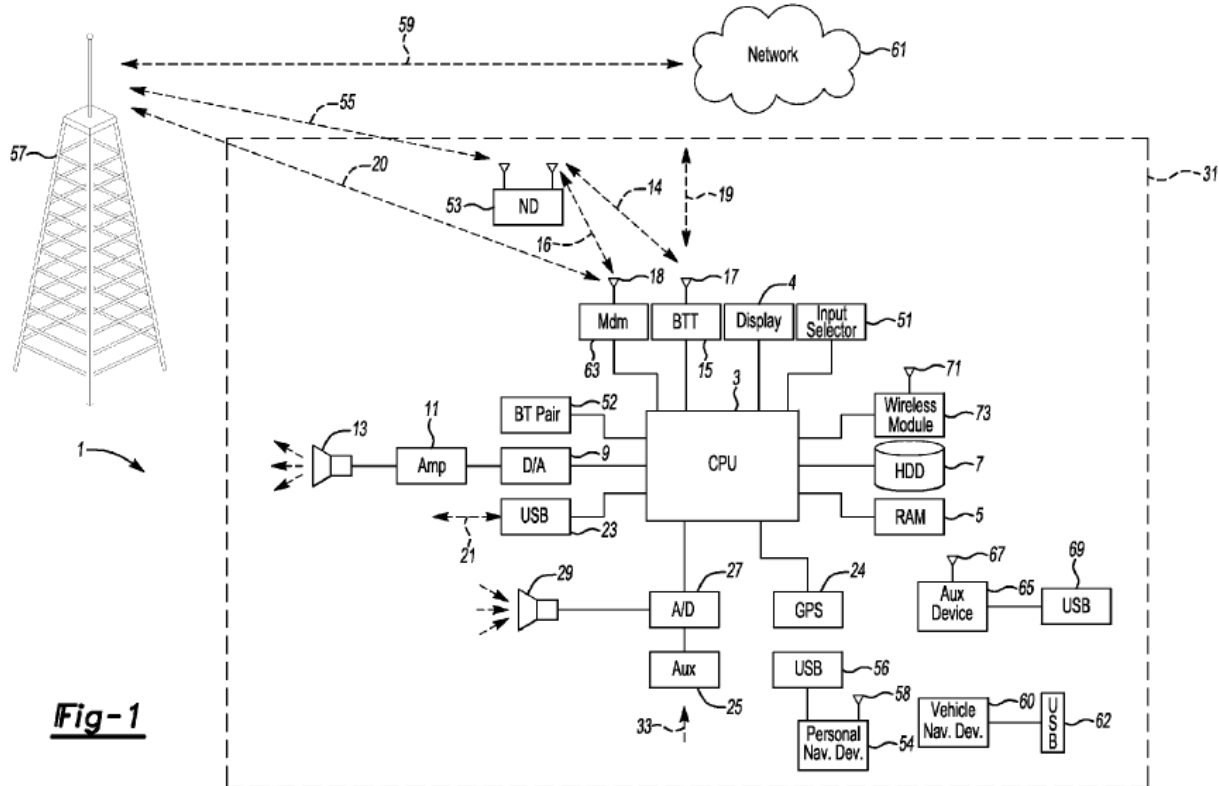
enable access to use the vehicle via one or more electronic keys is provided.”); Kleve at ¶¶ [0044]-[0045] (describing implementation of a “virtual key feature” for use in the “vehicle rental micro-business system”); Hatton at 1:6-8 (“The present invention relates to an electronic key system and a vehicle computing system for managing a vehicle electronic key.”).

2. Independent Claim 1

1[pre]: “A sub-system of a vehicle, the vehicle having an on-board computer interfaced with the sub-system for processing instructions to enable use of an electronic key (eKey), the sub-system comprising:”

116. In my opinion, Kleve discloses this limitation.

117. First, Kleve discloses a “vehicle based computing system” or “VCS.” Kleve at ¶¶ [0021]-[0022]. The VCS is depicted in Figure 1, reproduced below.



118. More specifically, Kleve's VCS includes "a processor 3" which is an **on-board computer**. *Id.* at ¶ [0022]. The processor is "[p]rovided within the vehicle," "allows onboard processing of commands and routines," and "controls at least some portion of the operation of the vehicle-based computing system." *Id.*; see also *id.* at ¶ [0035] ("In all solutions, it is contemplated that at least the vehicle computing system (VCS) located within the vehicle itself is capable of performing the exemplary processes."). The vehicle may also include numerous "vehicle components and auxiliary components"—each of which is a sub-system of the vehicle, or part of a sub-system—that are "in communication with the VCS" and

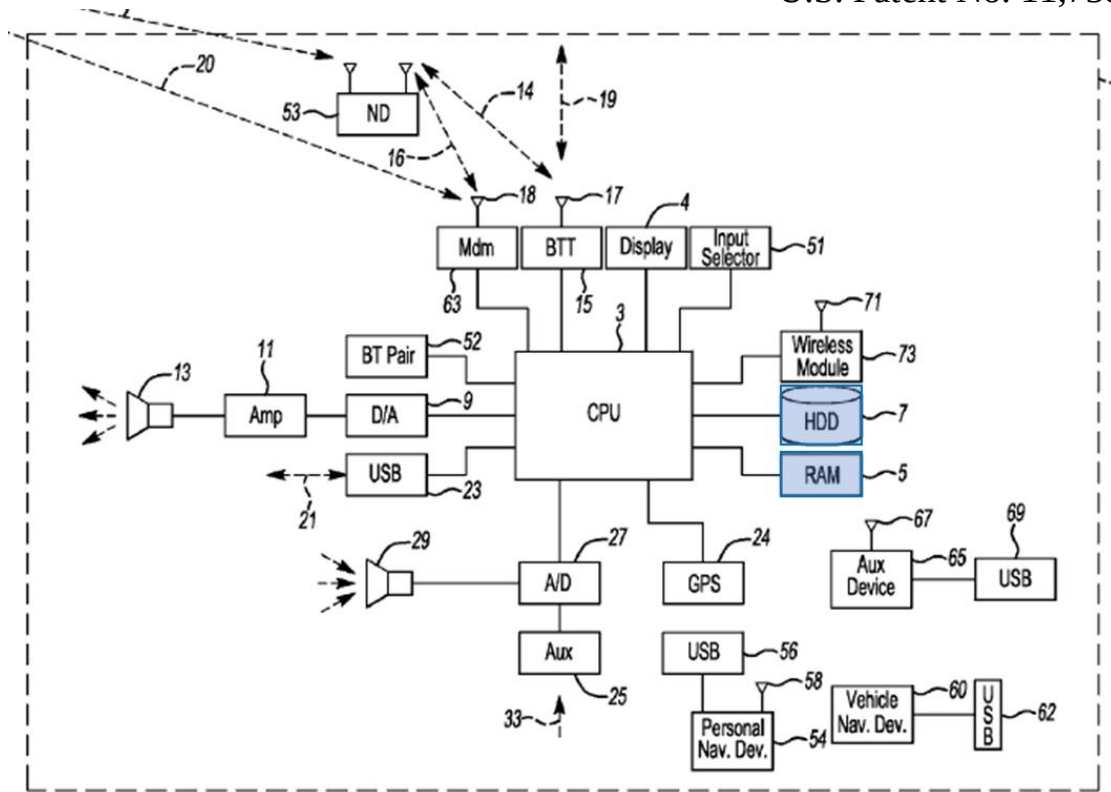
“may use a vehicle network (such as, but not limited to, a CAN bus) to pass data to and from the VCS (or components thereof).” *Id.* at ¶ [0023]; *see also id.* at ¶ [0076] (describing the use of “subsystems throughout the vehicle” with “VCS monitoring sensors” to monitor a Temporary User’s use of the vehicle).

119. Kleve’s processor also processes instructions to enable use of an electronic key. As I note above, Kleve’s processor “allows onboard processing of commands and routines,” which are instructions. *Id.* at ¶ [0022]. Kleve also discloses that its VCS enables the use of a “virtual key.” *Id.* at ¶¶ [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.”), [0048] (“The Temporary User may enter a virtual key outside or inside the vehicle, while credential authorization may be processed by the VCS, a server and/or by the vehicle Owner.”), [0063] (“The Temporary User identification and virtual key may be sent in an encrypted message to the VCS, Temporary User’s nomadic device, and/or vehicle Owners nomadic device.”), [0067] (“The virtual key credential ... can be collected by the vehicle itself through various input devices which may be connected to the VCS using a camera, matrix barcode scanner, optical scanner, fingerprint scanner or microphone.”), [0071]-[0074] (“At step 618, the Temporary User may ... use a vehicle input device, like camera, microphone, fingerprint scanner or retinal

scanner integrated with the VCS to capture his identity and/or payment credentials to enable a keyless drive-away.”). In my opinion, a POSITA would have understood that it is the processor within the VCS that would process virtual key information and Temporary User identification information to determine if the Temporary User is authorized, and to enable control of functions of the vehicle based on that determination.

1[a]: “memory associated with the on-board computer of the vehicle having program instructions for instructing unlocking and starting of the vehicle; and”

120. In my opinion, Kleve discloses memory associated with an on-board computer of the vehicle. As I discuss above, the processor in Kleve’s VCS is the on-board computer. Kleve at ¶ [0022]. As illustrated in Figure 1, annotated below, the VCS includes memory associated with the processor.



121. As shown in Figure 1, the memory associated with Kleve's processor includes random access memory (indicated as "RAM"), and persistent storage in the form of a hard disk drive (indicated as "HDD") (both highlighted in blue above). Kleve at ¶ [0022].

122. Kleve explains that flash memory may also be used instead of a hard disk drive. *Id.* "[D]ata can be stored on the HDD or other storage media." *Id.* at ¶ [0031]. A POSITA would have understood that program instructions would also be stored in memory—for example, in RAM when a program is loaded or executing—because processors must store instructions somewhere in order to process them, and computers store instructions in memory.

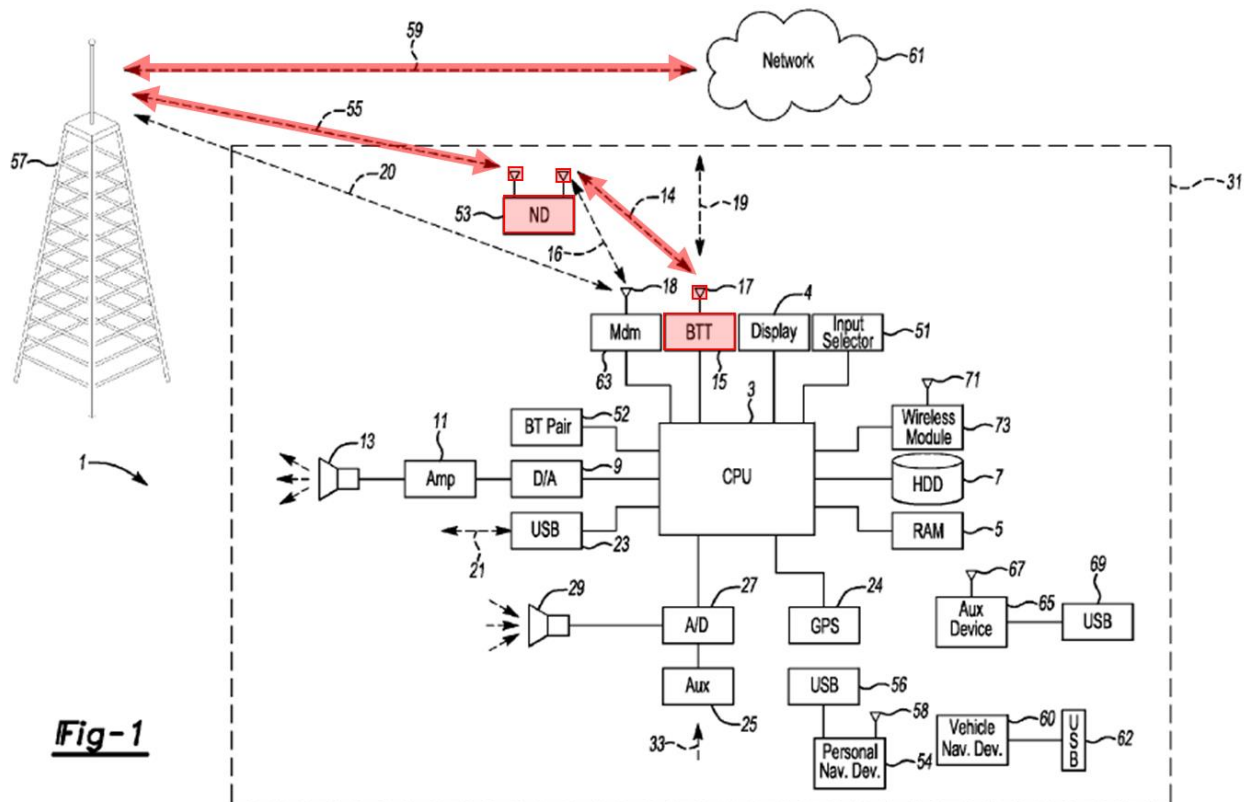
123. The instructions that Kleve's processor can execute includes instructions for unlocking and starting the vehicle. For example, Kleve's processor can "enable a vehicle rental transaction" by, among other things "activat[ing] the vehicle during a prescribed rental period" and, for an authorized virtual key, "enabl[ing] a keyless drive-away." *Id.* at ¶ [0009]. Specifically, "the Temporary User may send the virtual key to the server requesting access to the vehicle," and once the Temporary User is authenticated, the virtual key may be used "to unlock and drive." *Id.* at ¶ [0071].

1[b]: "communications circuitry of the vehicle interfaced with the on-board computer of the vehicle and the sub-system, the communications circuitry is configured to process program instructions to enable communication with a server,"

124. In my opinion, Kleve discloses communications circuitry interfaced with its on-board computer and vehicle sub-systems. The communications circuitry processes program instructions that are used to communicate with a server located on a cloud network.

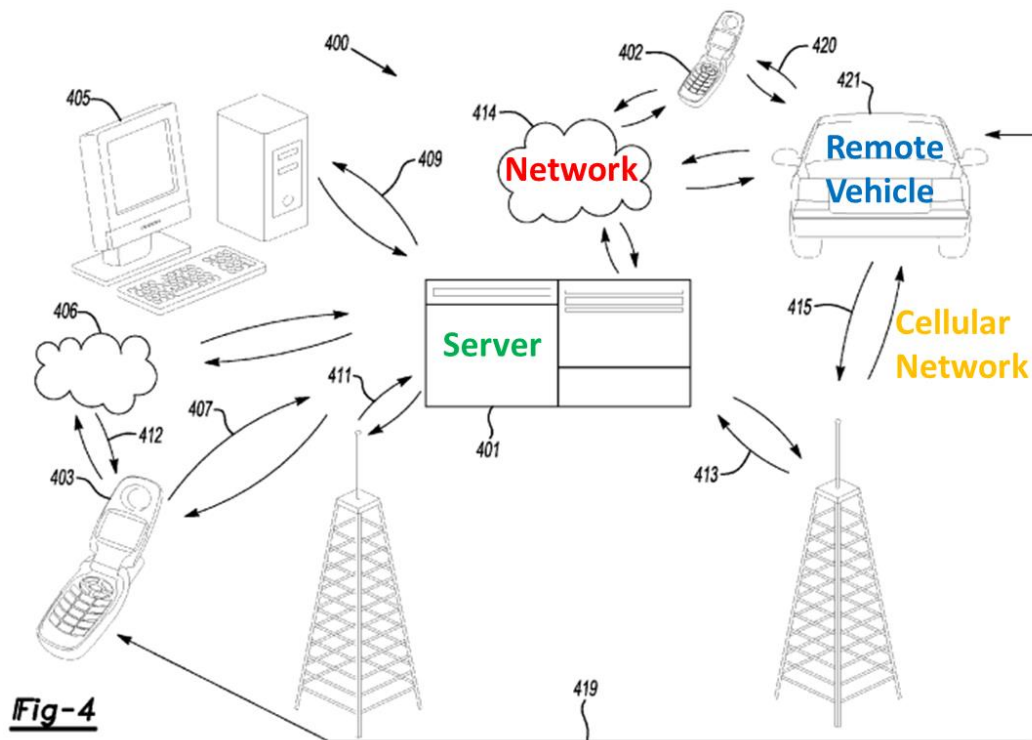
125. Kleve discloses that the VCS may include a "BLUETOOTH transceiver 15 to communicate 17 with a user's nomadic device 53 (*e.g.*, cell phone, smart phone...)." Kleve at ¶ [0025]. The user's mobile device in turn communicates "with a network 61 outside the vehicle 31." *Id.* Kleve discloses that other

communications protocols may also be used, such as WiFi. *Id.* at ¶ [0029] (“IEEE 802 LAN (local area network) protocols include WiFi and have considerable cross-functionality with [Bluetooth]. Both are suitable for wireless communication within a vehicle.”), [0030] (“[T]he ND 53 may be a wireless local area network (LAN) device capable of communication over, for example (and without limitation), an 802.11g network (i.e., WiFi) or a WiMax network.”). The communication path from the processor, through the communications circuitry (in this case, the Bluetooth transceiver), to the mobile device, and then to an external network is illustrated in Figure 1, annotated below.



