

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.

---

Post Grant Review No. 2026-00008  
U.S. Patent No. 12,337,715

---

**DECLARATION OF KEVIN C. ALMEROOTH, PH.D.  
IN SUPPORT OF PETITION FOR POST GRANT REVIEW OF  
U.S. PATENT NO. 12,337,715**

## TABLE OF CONTENTS

|      |  |    |
|------|--|----|
| I.   | Introduction.....  | 1  |
| II.  | Qualifications and Background .....  | 2  |
| III. | Materials Considered.....  | 15 |
| IV.  | Legal Standards .....  | 17 |
|      | A. Claim Construction .....  | 17 |
|      | B. Anticipation Under 35 U.S.C. § 102.....   | 18 |
|      | C. Obviousness Under 35 U.S.C. § 103.....  | 18 |
|      | D. Priority Under 35 U.S.C. § 120 and Written Description and Enablement Under § 112.....                      | 22 |
| V.   | The '715 patent.....   | 24 |
|      | A. Overview of the '715 patent.....  | 24 |
|      | B. Prosecution History of the '715 patent.....   | 29 |
|      | C. The '715 patent's claims are entitled to an effective filing date of no earlier than October 25, 2013 ..... | 32 |
|      | D. Person of Ordinary Skill in the Art .....   | 40 |
| VI.  | Claim Construction of Terms of the '715 patent.....  | 42 |
| VII. | Summary of Opinions on Unpatentability.....  | 43 |
|      | A. Ground 1: Sekiyama, Kleve, Hatton, and Xiao .....   | 43 |
|      | 1. Sekiyama (Japanese Laid Open Patent App. Pub. No. 2010-126949).....   | 43 |
|      | 2. Kleve (U.S. Patent Pub. No. 2014/0129053).....  | 44 |
|      | 3. Hatton (U.S. Patent No. 9,002,536).....   | 46 |
|      | 4. Xiao (U.S. Patent No. 8,737,913).....   | 47 |

|     |   |    |
|-----|---|----|
| 5.  | Motivation to Combine .....   | 48 |
| 6.  | Claim 1 .....   | 61 |
| 7.  | Claim 2 – The method of claim 1, wherein the request to share the e-key includes a setting to assign a privilege level for use of the vehicle when used via the e-key, the privilege level provides one or more conditions of use of the vehicle. ....  | 75 |
| 8.  | Claim 3 – The method of claim 2, wherein the one or more conditions of use defined via the privilege level is one of a geographic restriction for where the vehicle is allowed to be used, or a speed restriction, or an occupancy restriction, or a time fram of use, or an expiration-time of use, or unlocking of the vehicle, or driving of the vehicle, or combinations of two or more thereof. ....   | 76 |
| 9.  | Claim 4 – The method of claim 1, wherein the request is enabled via an application executed via the sharing device, the application provided by said manufacturer of the vehicle to enable initiation of sharing of the e-key, the application is associated wth an owner account for the vehicle. ....   | 76 |
| 10. | Claim 5 – The method of claim 1, wherein responsive to said request, the e-key is generated, the generation of the e-key includes one or more processes executed by the server associated with the manufacturer of the vehicle, one or more processes executedby one or more additional server, one or more processes executed by the recipient device, one or more processes executed by a computer, or a combination of two or more thereof. .... | 79 |
| 11. | Claim 6 – The method of claim 1, further comprising, encrypting the e-key, the e-key being encrypted using public/private key pairs that are generated and used for security in communication. ....   | 79 |
| 12. | Claim 7 – The method of claim 1, further comprising, receiving a deactivation request, the deactivation request   |    |

|     |   |    |
|-----|---|----|
|     | is used to disable the e-key for use by the recipient device on the vehicle. ....   | 80 |
| 13. | Claim 8 – The method of claim 1, wherein the message to share and enable the e-key for the recipient device is communicated over a network, the communication enables processing by one or more servers or devices, and said one or more servers or devices include a server associated with the sharing device or the recipient device, and the server associated with the manufacturer of the vehicle. .... | 82 |
| 14. | Claim 9 – The method of claim 1, wherein the recipient device is identified by one or more of an email address, a phone number, a text message, a message address, a notification, a link, a web address, a social network address, or combination of two or mre thereof. ....  | 84 |
| 15. | Claim 10 – The method of claim 1, wherein an application provided by a manufacturer of the vehicle includes a graphical user interface for registering the registered owner e-key for the vehicle and sharing of the e-key with one or more recipient devices. ....   | 84 |
| 16. | Claim 11 – The method of claim 1, wherein the e-key enabled for use on the vehicle using the recipient device enables unlocking and starting the vehicle when the recipient device uses the e-key with the vehicle, and the e-key is associated with at least ne privilege associated with a type of operation use of the vehicle. ....   | 86 |
| 17. | Claim 12 .....  | 87 |
| 18. | Claim 13 – The system of claim 12, wherein the request to share the e-key includes enabling a setting to apply a privilege level for use of the vehicle via the e-key, the privilege level provides one or more conditions of use of the vehicle via the e-key .....  | 88 |

|     |  |    |
|-----|--|----|
| 19. | Claim 14 – The system of claim 12, wherein the e-key is encrypted, and wherein encryption uses a public/private process for security. ....   | 88 |
| 20. | Claim 15 – The system of claim 12, wherein the application includes a selectable option for disabling the e-key from use by the recipient device on the vehicle.....   | 89 |
| 21. | Claim 16 – The system of claim 12, wherein the e-key enabled for use on the vehicle using the recipient device enables unlocking and starting the vehicle when the recipient device uses the e-key with the vehicle, and the e-key is associated with at least one privilege associated with a type of operational use of the vehicle. ....  | 89 |
| 22. | Claim 17 .....   | 89 |
| 23. | Claim 18 – The method of claim 17, wherein the e-key is associated with at least one privilege associated with use of the vehicle, the at least one privilege is defined based on a setting associated with the sharing request, and wherein the recipient device is one of a smartphone, or a smartwatch, or smart glasses, or a computer, or a digital assistant, or a key fob, and wherein the e-key is unique for said sharing request and said use by said recipient device. .... | 91 |
| 24. | Claim 19 – The method of claim 17, wherein the e-key is caused to be generated by either one of said owner device, the server, the recipient device, a computer, the vehicle, or a combination of two or more thereof. ....  | 92 |
| 25. | Claim 20 – The method of claim 17, wherein the e-key is securely generated for the recipient device, and wherein the owner device has an owner e-key that was initially generated for the owner device to enable said sharing request, and the e-key is encrypted, and wherein encryption uses a public/private process for security. ....   | 92 |
| 26. | Claim 21 – The method of claim 17, wherein the e-key, once enabled, provides access to information via the recipient device regarding a level of charge of a battery of  |    |

|   |     |
|---|-----|
| the vehicle for when the vehicle is an electric vehicle (EV).<br>.....  | 93  |
| 27. Claim 22 – The method of claim 17, wherein the e-key enabled for use on the vehicle using the recipient device enables unlocking and starting the vehicle when the recipient device uses the e-key with the vehicle, and the e-key is associated with at least one privilege associated with a type of operational use of the vehicle. .... | 95  |
| 28. Claim 23 .....  | 95  |
| 29. Claim 24 – The system of claim 23, wherein the e-key enabled for use on the vehicle using the recipient device enables unlocking and starting the vehicle when the recipient device uses the e-key with the vehicle, and the e-key is associated with at least one privilege associated with a type of operational use of the vehicle. .... | 97  |
| B. Ground 2: Claims 1–11, 17–24 lack written description and enablement support.....  | 97  |
| 1. What the ’715 specification discloses (request to cloud/server; server-to-recipient delivery; optional notification).....  | 98  |
| 2. No support for “message-caused” initiation of the sharing request (claims 1 and 23 (and their dependents)) .....   | 99  |
| 3. No support for “confirmation” events (independent claim 17 and dependents).....  | 100 |
| VIII. Secondary Considerations of Non-Obviousness .....   | 101 |
| IX. Conclusion .....  | 102 |

## **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. 12,337,715 (the “’715 patent”), and I have been asked to provide my opinions as to the patentability of the claims of the ’715 patent. I understand that the application for the ’715 patent was filed on October 11, 2023, claiming priority to 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 ’715 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 ’715 patent. As discussed herein, it is my opinion that claims 1-24 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 '715 patent based on certain prior art references, as well as whether certain claims have written description support in the specification. 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 1-24 of the '715 patent are unpatentable for the reasons provided below.

## **II. Qualifications and Background**

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

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

7. I hold three degrees from the Georgia Institute of Technology: (1) a Bachelor of Science degree in Information and Computer Science (with minors in

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

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

delivery in wireless networks.

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

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

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

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

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

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

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

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

in stabilizing the response time of a system. This capability is particularly useful in systems where content is downloaded or streamed on-demand to users.

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

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

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

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

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

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

For wireless protocols, this research includes functions like network acquisition and channel bonding.

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

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

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

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

things related to multicast in the IETF. Finally, I was the Chair of the Internet2 Multicast Working Group for seven years.

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

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

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

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

Communication (NGC) workshop, and the Global Internet Symposium, and I have served on the program committees for numerous conferences.

25. Furthermore, in the courses I taught at UCSB, a significant portion of my curriculum covered aspects of the Internet and network communication, including the physical and data link layers of the Open System Interconnect (OSI) protocol stack, and standardized protocols for communicating across a variety of physical media such as cable systems, telephone lines, wireless, and high-speed Local Area Networks (LANs). The courses I have taught also cover most major topics in Internet communication, including data communication, multimedia encoding, and mobile application design. My research and courses have covered a range of physical infrastructures for delivering content over networks, including cable, Integrated Services Digital Network (ISDN), Ethernet, Asynchronous Transfer Mode (ATM), fiber, and Digital Subscriber Line (DSL). For a complete list of courses I have taught, see my curriculum vitae (CV) (Ex. 1019).

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

services including IPv6, multicast, Quality of Service (QoS), satellite-based communication, and security. Applications for this emulation program included communication of a variety of multimedia-based services, including video conferencing and video-on-demand.

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

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

challenges of deploying, monitoring, managing, and scaling communication infrastructure to support evolving Internet services like streaming media, conferencing, content exchange, social networking, and e-commerce.

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

### III. Materials Considered

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

| Ex.  | Description  |
|------|--|
| 1001 | U.S. Patent No. 12,337,715 (“the ’715 patent”)             |
| 1002 | Prosecution History for U.S. Patent No. 12,337,715         |
| 1003 | Declaration of Dr. Kevin Almeroth                          |
| 1004 | U.S. Pat. Pub. No. 2014/0129053 to Kleve et al.            |
| 1005 | Certified Translation of JP2010-126949A to Sekiyama et al. |
| 1006 | JP 2010-126949   |
| 1007 | Declaration of Herman Kahn                                 |
| 1008 | U.S. Patent No. 9,002,536 to Hatton                        |
| 1009 | U.S. Pat. Pub. No. 2011/0312273 to Harris                  |
| 1010 | U.S. Pat. No. 8,737,913 to Xiao et al.                     |
| 1011 | U.S. Pat. No. 8,977,408 to Cazanias et al.                 |
| 1012 | U.S. Pat. App. No. 61/478,436                              |
| 1013 | U.S. Pat. App. No. 61/745,729                              |

|      |   |
|------|---|
| 1014 | U.S. Pat. App. No. 13/452,882   |
| 1015 | U.S. Pat. App. No. 13/842,158   |
| 1016 | U.S. Pat. App. No. 14/063,638   |
| 1017 | Order Granting Request For Ex Parte Reexamination,<br>Reexamination Control No. 90/019,456, Patent No.<br>11,738,659 (April 15, 2024) |
| 1018 | Text Comparison of U.S. Pat. App. No. 13/842,158 to U.S. Pat.<br>App. No. 14/063,638  |
| 1019 | <i>Curriculum Vitae</i> of Dr. Kevin Almeroth   |
| 1020 | U.S. Patent No. 7,868,736 to Fukushima et al.   |
| 1021 | U.S. Pat. App. No. 14/303,442   |
| 1022 | U.S. Pat. App. No. 15/180,306   |
| 1023 | U.S. Pat. App. No. 15/344,566   |
| 1024 | U.S. Pat. App. No. 15/607,418   |
| 1025 | U.S. Pat. App. No. 15/854,241   |
| 1026 | U.S. Pat. App. No. 16/653,958   |
| 1027 | U.S. Pat. App. No. 17/461,959   |
| 1028 | U.S. Pat. App. No. 18/125,448   |
| 1029 | BLUETOOTH Core Specification v4.0   |
| 1030 | Ex Parte Reexamination Control Number 90/019,456, Final<br>Rejection  |

#### **IV. Legal Standards**

31. In forming my opinions and considering the subject matter of the '715 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 a post grant review proceeding under the same claim construction standard that is used in a United States federal court. I understand that under this standard, the meaning of claim terms is considered from the viewpoint of one of ordinary skill in the art at the time of the alleged invention.

35. I understand that claim terms are generally given their ordinary and

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

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

**B. Anticipation Under 35 U.S.C. § 102**

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

**C. Obviousness Under 35 U.S.C. § 103**

38. I understand that a patent claim is invalid as obvious if the claimed invention would have been obvious to a person of ordinary skill in the art (“POSITA”) at the time the claimed invention was made. This means that even if all

of the elements of the claim cannot be found in a single prior art reference that would anticipate the claim, a person of ordinary skill in the field who knew about all the prior art would have come up with the claimed invention. I understand that in an obviousness determination, the person of ordinary skill in the art is presumed to have knowledge of all material prior art. I understand that whether a claim is obvious is based upon the determination of several factual issues.

39. I understand that obviousness is a determination of law based on underlying determinations of fact. I understand that these factual determinations include the scope and content of the prior art, the level of ordinary skill in the art, the differences between the claimed invention and the prior art, and secondary considerations of non-obviousness.

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

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

42. I understand that a patent claim composed of several elements is not

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

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

44. I understand that there is no rigid rule that a reference or combination of references must contain a “teaching, suggestion, or motivation” to combine

references. But I also understand that the “teaching, suggestion, or motivation” test can be a useful guide in establishing a rationale for combining elements of the prior art. I have been told that this test poses the question as to whether there is an express or implied teaching, suggestion, or motivation to combine prior art elements in a way that realizes the claimed invention, and that it seeks to counter impermissible hindsight analysis.

45. I understand that one may consider, e.g., whether (1) the change was merely the predictable result of using prior art elements according to their known functions, or whether it was the result of true inventiveness; (2) there is some teaching or suggestion in the prior art to make the modification or combination of elements claimed in the patent; (3) the claimed innovation applies a known technique that had been used to improve a similar device or method in a similar way; (4) the claimed invention would have been obvious to try, meaning that the claimed innovation was one of a relatively small number of possible approaches to the problem with a reasonable expectation of success by those skilled in the art; (5) the invention merely substituted one known element for another known element in order to obtain predictable results; (6) the invention merely applies a known technique to a known device, method, or product to yield predictable results; or (7) known work in the field may have prompted variations of use of the same inventions in the same or different fields due to market forces or design incentives that would have been

predictable to a person of ordinary skill in the art.

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

**D. Priority Under 35 U.S.C. § 120 and Written Description and Enablement Under § 112**

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.