-65-
Kia Ex. 1004

401,” as illustrated in Figure 4, annotated below. *Id.* at ¶ [0056]. In one embodiment, “the centralized system is a server system.” *Id.* at ¶ [0057]. The server “may include an automated call server and/or web host,” and “may route an incoming signal from a nomadic device (ND) 403 to the appropriate remote vehicle to enable a Temporary User keyless access and drive away capabilities of the Owner’s vehicle.” *Id.*



128. A POSITA would have understood that Kleve’s communications circuitry (such as modem 63, Bluetooth transceiver 15, and wireless router 73) processes program instructions when it communicates with the network and server. A vehicle manufacturer such as Ford does not normally develop and build standard electronic components, such as modems, Bluetooth transceivers, or WiFi routers.

Instead, these are typically purchased from a component supplier that supplies them as separate chips or boards including an embedded processor or controller that executes programs and instructions to communicate using a particular wireless protocol. A POSITA would have understood that Kleve's system uses such components for its modem, Bluetooth transceiver, and wireless router.

1[c]: “the communications circuitry includes wireless communication circuitry for enabling local connection with a mobile device, the mobile device is configured to use the eKey for said unlocking and said starting the vehicle;”

129. In my opinion, Kleve discloses communications circuitry including wireless communication circuitry. For example, as I discuss above for limitation 1[b] (“communications circuitry of the vehicle interfaced with the on-board computer of the vehicle and the sub-system”), Kleve discloses that the VCS may include a Bluetooth transceiver, a modem, or a WiFi router in communication with the processor. See Kleve at ¶ [0025] (Bluetooth), [0028] (Modem), [0029], [0034] (WiFi). Kleve also describes using the wireless communication circuitry to connect the vehicle to a local mobile device. See *id.* at ¶ [0025] (“[T]he system 1 uses the BLUETOOTH transceiver 15 to communicate 17 with a user's nomadic device 53 (e.g., cell phone, smart phone, PDA, or any other device having wireless remote

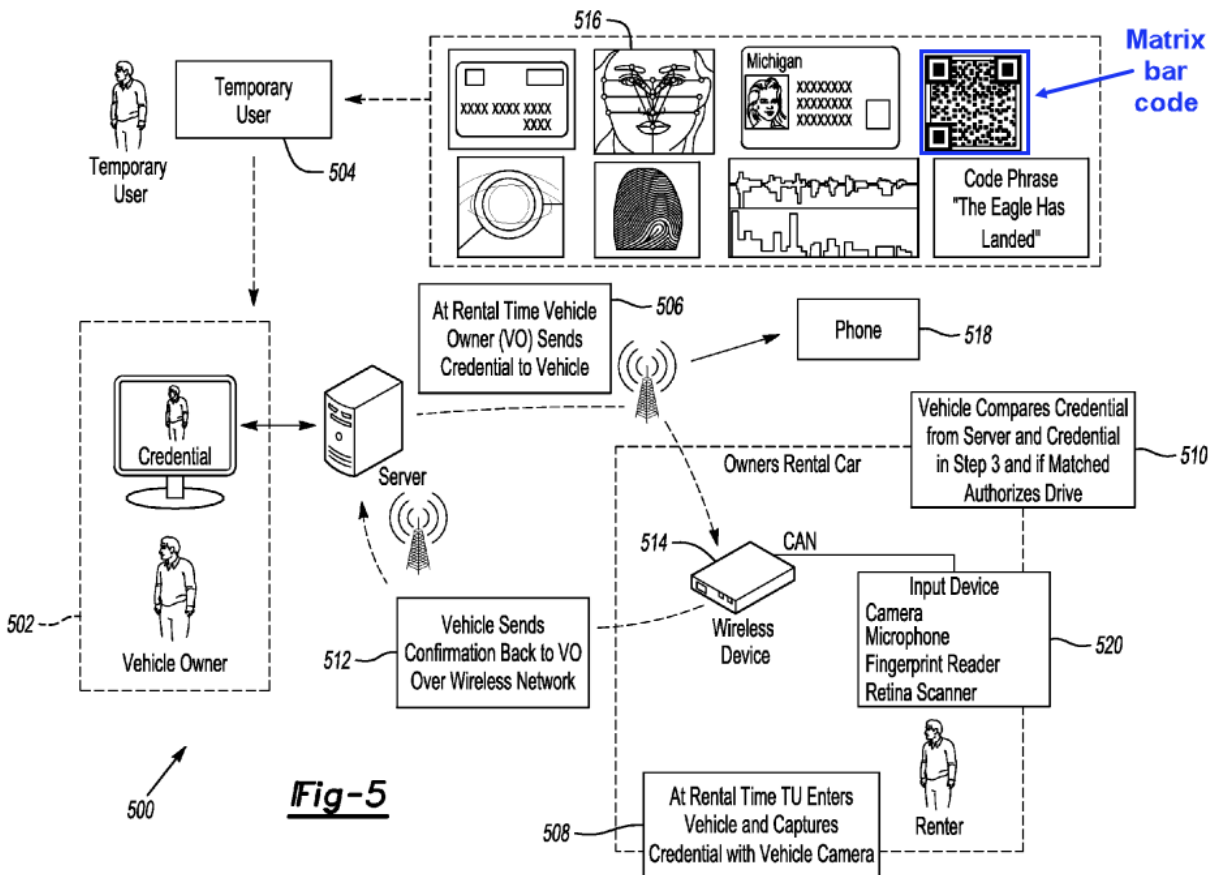
connectivity.”), [0029]-[0030] (describing communication between the vehicle and nomadic device over WiFi),

130. Kleve also discloses that the mobile device is configured to use the virtual key to unlock and start the vehicle. For example, Kleve discloses that a mobile device configured with a virtual key may be used to “unlock” and “drive” (which necessarily entails starting) the vehicle. *See id.* at ¶ [0009] (“The processor may establish communication with a wireless device brought within proximity of a vehicle [and] receive user input corresponding to an attempt to activate the vehicle during the rental period and ... enable a keyless drive-away.”), [0071] (“[T]he Temporary User may send the virtual key to the server requesting access to the vehicle, or use a vehicle input device, like a camera, microphone, fingerprint scanner or retinal scanner integrated with the VCS to capture his identity and/or payment credentials to enable a keyless drive-away [T]he Temporary User may again input the same identifying credentials to unlock and drive.”).

1[d]: “wherein the wireless communications circuitry of the vehicle is configured to receive coded data from the mobile device when using the eKey, the coded data enables functions of said eKey for said unlocking and use of the vehicle, the coded data is associated to the eKey for use by the mobile device,”

131. In my opinion, Kleve discloses wireless communications circuitry configured to receive coded data from a mobile device when using a virtual key.

132. For example, in one embodiment, Kleve discloses using a “matrix barcode (ex. two-dimensional code) ... as the virtual key being recognized by the VCS.” Kleve at ¶ [0044]. A matrix barcode may be an image, such as a QR code, as shown in Figure 5 of Kleve, annotated below. A “smart phone may be used to communicate the matrix barcode information to the vehicle rental micro-business system directly.” *Id.* For example, the vehicle may have “input devices which may be connected to the VCS,” such as “a camera” or “matrix barcode scanner.” *Id.* at ¶ [0067]. These input devices use wireless communications because they can read coded data from a mobile device without a wired connection—for example, by capturing an image of a matrix barcode displayed on a mobile device.



133. Kleve’s matrix barcode is associated to the eKey for use by the mobile device and enables functions of the virtual key for unlocking and use of the vehicle. For example, Kleve discloses that “Temporary User identification” may be “used as a virtual key, or in addition to the virtual key, allowing the Temporary User access to the Owner’s vehicle while enabling a keyless drive-away.” *Id.* at ¶ [0063]. The Temporary User’s information may include a “matrix barcode.” *Id.* “Once the Temporary User has the matrix barcode scanned by the vehicle, the smart phone may be able to connect with the VCS and be used to enter and enable the vehicle drive

away event.” *Id.* at ¶ [0044]; *see also id.* at ¶ [0071] (“[T]he Temporary User may send the virtual key to the server requesting access to the vehicle, or use a vehicle input device, like camera ... integrated with the VCS to capture his identity and/or payment credentials to enable a keyless drive-away. ... For the duration of the rental term, the Temporary User may again input the same identifying credentials to unlock and drive.”).

134. In my opinion, it also would have been obvious to a POSITA to also use Kleve’s modem, Bluetooth transceiver, or WiFi router to receive encrypted data associated with a virtual key from a user’s mobile device in order to enable unlocking and use of the vehicle, as disclosed in Hatton.

135. Kleve teaches that “Temporary User identification and virtual key may be sent in an encrypted message to the VCS.” Kleve at ¶ [0063]. An encrypted message is a type of coded data—specifically, data encoded according to an encryption scheme. Because Kleve uses wireless communication circuitry (*e.g.*, the modem, Bluetooth transceiver, or wireless router that I discuss above for Limitations 1[b] and 1[c]) to communicate with a server and a user’s mobile device, a POSITA would have understood that the wireless communication circuitry would receive the encrypted message.

136. Hatton further discloses that a “mobile device 124 may be configured using a software application to communicate with the VCS.” Hatton at 7:21-23. The communication may use “wireless communication technologies including, but not limited to Bluetooth, WiFi, cellular, and/or near field communication.” *Id.* at 7:56-60. The vehicle stores a copy of the encrypted data, associated with a particular authorized electronic key. *See id.* at 7:33-45 (showing a look-up table (“LUT”) that includes multiple entries for different keys, each with a corresponding “encrypted data” field). The VCS then uses “mobile device transmitted encrypted data” to “recognize the mobile device associated to a user.” *Id.*, 7:49-56. If the encrypted data received from the mobile device with the electronic key matches the encrypted data for an electronic key stored by the vehicle, the system “allows the vehicle to start the engine.” *Id.*, 7:18-20; *see also id.* at 13:24-27 (describing use of the mobile device for “keyless control of starting the vehicle, unlocking/locking doors, and/or opening the trunk”).

137. As I explain above in the section titled “Motivation to Combine Kleve and Hatton and Reasonable Expectation of Success,” a POSITA would have been motivated to use wireless communications circuitry such as Kleve’s modem, Bluetooth transceiver, or WiFi router to receive encrypted data from a mobile device operating as a virtual key and use the received encrypted data to enable virtual key

functions such as unlocking and use of a vehicle, as described in Hatton. In short, using radio communications to exchange the encrypted data to activate the electronic key would enhance the user experience by simplifying activation and use of the virtual key; and encrypting the virtual key data would enhance security by preventing unauthorized access to the vehicle.

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

138. In my opinion, Kleve discloses coded data including privilege settings associated with a virtual key for limiting types of use of the vehicle when using the eKey with the vehicle. As I discuss above for Limitation 1[d], Kleve discloses that coded data such as “matrix barcode (ex. two-dimensional code)” may be used “as the virtual key being recognized by the VCS.” Kleve at ¶¶ [0044], [0063].

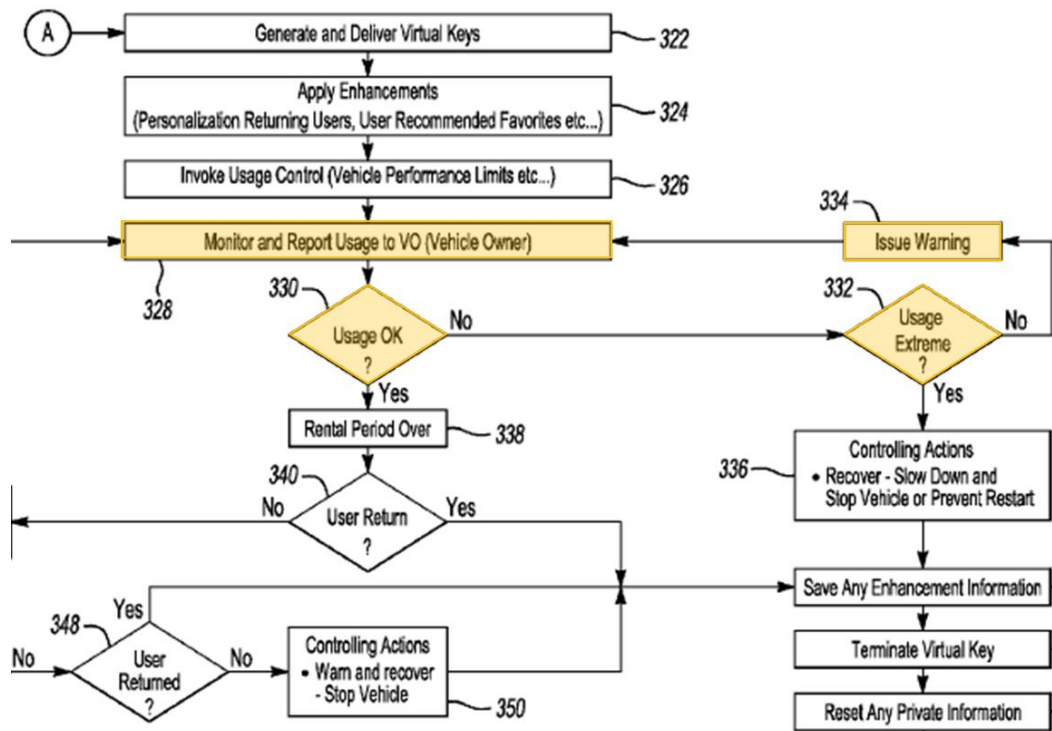
139. Kleve further discloses that the virtual key includes restrictions on the types of use of the vehicle by a Temporary User using the virtual key. For example, Kleve discloses that the “Owner may set user restrictions,” and “[t]he restrictions may be based on, but not limited to, the owner’s selection of parameters including, but not limited to, speed, global position coordinates, or load weight restrictions.” *Id.* at ¶ [0040]. The selection of restrictions may be based on the types of use agreed to between the Owner and the Temporary User when negotiating the terms of the

rental. For example, the Temporary User may request to rent a vehicle for running errands, and not for towing and hauling cargo, and the virtual key may thus be configured to monitor for unauthorized cargo or an unauthorized trailer tow. *Id.* at ¶¶ [0083] (“The owner may review the requested rental based on what the Temporary User is looking to use the vehicle for (e.g. without limitation, for towing, hauling, or errands), when the requested use will be taking place, and where.”), [0076] (“The monitoring done by the vehicle rental micro-business may include, but not limited to, unauthorized objects or cargo, unauthorized driving behavior, unauthorized driver, and/or an unauthorized trailer tow.”).

140. In my opinion, it also would have been obvious to a POSITA to include the restrictions on types of use of the vehicle as part of the coded data associated with a virtual key—for example, as part of the encrypted data described in Hatton. See Hatton at 7:33-56. As I explain above in the section titled “Motivation to Combine Kleve and Hatton and Reasonable Expectation of Success,” a POSITA would have been motivated to include data identifying restrictions on a Temporary User’s use of the vehicle as part of the encrypted data transmitted with the electronic key or as part of the electronic key so that the Temporary User cannot modify those restrictions at his or her mobile device and circumvent the restrictions.

1[f]: “wherein use of the vehicle using the eKey is tracked to identify and log actions taken using the vehicle while the eKey is used.”

141. In my opinion, Kleve discloses that use of the vehicle with the virtual key is monitored to identify and record actions taken by the Temporary User using the virtual key. For example, Kleve discloses “use restrictions” that “may be monitored and if a restriction exceeds a limit the Temporary User and Owner may be notified.” Kleve at ¶ [0040]. Figure 3B, reproduced and annotated below, illustrate the steps of monitoring within Kleve.



142. A virtual key is delivered to the vehicle’s VCS and the Temporary User in step 322. *Id.* at ¶ [0048]. At step 326, “Usage Control ([e.g.,]Vehicle Performance

Limits)” may be invoked. *Id.* at Fig. 3B; *see also id.* at ¶ [0051]. At step 328, “the control usage of the vehicle by the Temporary User may be monitored by the vehicle owner.” *Id.* at ¶ [0052]. Data regarding the actions taken by the Temporary User while using the vehicle—such as “location, speed, and driving behavior,” may be “record[ed]” and “transmitted ... to the vehicle owner.” *Id.*

3. Claim 3: “The sub-system of the vehicle of claim 1, wherein the vehicle is configured to receive or securely store information from the server to perform authentication or verification that the coded data received from the mobile device should activate the eKey.”

143. In my opinion, Kleve discloses that the vehicle is configured to receive or securely store information from the server to authenticate or verify that coded data received from the mobile device should activate the virtual key.

144. As I discuss above for Limitation 1[d], Kleve discloses using a “matrix barcode (ex. two-dimensional code) ... as the virtual key being recognized by the VCS,” and communicating the matrix barcode information from the mobile device to the VCS using an input device in the vehicle such as a “camera” or “matrix barcode scanner.” Kleve at ¶¶ [0044], [0067]; *see also id.* at ¶ [0071] (“[T]he Temporary User may send the virtual key to the server requesting access to the vehicle, or use a vehicle input device, like camera ... integrated with the VCS to capture his identity and/or payment credentials to enable a keyless drive-away. ...

For the duration of the rental term, the Temporary User may again input the same identifying credentials to unlock and drive.”).

145. Kleve also teaches that “[t]he Temporary User identification [*e.g.*, matrix barcode] and virtual key may be sent in an encrypted message to the VCS,” allowing the vehicle to receive and securely store that information. *Id.* at ¶ [0063]. When the Temporary User scans the matrix barcode at the vehicle, the vehicle “may compare the identity credentials just inputted at the vehicle and the one previously sent virtual key to the vehicle ... to determine authorization.” *Id.* at ¶ [0071]. “If the comparison is successful, the vehicle may enable drive-away access to that Temporary User.” *Id.*

146. Kleve also discloses an additional “remote credential verification” step that may take place “at the vehicle ... by the VCS, using a server.” Kleve at ¶¶ [0048]-[0049]. For remote credential verification, the Temporary User performs a “credential verification” at the vehicle, and the VCS “compare[s] and verif[ies] authorization.” *Id.* at ¶ [0049].