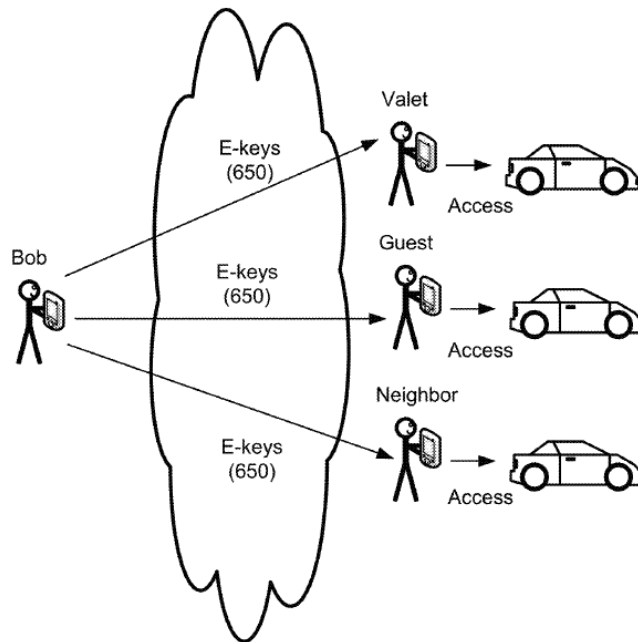
## **V. The '715 patent**

### **A. Overview of the '715 patent**

54. The application that led to the '715 patent was filed on October 11, 2023. It is my opinion that the earliest date to which the challenged claims of the '715 patent can claim priority, as explained in further detail in section V.C, is

October 25, 2013. The '715 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 '715 patent could claim priority back to any of these dates (which it cannot), my ultimate conclusions as to the invalidity of the '715 patent would not change. To be clear, if the '715 patent is not entitled to a priority date earlier than October 25, 2013, then I have been informed that Sekiyama, Kleve, Hatton, and Xiao are prior art and render obvious the Challenged Claims. But even if the '715 patent is entitled to the earliest priority date, I have been informed that Sekiyama and Xiao are prior art regardless of the '715 patent priority date.

55. **The '715 patent** is directed to a system in which a vehicle owner assigns an electronic key to a user for enabling access and use of a shared vehicle by the user. Ex. 1001 at Abstract. For example, in Figure 29, vehicle owner Bob shares electronic keys 650 with users “valet,” “guest,” and “neighbor” for vehicle access. *Id.* at 42:35-37. The specification explains that “[e]ach e-key, in one embodiment, will include a unique access code or substantially unique access code.” *Id.* at 42:50-51. 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 42:58-61.



'715 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 43:51-53), which “will then be encrypted by the server and then sent as encrypted e-keys 722<sup>1</sup> to Bob’s device 704.” *Id.* at 43:53-55.

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

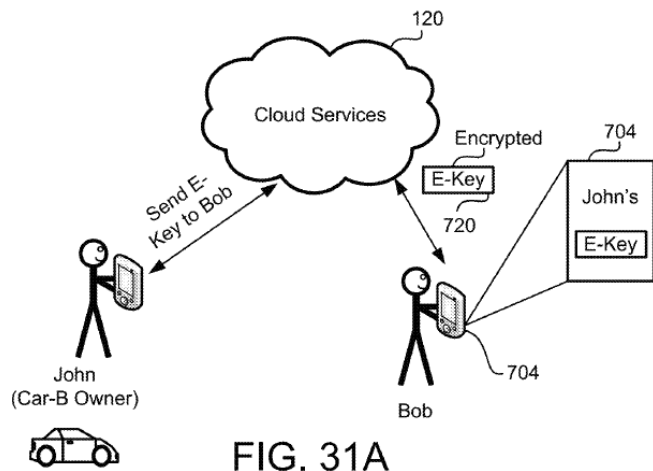


FIG. 31A

'188 patent, Fig. 31A.

57. Next, in Figure 32, user Bob “will transfer the encrypted e-keys 720 to the vehicle that belongs to John (car-B). . . At the vehicle, the vehicle will receive the encrypted e-keys and the device ID of Bob’s device 704. The vehicle will hold a private key to unlock and un-encrypt the encrypted e-keys 720.” *Id.* at 43:61-44:3.

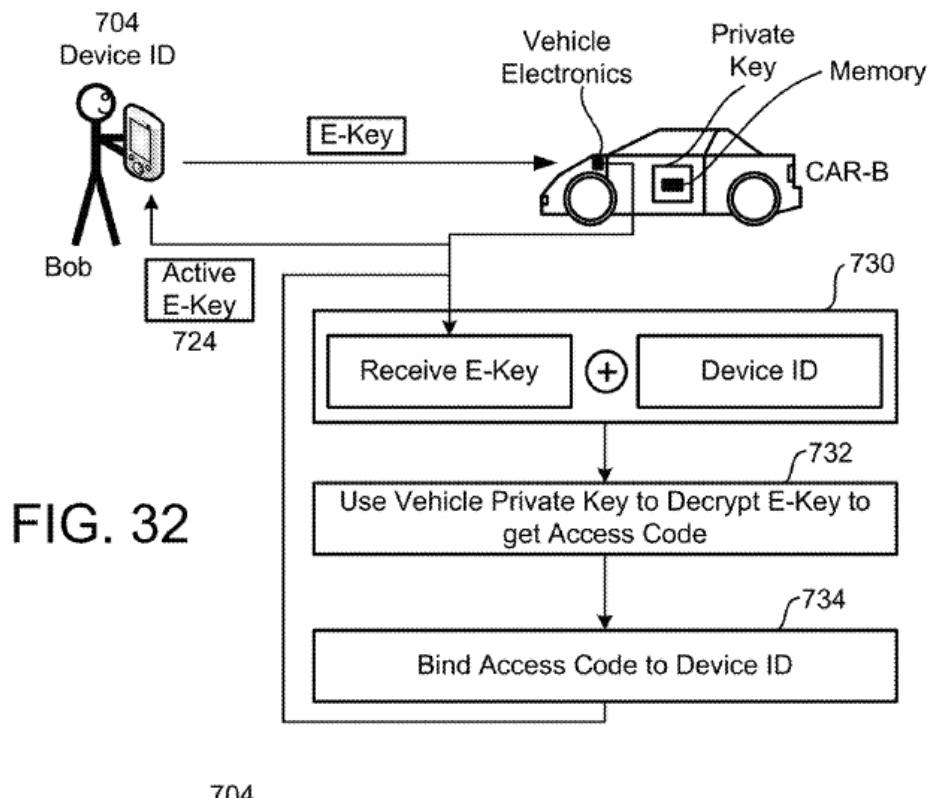


FIG. 32

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 44:8-10. In step 732, “the vehicle private key is used to decrypt the e-keys to get access to an access code.” *Id.* at 44:18-20. 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.*, 44:23-27. The ’715 patent discloses that the unique access code “can be generated by a number generator, and [sic] alphanumeric random generator, in [sic] incremental number generator, or any other generation device that can generate codes that are unique or substantially unique.” *Id.* at 44:64-67.

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 42:37-38. For example, “electronic keys for each user can be associated with a different expiration time.” *Id.* at 42:48-49; *see also id.* at 49:53-55 (“the privileges can be assigned by selecting . . . time durations[.]”). 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 44:25-27.

**B. Prosecution History of the ’715 patent**

60. I have reviewed the prosecution history of the application that led to the ’715 patent. Ex. 1002. I note that the examiner rejected the claims based on double-patenting over related U.S. Patent Nos. 11,738,659 and 11,794,601. EX1002, Non-Final Rejection, at 4. On February 5, 2025, Applicant filed terminal disclaimers to overcome the rejection. *See* EX1002, Amendment, at 8. On March 12, 2025, the examiner issued a Notice of Allowance, including as reason for allowance that the “closest prior art by Suyama ([U.S.] Pat. No.: 7,375,440[]) does not teach or suggest . . . *a server associated with the manufacturer* of the vehicle configured to enable sharing of e-key with a recipient device.” EX1002, Notice of Allowability, at 2 (emphasis added).

61. As discussed below, I have been informed that the phrase “associated with a manufacturer of the vehicle” is nonfunctional descriptive material, and therefore is not entitled to patentable weight under the printed matter doctrine because “it claims the content of information” (*i.e.*, who operates the server) and lacks any “functional relationship” to the server. Who owns/operates or is “associated with” the server does not alter the server’s structure or the method’s operation.

62. Further, as discussed below, in my opinion, a POSITA would have understood that Sekiyama’s (JP 2010-126949 A, not Suyama) server is *associated with a manufacturer of the vehicle*. Sekiyama is a Japanese patent application invented by employees of Toyota Motor Corp. and assigned to Toyota Motor Corp. EX1005. Accordingly, a POSITA would have recognized that the “center server” described in Sekiyama was a server associated with the manufacturer of the vehicle, as the “electronic key system” described in Sekiyama would have been understood to have been developed for use by Toyota and its vehicles.

63. It is also my opinion that it would have been an obvious option to host Sekiyama’s server functions on a server operated by (or on behalf of) the vehicle manufacturer. Multiple contemporaneous references teach manufacturer-associated servers for e-key services. For example, Xiao explains that its wireless automobile key service servers “may be associated with an automobile company.” EX1010,

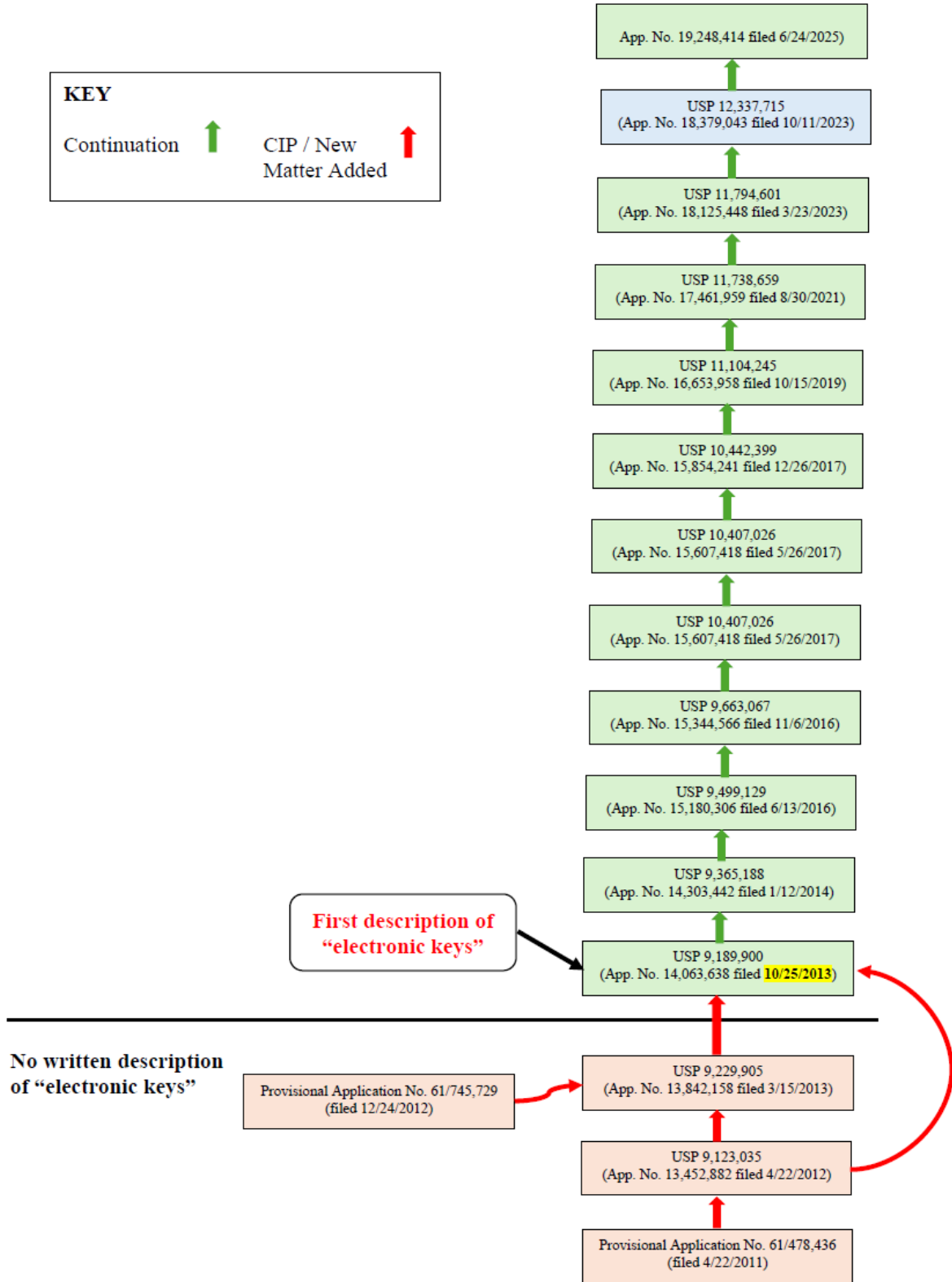
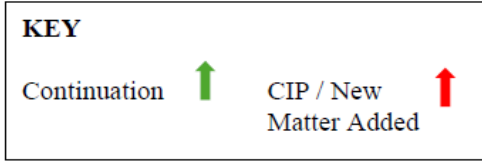
3:12–21; *see also id.*, 3:46–54, 4:46–56, 12:8–13, 16:48–54.<sup>2</sup> Thus, a POSITA would have found it obvious to implement Sekiyama’s saving of e-key information on a manufacturer-associated server as one of a finite, predictable set of options for the owner/operator of the server (*e.g.*, vehicle manufacturer, telematics provider, carrier, third-party) with no change to functionality and with a reasonable expectation of success.

64. I am not aware of anything in the prosecution history that changes my opinions expressed in this declaration. To the extent Patent Owner relies on the prosecution history for some point relevant to my opinions, I reserve the right to respond in a future declaration.

<sup>2</sup> In the relevant period, OEM-hosted cloud servers and account-based provisioning for mobile/vehicle services were conventional. *See, e.g.*, EX1009 (Harris), ¶[0038] (OEM server provisioning/authentication); EX1011 (Cazanas), 6:27–34, 12:13–30, 15:4–32 (cloud accounts storing user/vehicle identifiers and policies). These references are cited as background corroboration of industry practice; in any event, the manufacturer-associated-server limitation is satisfied by Xiao.

**C. The '715 patent's claims are entitled to an effective filing date of no earlier than October 25, 2013**

65. The application leading to the '715 patent claims priority to U.S. Application Nos. 18/125,448 (now U.S. Patent No. 11,794,601), 17/461,959 (now U.S. Patent No. 11,738,659), 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. 1012-1016, 1021-1028. The chart below summarizes the relationships between the different applications.



66. I observe that Application No. 14/063,638 (Ex. 1016) describes itself as a “continuation-in-part” of Application No. 13/842,158 (Ex. 1015) and Application No. 13/452,882 (Ex. 1014). 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 ’715 patent is related to Application No. 14/063,638 via multiple continuation applications.

67. There are numerous differences between the ’638 Application and the ’158 Application, which are evident from a computerized comparison of the two. *See* EX1018. 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 related to methods and systems for sharing, requesting, processing, generating, and enabling use of electronic keys (e-keys) (such as “sharing electronic keys,” “processing a request to share an electronic key,” “enabling use and sharing of an electronic key,” “enabling sending a request to share the e-key,” “enabling the e-key for use,” “request to share