147. In my opinion, it also would have been obvious to a POSITA to use the encrypted data sent from the server to authenticate or verify a virtual key based on encrypted data received from the mobile device, as taught by Hatton. As I discuss above for Limitation 1[d], Kleve’s VCS may receive and store a virtual key as “an

encrypted message” from the server, and Hatton describes how encrypted data associated with specific virtual keys may be stored in a look-up table at the vehicle. Kleve at ¶ [0063]; Hatton at 7:33-45. Hatton also teaches that the VCS “recognize[s] the mobile device associated to a user using ... the mobile device transmitted encrypted data.” Hatton at 7:52-56. If the encrypted data stored in the vehicle’s look-up table “matches” the encrypted data received from the virtual key, the VCS activates the virtual key by “allow[ing] the vehicle to start the engine.” *Id.* at 7:12-20.

148. As I explain above in the section titled “Motivation to Combine Kleve and Hatton and Reasonable Expectation of Success,” a POSITA would have been motivated to use encrypted virtual key data received from the server to authenticate or verify a user using encrypted virtual key data provided by the mobile device, as described in Hatton. Authenticating the virtual key by comparing encrypted data in this manner would enhance the user experience by simplifying activation and use of the virtual key; and the use of encryption for the virtual key data would enhance security by preventing unauthorized access to the vehicle.

4. **Claim 4: “The sub-system of the vehicle of claim 1, wherein the communications circuitry of the vehicle is configured to receive one or more additional requests from other mobile devices to use the vehicle, each request is associated with coded data generated by the server, such that each coded data is associated with a user account having privileges assigned by an administrator of the vehicle that enables assigning or use of eKeys to use the vehicle.”**

149. In my opinion, Kleve discloses that the communications circuitry in the VCS may receive additional requests from other mobile devices to use the vehicle. For example, Kleve discloses that its “vehicle rental authorization system” matches Temporary Users to vehicle owners and vehicles “based on location, trip type, date, vehicle type requested, scheduled number of hours needed, a certain day of the week, and vehicle condition.” Kleve at ¶ [0087]. The same vehicle could thus be rented to different Temporary Users on different days and times. Kleve also expressly describes how “potential Temporary Users” (plural) may review “one or more databases with a list of vehicle owners and rental vehicles available” and “select[] [a] vehicle to rent.” *Id.*, [0081]-[0082] (emphasis added). These descriptions would clearly convey to a POSITA that Kleve’s system may be utilized by different Temporary Users, who may request to rent the same vehicle for different rental periods.

150. In my opinion, a POSITA would have understood that in Kleve’s vehicle rental system, each request from a different user would be associated with coded data generated by the server and associated with a user account. Kleve expressly discloses that the virtual key is based on “Temporary User identification,” which includes coded data such as a “matrix barcode.” Kleve at ¶ [0063]. Rental requests for different users would thus have different coded data (associated with

each distinct Temporary User). This is also confirmed by Hatton, which expressly describes how the VCS stores encrypted data for different virtual keys (each of which may be associated with a different Temporary User and rental request) in a look-up table. Hatton at 7:33-45, 7:52-56.

151. In addition, in at least one embodiment, Kleve teaches that the Temporary User identification is “entered into the server” in order to be “used as a virtual key.” Kleve at ¶ [0063]. A POSITA would have understood this disclosure to indicate that in that embodiment, the server generates the virtual key using the Temporary User identification.

152. Kleve also teaches that virtual keys and coded data are associated with user accounts, which have associated privileges assigned by an owner of the vehicle responsible for administering rentals of the vehicle. For example, Kleve discloses that rental requests may include terms negotiated between the Owner and the Temporary Users. *Id.* at ¶ [0084]. These terms may include “vehicle restriction limits initially set by the Owner at the beginning of the rental term.” *Id.* at ¶ [0043]; *see also id.* at ¶¶ [0084] (“[T]he owner may negotiate additional terms and conditions based on the specific use and needs the Temporary User may use the vehicle for.”), [0089] (same). Kleve also discloses that Temporary Users “setup a user profile within the database,” which is used to enter into a rental agreement and set up a

virtual key. *Id.* at ¶ [0062]; *see also id.* at ¶¶ [0069] (describing setting up user profiles and generating a virtual key “by using Temporary User’s credentials”). After the Owner and Temporary User reach agreement, “the system may generate a virtual key to distribute to the Temporary User and VCS.” *Id.* at ¶ [0039].

5. Claim 5: “The sub-system of the vehicle of claim 1, wherein the wireless communication circuitry is associated with an NFC standard or a radio frequency standard for said local connection between the mobile device and the vehicle.”

153. In my opinion, it would have been obvious to a POSITA to use Kleve’s modem, Bluetooth transceiver, or WiFi router for local connection between the mobile device and vehicle and for receiving encrypted data at the VCS from the mobile device. I provide a detailed explanation above for Limitation 1[d]. In short, Kleve teaches that “Temporary User identification and virtual key may be sent in an encrypted messages to the VCS.” Kleve at ¶ [0063]. Kleve separately discloses the VCS includes a modem, Bluetooth transceiver, and/or wireless router, as I discuss above in Limitations 1[b] and 1[c]. Hatton also teaches that a mobile device may communicate with the VCS using “wireless communication technologies including, but not limited to Bluetooth, WiFi, cellular, and/or near field communication,” and specifically receives “mobile device transmitted encrypted data” to authenticate a mobile device operating as a virtual key. Hatton at 7:49-60. A POSITA would have been motivated to combine these teachings to simplify activation and use of the

virtual key while preventing unauthorized access to the vehicle, as I explain in my discussion of Limitation 1[d].

6. **Claim 6: “The sub-system of the vehicle of claim 1, wherein an application associated with said mobile device is configured to enable sharing of said eKey with a recipient user having a recipient mobile device, the sharing is enabled via a message initiated from said mobile device.”**

154. In my opinion, Kleve discloses an application associated with the mobile device that is configured to enable sharing of a virtual key with a recipient user’s mobile device. For example, Kleve discloses that its vehicle rental micro-business is implemented as a “smart phone application.” Kleve at ¶ [0036]. The “Owner and Temporary User may use [the smartphone application] to manage their assets and/or user profile.” *Id.* Among other things, the elements of the system include “distributing a virtual key to the Temporary User and VCS.” *Id.*

155. In my opinion, it would have been obvious to a POSITA that the same smartphone application may also be used to allow Temporary Users to share their virtual keys with other authorized Temporary Users. For example, multiple members of a family or travel group may collectively rent a single vehicle, and different members may each need to be able to access the vehicle using their respective mobile devices. A POSITA would have understood that multiple Temporary Users could thus be authorized in connection with the same vehicle rental. A POSITA would

thus have been motivated to enable each user to share the virtual key with other authorized users associated with the same rental request. Since Kleve's vehicle rental system is already configured to use a smartphone application to generate, authenticate, and distribute keys, a POSITA would have been capable of implementing sharing between Temporary Users using the same or similar software already included in Kleve's system to allow Owners to distribute virtual keys to temporary users.

156. Kleve further discloses that sharing or distributing of virtual keys is enabled by messages initiated at the mobile device. For example, Kleve discloses that a virtual key is distributed in response to "the Temporary User select[ing] the vehicle, pay[ing] the appropriate amount and sign[ing] a consent agreement." Kleve at ¶ [0039]. A virtual key may also be generated and distributed in response to the Temporary User and vehicle Owner "agree[ing] to terms" of a rental agreement and signing the agreement "using smart phones or a smart phone application." *Id.* at ¶¶ [0047]-[0048]. In one embodiment, the vehicle Owner may also use a mobile device to generate the virtual key and send the virtual key to the server and the Temporary User. *Id.* at ¶ [0069], Fig. 6. All of these examples involve messages initiated at the Vehicle Owner's or Temporary User's mobile device.

7. Claim 7: "The sub-system of the vehicle of claim 1, wherein the coded data is processed securely by the mobile device"

responsive to registering the e-Key to the mobile device, the registering being enabled by an owner of said vehicle or an administrator of said vehicle.”

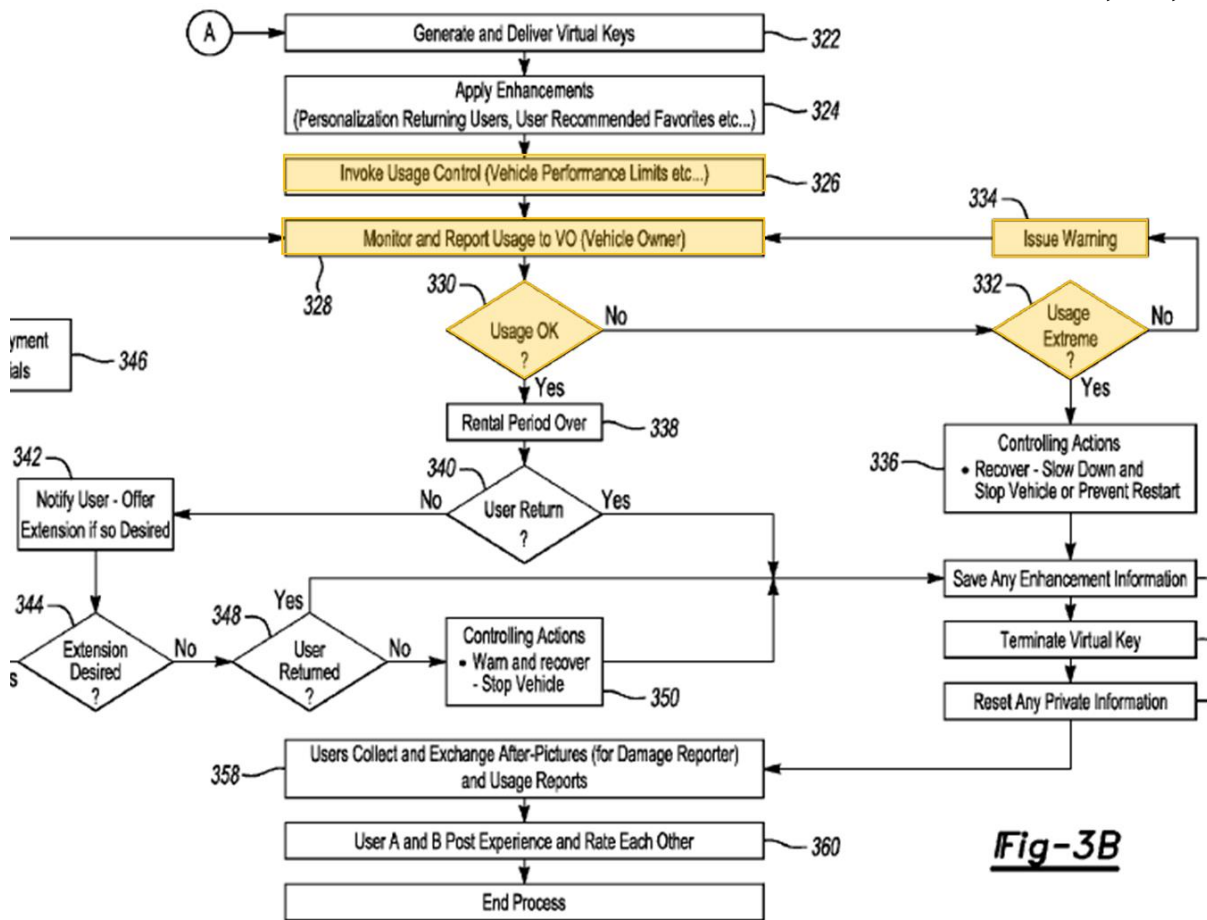
157. In my opinion, Kleve discloses that coded data is processed securely by the mobile device. As I explain above for Limitation 1[d], Kleve discloses that a “virtual key may be sent in an encrypted message to the ... Temporary User’s nomadic device.” Kleve at ¶ [0063]. Encrypted communications are used to ensure that messages are received and processed securely, and the mobile device would thus necessarily securely process the encrypted data.

158. Kleve also discloses that a virtual key is only received and securely processed after and in response to registration of the virtual key by an owner of the vehicle. For example, Kleve discloses that a virtual key is only delivered to a Temporary User after “identification of the Temporary User with an accepted agreement and payments made.” *Id.* at ¶ [0048]. Specifically, after the Owner and Temporary User “set up user profiles, enter into an agreement and make a payment to initiate the vehicle rental process,” then “the vehicle Owner may ... generate a virtual key.” *Id.* at ¶ [0069]. The process serves to register the virtual key to a Temporary User’s mobile device at least because the virtual key is generated using identification information supplied by the Temporary User through the Temporary User’s profile. *Id.* at ¶ [0063].

159. In addition, Kleve discloses “remote credential verification at the vehicle” using “the VCS, using a server, or allowing the Owner to verify the Temporary User’s request,” for example, by using a “credential verification password.” *Id.* at ¶ [0049]; *see also id.*, [0070] (describing different ways that the user may “enter the virtual key” at the vehicle and “validate authorization to access the vehicle”). The remote credential verification also serves to register the virtual key to the mobile device, and is enabled by the Owner, particularly where the Owner verifies the Temporary User’s request. After the virtual key is verified, the Temporary User’s mobile device “may be paired with the VCS.” *Id.* at ¶ [0072].

8. Claim 8: “The sub-system of the vehicle of claim 1, wherein a mode of allowed use of the vehicle using the eKey is configured to monitor said use of the vehicle, and said on-board computer is configured to transmit one or more notifications when a violation of a restriction is detected.”

160. In my opinion, Kleve discloses that a mode of allowed use of the vehicle using the virtual key is configured to monitor use of the vehicle, and the on-board computer is configured to transmit notifications when a violation of a restriction is detected. For example, as I discuss above for Limitation 1[f], Kleve discloses restrictions on types of use associated with a virtual key, and monitoring use of the vehicle to identify violations of those restrictions. *See* Kleve at ¶ [0040]. The monitoring process is illustrated in Figure 3B, reproduced and annotated below.

**Fig-3B**

161. Kleve also specifically discloses that “the VCS may monitor that a restriction threshold has been violated,” and when a violation is detected, “may send an issue warning to the vehicle display information center” and “a message to issue a warning to the Temporary User.” *Id.* at ¶ [0053]. The VCS is also configured to send notifications to the Owner “if a restriction exceeds a limit.” *Id.* at ¶¶ [0040], [0078] (describing “driver behavior” monitored by the VCS and “transmitted ... to the vehicle owner’s nomadic device”).

9. Claim 9: “The sub-system of the vehicle of claim 1, wherein the tracked use of the vehicle is configured to identify a

violation, and the violation is associated with one or more of driving too fast, or driving out of an area, or accelerating too fast, or stopping too fast, or parking too close to a structure or other vehicle, or coming in contact with a structure or another vehicle, or slamming a door of the vehicle, or turning on a radio, or texting while driving, or interfacing with vehicle controls while driving, or two or more thereof.”

162. As I describe in detail for Limitation 1[f] and Claim 8, Kleve discloses monitoring use of the vehicle to identify violations of restrictions on use.

163. In my opinion, Kleve also teaches that the violations may be associated with driving too fast, driving out of an area, accelerating too fast, stopping too fast, or coming in contact with a structure or another vehicle. See Kleve at ¶¶ [0041] (“driving to restricted areas”), [0078] (“driving the vehicle at excessive vehicle speeds”), [0078] (monitoring of “vehicle speed, acceleration force, wheel speed, breaking, steering, vehicle weight, throttle and pedal position”), [0079] (notifications indicating “the Temporary User has been in an accident or near miss based on airbag deployment, accelerometer data, and/or anti-lock brake information”).

10. Claim 10: “The sub-system of the vehicle of claim 1, wherein the tracked use of the vehicle is configured to

identify a violation, and the violation is associated with exceeding a speed limit, or time limit, or an area limit.”

164. As I describe in detail for Claims 8 and 9, Kleve discloses monitoring use of the vehicle to identify violations of restrictions on use.

165. In my opinion, Kleve specifically discloses violations associated with speed limits, time limits, and area limits. *See* Kleve at ¶¶ [0040] (restrictions based on “speed” and “global position coordinates”), [0041] (“driving to restricted areas”), [0043] (time limits), [0075] (speed limits), [0078] (“vehicle speed, acceleration force, wheel speed, breaking, steering, vehicle weight, throttle and pedal position”).

11. Independent Claim 11

166. As illustrated in the table below, every element of Limitations 11[pre]-11[c] and 11[e] of Claim 11 is also included in the corresponding Limitations 1[pre]-1[c] and 1[e] of Claim 1. Thus, based on my discussion above of Claim 1, limitations 11[pre]-11[c] and 11[e] are disclosed by Kleve.

1[pre]	A sub-system of a vehicle, the vehicle having an on-board computer interfaced with the sub-system for processing instructions to enable use of an electronic key (eKey), the sub-system comprising:	11[pre]	A system of a vehicle, the vehicle having an on-board computer for processing and communicating with the system for use of an electronic key (eKey), the system comprising:
1[a]	memory associated with the on-board computer of the	11[a]	memory associated with the on-board computer of the

	vehicle having program instructions for instructing unlocking and starting of the vehicle; and		vehicle having program instructions for controlling unlocking and starting of the vehicle; and
1[b]	communications circuitry of the vehicle interfaced with the on-board computer of the vehicle and the sub-system, the communications circuitry is configured to process program instructions to enable communication with a server,	11[b]	communications circuitry of the vehicle interfaced with the on-board computer of the vehicle,
1[c]	the communications circuitry includes wireless communication circuitry for enabling local connection with a mobile device, the mobile device is configured to use the eKey for said unlocking and said starting of the vehicle;	11[c]	the communications circuitry includes wireless communication circuitry for enabling local connection with a mobile device, the mobile device is configured to use the eKey for said unlocking and said starting of the vehicle;
1[d]	wherein the wireless communications circuitry of the vehicle is configured to receive coded data from the mobile device when using the eKey, the coded data enables functions of said eKey for said unlocking and use of the vehicle, the coded data is associated to the eKey for use by the mobile device,	11[d]	wherein the wireless communications circuitry of the vehicle is configured to receive coded data from the mobile device, the coded data is unique for said eKey,
1[e]	and the coded data includes privilege settings associated	11[e]	and the coded data includes privilege settings set for

	with the eKey for limiting types of use of the vehicle when using the eKey with the vehicle;		limiting types of use of the vehicle when using the vehicle via the eKey;
1[f]	wherein use of the vehicle using the eKey is tracked to identify and log actions taken using the vehicle while the eKey is used.	11[f]	wherein the eKey is associated with a user account, the user account is accessible via a user interface of an application executed by the mobile device, the eKey when active enables said unlocking of the vehicle and said starting of the vehicle.

167. I address Limitations 11[d] and 11[f] are below.

11[d]: “wherein the wireless communications circuitry of the vehicle is configured to receive coded data from the mobile device, the coded data is unique for said eKey,”

168. As I explained for Limitation 1[d], Kleve and Hatton render obvious that the wireless communications circuitry of the vehicle is configured to receive coded data from the mobile device. Kleve’s disclosure of a matrix barcode (*e.g.*, Kleve at ¶¶ [0044], [0063], [0067]) and Hatton’s disclosure of encrypted data (*e.g.*, Hatton at 7:18-23, 7:33-45, 7:49-56, 13:24-27) each independently disclose that aspect of the limitation.

169. Claim 11[d] also requires that the coded data is “unique for said eKey.” In my opinion, this is disclosed by Kleve. For example, Kleve discloses that coded

data for a virtual key, such as a “matrix barcode,” is generated based on a Temporary User’s identification information. Kleve at ¶ [0037] (describing examples of Temporary User Identification, including “matrix barcode”), [0063] (“Additional Temporary User identification 504 may be sent to the vehicle Owner allowing for this information to be entered into the server and used as a virtual key, or in addition to the virtual key.”). Because each Temporary User will have different personal identification information, the coded data associated with each Temporary User’s virtual key (based on the Temporary User identification information) will also be unique. Hatton demonstrates that the VCS in Kleve stores different encrypted data separately for each authorized key in the look-up table. Hatton at 7:33-45.

11[f]: “wherein the eKey is associated with a user account, the user account is accessible via a user interface of an application executed by the mobile device, the eKey when active enables said unlocking of the vehicle and said starting of the vehicle.”

170. In my opinion, Kleve discloses that a virtual key is associated with a user account. For example, Kleve discloses that a temporary user may “set[] up a user profile that is saved in a database within the vehicle rental authorization system.” Kleve at ¶ [0086]; *see also id.* at ¶ [0037] (the “Temporary User may set up a user profile ... to include ... matrix barcode (ex. two-dimensional code), ... or other types of unique Temporary User identification to validate and pay for the rental

service.”). The Temporary User accesses the vehicle rental system by logging in using his or her user profile. *Id.* at ¶ [0047] (“The Temporary User can log-in to the website to begin browsing the database of available vehicles to rent.”). The system “generate[s] and deliver[s] virtual keys to the Temporary User” based on rental agreements that the Temporary User enters into using his or her profile. *Id.* at ¶ [0048]. The resulting virtual keys are thus associated with the user’s profile. Virtual keys are also associated with a Temporary User’s profile because they use Temporary User identification information entered into that profile to verify the Temporary User’s credentials when the virtual key is used. *Id.* at ¶¶ [0037] (describing entry of identification information in the user profile), [0063] (describing the use of “Temporary User Identification,” including the user’s “mobile web login IDs and password” or “matrix barcode” as the virtual key).

171. Kleve also discloses that a Temporary User’s profile is accessible via a user interface of a smart phone application. *Id.* at ¶ [0036] (“The vehicle rental micro-business 200 may include 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.”).

172. Kleve also discloses that an activated virtual key enables unlocking of a vehicle and starting of the vehicle. For example, Kleve discloses that a mobile

device configured with a virtual key may be used to “unlock” and “drive” (which necessarily entails starting) the vehicle. *See id.* at ¶ [0009] (“The processor may establish communication with a wireless device brought within proximity of a vehicle ... [and] receive user input corresponding to an attempt to activate the vehicle during the rental period and ... enable a keyless drive-away.”), [0071] (“[T]he Temporary User may send the virtual key to the server requesting access to the vehicle, or use a vehicle input device, like camera, microphone, fingerprint scanner or retinal scanner integrated with the VCS to capture his identity and/or payment credentials to enable a keyless drive-away. ... [T]he Temporary User may again input the same identifying credentials to unlock and drive.”).

12. Claim 12: “The system of a vehicle as recited in claim 11, wherein a server is configured for communication with the application executed by the mobile device, the server is one of a plurality of servers, and one of said servers is associated with a manufacturer of the vehicle.”

173. In my opinion, Kleve discloses a server configured for communication with an application executed by the mobile device. For example, Kleve discloses a “centralized system” that is a “server system that includes processing capability for incoming nomadic device signals designated to interact with a remote vehicle.” Kleve at ¶ [0057]. Kleve explains that the server “may route an incoming signal from

a nomadic device (ND) 403 to the appropriate remote vehicle to enable a Temporary User keyless access and drive away capabilities.” *Id.*

174. Kleve also discloses that the server may be one of a plurality of servers. For example, Kleve’s server system may include at least two distinct servers, specifically, an “automated call server and/or web host.” *Id.* at ¶ [0057]. A POSITA would expect each of these to be implemented as a distinct server, as each function is distinct and can more easily be managed and operated when configured as separate servers.

175. Claim 12 also requires that one of the servers “is associated with a manufacturer of the vehicle.” I am informed by counsel that that limitation should not receive any patentable weight because it just describes information about entities associated with a server, which has no functional relationship to the functionality or operation of the server itself. Specifically, the identity of the owner or operator of the server does not change the underlying implementation or operation of the server.

176. Even if the “manufacturer” limitation is found to have patentable weight, a POSITA would have understood—and, at a minimum, it would have been obvious—that the server may be associated with the manufacturer of the vehicle. Kleve is a Ford patent; thus, a POSITA reviewing Kleve would have understood that the disclosed system is a system developed by or for Ford. Kleve even identifies a

specific Ford system that may be used as the VCS—specifically, “the SYNC system manufactured by THE FORD MOTOR COMPANY.” Kleve at ¶ [0021]. In any event, a POSITA would have been well aware of existing electronic key systems operated or otherwise associated with vehicle manufacturers as of the priority date of the ’659 patent. For example, Xiao (discussed in more detail in other grounds below) (describes an “automobile service server” and “automobile web service server” that are “associated with an automobile company.” Xiao at 3:12-20, 3:46-54, 4:46-56.

13. Claim 13

13[a]: “The system of a vehicle as recited in claim 11, wherein the eKey is securely generated on the mobile device, and”

177. In my opinion, Kleve renders obvious that a virtual key may be securely generated on a mobile device. For example, Kleve teaches that the “exemplary processes” described in the reference—such as, for example, the processes for generating virtual keys and their associated coded or encrypted data—“may be executed by a computing system in communication with a vehicle computing system.” Kleve at ¶ [0035]. This external computing system “may include ... a wireless device (e.g., and without limitation, a cellular telephone) or a remote computing system (e.g., and without limitation, a server),” and is collectively

referred to by Kleve as “vehicle associated computing systems (VACS).” *Id.* Kleve explains that “[i]n certain embodiments, particular components of the VACS may perform particular portions of a process depending on the particular implementation of the system,” and that “[o]ne of ordinary skill in the art will understand when it is inappropriate to apply a particular VACS to a given solution.” *Id.* A POSITA would thus understand that, in general, the various processes disclosed in Kleve may be performed by either the server **or** the mobile device, excepted in limited instances where a POSITA would understand that one or the other would not be appropriate for a particular solution. A POSITA would thus understand that in Kleve’s system, the server **or** the mobile device could be used to generate virtual keys. This would have been consistent with the general understanding of a POSITA that many processes in a client-server architecture may be performed at the client **or** at the server, depending on the particular implementation, and that that decision may be a design choice.

178. A POSITA would have understood that generating virtual keys is **not** one of the limited instances where it is **only** appropriate to use the server, and that the mobile device could equally be used to generate the virtual key, as Kleve suggests. From a technical perspective, by October 2013, mobile devices frequently included processors that would have been capable of performing the data processing

necessary to generate a virtual key (*e.g.*, encryption operations to generate the coded data associated with the virtual key, which I discuss in more detail for Claims 14 and 15 below). Similarly, by October 2013, mobile devices included sufficient memory to store data that may be used for generating the virtual key, such as security codes associated with the vehicle itself, or other information that may be encoded into the virtual key to allow the vehicle to recognize that it is an authorized key. In addition, as I explain above in the section titled “Motivation to Combine Kleve and Hatton and Reasonable Expectation of Success,” a POSITA would have also been motivated to configure Kleve’s system to generate virtual keys on the mobile device in order to make it easier for a Vehicle Owner to generate and distribute virtual keys—for example, when the Vehicle Owner or Temporary User cannot connect to the server.

13[b]: “wherein a server associated with a manufacturer of the vehicle is configured to communicate with the application, the application further being associated with a manufacturer of the vehicle.”

179. As I explain above for Claim 12, Kleve discloses a server configured to communicate with an application. Kleve at ¶ [0057]. To the extent the server being associated with a manufacturer of the vehicle is determined to have patentable weight, Kleve at least renders that limitation obvious because it is a Ford patent, and

discloses a Ford system (*i.e.*, a system associated with a vehicle manufacturer). *See id.* at ¶ [0021].

180. Claim 13 additionally requires that the application is “associated with a manufacturer of the vehicle.” I am informed by counsel that this limitation also should not receive any patentable weight, for the same reason as the “manufacturer” limitation in claim 12—that is, because the entity associated with the application has no functional relationship to the functionality or implementation of the application.

181. Even if the “manufacturer” limitation is found to have patentable weight, a POSITA would have understood that the software application may be associated with a manufacturer of the vehicle because Kleve is a Ford patent, as I discuss above. In addition, Hatton makes clear that the “software application 212” “may be an application that was developed and/or associated with the vehicle manufacturer.” Hatton at 12:46-51.

14. Claim 14: “The system of a vehicle as recited in claim 11, wherein said on-board computer includes logic for processing encryption operations of said eKey in coordination with logic of said mobile device.”

182. In my opinion, Kleve and Hatton render obvious that the VCS processor includes logic for processing encryption operations of a virtual key in coordination with logic of a mobile device. As I explained above in connection with Limitation 1[d], Kleve teaches that a virtual key may be sent “in an encrypted message” to “the

VCS, Temporary User's nomadic device, and/or vehicle Owners nomadic device.”

Kleve at ¶ [0063]. I also explain why it would have been obvious to a POSITA in view of Hatton to configure Kleve's wireless communication circuitry to receive encrypted data directly from a mobile device. Because the mobile device and the VCS are operating on the same encrypted data, both computing systems would need to be capable of processing encryption operations in order to be able to process the encrypted data. Further, the VCS and the mobile device must coordinate as to the encryption—for example, by using the same encryption scheme—or the VCS will not be able to decrypt the encrypted data sent by the mobile device.

15. Claim 15: “The system of a vehicle as recited in claim 14, wherein said encryption operations use secure public/private key pair encryption operations.”

183. In my opinion, Kleve and Hatton render obvious encryption operations using secure public/private key pair encryption. I explained above for Claim 14 why Kleve and Hatton render obvious encryption operations. It would have been obvious to a POSITA to use public/private key pair encryption for the encryption operations. Public/private key pair encryption refers to a well-known encryption scheme, sometimes also referred to as “public key encryption,” “public key cryptography,” or “asymmetric cryptography,” where encryption uses pairs of related keys to encrypt and decrypt information. The public key in the key pair is generally public,

and can be used by anyone to encrypt a message. The private key, by contrast, is kept secret, and can only be used by the intended recipient to decrypt and read the message. Public/private key pair encryption has been known and in use for decades. One particularly well-known example is Pretty Good Privacy (PGP), an encryption program developed in the 1990s for digitally signing and encrypting/decrypting text, such as e-mails, files, etc.

184. It would have been obvious to POSITA to use public/private key pair encryption, as a generally known encryption technique, for the encryption operations used by Kleve and Hatton. In addition, public/private key pair encryption would have been particularly effective in an electronic key system such as Kleve's and Hatton's, because it would allow distribution of public keys to authorized Temporary Users, so that they may generate encrypted data to authenticate with the VCS, while keeping private keys secret, so that the same Temporary Users cannot forge unauthorized virtual keys for the same or other vehicles at a later date. A POSITA would have been readily capable of implementing such encryption in Kleve's and Hatton's systems, given how well-known and documented the technology is.

185. Other prior art in the field of electronic key systems illustrates that public/private key pair encryption was well-known for years before the '659 patent's priority date, and was used in electronic key systems for vehicles. *See* Fukushima at

15:34-51 (describing use of a “public key pair” and “private key” used in a “security device” of a vehicle).

- 16. Claim 16: “The system of a vehicle as recited in claim 11, wherein said wireless communication circuitry facilitates one or more of Bluetooth, near field communication (NFC), WiFi, or radio communication.”**

186. In my opinion, Kleve and Hatton render obvious wireless communication circuitry that facilitates Bluetooth, NFC, WiFi, and radio communication. I discuss this in detail for Claim 5.

- 17. Claim 17: “The system of a vehicle as recited in claim 11, wherein said eKey is validated and securely bound to the mobile device to prevent unauthorized transfers of the ekey.”**

187. In my opinion, Kleve discloses validating a virtual key and binding the virtual key to the mobile device to prevent unauthorized transfers of the virtual key. For example, as I discuss above for Limitation 11[f], Kleve discloses associating a virtual key with a Temporary User and the user’s mobile device using the Temporary User’s profile. See Kleve at ¶¶ [0037], [0063], [0086]. It would have been obvious to a POSITA in view of Hatton to also bind the virtual key to the Temporary User’s mobile device to prevent unauthorized transfers.

188. Hatton, in particular, describes several ways by which a virtual key may be bound to a specific mobile device. In one example, the mobile device must be

configured to operate as a virtual key by receiving “vehicle security codes” via the VCS. Hatton at 12:65-13:4, 14:61-15:6. Hatton also teaches that configuring the mobile device as an electronic key may require additional validation steps, such as “plac[ing] [the mobile device] in a backup slot before transmission of codes.” *Id.*, 13:14-18. Hatton discloses that only after the security codes are transferred, the user may “now use the mobile device 210 to initiate the VCS 218.” *Id.* at 13:18-21. A POSITA would have understood that the transmission of the security codes effectively binds the associated virtual key to the mobile device, because no other mobile device can use the same virtual key unless it is configured with the same security codes via the VCS.

189. As I explain above in the section titled “Motivation to Combine Kleve and Hatton and Reasonable Expectation of Success,” a POSITA would have been motivated to configure Kleve’s system to bind a virtual key to a mobile device, as described in Hatton. In short, binding the virtual key to a specific mobile device would enhance security by preventing unauthorized transfer of the virtual key, and thus unauthorized access to the vehicle.

18. Independent Claim 18

190. As illustrated in the table below, every element of every Limitation of Claim 18 is included in the corresponding Limitations of Claim 1. Thus, based on

my discussion above of Claim 11, Claim 18 is rendered obvious by Hatton and Kleve.

11[pre]	A system of a vehicle, the vehicle having an on-board computer for processing and communicating with the system for use of an electronic key (eKey), the system comprising:	18[pre]	A vehicle having an on-board computer for processing and communicating an electronic key (eKey), the vehicle comprising:
11[a]	memory associated with the on-board computer of the vehicle having program instructions for controlling unlocking and starting of the vehicle; and	18[a]	memory associated with the on-board computer of the vehicle having program instructions for controlling unlocking and starting of the vehicle; and
11[b]	communications circuitry of the vehicle interfaced with the on-board computer of the vehicle,	18[b]	communications circuitry of the vehicle interfaced with the on-board computer of the vehicle,
11[c]	the communications circuitry includes wireless communication circuitry for enabling local connection with a mobile device, the mobile device is configured to use the eKey for said unlocking and said starting of the vehicle;	18[c]	the communications circuitry includes wireless communication circuitry for enabling local connection with a mobile device, the mobile device is configured to use the eKey for said unlocking and said starting of the vehicle;
11[d]	wherein the wireless communications circuitry of the vehicle is configured to receive coded data from the	18[d]	wherein the wireless communications circuitry of the vehicle is configured to receive coded data from the mobile device, the coded data

	mobile device, the coded data is unique for said eKey, and		is unique for said eKey to be used via the mobile device, and
11[e]	the coded data includes privilege settings set for limiting types of use of the vehicle when using the vehicle via the eKey;	18[e]	the coded data includes privilege settings for use of the vehicle when using the eKey with the vehicle;
11[f]	wherein the eKey is associated with a user account, the user account is accessible via a user interface of an application executed by the mobile device, the eKey when active enables said unlocking of the vehicle and said starting of the vehicle.	18[f]	wherein the eKey is associated with a user account, the user account is accessible via a user interface of an application executed by the mobile device, the eKey when active enables said unlocking of the vehicle and said starting of the vehicle.