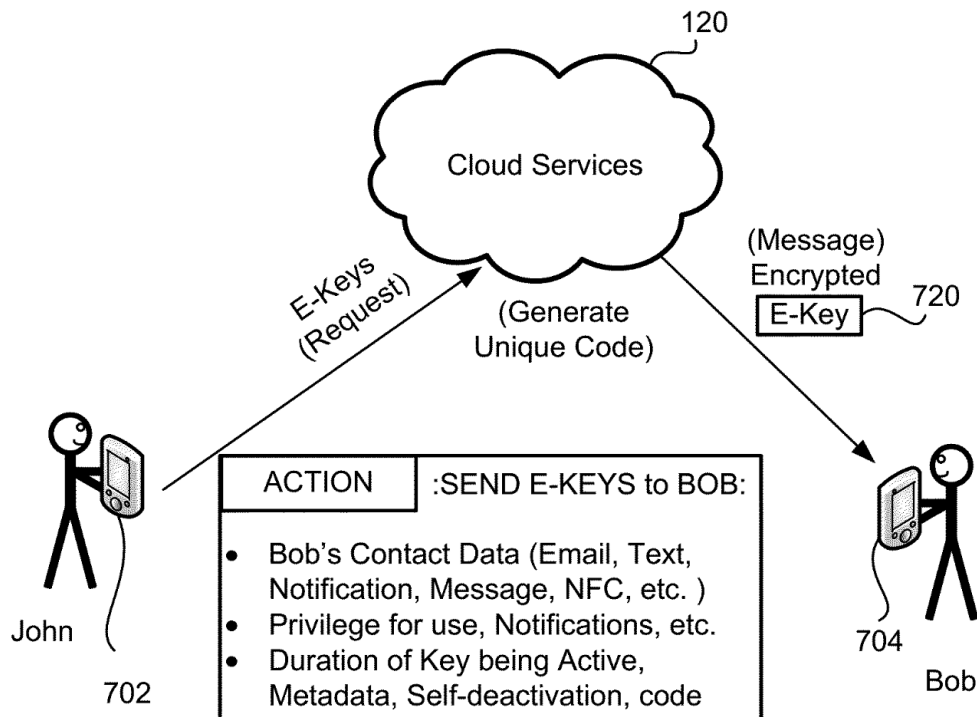
the e-key,” “enable generation of the e-key”) as required by every claim of the ’715 patent, are not found in the earlier applications.

68. The new matter introduced in the ’638 Application, is not present in any of the preceding filings. *See* Exs. 1012-1016, Ex. 1018. This new matter is the only basis on which the specification for the ’715 patent even arguably conveys to a person of ordinary skill in the art that the inventors had developed a system or methods for sharing, requesting, processing, generating, and enabling use of e-keys.

69. For example, Figures 17 through 35 of the ’638 Application (which are the same as Figures 17 through 35 of the ’715 patent) and their descriptions were introduced in the ’638 Application and discuss in detail the requesting, generating, transmission, and use of e-keys. *See, e.g., id.*, 105 (“FIGS. 17-30B ... describe the use of electronic keys (e-keys) in accordance with several embodiments.”); 122 (“Figure 29 illustrates an example where an owner of the vehicle Bob, is able to assign electronic keys (e-keys) 650 to any number of users.”); *id.* (“Each e-key, in one embodiment, will include a unique access code [which] can be generated by a server ...”); 126 (“FIG. 33 illustrates an example where Bob utilizes his device 704 to activate, open, lock, turn on, unlock, John’s vehicle ... facilitated by the activated e-keys 724, which are used via device 704 ...”); *id.* (“FIG. 31B illustrates ... when a request to send e-keys to a recipient is received [by c]loud services [which] can include identification of the recipient and the privileges defined by the requester for

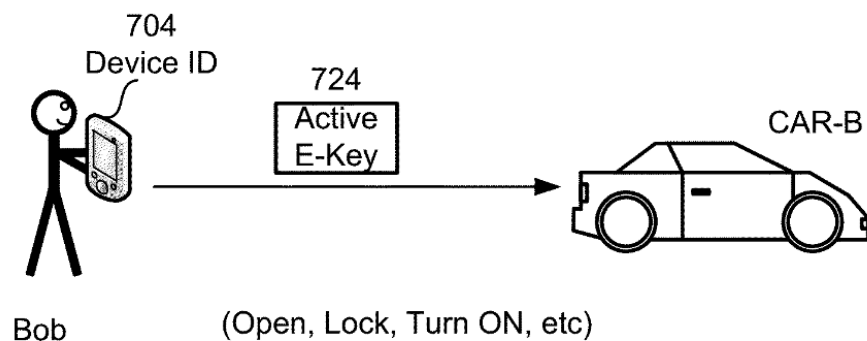
that issuance of e-keys ...”); 128 (“FIG. 35 illustrates an example where a request is sent by John via device 702 to cloud services 120 [which] can generate the unique access code which is then encrypted in a message and sent as encrypted e-keys 720 to the recipient, Bob, who receives it via device 704. ... The duration that the e-keys will remain active can also be set by the requester.”).

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



**FIG. 35**

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



**FIG. 33**

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

73. 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 sharing, requesting, processing, generating, and enabling use of e-keys.

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

75. 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 sharing, requesting, processing, generating, and enabling use of e-keys. *See, e.g.*, Ex. 1015 at 42 (“In some embodiments, this allows verification that the user driving the vehicle 200, from the shared network, is the driver that unlocked the vehicle from a remote location (such as a mobile device).”); 28 (“Any vehicle can be abstracted so that any user can log into any vehicle if they have an account that allows access to that vehicle.”); 60-61 (“In one embodiment, the services provided by the electronic systems of a vehicle can include services that access the various components or subsystems of a vehicle, such as door locks, ..., auto-engine start/shut-off remotely via smart devices, ...”).

76. 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.

77. Accordingly, in my opinion, the '715 patent's claims are not entitled to a filing date before October 25, 2013. None of the applications prior to this date describe the subject matter of the Challenged Claims including methods and systems

for sharing, requesting, processing, generating, and enabling use of electronic keys (e-keys). The earliest priority date to which the asserted claims could be entitled is October 25, 2013. Thus, it is my opinion that the applicant was not in possession of the claimed subject matter directed to e-keys prior to that date.

78. I also understand that in related IPR2024-00981 and IPR2024-01167, Patent Owner did not claim a priority date earlier than Oct. 25, 2013. In its Institution Decisions, the Board noted: “Patent Owner agrees that the [related patents directed to e-keys are] entitled to a priority date of at least Oct. 25, 2013” and “does not assert that any of petitioner’s references fail to qualify as prior art” based on an earlier priority date. IPR2024-00981, Paper 10, at 33–34; IPR2024-01167, Paper 14, at 30–31.

79. I further understand that in its Final Rejection in ex parte reexamination of related patent U.S. Pat. No. 11,738,659 that similarly recites e-keys, the U.S. Patent and Trademark Office (“PTO”) found:

The claims of the patent under reexamination here include subject matter first introduced in the ‘638 application and are therefore being examined with a benefit date no earlier than 10/25/2013. Furthermore, this reexamination proceeding is being examined under the first inventor to file provisions of the AIA.

Subject matter first appearing in the ‘638 application includes FIGs 17-35 and their accompanying descriptions. “E-keys” consistent with the claims are not depicted or described prior to the ‘638 application but they are depicted in newly-presented FIGs 29-35. In contrast, the term/stem “key” appears in the earlier ‘158 application as filed only

three times: p. 18 (historical use of a vehicle's keys), p. 27 (communication pairing using pairing keys) and p. 27 (vehicle settings synced to a key fob).

Ex. 1030, Application/Control Number: 90/019,456, Final Rejection, at 2–3. The PTO further noted that the Patent Owner “does not seek to traverse any prior art currently of record based on priority.” *Id.*

80. 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**

81. 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 '715 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.

82. 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.

83. The '715 patent claims the benefit of U.S. Provisional Application No. 61/478,436 (Ex. 1012) filed April 22, 2011, U.S. Provisional Application No. 61/745,729 (Ex. 1013) filed December 24, 2012, U.S. Application No. 13/452,882 (Ex. 1014) filed April 22, 2012, and U.S. Application No. 13/842,158 (Ex. 1015) filed March 15, 2013. However, as discussed herein, in my opinion, the challenged claims of the '715 patent are not entitled to a priority date any earlier than October 25, 2013.

84. In my opinion, a person of ordinary skill in the art pertinent to the '715 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.

85. Although I surpass this definition of one of ordinary skill in the art now and at the priority date of the '715 patent, my analysis regarding the '715 patent has been based on the perspective of one ordinary skill in the art as of the priority date of the '715 patent.

86. I am also familiar with the knowledge of the person of ordinary skill in the art as of the priority date of the '715 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 '715 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.

87. 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 '715 patent**

88. 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.