19. Claim 19: “The vehicle of claim 18, wherein the privilege settings being unrestricted for an owner of the vehicle and restricted for a shared user of the vehicle, the shared user of the vehicle receives a shared eKey responsive to said owner of the vehicle causing the shared eKey to be sent for shared use of the vehicle.”

191. In my opinion, Kleve discloses that privilege settings are unrestricted for an owner of a vehicle and restricted for a shared user of a vehicle. For example, Kleve discloses that an Owner “may set user restrictions by use of the website or nomadic device ... based on, but not limited to, the owner’s selection of parameters including, but not limited to, speed, global position coordinates, or load weight restrictions.” Kleve at [0040]; *see also id.*, [0043] (“vehicle restriction limits [are]

initially set by the Owner at the beginning of the rental term”). Because these restrictions are applied to Temporary Users, a POSITA would have understood that the Owner would naturally have unrestricted use of the vehicle. This is further confirmed by the fact that Kleve discloses that a virtual key may provide a different “driver status signal” for an Owner and a Temporary User, such that “vehicle functionality may be restricted or limited” only when “the driver is the Temporary User.” *Id.* at ¶ [0045].

192. Kleve also discloses that a shared user of the vehicle receives a shared virtual key in response to the Owner causing the shared virtual key to be sent for shared use of the vehicle. For example, in Kleve’s system, the virtual key is generated and delivered to a Temporary User only after the Owner and Temporary User agree to the terms of the rental, and the Temporary User “pays the appropriate amount and signs a consent agreement.” *Id.* at ¶ [0039]. By agreeing to the terms of the rental and signing the agreement, the Owner causes the virtual key to be sent to the Temporary User for use of the vehicle. In one embodiment, Kleve also discloses that the Owner may generate and deliver the virtual key using the Owner’s mobile device, which would necessarily require the Owner to cause the virtual key to be sent. *See id.* at Fig. 6. Kleve also describes embodiments that use “remote credential verification,” which also separately require “the Owner to verify the Temporary

User's request" when the temporary user attempts to access the vehicle. *Id.* at ¶ [0049].

- 20. Claim 20: "The vehicle of claim 18, wherein the eKey is securely generated on the mobile device, and wherein a server associated with a manufacturer of the vehicle is configured to communicate with the application, the application further being associated with a manufacturer of the vehicle."**

193. Claim 20 recites the same additional limitations as Claim 13. Accordingly, Claim 20 is rendered obvious by Kleve and Hatton for the same reasons I discuss above for Claim 13.

- 21. Claim 21: "The vehicle of claim 18, wherein encryption operations are associated with use of said eKey, and said encryption operations use public/private key pair encryption, and wherein said wireless communication circuitry uses one or more of Bluetooth, or near field communication (NFC), or WiFi, or radio communication."**

194. Claim 21 recites the same additional limitations as each of claims 14 (encryption operations for use of the electronic key), 15 (public/private key pair encryption), and 16 (wireless communication circuitry using Bluetooth, NFC, WiFi, or radio communication). Accordingly, Claim 21 is rendered obvious by Kleve and Hatton for the same reasons I discuss above for Claims 14, 15, and 16.

B. Ground 2: Kleve in view of Hatton and Sekiyama renders obvious

claim 2 under Section 103

195. Sekiyama is a Toyota patent that, like Kleve and Hatton, describes an electronic key system for a vehicle. In Sekiyama's system, a vehicle owner can create a duplicate electronic key and configure the duplicate electronic key to only have limited functionality, including limited access to different areas of the vehicle, such as the door locks and trunk. As I discuss below, a POSITA would have found it obvious to combine Kleve and Hatton with Sekiyama to add support for additional use restrictions such as limited door lock and trunk access.

1. Motivation to Combine Kleve, Hatton, and Sekiyama and Reasonable Expectation of Success

196. In my opinion, a POSITA would have been motivated to apply Sekiyama's teachings of duplicate keys that restrict access to the door locks and trunk of a vehicle to Kleve's rental car system (as modified in view of Hatton) because there would have been clear benefits to adding such restrictions to Kleve's vehicle rental system. As I discuss in Ground 1, Kleve already provides for virtual keys that restrict types of use of a vehicle. Additional options for such restrictions would make Kleve's system more versatile by providing vehicle owners with more control over the use and types of use of their vehicle by a Temporary User. For example, for a vehicle rental intended for short errands within a limited geographic range, the vehicle Owner could disable trunk access, as the rental agreement does

not contemplate long distances that may require storage, or hauling cargo that may need to be stored in a trunk. Similarly, adding restrictions to door lock and trunk access would allow Kleve's system to be generalized for other key sharing applications beyond vehicle rentals, such as using the system to generate a temporary electronic key for use by a valet (as contemplated by Sekiyama).

197. Indeed, Sekiyama provides an explicit reason to apply its teachings regarding restricted door lock and trunk access to Kleve's system. Specifically, Sekiyama teaches that in certain circumstances, when a non-owner is given access to a vehicle (in particular, in the case of valet parking), "lending a dedicated vehicle key to another person could pose a security risk." Sekiyama at ¶ [0004]. Sekiyama proposes to solve that concern by "allow[ing] restrictions on the functions that can be executed with a duplicate electronic key." *Id.* at ¶ [0005]. The restrictions contemplated by Sekiyama specifically include "locking and unlocking of the door lock" and "locking and unlocking of the trunk." *Id.* at ¶ [0018].

198. In my opinion, a POSITA would also have reasonably expected this combination to succeed. As I note above, Kleve already discloses restrictions on types of use that may be applied to a virtual key, as well as using the virtual key to control different sub-systems of the vehicle via the processor in the VCS. Kleve at ¶¶ [0023], [0040], [0076]. Hatton also specifically describes that the VCS operating

with a virtual key may be used to control “unlocking/locking doors, and/or opening the trunk with the mobile device.” Hatton at 13:24-27. A POSITA would have been capable of adding an additional restriction on access to the vehicle’s door locks and trunk using the same software that Kleve already uses to implement other restrictions and to control other parts of the vehicle via the VCS processor. Adding door lock and trunk restrictions, as described by Sekiyama, to Kleve’s well-defined framework would have been well within the capabilities of a POSITA, and would have required little more than routine software engineering to extend Kleve’s design to additionally support door lock and trunk restrictions.

199. In my opinion, Kleve, Hatton, Sekiyama, and the ’659 patent are all directed to the same field of endeavor, the field of electronic key systems. *See* ’659 patent at Abstract (“A vehicle configured to communicate with a server of a cloud system to enable access to use the vehicle via one or more electronic keys is provided.”); Kleve at ¶¶ [0044]-[0045] (describing implementation of a “virtual key feature” for use in the “vehicle rental micro-business system”); Hatton at 1:6-8 (“The present invention relates to an electronic key system and a vehicle computing system for managing a vehicle electronic key.”); Sekiyama at ¶ [0005] (“[I]t [is] an object of the present invention to provide an electronic key system that allows restrictions

on the functions that can be executed with a duplicate electronic key to be imposed when such a key is generated.”).

2. Claim 2: “The sub-system of the vehicle of claim 1, wherein said privileges function as restrictions that enable access to specific vehicle areas that include one or more of vehicle door operation, or trunk operation.”

200. As I discuss in Ground 1 above, Kleve and Hatton render obvious Claim 1.

201. In my opinion, it would have been obvious to a POSITA to extend Kleve’s virtual key system, including the options for restricting uses and types of use of the vehicle with a virtual key, to control a Temporary User’s access to the door lock and trunk of a vehicle, as taught by Sekiyama. Sekiyama describes an “electronic key system ... whereby a duplicate electronic key containing a signal that allows execution of only a subset of functions is transmitted to another terminal.” Sekiyama at ¶ [0007]. The “subset of functions” includes “a function of locking/unlocking a door lock of a vehicle” and “a function of starting a drive source of the vehicle.” *Id.* at ¶ [0008]. At the same time, the duplicate key may “disable execution of other functions,” such as “unlocking the trunk,” “unlocking the console compartment,” and “electronic devices such as the navigation system.” *Id.*; *see also id.* at ¶ [0018] (describing a “function restriction unit 43” that “controls the enablement of execution or disablement of execution of various functions of the

vehicle 40 based on the key information recognized by the electronic key recognition unit,” including “controlling the locking and unlocking of the door lock” and “controlling the locking and unlocking of the trunk”). Sekiyama explains that this “enhanc[es] security features and strengthen[s] the protection of personal information.” *Id.* at ¶ [0008].

202. As I explain above in the section titled “Motivation to Combine Kleve, Hatton, and Sekiyama and Reasonable Expectation of Success,” a POSITA would have been motivated to apply Sekiyama’s use restrictions relating to door lock and trunk access to Kleve’s vehicle rental system in order to “enhanc[e] security features and strengthen[] the protection of personal information.” Sekiyama at ¶ [0008]. The additional feature would also offer the vehicle owner more flexibility and control over the types of access that Temporary Users may have to the vehicle.

C. Ground 3: Mikan anticipates or renders obvious claims 1-3, 5 and 8-10 under Section 102 or Section 103

203. A summary of this ground is as follows: Mikan discloses a vehicle key system that supports electronic keys embedded in a mobile device to enable keyless access to and operation of the vehicle. The vehicle includes a control unit that communicates wirelessly with a server and an electronic key. A secure ID check and secure identifier are used to verify a mobile device operating as an electronic key. A vehicle operation policy is associated with each key and stored both at a local

database at the vehicle, and a master database at a server. The vehicle operation policy defines permitted and prohibited uses of the vehicle, and monitors use of the vehicle to determine whether a rule is being violated. If a rule within the policy is violated, a notification is sent.

1. Claim 1

1[pre]: “A sub-system of a vehicle, the vehicle having an on-board computer interfaced with the sub-system for processing instructions to enable use of an electronic key (eKey), the sub-system comprising:”

204. In my opinion, Mikan discloses this limitation.

205. Mikan discloses a “control unit” in a vehicle. Mikan at ¶ [0051]. The control unit may be “any combination of hardware and/or software,” and may be “an onboard computer.” *Id.* The control unit “is in operative communication with vehicle 201.” *Id.* For example, the control unit may “control vehicle functions” or “sense operation of vehicle 201.” *Id.* at ¶ [0053]. The control unit is also “in communication with wireless network 207,” which may be a cellular network (*e.g.*, GSM, GPRS, EDGE, W-CDMA) or a Wi-Fi network (*i.e.*, 802.121 WLAN). *Id.* at ¶ [0052]. Mikan discloses that “any aspect of the vehicle that may be controlled by an electrical signal may be controlled by control unit 202, and [any] aspect of the vehicle operation that may be sensed and converted to an electronic signal may be sensed by control unit 202.” *Id.* at ¶ [0053]. Mikan explains that these controllable aspects “may be

considered a vehicle operation feature,” and “one or more vehicle subsystems that control one or more of such vehicle operation features may be in operative communication with, for example, wireless vehicle security system 200.” *Id.* at ¶ [0060]. Thus, Mikan’s control unit, which is part of the wireless vehicle security system, is in communication with vehicle subsystems that control vehicle operation features.

206. Mikan does not expressly state that the control unit processes instructions to perform different functions, but because the control unit may be a computer, a POSITA would have understood the control unit processes instructions. The way that computers perform tasks is by processing instructions that comprise a program or software application to be executed by the computer.

207. Mikan’s control unit enables the use of electronic keys. For example, Mikan discloses that the system may have several keys, “key 205A-C,” that “communicate directly with control unit 202.” Mikan at ¶ [0051]. “Keys 205A-C may be electronic keys,” including “embedded in a wireless device such as a cellular telephone or Personal Digital Assistant (PDA).” *Id.* at ¶ [0050].

1[a]: “memory associated with the on-board computer of the vehicle having program instructions for instructing unlocking and starting of the vehicle; and”

208. In my opinion, Mikan discloses memory associated with the control unit. For example, the control unit “may be in operative communication with local database 203,” which “may be resident within vehicle 203.” Mikan at ¶ [0051]. “Local database 203 may be any software system or device suitable for storing and retrieving data records.” *Id.* A system or device that stores and retrieves data by definition is or includes memory.

209. The local database stores “vehicle operation policies” that, in turn, include “access control rules.” *Id.* at ¶ [0060]. Access control rules “may operate to enable, partially enable, or disable the related vehicle operation feature.” *Id.* The access control features may include “unlocking a door, opening a trunk, opening a glove box, engaging an ignition, directing the vehicle from a one [*sic*] geographic location to another geographic location, and accelerating the vehicle, for example.” *Id.*

210. A POSITA would have understood that the access control rules are or comprise program instructions, since they are used to control operation of the control unit, which processes and executes instructions. For example, the control unit “may block and/or limit the operation of the vehicle” when an “access request is inconsistent with the retrieved vehicle operation policy.” *Id.* at ¶ [0074]. The control unit may also “monitor the status of a particular vehicle operation feature and

confirm[] its conformance with vehicle operation policy 311 associated with the key 205A-C that is currently in use.” *Id.* at ¶ [0076]. In addition, a POSITA would have understood that other program instructions to be processed and executed by the control unit would be stored in memory, because processors must store instructions somewhere in order to process them, and computers store instructions in memory.

1[b]: “communications circuitry of the vehicle interfaced with the on-board computer of the vehicle and the sub-system, the communications circuitry is configured to process program instructions to enable communication with a server,”

211. In my opinion, Mikan discloses communications circuitry interfaced with its control unit and vehicle subsystems.

212. Mikan discloses that its control unit (on-board computer) and associated subsystems interface with communications circuitry to communicate with a server. The communications circuitry processes program instructions that are used to communicate with a server platform.

213. Mikan discloses that its control unit communicates with a server over a wireless network. Mikan at ¶¶ [0052] (“Control unit 202 may be in communication with wireless network 207,” which “may host master database 208 and application 209”), [0055] (“[M]aster application 209 may be software resident on a server platform.”).

214. A POSITA would have understood that in order for Mikan's system to communicate wirelessly, it must include communications circuitry interfaced with the control unit for enabling communication with a wireless network. As I discuss above in Ground 1, a POSITA would have understood that the developer of an electronic key system would typically not develop standard wireless communication components, and would instead source those from a component supplier. Such components are typically supplied as separate circuitry, *i.e.*, a chip or board with an embedded processor or controller that executes programs and instructions to communicate using a particular wireless protocol. A POSITA would have understood that Mikan's system includes such components to communicate with the wireless network, particularly since Mikan discloses using well-known and conventional wireless communication protocols, such as "Bluetooth protocol, WiFi, RF-ID, cellular, and the like." *Id.* at ¶ [0067]. For the same reason, a POSITA would have understood that the communication circuitry processes program instructions.

215. A POSITA would have also understood that other sub-systems in the vehicle interface with the communication circuitry. At a minimum, the sub-systems interface with the communication circuitry through the control unit, which accesses vehicle operation policies used to control those sub-systems via the communication

circuitry (*e.g.*, by retrieving them from the master database) and directly interfaces and controls the vehicle sub-systems. *Id.* at ¶¶ [0053], [0058]-[0060].

1[c]: “the communications circuitry includes wireless communication circuitry for enabling local connection with a mobile device, the mobile device is configured to use the eKey for said unlocking and said starting the vehicle;”

216. In my opinion, Mikan discloses communication circuitry including wireless communication circuitry. For example, as I discuss above for Limitation 1[b] (“communications circuitry of the vehicle interfaced with the on-board computer of the vehicle and the sub-system”), Mikan discloses that the control unit communicates with a wireless network. Mikan at ¶ [0052]. Mikan also identifies several exemplary wireless protocols that may be used for communication, including “Bluetooth protocol, WiFi, RF-ID, cellular, and the like.” *Id.* at ¶ [0067]. Mikan also discloses that the control unit, via the wireless communication circuitry, enables local connection with a mobile device. For example, the control unit may communicate with “electronic keys” that “may be embedded in a wireless device such as a cellular telephone or Personal Digital Assistant (PDA).” *Id.* at ¶ [0050]. “[K]ey 205A-C and control unit 202 may communicate directly via a radio frequency transmission.” *Id.* at ¶ [0051].

217. The wireless device operating as an electronic key may be used to unlock and start a vehicle. For example, Mikan discloses that each electronic key has an associated “vehicle operation policy.” *Id.* at ¶ [0052]. The vehicle operation policy may be used to process requests such as “unlocking a door” or “engaging an ignition.” *Id.* at ¶ [0073]; *see also id.* at ¶ [0077] (describing example where a key “signals an access request to vehicle 201 to unlock a door and the access request is not allowed by vehicle operation policy 311 retrieved for that specific key 205A-C”).

1[d]: “wherein the wireless communications circuitry of the vehicle is configured to receive coded data from the mobile device when using the eKey, the coded data enables functions of said eKey for said unlocking and use of the vehicle, the coded data is associated to the eKey for use by the mobile device,”

218. In my opinion, Mikan discloses wireless communications circuitry configured to receive coded data from a mobile device using a virtual key. For example, when “a user attempt[s] to access or operate vehicle 201 with a key 205A-C,” the control unit initiates an authentication process. Mikan at ¶ [0070]. The control unit “may authenticate key 205A-C via secure ID check 315.” *Id.* at ¶ [0071]. To authenticate an electronic key, a “[s]ecure identifier 407 may be received ... at control unit 202.” *Id.* at ¶ [0070]. The secure identifier may be coded data, such as “a digital signature associated with [a] wireless device,” or “a digital signature

associated with a key,” both of which may be “the product of a public key encryption system.” *Id.* at ¶¶ [0059], [0066].

219. When the electronic key is authenticated using the secure identifier, the key is enabled to perform vehicle functions (allowed under the vehicle operation policy). For example, after the key authentication step (*e.g.*, step 504 in Figure 5), the control unit retrieves a “vehicle operation policy ... based on authenticated key 205A-C.” *Id.* at ¶ [0072]. As I discussed above, the vehicle operation policy controls various “vehicle operation features,” including “unlocking a door” and “engaging an ignition.” *Id.* at ¶¶ [0060]-[0061].

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

220. In my opinion, Mikan discloses that the coded data includes privilege settings for the electronic key that limit the types of use of the vehicle. For example, Mikan teaches that each electronic key may be mapped to a corresponding vehicle operation policy. Mikan at ¶¶ [0061] (“Mapping 312 may link vehicle operation policy 311 and keys 205A-C. ... The first key, in this example illustration, may be related via mapping 312 to access control rule 317 that enables all vehicle operation features. The second key, in this illustration, may be a ‘valet key’ with limited functionality.”). [0076]-[0077] (describing the control unit monitoring vehicle use

and processing access requests based on the “vehicle operation policy 311 retrieved for that specific key 205A-C”).

221. It would have been obvious to a POSITA to transmit the vehicle operation policy as additional coded data, either as part of or in addition to Mikan’s secure identifier. The purpose of the vehicle operation policy is to prevent certain users from taking certain actions when using the vehicle. If the vehicle operation policy is transmitted in unencrypted form, a user may be able to access the policy and modify it to enable unauthorized access to certain vehicle features. A POSITA would thus have been motivated to encrypt or otherwise encode the vehicle operation policy for transmission so that users cannot tamper with the vehicle operation policies and associated access control rules.

222. In my opinion, a POSITA would have reasonably expected to succeed at encrypting and transmitting the vehicle operation policy. As discussed above, Mikan’s system already supports wireless communication and coded data. A POSITA could have used the same or substantially similar encryption and wireless communication techniques already implemented in Mikan in order to encrypt and transmit the vehicle operation policy. The modification would require basic engineering skills that would have been well within the capabilities of a POSITA.

223. Mikan’s vehicle operation policy limits the types of use of the vehicle when the vehicle is accessed using an electronic key. For example, Mikan describes the following features as examples of functionalities that the vehicle operation policy may control for a particular key: “unlocking a door, opening a trunk, opening a glove box, engaging an ignition, directing the vehicle from a first geographic location to a second geographic location, and accelerating the vehicle.” Mikan at ¶¶ [0060], [0073]-[0074]. By limiting and controlling access to these functions, the types of use of the vehicle are restricted. As an example, if the owner of a vehicle wishes to limit a particular key for use only as a valet key—that is, for parking a vehicle on behalf of the owner—the owner may define a vehicle operation policy that limits use of the key to valet functions by, for example, restricting access to the trunk, preventing driving over a certain speed or beyond a certain acceleration, and preventing directing the vehicle to a geographic location outside of certain range.

1[f]: “wherein use of the vehicle using the eKey is tracked to identify and log actions taken using the vehicle while the eKey is used.”

224. In my opinion, Mikan discloses that use of the electronic key is tracked to identify and log actions taken using the vehicle. For example, Mikan discloses that the wireless vehicle security system “enable[s] a user to ... monitor” use of the vehicle. Mikan at ¶ [0056]. When a user initiates an access request using an

electronic key—for example, by trying to “unlock a vehicle door” or “press the accelerator of the vehicle,” the control unit determines whether “the access request is consistent with the retrieved vehicle operation policy.” *Id.* at ¶¶ [0073]-[0074]. The control unit may then “notify a user or a system by signaling an indication of whether an access request conformed with the retrieved vehicle operation policy.” *Id.* at ¶ [0075]. This notification process may include logging the actions taken by the vehicle, for example, by “appending a text string to a log file.” *Id.*

2. Claim 2: “The sub-system of the vehicle of claim 1, wherein said privileges function as restrictions that enable access to specific vehicle areas that include one or more of vehicle door operation, or trunk operation.”

225. In my opinion, Mikan discloses that vehicle operation policies may function as restrictions that enable access to specific vehicle areas, including vehicle door operation and trunk operation. For example, Mikan teaches that the vehicle operation policy enables restrictions on “vehicle operation features,” including “unlocking a door” and “opening a trunk.” Mikan at ¶¶ [0060], [0073]. In practice, the control unit processes an “access request” from the user of the electronic key and compares the request to the vehicle operation policy to determine if they are “inconsistent.” *Id.* at ¶¶ [0073]-[0074]. If the access request and the vehicle operation policy are inconsistent, the control units will “block and/or limit the operation of the vehicle.” *Id.* at ¶ [0074].

3. **Claim 3: “The sub-system of the vehicle of claim 1, wherein the vehicle is configured to receive or securely store information from the server to perform authentication or verification that the coded data received from the mobile device should activate the eKey.”**

226. In my opinion, Mikan discloses that the vehicle is configured to receive and securely store information from a server to authenticate coded data for activating an electronic key. As I discussed above, Mikan’s vehicle includes a “local database.” Mikan at ¶ [0054]. The local database “may regularly poll [a] master database ... to maintain consistent data.” *Id.* The master database may be “resident on a server platform.” *Id.* at ¶ [0055]. The “local database 203 and master database 208 may communicate an update to the other after a record change.” *Id.* at ¶ [0054]. Thus, the local database at the vehicle is configured to receive and store updated information from the master database at the server.

227. Both the local database and the master database store “key set,” which includes “data representing a collection of keys.” *Id.* at ¶¶ [0058]-[0059]. The “key set” may include a “secure ID check 315 associated with a key 205A-C within the set.” *Id.* at ¶ [0059]. “Control unit 202 may authenticate key 205A-C via secure ID check 315.” *Id.* at ¶ [0071]. For example, the control unit may authenticate the key by “verifying a digital signature,” which may be a “digital signature associated with a key 205A-C” or “a digital signature associated with the wireless device 400.” *Id.*

at ¶¶ [0059], [0065], [0071]. A digital signature includes coded data, such as encrypted data that can be used to authenticate the signer.

228. A POSITA would have understood that the key set and secure ID check used for authentication are retrieved from the master database by the local database. For example, if a new authorized electronic key for a vehicle is added to the master database, the vehicle must make a copy of the new key data from the master database, so that the key can be used to access the vehicle.

4. Claim 5: “The sub-system of the vehicle of claim 1, wherein the wireless communication circuitry is associated with an NFC standard or a radio frequency standard for said local connection between the mobile device and the vehicle.”

229. In my opinion, Mikan discloses wireless communication circuitry associated with a radio frequency standard for local connection between the mobile device and the vehicle. As I discuss above for Limitation 1[c] (“the communications circuitry includes wireless communication circuitry for enabling local connection with a mobile device”), Mikan discloses that the control unit communicates with a wireless network. Mikan at ¶ [0052]. Mikan specifically discloses that “key 205A-C and control unit 202 may communicate directly via a radio frequency transmission.” *Id.* at ¶ [0051].

230. Mikan separately teaches that a “wireless device 400 equipped for use as a key 205A-C” may “communicate with vehicle 201 ... via any wireless protocol

suitable for the transmission of data.” *Id.* at ¶ [0067]. The supported protocols include “Bluetooth protocol, WiFi, RF-ID, cellular, and the like,” all of which are radio frequency standards. *Id.* In order to use those protocols to communicate with the vehicle, the vehicle would also need to have wireless communication circuitry that implements the same wireless communication protocols (*e.g.*, Bluetooth or WiFi) as the wireless device; otherwise, the vehicle will not be able to receive the transmissions from the wireless device.

5. **Claim 8: “The sub-system of the vehicle of claim 1, wherein a mode of allowed use of the vehicle using the eKey is configured to monitor said use of the vehicle, and said on-board computer is configured to transmit one or more notifications when a violation of a restriction is detected.”**

231. In my opinion, Mikan discloses that a mode of allowed use of the vehicle using the electronic key is configured to monitor use of the vehicle, and the on-board computer is configured to transmit notifications when a violation of a restriction is detected. For example, as I discuss above for Limitation 1[f], Mikan discloses a vehicle operation policy, which the control unit uses to “monitor the status of a particular vehicle operation feature and confirming its conformance with vehicle operation policy 311 associated with the key 205A-C that is currently in use.” Mikan at ¶ [0076]. If the control unit determines that a feature “being monitored no longer conforms with vehicle operation policy 311,” the control unit

may either “disallow the operation,” or may “initiate an enforcement action.” *Id.* at ¶¶ [0076]-[0077]. The enforcement action may include transmitting a notification when the violation is detected, such as by “sending an electronic message.” *Id.* at ¶ [0078]; *see also id.* at ¶ [0075] (describing triggering a “notification” when an access request is blocked, such as “e-mail, ... [or] a text message via Short Message Service (SMS)”).

6. **Claim 9: “The sub-system of the vehicle of claim 1, wherein the tracked use of the vehicle is configured to identify a violation, and the violation is associated with one or more of driving too fast, or driving out of an area, or accelerating too fast, or stopping too fast, or parking too close to a structure or other vehicle, or coming in contact with a structure or another vehicle, or slamming a door of the vehicle, or turning on a radio, or texting while driving, or interfacing with vehicle controls while driving, or two or more thereof.”**

232. As I describe in detail for Limitation 1[f] and Claim 8, Mikan discloses monitoring use of the vehicle to identify violations of a vehicle operation policy. *See also* Mikan at ¶ [0076] (“For example, where vehicle operation policy 311 includes setting a maximum speed for the operation of vehicle 201, monitoring continuously checks the speed of vehicle 201 and compares it to the maximum imposed by vehicle operation policy 311. If vehicle 201’s speed exceeds that defined by policy 311, notification and/or enforcement action may be taken.”)

233. In my opinion, Mikan also teaches that violations of access control rules may be associated with driving too fast, accelerating too fast, or driving out of an area. See Mikan at ¶¶ [0060] (“[A]ccess control rule 317 may establish a maximum acceleration for the vehicle, [or] a geographic range within which the vehicle may be operated. ... For illustration, access control rule 317 may indicate ... that the vehicle may not be operated above 65 miles per hour.”).

7. Claim 10: “The sub-system of the vehicle of claim 1, wherein the tracked use of the vehicle is configured to identify a violation, and the violation is associated with exceeding a speed limit, or time limit, or an area limit.”

234. As I describe in detail for Claims 8 and 9, Mikan discloses monitoring use of the vehicle to identify violations of a vehicle operation policy.

235. In my opinion, Mikan specifically discloses access control rules and violations associated with speed limits, time limits, and area limits. See Mikan at ¶¶ [0060] (“For example, access control rule 317 may establish ... a *range of time* within which the vehicle may be operated, [or] a *geographic range* within which the vehicle may be operated ...”), [0061] (describing a rule “that limits the maximum speed to 35 miles per hour”).

D. Ground 4: Mikan in view of Xiao renders obvious claims 4, 11-18, and 20-21 under Section 103

236. Xiao describes “a wireless automobile key service” similar to Mikan’s. Xiao at Abstract. In Xiao’s system, a mobile device may be used to “command[] an

automobile.” *Id.* at 2:29-30. A “wireless automobile key service application” is used to “register for the disclosed wireless automobile key service 104 and create an account for one or more mobile devices 110, automobile operators, and/or automobiles 112.” *Id.* at 4:46-56. A user’s account may include information about the user’s “mobile ID 610, operator authentication information 612, operator profile information 614, automobile permissions information 616, and a default automobile ID 617.” *Id.* at 12:8-13. As I discuss below, a POSITA would have found it obvious to combine Mikan with Xiao to add support for user accounts and profiles to Mikan’s electronic key system.

1. Motivation to Combine Mikan and Xiao and Reasonable Expectation of Success

237. In my opinion, a POSITA would have been motivated to apply Xiao’s teachings relating to user accounts to Mikan’s electronic key system because there would have been clear advantages to using user profiles and accounts in a mobile device-based electronic key system.

238. Allowing a user’s personal mobile device to operate as a vehicle key is convenient, but it also increases the risk that an unauthorized user will gain access to the electronic key and, by extension the vehicle. Thus, it is critical in these systems to ensure that only authorized users have access to the vehicle, and that the electronic key is not obtained and improperly used by other unauthorized individuals. By

requiring users to register and log into an account in order to use an electronic key, the administrator of the electronic key system and the vehicle owner may verify the identity of a user before providing the user with an electronic key, thus confirming that the user should receive an electronic key for that vehicle. In addition, by associating electronic keys with user accounts, recipients of electronic keys are encouraged to operate the vehicle safely and consistent with any agreed upon terms or restrictions for use of the vehicle, as users know they will be accountable for their actions, and violations may be enforced. The addition of user accounts also allows the administrator of the system to identify users who violate the platform's policies or an owner's vehicle policies.

239. User profiles would have also benefited Mikan's system in particular by facilitating the tracking of vehicles, keys, and vehicle policies. As disclosed, and as discussed further below, Mikan uses a database to track the potentially large number of vehicles, keys, and vehicle policies administered by the system. The organization, tracking, searching, and retrieval of information about the vehicles, keys, and policies would be significantly enhanced if user accounts are associated with keys, vehicles, and vehicle operation policies. For example, instead of separately storing a vehicle operation policy for each key or owner, an owner may define a vehicle operation policy to be universally applied to that owner's electronic

keys and vehicles. The system need only store one copy of the policy, and refer to that policy for every electronic key issued by that owner. Such a system also enhances the user experience, as an owner may define a single vehicle operation policy and apply it to all subsequent electronic keys and vehicles, rather than having to specify a separate policy for each vehicle and each key.

240. In my opinion, a POSITA would also have reasonably expected this combination to succeed. Online services with user accounts were ubiquitous by the priority date of the '659 patent, and user accounts were used to store a vast array of information about users, their preferences, and their devices. Implementing user accounts in Mikan's system would have required only basic software engineering capabilities to apply well known and conventional software and user interface techniques, and would have been well within the capabilities of a POSITA.

241. In my opinion, Mikan, Xiao, and the '659 patent are all directed to the same field of endeavor, the field of electronic key systems. *See* '659 patent at Abstract ("A vehicle configured to communicate with a server of a cloud system to enable access to use the vehicle via one or more electronic keys is provided."); Mikan at Abstract ("Methods and wireless devices for providing secure operation of a vehicle. ... The key may be embedded within a wireless device such as a cellular telephone."); Xiao at Abstract ("Systems and methods for providing a wireless

automobile key service are disclosed.”), 2:29-30 (“One aspect of the disclosure relates to a method for commanding an automobile using a mobile device.”).

2. **Claim 4: “The sub-system of the vehicle of claim 1, wherein the communications circuitry of the vehicle is configured to receive one or more additional requests from other mobile devices to use the vehicle, each request is associated with coded data generated by the server, such that each coded data is associated with a user account having privileges assigned by an administrator of the vehicle that enables assigning or use of eKeys to use the vehicle.”**

242. In my opinion, Mikan discloses that the communications circuitry interfaced with the control unit may receive additional requests from other mobile devices to use the vehicle. For example, Mikan discloses that the control unit of the vehicle may be “in operative communication with [a plurality of] keys 205A-C.” Mikan at ¶ [0050]. Mikan further discloses that the keys used in its system may be “electronic keys ... embedded in a wireless device.” *Id.* at ¶ [0049]. As an example, in the embodiment shown in Figure 2, annotated and reproduced below, Keys 205A and 205B are both embedded in wireless devices.

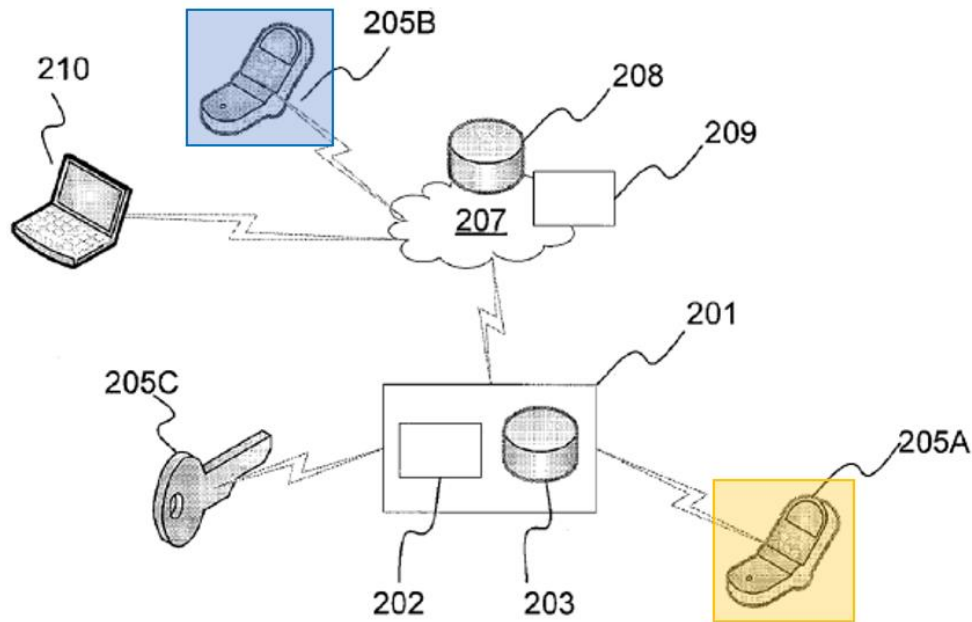
200

FIG. 2

243. In my opinion, Mikan discloses that each electronic key and its corresponding requests may be associated with coded data generated by the server. For example, as I explain above in Ground 3 for Limitation 1[d], Mikan discloses that access requests from a user using an electronic key will cause the control unit to “authenticate key 205A-C via secure ID check 315.” *Id.* at ¶ [0071]. Authentication is performed using a “secure identifier,” which includes coded data such as a “digital signature.” *Id.* at ¶¶ [0059], [0066], [0070].