89. 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. Summary of Opinions on Unpatentability

90. In the analysis that follows, I identify the following combination of prior art that, in my opinion, renders obvious the '715 patent claims; and I identify certain claims that are also invalid for lack of written description and enablement:

| <b>Grounds of Unpatentability</b> |   |
|-----------------------------------|---|
| 1                                 | <i>Sekiyama, Kleve, Hatton &amp; Xiao</i> render obvious claims 1-24 under Section 103              |
| 2                                 | Claims 1-11, and 17-24 are invalid for lack of written description and enablement under Section 112 |

### A. Ground 1: Sekiyama, Kleve, Hatton, and Xiao

#### 1. Sekiyama (Japanese Laid Open Patent App. Pub. No. 2010-126949)

91. Sekiyama was filed on November 26, 2008, and published on June 10, 2010. I am informed that it is thus prior art under at least §102(a)(1), or pre-AIA §§102(a)-(b).

92. Sekiyama is a Toyota patent application publication that describes an “electronic key system that allows restrictions on functions that can be executed with a duplicate electronic key.” EX1005, Abstract. Sekiyama teaches restricting a “duplicate electronic key” so that it “allows execution of only a subset of functions out of a plurality of functions.” *Id.*, ¶[0007]. The subset of functions may include

“locking/unlocking a door lock of a vehicle, . . . starting a drive source of the vehicle . . . [or] unlocking the trunk.” *Id.*, ¶¶[0008] (internal quotation marks omitted).

93. Sekiyama further discloses a server-mediated e-key issuance flow in which a first mobile device (portable telephone A) sets restriction items and transmits a restricted duplicate e-key issuance request to a center server; the server issues the restricted duplicate e-key and returns it to portable telephone A, which then transmits the received e-key to a second mobile device (portable telephone B). The recipient device (portable telephone B) stores and uses the e-key with the vehicle’s electronic-key ECU (*e.g.*, ECU 41) to control locking/unlocking and engine start. *Id.*, ¶¶[0032]–[0040], [0018].

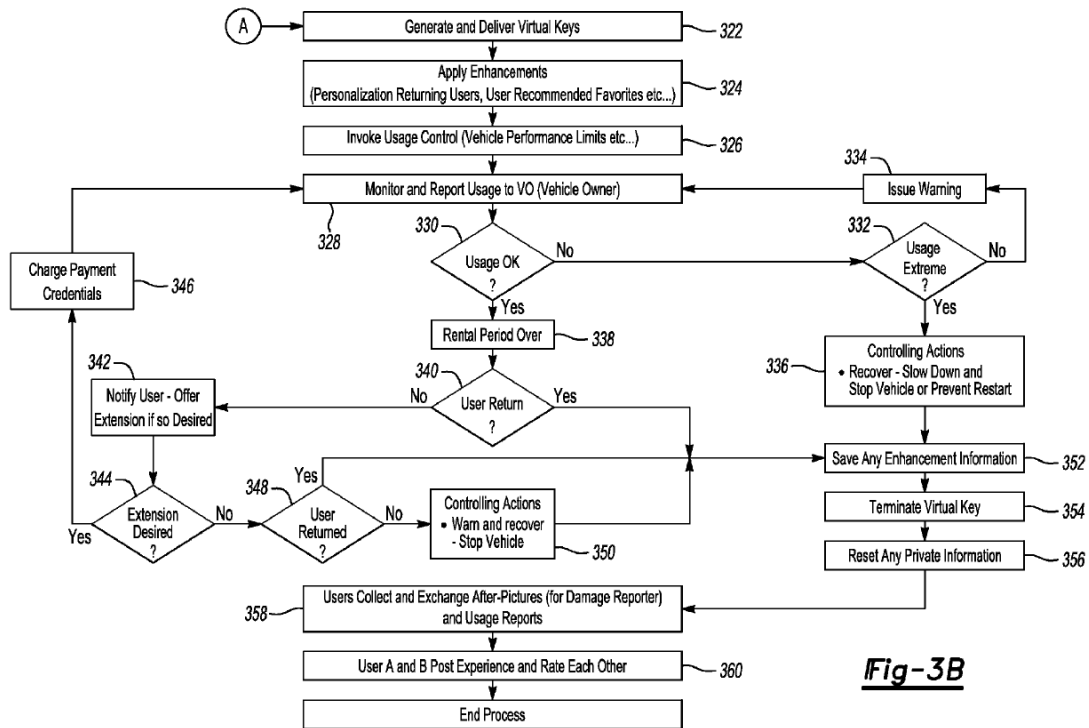
## **2. Kleve (U.S. Patent Pub. No. 2014/0129053)**

94. Kleve was filed November 7, 2012, and published May 8, 2014. I am informed that it is thus prior art under at least §102(a)(2), or pre-AIA §102(e).

95. Kleve is a Ford patent application publication directed to an owner-to-temporary-user “rental micro-business” implemented via a smartphone application and a website. EX1004, Abstract, ¶¶[0036], [0056]. Once rental terms are agreed to, the Owner “enter[s] . . . authorization credentials . . . to set up a virtual key,” and the system “may generate a virtual key to distribute to the Temporary User and VCS [vehicle computing system],” which it then sends “in an encrypted message” to the Temporary User’s nomadic device (*e.g.*, smartphone); the virtual key is “used to

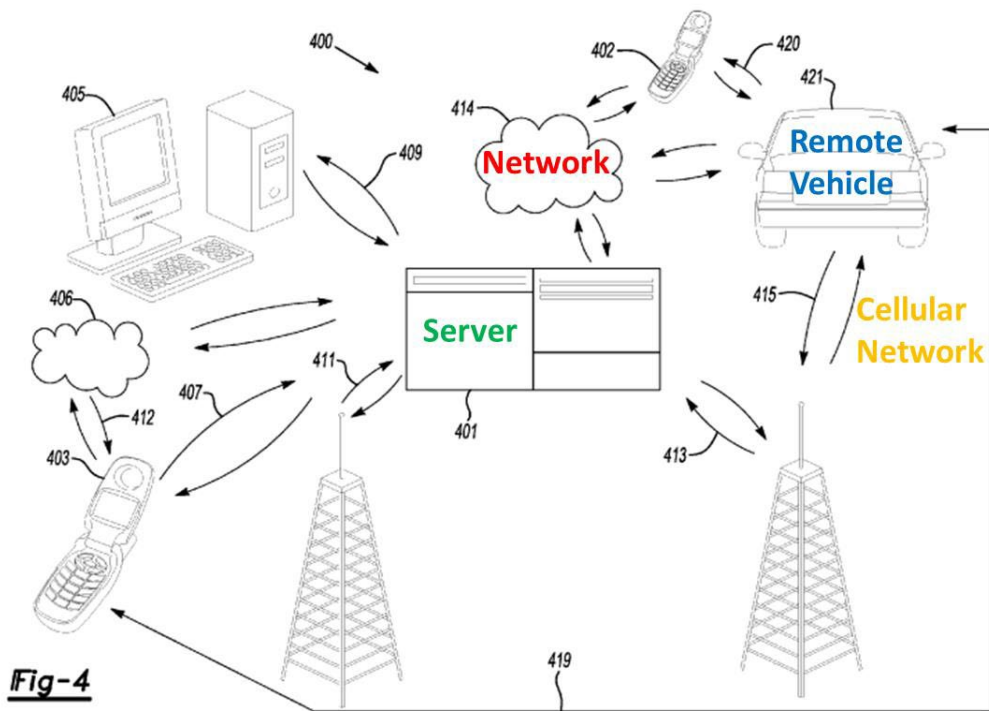
enter and enable the vehicle drive away event.” *Id.*, ¶¶[0039], [0044], [0062]–[0063],

Fig. 3B.



**Fig-3B**

96. Kleve’s vehicle includes a VCS that communicates wirelessly with a server system (depicted as “server(s) 401”), either directly or via a user’s mobile device (*e.g.*, over Bluetooth or cellular), and the server “may route an incoming signal from a nomadic device ... to the appropriate remote vehicle.” *Id.*, ¶¶[0035], [0057], [0060], Fig. 4.