244. The secure ID check may be maintained at a master database on a server, and mirrored to the local databases associated with particular vehicles and control units. For example, Mikan describes an embodiment, illustrated in Figure 3, where a key set for a vehicle is maintained in the master database at a server, and mirrored by the local database at the vehicle. Mikan at ¶ [0058] (“Master database 200 may include any number of vehicle records 302. ... In one embodiment, vehicle record 302 may include key set 310 ... [which] may include data representing a collection of keys 205A-C.”), [0059] (“Local database 303 may include vehicle ID 301, [and] key set 310 Vehicle ID 301 in local database 303 may map directly to that in master database 300.”), [0084] (“[L]ocal database 203 and master database 208 may synchronize. ... In one embodiment, consistency may be achieved by making the data of local database 203 mirror that of corresponding vehicle record 302.”). Mirroring the key set and associated secure ID checks at the local database would require receiving the original copy of the key set and secure ID checks from the master database on the server.

245. Figure 3, reproduced and annotated below, shows the contents of the master database (in Figure 3A) and the local database (in Figure 3B) for one embodiment. Of particular relevance, both databases store information including

vehicle records (yellow), key sets (red), secure ID checks (blue), and key/policy mappings (purple):

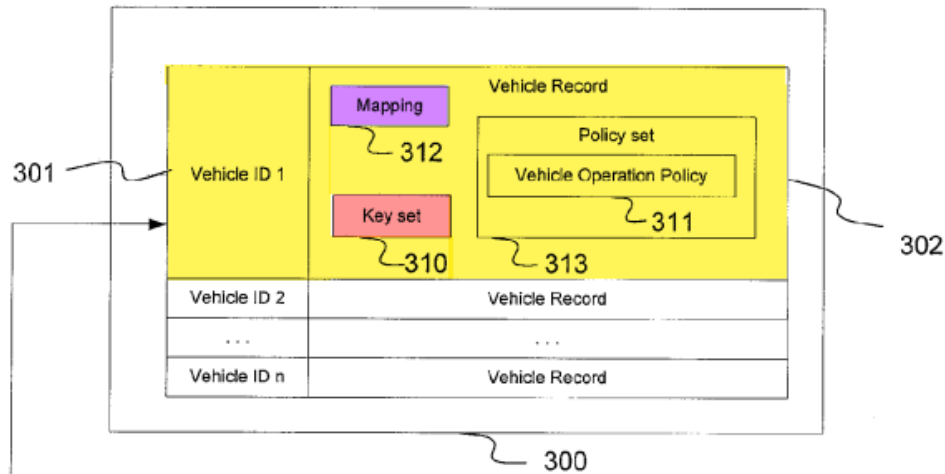


FIG. 3A

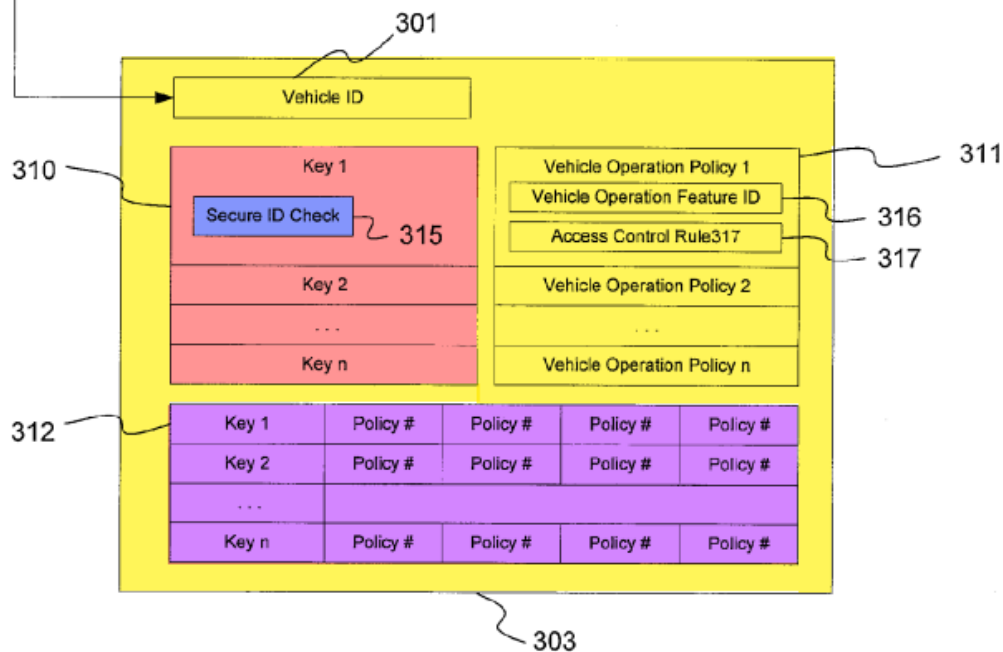


FIG. 3B

246. As illustrated in Figure 3, each key in the key set (shown in red) has an associated secure ID check (shown in blue). The secure ID check may include a digital signature associated with the key, which is coded data that is used to authenticate a key when used by a user. *See id.* at ¶¶ [0059] (“Key set 310 may include a secure ID check 315 associated with a key 205A-C within the set. ... In one embodiment, secure ID check 315 may be a digital signature associated with a key 205A-C.”), [0065] (“In one embodiment, secure identifier 407 may authenticate wireless device 400 as a key 205A-B as discussed above in connection with FIG. 2. ... In one embodiment, secure identifier 407 may be a digital signature associated with wireless device 400.”) [0071] (“Control unit 202 may authenticate key 205A-C via secure ID check 315. ... The authentication may include verifying a digital signature and timestamp, for example.”).

247. In my opinion, Mikan also discloses that coded data is associated with privileges assigned by an administrator of the vehicle that enables assigning or use of eKeys to use the vehicle. As illustrated in Figure 3 above, each key is mapped to vehicle operation policies (mappings shown in purple). The vehicle operation policies define the access control rules that function as the claimed privileges, controlling how the holder of the electronic key may use the vehicle. *Id.* at ¶¶ [0060]-[0061]. Mikan discloses that the database, which includes the vehicle operation

policies and their associated access control rules, may be set and updated by an owner or administrator. *Id.* at ¶ [0056] (“[C]omputer 210 and key 205B may provide a user interface with wireless vehicle security system 200 to enable a user to manage and monitor system 200. For example, where key 205B is part of a mobile telephone, the user of the mobile telephone may use the mobile telephone to send updates to master database 208 via master application 209.”), [0080] (“The update request may have originated at a computing device, such as a wireless telephone, a computer 210, ... [or] key 205B The update request may include ... a[n] access control rule.”).

248. In my opinion, it would have been obvious to a POSITA in view of Xiao to assign vehicle operation policies and access control rules to a user account associated with an electronic key, rather than to the electronic key itself. Xiao discloses that “the owner or operator [of a vehicle] must have an account with the system 100 to take advantage of the disclosed wireless automobile key security service.” Xiao 3:23-25. The account includes information such as the user’s “automobile permissions information 616.” *Id.* at 12:8-13.

249. As I explain above in the section titled “Motivation to Combine Mikan and Xiao and Reasonable Expectation of Success,” a POSITA would have been motivated to add user accounts as taught by Xiao to Mikan’s electronic key system, and to assign vehicle operation policies to the user accounts, in order to more

efficiently organize and track information about users, vehicles, and electronic keys within Mikan's system.

3. Independent Claim 11

250. As illustrated in the table below, every element of Limitations 11[pre]-11[c] and 11[e] of Claim 11 is also included in the corresponding Limitations 1[pre]-1[c] and 1[e] of Claim 1. Thus, based on my discussion in Ground 3 of Claim 1, limitations 11[pre]-11[c] and 11[e] are disclosed by Mikan.

1[pre]	A sub-system of a vehicle, the vehicle having an on-board computer interfaced with the sub-system for processing instructions to enable use of an electronic key (eKey), the sub-system comprising:	11[pre]	A system of a vehicle, the vehicle having an on-board computer for processing and communicating with the system for use of an electronic key (eKey), the system comprising:
1[a]	memory associated with the on-board computer of the vehicle having program instructions for instructing unlocking and starting of the vehicle; and	11[a]	memory associated with the on-board computer of the vehicle having program instructions for controlling unlocking and starting of the vehicle; and
1[b]	communications circuitry of the vehicle interfaced with the on-board computer of the vehicle and the sub-system, the communications circuitry is configured to process program instructions to	11[b]	communications circuitry of the vehicle interfaced with the on-board computer of the vehicle,

	enable communication with a server,		
1[c]	the communications circuitry includes wireless communication circuitry for enabling local connection with a mobile device, the mobile device is configured to use the eKey for said unlocking and said starting of the vehicle;	11[c]	the communications circuitry includes wireless communication circuitry for enabling local connection with a mobile device, the mobile device is configured to use the eKey for said unlocking and said starting of the vehicle;
1[d]	wherein the wireless communications circuitry of the vehicle is configured to receive coded data from the mobile device when using the eKey, the coded data enables functions of said eKey for said unlocking and use of the vehicle, the coded data is associated to the eKey for use by the mobile device,	11[d]	wherein the wireless communications circuitry of the vehicle is configured to receive coded data from the mobile device, the coded data is unique for said eKey,
1[e]	and the coded data includes privilege settings associated with the eKey for limiting types of use of the vehicle when using the eKey with the vehicle;	11[e]	and the coded data includes privilege settings set for limiting types of use of the vehicle when using the vehicle via the eKey;
1[f]	wherein use of the vehicle using the eKey is tracked to identify and log actions taken using the vehicle while the eKey is used.	11[f]	wherein the eKey is associated with a user account, the user account is accessible via a user interface of an application executed by the mobile device, the eKey when active enables said

			unlocking of the vehicle and said starting of the vehicle.
--	--	--	--

251. I address Limitations 11[d] and 11[f] are below.

11[d]: “wherein the wireless communications circuitry of the vehicle is configured to receive coded data from the mobile device, the coded data is unique for said eKey, “

252. As I explained for Limitation 1[d] in Ground 3, Mikan discloses that the wireless communications circuitry of the vehicle is configured to receive coded data from the mobile device, such as a digital signature. See Mikan at ¶¶ [0059] (“Key set 310 may include a secure ID check 315 associated with a key 205A-C within the set. ... In one embodiment, secure ID check 315 may be a digital signature associated with a key 205A-C.”), [0065] (“In one embodiment, secure identifier 407 may authenticate wireless device 400 as a key 205A-B as discussed above in connection with FIG. 2. ... In one embodiment, secure identifier 407 may be a digital signature associated with wireless device 400.”) [0071] (“Control unit 202 may authenticate key 205A-C via secure ID check 315. ... The authentication may include verifying a digital signature and timestamp, for example.”).

253. In addition, as I discuss above for Claim 4, Mikan discloses that the coded data is unique for each electronic key. For example, as illustrated in Figure 3, each electronic key has its own associated secure ID check, which may include a

digital signature associated with the key. *See id.* at ¶¶ [0059], [0065], [0071], Fig. 3.

Much like a real signature serves to uniquely identify a person, a digital signature is intended to uniquely identify a digital object (in this case, a key within Mikan's system). Thus, a POSITA would have understood that the digital signature is unique for each electronic key.

11[f]: “wherein the eKey is associated with a user account, the user account is accessible via a user interface of an application executed by the mobile device, the eKey when active enables said unlocking of the vehicle and said starting of the vehicle.”

254. In my opinion, it would have been obvious to a POSITA in view of Xiao to associate an electronic key in Mikan's system with a user account, and to provide access to the user account via an application on the mobile device. For example, Xiao discloses that “the owner or operator [of a vehicle] must have an account with the system 100 to take advantage of the disclosed wireless automobile key security service.” Xiao at 3:23-25. The user's account includes the user's “mobile ID 610, operator authentication information 612, operator profile information 614, automobile permissions information 616, and a default automobile ID 617.” *Id.* at 12:8-13.

255. Xiao also discloses that a user account is accessible from a “wireless automobile key service page” that may be part of an “automobile key service

application” and “displayed to an automobile operator using mobile device 110.” *Id.* at 16:48-54. Mikan also separately discloses “security application” on a mobile device that is configured to operate as an electronic key. Mikan at ¶ [0067]. The security application “may provide a user with customizable features that may be presented by user interface module 402.” When combined with Xiao, the customizable features presented by Mikan’s security application would be stored as part of a user account.

256. As I explain above in the section titled “Motivation to Combine Mikan and Xiao and Reasonable Expectation of Success,” a POSITA would have been motivated to add user accounts as taught by Xiao to Mikan’s electronic key system, and to assign electronic keys to the user accounts, in order to more efficiently organize and track information about users, vehicles, and electronic keys within Mikan’s system.

257. Mikan also discloses that an electronic key, when authenticated, may be used to unlock and start the vehicle. See Mikan at ¶¶ [0060] (“Local database 303 may include vehicle operation policy 311. Vehicle operation policy 311 may include vehicle operation feature ID 316 and a related access control rule 317. ... Vehicle 201 may support various vehicle operation features such as unlocking a door, ... [or] engaging an ignition.”), [0070] (“At 504, a user attempt to access or operate vehicle

201 with a key 205A-C is detected, which may initiate the authentication ... of key 205A-C.”), [0072] (“At 506 vehicle operation policy 311 may be retrieved by, for example, querying local database 203. In one embodiment, the query may be based on authenticated key 205A-C.”).

- 4. Claim 12: “The system of a vehicle as recited in claim 11, wherein a server is configured for communication with the application executed by the mobile device, the server is one of a plurality of servers, and one of said servers is associated with a manufacturer of the vehicle.”**

258. In my opinion, Mikan discloses a server configured for communication with an application executed by the mobile device. For example, Mikan’s wireless device includes a “security application” and “user interface module” that process update requests and access requests, and a “wireless communications module” that communicates the requests via a wireless network. Mikan at ¶¶ [0063] (“User interface module 402 may be enabled receive user requests from the user, such as an update request and an access request, for example. The update request may include access control rule 317 from the user.”), [0064] (“Wireless communications module 403 may communicate the update request via wireless network 207.”), [0067] (“In one embodiment, security application 409 may provide a user with customizable features that may be presented by user interface module 402.”). Update and access requests are sent to the master application, which may be hosted on a server platform.

Id., [0055] (“Master application 209 ... may be software resident on a server platform.”), [0080]-[0082] (“[M]a[s]ter application 209 may receive an update request ... [that] originated at a computing device such as a wireless telephone.”). As software on a server **platform**, a POSITA would understand that the master application may comprise multiple servers.

259. As I discussed above for Claim 12 in Ground 1, I am informed by counsel that the “manufacturer” limitation of Claim 12 is not entitled to any patentable weight under the printed matter doctrine.

260. Even if the “manufacturer” limitation is found to have patentable weight, it would have been obvious to a POSITA that servers within the server platform may be associated with a manufacturer of the vehicle because vehicle manufacturers frequently provide keys and other vehicle-related services to customers. A POSITA would also have been well aware of existing electronic key systems operated or otherwise associated with vehicle manufacturers as of the priority date of the ’659 patent. For example, Xiao describes an “automobile service server” and “automobile web service server” that “may be associated with an automobile company.” Xiao at 3:12-20, 3:46-54, 4:46-56.

5. **Claim 13**

13[a]: “The system of a vehicle as recited in claim 11, wherein the eKey is securely generated on the mobile device, and”

261. In my opinion, Mikan discloses that the electronic key is securely generating on the mobile device. For example, Mikan teaches that the wireless device includes a “security application” with “software relating to the management of secure identifiers.” Mikan at ¶ [0067]. The security application software “may perform cryptographic functions related to the secure identifier, an authentication process, or cryptographic key generation.” *Id.* Cryptographic key generation would enable the wireless device to generate a secure identifier, such as the digital signature that may be used to authenticate an electronic key. *Id.* at ¶ [0065]. A POSITA would have thus understood that by using the cryptographic key generation functionality in Mikan’s security application, a wireless device could be used to generate an electronic key on the mobile device.

13[b]: “wherein a server associated with a manufacturer of the vehicle is configured to communicate with the application, the application further being associated with a manufacturer of the vehicle.”

262. As I explain above for Claim 12, Mikan discloses a master application on a server configured to communicate with a security application on a wireless device. Mikan at ¶¶ [0055], [0063], [0064], [0067], [0080]-[0082]. To the extent the

server being associated with a manufacturer of the vehicle is determined to have patentable weight, Mikan at least renders that limitation obvious in view of Xiao, which discloses a server associated with an automobile company. Xiao at 3:12-20, 3:46-54, 4:46-56.