97. The vehicle owner may impose time-bounded (*i.e.*, rental period), speed, and geographic restrictions on usage, and the system monitors and enforces them—issuing warnings, preventing start and restart or slowing and stopping the vehicle upon violations, and terminating and clearing the virtual key at the end of the rental. *Id.*, ¶¶[0040]–[0043], [0051]–[0055], [0068].

### 3. Hatton (U.S. Patent No. 9,002,536)

98. Hatton was filed March 14, 2013, and issued April 7, 2015. I am informed it is thus prior art under at least §102(a)(2), or pre-AIA §102(e).

99. Hatton, like Kleve, is a Ford patent. Hatton describes an “electronic key system and a vehicle computing system for managing a vehicle electronic key.” EX1008, 1:6–8. Hatton uses the same VCS architecture (*see* Fig. 1) as Kleve.

*Compare* EX1004 (Kleve), Fig. 1, *with* EX1008 (Hatton), Fig. 1. Hatton teaches that a “mobile device 124 may be configured using a software application to communicate with the VCS,” with encrypted data used for device recognition and to unlock and start the vehicle. EX1008, 7:21–23; *see also id.*, 7:11–45, 7:49–56. The application “may be ... developed and/or associated with the vehicle manufacturer.” *Id.*, 12:46–51.

100. Hatton further teaches secure, app-mediated key data on the device—for example, a user “typ[es] a pin number on the [software] application,” which is “associated as the primary or secondary key.” *Id.*, 15:37–41. Once recognized, the mobile device can “start[] the vehicle” and “unlock[]/lock[] doors,” with wireless communication technologies used for mobile-VCS exchanges. *Id.*, 13:24–27; *see also id.*, 7:56–60.

#### **4. Xiao (U.S. Patent No. 8,737,913)**

101. Xiao was filed on December 22, 2010, published on June 28, 2012, and issued May 27, 2014. I am informed it is thus prior art under at least §102(a)(1), or pre-AIA §§102(a)-(b).

102. Xiao generally describes “providing a wireless automobile key service.” EX1010, Abstract. Xiao’s system uses a mobile device to “command[] an automobile.” *Id.*, 2:29–30. The mobile device includes a “wireless automobile key service application” through which the operator of the vehicle “register[s] for the

disclosed wireless automobile key service ... and create[s] an account for one or more mobile devices 110, automobile operators, and/or automobiles 112.” *Id.*, 4:33–36, 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.*, 12:8–13. Xiao further teaches that the server infrastructure “may be associated with an automobile company,” and mobile–server communication over cellular and PAN (*e.g.*, Bluetooth) links. *Id.*, 3:18–19, 3:46–54, 4:46–56, Fig. 4. In operation, the mobile device can request automobile health and status information—including “battery charge level”—and receive/display a report on the device. *Id.*, 6:49–63, 7:35–55.

## **5. Motivation to Combine**

103. In my opinion, as discussed in detail below, a POSITA would have been motivated to combine Sekiyama’s system of sharing of e-keys with (i) Kleve’s website for owner and recipient to agree to terms, (ii) Hatton’s manufacturer-provided mobile application and encrypted device with VCS key handling, and (iii) Xiao’s automobile company-associated server and account framework, with a reasonable expectation of success and predictable results.

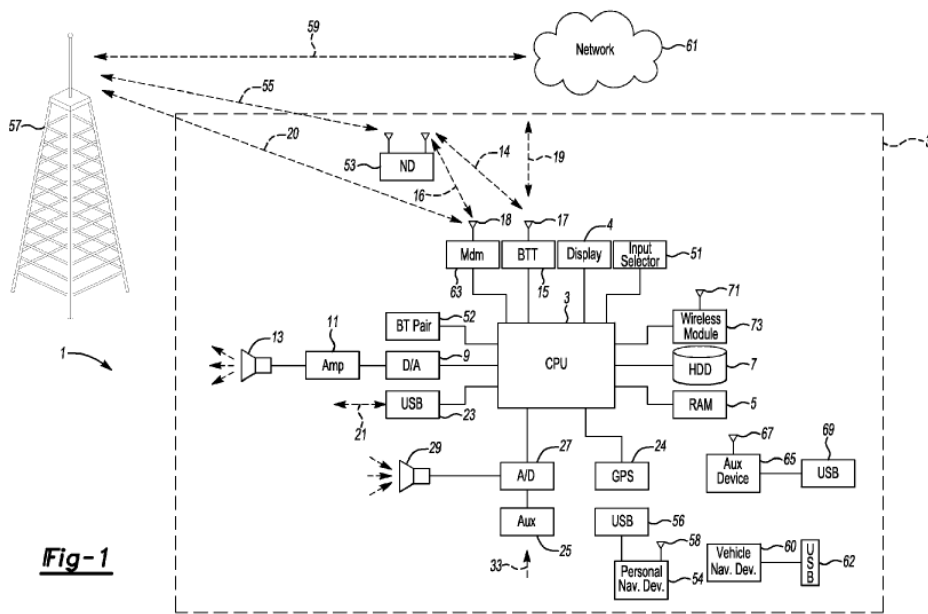
**(a) Pre-agreement of restrictions and distribution of e-key (Sekiyama + Kleve)**

104. Sekiyama teaches an e-key sharing system designed to enable owners to “lend” their vehicles to others (e.g., valets or other “borrowers”), with restrictions on usage time, vehicle access, and functions. *See, e.g.*, EX1005, Abstract; ¶[0038] (“This eliminates the need to *lend* a physical key.”); ¶[0047] (“the restricted duplicate electronic key has been transmitted *from owner A to borrower B.*”); ¶[0048] (“it becomes possible to *lend a duplicate electronic key to another person* while resolving the security problems involved . . . Moreover, by lending a restricted duplicate electronic key with a *set expiration time*, the need for the *borrower* to perform the action of returning the duplicate key is eliminated.”) In such lending scenarios, a POSITA would have recognized the practical need to capture agreed terms before issuance (e.g., identity, duration, permitted functions) to ensure controlled access and auditability.

105. In my opinion, a POSITA would have found it obvious to agree to the terms of the restricted usage, such as the expiration period, prior to generating the restricted e-key. Further, a POSITA would have understood that Sekiyama’s restricted e-key could be monetized in a rental or car-sharing business context and would have been motivated to look to contemporaneous rental/car-sharing art for known mechanisms to capture agreed terms before issuance. Kleve is one such

example, teaching a website/app workflow where the parties agree to terms that the server then uses to issue a virtual key. EX1004, ¶¶[0036]–[0039], [0062]–[0063].

106. Both Sekiyama and Kleve depict the same client-server/VCS pattern (owner device ↔ server ↔ VCS/vehicle controller, with PAN/cellular links), so Kleve’s Fig. 1 serves as a representative diagram of this Sekiyama/Kleve architecture. See EX1004, ¶¶[0021]–[0036], Fig. 1; EX1005, ¶¶[0014]–[0016], [0021], [0031], [0034]–[0039].



107. In the combined system, a POSITA would use Kleve’s server-hosted owner profile/account (with owner credentials and vehicle data, EX1004, ¶¶[0036]) to authenticate the owner and bind sharing requests and restriction settings to the owner’s registered e-key (master key) within the Sekiyama/Kleve architecture by

using the logged-in owner profile to look up and apply the restriction items associated with the master e-key during issuance (EX1005, ¶¶[0012], [0036]), with ECU authentication against stored encrypted data (EX1005, ¶[0015]). This is a routine server-side association of account → key → restrictions familiar to a POSITA. Using Kleve's term-capture/UI flow to populate Sekiyama's server-side restriction fields is a routine integration of complementary components in a shared client-server/VCS architecture, with predictable results and a reasonable expectation of success. In short, the combination yields a flexible platform that supports different sharing scenarios.