263. Claim 13 additionally requires that the application is “associated with a manufacturer of the vehicle.” I am informed by counsel that this limitation also should not receive any patentable weight, for the same reason as the “manufacturer” limitation in claim 12—that is, because the entity associated with the application has no functional relationship to the functionality or implementation of the application.

264. Even if the “manufacturer” limitation is found to have patentable weight, a POSITA would have understood that Mikan’s security application may be associated with a manufacturer of the vehicle because vehicle manufacturers frequently provide keys and other vehicle-related services to customers. A POSITA would also have been well aware of existing electronic key systems operated or otherwise associated with vehicle manufacturers as of the priority date of the ’659 patent. In particular, a POSITA would understand in view of Xiao’s disclosure of a server associated with an automobile company that a software application may also be associated with an automobile company.

6. Claim 14: “The system of a vehicle as recited in claim 11, wherein said on-board computer includes logic for

**processing encryption operations of said eKey in
coordination with logic of said mobile device.”**

265. In my opinion, Mikan discloses that its control unit includes logic for processing encryption operations of an electronic key in coordination with logic of a mobile device. As described above, Mikan teaches that an electronic key is authenticated using a secure ID check. Mikan at ¶¶ [0059], [0071]. As illustrated in Figure 3, the secure ID check is stored at the master database on the server platform and in the local database of the vehicle, and a secure identifier associated with the electronic key is also stored in the memory of the wireless device. *Id.* at ¶¶ [0059], [0065], Fig. 3. Mikan also discloses that the secure identifier and secure ID check may include a “digital signature,” which may be “the product of a public key encryption system.” *Id.* at ¶ [0065]. A security application on the mobile device also includes software with logic that “perform[s] cryptographic functions related to the secure identifier, [or] authentication process.” *Id.* at ¶ [0067].

266. The control unit on the vehicle uses the secure identifier and the secure ID check to authenticate the electronic key, and may do so by “verifying a digital signature and timestamp.” *Id.* at ¶ [0071]. These disclosures make clear to a POSITA that both the control unit and the wireless device in Mikan’s system must be able to perform encryption operations in order to generate and process the secure ID check and secure identifier, including the digital signature. In addition, the wireless device

and control unit would have to coordinate to use the same encryption scheme, otherwise the authentication process would not be able to succeed, as the control unit would not be able to process the digital signature sent by the wireless device.

7. Claim 15: “The system of a vehicle as recited in claim 14, wherein said encryption operations use secure public/private key pair encryption operations.”

267. In my opinion, Mikan discloses encryption operations using secure public/private key pair encryption operations. As I discuss above for Claim 14, Mikan discloses authenticating an electronic key based on a digital signature. Mikan at ¶¶ [0059], [0065], [0071]. Mikan expressly states that the digital signature may be “the product of a public key encryption system.” *Id.* at ¶¶ [0059], [0065]. A POSITA would have understood that Mikan’s public key encryption refers to an old and well-known encryption scheme commonly referred to as “public key encryption,” “public key cryptography,” or “asymmetric cryptography,” which is the same as the claimed “public/private key pair encryption.”

8. Claim 16: “The system of a vehicle as recited in claim 11, wherein said wireless communication circuitry facilitates one or more of Bluetooth, near field communication (NFC), WiFi, or radio communication.”

268. In my opinion, Mikan discloses wireless communication circuitry that facilitates Bluetooth, WiFi, and radio communication. I discuss this in detail in Ground 3 for Claim 5.

9. Claim 17: “The system of a vehicle as recited in claim 11, wherein said eKey is validated and securely bound to the mobile device to prevent unauthorized transfers of the ekey.”

269. In my opinion, Mikan discloses that an electronic key is validated and securely bound to a wireless device to prevent unauthorized transfers of the electronic key. For example, Mikan’s “security application” validates and securely binds an electronic key to a wireless device. Specifically, Mikan’s security application “manage[s] secure identifiers” and “perform cryptographic functions related to the secure identifier, an authentication process, or cryptographic key generation.” Mikan at ¶ [0067]. Mikan discloses that the secure identifier “may be a digital signature,” such as “the product of a public key encryption system,” and “may authenticate wireless device 400 as a key.” *Id.* at ¶ [0065]. These disclosures expressly describe validating an electronic key on a wireless device. Mikan also discloses that the digital signature used for authentication may be “a digital signature associated with the wireless device.” *Id.* A POSITA would have understood that if a digital signature associated with the wireless device is used to validate the electronic key, the key would then be bound to that wireless device—as a digital signature is unique to a given mobile device, and no other wireless device would be capable of generating the same digital signature for authentication.

10. Independent Claim 18

270. As illustrated in the table below, every element of every Limitation of Claim 18 is included in the corresponding Limitations of Claim 1. Thus, based on my discussion above of Claim 11, Claim 18 is rendered obvious by Mikan and Xiao.

11[pre]	A system of a vehicle, the vehicle having an on-board computer for processing and communicating with the system for use of an electronic key (eKey), the system comprising:	18[pre]	A vehicle having an on-board computer for processing and communicating an electronic key (eKey), the vehicle comprising:
11[a]	memory associated with the on-board computer of the vehicle having program instructions for controlling unlocking and starting of the vehicle; and	18[a]	memory associated with the on-board computer of the vehicle having program instructions for controlling unlocking and starting of the vehicle; and
11[b]	communications circuitry of the vehicle interfaced with the on-board computer of the vehicle,	18[b]	communications circuitry of the vehicle interfaced with the on-board computer of the vehicle,
11[c]	the communications circuitry includes wireless communication circuitry for enabling local connection with a mobile device, the mobile device is configured to use the eKey for said unlocking and said starting of the vehicle;	18[c]	the communications circuitry includes wireless communication circuitry for enabling local connection with a mobile device, the mobile device is configured to use the eKey for said unlocking and said starting of the vehicle;

11[d]	wherein the wireless communications circuitry of the vehicle is configured to receive coded data from the mobile device, the coded data is unique for said eKey, and	18[d]	wherein the wireless communications circuitry of the vehicle is configured to receive coded data from the mobile device, the coded data is unique for said eKey to be used via the mobile device, and
11[e]	the coded data includes privilege settings set for limiting types of use of the vehicle when using the vehicle via the eKey;	18[e]	the coded data includes privilege settings for use of the vehicle when using the eKey with the vehicle;
11[f]	wherein the eKey is associated with a user account, the user account is accessible via a user interface of an application executed by the mobile device, the eKey when active enables said unlocking of the vehicle and said starting of the vehicle.	18[f]	wherein the eKey is associated with a user account, the user account is accessible via a user interface of an application executed by the mobile device, the eKey when active enables said unlocking of the vehicle and said starting of the vehicle.

11. Claim 20

271. Claim 20 recites the same additional limitations as Claim 13. Accordingly, Claim 20 is rendered obvious by Mikan and Xiao for the same reasons I discuss above for Claim 13.

12. Claim 21: “The vehicle of claim 18, wherein encryption operations are associated with use of said eKey, and said encryption operations use public/private key pair encryption, and wherein said wireless communication

circuitry uses one or more of Bluetooth, or near field communication (NFC), or WiFi, or radio communication.”

272. Claim 21 recites the same additional limitations as each of claims 14 (encryption operations for use of the electronic key), 15 (public/private key pair encryption), and 16 (wireless communication circuitry using Bluetooth, NFC, WiFi, or radio communication). Accordingly, Claim 21 is rendered obvious by Mikan and Xiao for the same reasons I discuss above for Claims 14, 15, and 16.

E. Ground 5: Mikan in view of Sekiyama renders obvious claims 6 and 7 under Section 103

273. As discussed above, Sekiyama is a Toyota patent that, like Mikan and Xiao, describes an electronic key system for a vehicle. In Sekiyama’s system, a vehicle owner can register a duplicate electronic key, and then share the duplicate key with another mobile device. As I discuss below, a POSITA would have found it obvious to combine Mikan with Sekiyama to add support electronic key registration and sharing of electronic keys between mobile devices.

1. Motivation to Combine Mikan and Sekiyama and Reasonable Expectation of Success

274. In my opinion, a POSITA would have been motivated to apply Sekiyama’s teachings relating to registration and sharing of electronic keys to Mikan’s electronic key system because doing so would have enhanced the user experience without compromising the security of the system. By enabling the mobile

device to register an electronic key and share it with a secondary mobile device, the vehicle owner would be able to more easily generate and share an electronic key using a single application (*i.e.*, the security application of the mobile device). Such functionality would be particularly useful when the vehicle owner needs to generate and share an electronic key in circumstances where registering or transmitting the electronic key in advance may not be an option—for example, to provide a duplicate key to a valet, whose identity may not be known until the vehicle owner arrives at a destination. By allowing the mobile device to register and share an electronic key, the key can also be shared even when the mobile device and the vehicle are unable to connect to Mikan's master database (for example, in areas with poor wireless or cellular connectivity). Here, the owner could register the duplicate key in advance, and then share the secondary key with the recipient (such as a valet) at a later time—for example, in an underground parking lot, where communication with the master database at the server may not be possible.

275. In my opinion, a POSITA would also have reasonably expected this combination to succeed. The elements necessary to implement Sekiyama's key registration and sharing techniques are largely already present in Mikan's wireless devices. In particular, Mikan's wireless device is already configured to use wireless communication to send and receive electronic key information (such as a secure ID

check or secure identifier), Mikan's security application on the wireless device is already configured to "perform cryptographic functions related to ... an authentication process, or cryptographic key generation." Mikan at ¶ [0067]. The security application could thus be used to register and generate a new electronic key using a secure ID check generated by the security application on the wireless device, and to verify that a recipient mobile device is authorized and should receive a duplicate electronic key. Using these pre-existing features of Mikan to register an electronic key and share it with other mobile devices would have required basic software engineering skills, which would have been well within the capabilities of a POSITA.

276. In my opinion, Mikan, Sekiyama, and the '659 patent are all directed to the same field of endeavor, the field of electronic key systems. *See* '659 patent at Abstract ("A vehicle configured to communicate with a server of a cloud system to enable access to use the vehicle via one or more electronic keys is provided."); Mikan at Abstract ("Methods and wireless devices for providing secure operation of a vehicle. ... The key may be embedded within a wireless device such as a cellular telephone."); Sekiyama at ¶ [0005] ("[I]t [is] an object of the present invention to provide an electronic key system that allows restrictions on the functions that can be

executed with a duplicate electronic key to be imposed when such a key is generated.”).

2. **Claim 6: “The sub-system of the vehicle of claim 1, wherein an application associated with said mobile device is configured to enable sharing of said eKey with a recipient user having a recipient mobile device, the sharing is enabled via a message initiated from said mobile device.”**

277. Mikan discloses that electronic keys within its system may include a key with an access control rule “that enables all vehicle operation features,” and a second key that may be a “valet key” with “limited functionality.” Mikan at ¶ [0061]. Mikan also teaches that the mobile device may include a “security application” used to “manage secure identifiers” and “perform cryptographic functions related to the secure identifier, an authentication process, or cryptographic key generation.” *Id.* at ¶ [0067]. A vehicle access module may be used in conjunction with the security application to communicate electronic key information (such as a secure identifier) to a vehicle. *Id.*

278. In my opinion, it would have been obvious to a POSITA in view of Sekiyama to use Mikan’s security application to share electronic key information with an authorized mobile device, in addition to a vehicle. For example, Sekiyama discloses that “key information [may] be transmitted from portable telephone A (first terminal) 10, which functions as a master key, to portable telephone B (second

terminal) 30, which functions as a duplicate electronic key.” Sekiyama at ¶ [0011].

In Sekiyama’s system, the sharing of a key is enabled by sending messages between the mobile device associated with the master key on the one hand, and a management center and the recipient mobile device on the other hand. *Id.* at ¶¶ [0032]-[0039]. More specifically, the mobile device of the master key sends a connection request to a management center and send messages indicating the functionality that should be enabled in the duplicate key, and the management center generates the duplicate key in response. *Id.* at ¶¶ [0034]-[0037]. The mobile device of the master key may then “transmit[] the received electronic key to portable telephone B” by “send[ing] the key information for the restricted duplicate electronic key to portable telephone B.” *Id.* at ¶ [0038].

279. As I explain above in the section titled “Motivation to Combine Mikan and Sekiyama and Reasonable Expectation of Success,” a POSITA would have been motivated to configure Mikan’s security application to share electronic key information with other mobile devices, as taught by Sekiyama, because the additional functionality would facilitate transmission of secondary electronic keys, for example, to a valet for parking a vehicle.

3. **Claim 7: “The sub-system of the vehicle of claim 1, wherein the coded data is processed securely by the mobile device responsive to registering the e-Key to the mobile device, the registering being enabled by an owner of said vehicle or an**

administrator of said vehicle.”

280. In my opinion, Mikan discloses that coded data is processed securely by the mobile device. *See, e.g.*, Mikan at ¶ 0057 (discussing the “security application” performing “cryptographic functions” relating to “secure identifier”).

281. In my opinion, it would have been obvious to a POSITA in view of Sekiyama that Mikan’s security application may also be used by a vehicle owner to register a new electronic key. As taught by Mikan, the software in the security application may “perform cryptographic functions” such as “cryptographic key generation,” which would enable registration of an electronic key using a mobile device. *Id.* at ¶ [0067]. Sekiyama further discloses that an owner must register an electronic key at a “management center” before sharing the key with other mobile devices. Sekiyama at ¶ [0034]. The registration process includes “set[ting] restriction items for the restricted duplicate key” and sending a “restricted duplicate electronic key issuance request” to the server. *Id.* at ¶¶ [0034]-[0035]. After the electronic key has been issued, the owner may “transmit[] the electronic key to portable telephone B,” a second mobile device. *Id.* at ¶ [0038]. In the context of Mikan’s system, the mobile device receiving the newly registered electronic key would use its local security application to process and authenticate the electronic key.

282. As I explain above in the section titled “Motivation to Combine Mikan and Sekiyama and Reasonable Expectation of Success,” a POSITA would have been motivated to configure Mikan’s security application to register and distribute electronic keys, as taught by Sekiyama, because the additional functionality would facilitate creation and transmission of secondary electronic keys, for example, to a valet for parking a vehicle.

F. Ground 6: Mikan in view of Xiao and Sekiyama renders obvious claim 19 under Section 103

283. Mikan and Xiao render obvious every limitation of Claim 18, from which Claim 19 depends. Mikan also teaches that electronic keys may either enable all vehicle operation features (for an owner), or may have limited functionality (for someone else, such as a valet). Sekiyama teaches that the vehicle owner may cause a duplicate, limited functionality key to be sent to a shared user for shared use of the vehicle.

284. I explained in Ground 4 why a POSITA would have been motivated to combine Mikan and Xiao, and would have reasonably expected the combination to succeed, with respect to claim 18. I also explained in Ground 5 why a POSITA would have specifically been motivated to combine Mikan with Sekiyama’s key sharing functionality, and why a POSITA would have reasonably expected that combination to succeed. The same reasoning applies here for combining Mikan with Xiao’s

teaching of user profiles, on the one hand, and with Mikan's teaching of key sharing, on the other hand.

1. **Claim 19: "The vehicle of claim 18, wherein the privilege settings being unrestricted for an owner of the vehicle and restricted for a shared user of the vehicle, the shared user of the vehicle receives a shared eKey responsive to said owner of the vehicle causing the shared eKey to be sent for shared use of the vehicle."**

285. Mikan discloses that electronic keys within its system may include a key with an access control rule "that enables all vehicle operation features," and is thus unrestricted, and a second key that may be a "valet key" with "limited functionality." Mikan at ¶ [0061]. A POSITA would have understood that the key that enables all vehicle operation features would belong to the vehicle owner, who would be expected to have unrestricted access to his own vehicle.

286. Mikan also teaches that the mobile device may include a "security application" used to "manage secure identifiers" and "perform cryptographic functions related to the secure identifier, an authentication process, or cryptographic key generation." *Id.* at ¶ [0067]. A vehicle access module may be used in conjunction with the security application to communicate electronic key information (such as a secure identifier) to a vehicle. *Id.*

287. In my opinion, it would have been obvious to a POSITA in view of Sekiyama to use Mikan's security application to share electronic key information

with an authorized mobile device, in addition to a vehicle. For example, Sekiyama discloses that “key information [may] be transmitted from portable telephone A (first terminal) 10, which functions as a master key, to portable telephone B (second terminal) 30, which functions as a duplicate electronic key.” Sekiyama at ¶ [0011]. To create and share the duplicate key, the mobile device of the master key sends a connection request to a management center and identifies the functionality that should be enabled in the duplicate key, and the management center generates the duplicate key in response. *Id.* at ¶¶ [0034]-[0037]. The mobile device of the master key may then “transmit[] the received electronic key to portable telephone B” by “send[ing] the key information for the restricted duplicate electronic key to portable telephone B.” *Id.* at ¶ [0038].

288. As I explain above in Ground 5 in the section titled “Motivation to Combine Mikan and Sekiyama and Reasonable Expectation of Success,” a POSITA would have been motivated to configure Mikan’s security application to share electronic key information with other mobile devices, as taught by Sekiyama, because the additional functionality would facilitate transmission of secondary electronic keys, for example, to a valet for parking a vehicle.

IX. Secondary Considerations of Non-obviousness

289. I am not aware of any secondary considerations, or so-called

“objective indicia of non-obviousness” for the challenged claims.

290. 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.

291. 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 '659 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 '659 patent of which I am aware.

292. 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.

293. 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

294. For the reasons set forth above, I believe claims 1-21 of the '659 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.

295. 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: July 15, 2024

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