108. Moreover, a POSITA would also be motivated because an executed agreement between the parties would allow the owner legal recourse via contract law. It would also clearly set out the applicable restrictions for the recipient—reducing inadvertent violations. For example, knowing the usage period in advance helps ensure the vehicle is returned to the proper location before expiration. Rental and car-sharing arrangements routinely employ written agreements that specify who may use the vehicle, for how long, and under what conditions; these agreements are pervasive in vehicle-sharing contexts. Integrating that contract workflow (including the agreed restrictions) into the e-key issuance process is a straightforward application of common industry practice, ensuring the server captures the parameters before issuance, enabling automated enforcement, and improving auditability—a

routine design choice with predictable results and a reasonable expectation of success.

109. Once terms are finalized and a key must be delivered, there are a finite number of well-known delivery models in secure access systems—*e.g.*, server-to-recipient-device issuance (as in Kleve, EX1004), owner-device relay to the recipient device (*e.g.*, Bluetooth or e-mail, as in Sekiyama, EX1005, ¶[0031]), or physical handover. A POSITA would understand the scenario-dependent tradeoffs: server issuance provides remote immediacy, centralized logging, and automation, but depends on network availability; short-range relay (*e.g.*, Bluetooth) is simple and offline-capable, but requires proximity and compatible devices; e-mail relay enables remote delivery without proximity, but introduces manual steps and third-party client handling; physical handover offers direct control, but requires in-person exchange and lacks automation. Given these known options, a POSITA would view Kleve’s server-to-device issuance as an obvious choice to try within Sekiyama’s restricted e-key framework, particularly where convenience, auditability, and remote access are desired—fitting naturally into the shared client-server/VCS architecture and yielding predictable results with a reasonable expectation of success.

**(b) Secure mobile-to-vehicle exchanges via manufacturer app (Sekiyama + Kleve + Hatton)**

110. In my opinion, with any e-key system, a POSITA would have been motivated to enhance security, including securing exchanges among the server, mobile devices, and the vehicle using well-known encryption and authentication methods.

111. For example, Sekiyama explains that conventional e-key systems “perform authentication” between an e-key and a vehicle using wireless communication (e.g., transmitting “ID codes” or “key codes” with expirations) and that security can be improved by “imposing restrictions on the number of activations” and/or by “generating signature data based on random numbers during communication between an electronic key and a vehicle.” EX1005, ¶¶[0002]-[0003]. In Sekiyama’s e-key system, the vehicle ECU “performs *authentication* of the electronic key” before enabling “locking/unlocking of the door lock” and “permission to start the engine,” based on recognized key information; the ECU’s “electronic key recognition unit 42” compares “the *encrypted* data stored in the storage unit with the key information read from the portable telephone 10, 30.” *Id.*, ¶¶[0015], [0040].

112. Kleve likewise employs a smartphone app/website within a VCS ecosystem and sends a virtual key to the recipient device “in an *encrypted* message.”

EX1004, ¶¶[0036]–[0039], [0063]. Kleve further teaches secure BLUETOOTH communications between a renter’s smartphone and the vehicle’s VCS (e.g., Ford SYNC). *Id.*, Abstract, ¶¶[0008]–[0009], [0021], *see also* [0031] (“incoming data can be passed through the nomadic [smartphone] device ... through the onboard BLUETOOTH transceiver and into the vehicle’s internal processor 3.”)

113. In my opinion, a POSITA would recognize that when control of—or access to—an asset occurs electronically, significant security protections are needed, and would continually look to strengthen those protections to increase owner trust—even for short term scenarios (e.g., valet). Within that effort, a domain-aligned reference like Hatton would be a natural source of additional, well-understood security mechanisms for app-mediated VCS exchanges.

114. Hatton discloses a mobile application (optionally manufacturer-provided) that communicates with the vehicle computing system (“VCS”) using encrypted data, supports device recognition, and enables a user to enter a PIN associated “as the primary or secondary key.” EX1008, 7:11–56, 12:46–51, 13:24–27, 15:37–41.

115. Having captured terms per Kleve, a POSITA would next secure the mobile-to-VCS exchanges (e.g., activation and command flows) to protect contract-bounded access and key material in the Sekiyama + Kleve rental context—where restricted e-keys are issued, a virtual key is generated and delivered to the recipient,

and restrictions (functions/time) are enforced. EX1005, ¶¶[0007]–[0008], [0017], [0034]; EX1004, ¶¶[0036]–[0039], [0062]–[0063]. Among the finite, well-known methods in VCS ecosystems are app-mediated encrypted communications with device recognition, and PIN gating—precisely the pattern Hatton supplies in the same Ford VCS-style architecture. Selecting a known security pattern (Hatton) to harden a known issuance/use flow (Sekiyama + Kleve) is combining familiar elements according to known methods with predictable results.

116. Each reference depicts an in-vehicle computing node with processor/memory, user I/O (*e.g.*, display, microphone), wireless transceivers (*e.g.*, Bluetooth and cellular modems) for pairing with a nomadic device and server communications, and a vehicle network interface (*e.g.*, CAN) to body/engine control modules (locks, start/ignition). *See* EX1004, ¶¶[0021]–[0036], Fig. 1; EX1008, 2:54–5:53, Fig. 1; EX1005, ¶¶[0014]–[0016], [0039]–[0040]. This shared topology confirms drop-in interoperability and supports a reasonable expectation of success (see §5(e)).

117. A POSITA would further be motivated to select Hatton’s manufacturer-associated app implementation (EX1008, 12:46–51) to align the mobile application with OEM VCS services and security (PIN control, device recognition, encrypted exchanges), a routine fit in the same client–server/VCS architecture. And because Kleve ties the app to an owner account (user profile) for initiating key sharing

(EX1004, ¶¶[0036]–[0037], [0047]), integrating Hatton’s app preserves that owner-account association while adding the OEM app’s security/usability features—yielding predictable results with a reasonable expectation of success (*see* §5(e)).

**(c) Account-backed, manufacturer-associated backend and telemetry (Sekiyama + Kleve + Hatton + Xiao)**

118. Sekiyama, developed by Toyota, and Kleve/Hatton by Ford, are e-key systems operating in an OEM vehicle-computing context (cloud-connected servers, mobile devices and onboard vehicle computing systems). Starting from that combined baseline, a POSITA would first inventory the backend’s expected duties—hosting owner/recipient accounts and permissions (per Kleve), enforcing restriction/expiration (per Sekiyama), and supporting secure app↔VCS exchanges (per Hatton)—and then look to contemporaneous automotive backend art implementing those duties in practice (often on OEM-associated cloud servers) and exposing device-visible status/telemetry.

119. Kleve already teaches user accounts and a mobile/website flow that captures terms and delivers a virtual key. EX1004, ¶¶[0036]–[0039], [0062]–[0063]. Sekiyama provides server-side issuance and restriction enforcement. EX1005, ¶¶[0007]–[0008], [0017], [0034]. Hatton supplies secure, app-mediated exchanges with the VCS (encrypted communications, device recognition, PIN gating). EX1008, 7:11–56, 13:24–27, 15:37–41. Together these references play

complementary roles: Sekiyama supplies restricted e-key issuance/enforcement; Kleve supplies the account/app term-capture and delivery workflow; Hatton supplies app-layer security (encrypted exchanges, device recognition, PIN gating); and Xiao adds OEM-associated hosting and device-visible telemetry—yielding predictable benefits in security, manufacturer integration, and status visibility.

120. Xiao contributes two conventional backend elements that complement this base: (i) servers “associated with an automobile company” communicating with the mobile app over cellular and PAN (*e.g.*, Bluetooth), and (ii) device-visible vehicle status/telemetry, including battery charge level requested from the vehicle and displayed on the device. EX1010, 3:12–20, 3:46–54, 4:33–36, 4:46–56, 6:49–63, 7:35–55, 12:8–13.

121. A POSITA would have been motivated to add Xiao because the base system (restricted e-keys in a contractual setting with secure app↔VCS exchanges) benefits from a manufacturer-associated backend for service integration and policy propagation, and from surfacing status to the device after issuance. The references are architecture-compatible: Kleve’s account/app flow remains the account mechanism; Sekiyama’s server enforces restrictions; Hatton secures the app↔VCS path; and Xiao adds manufacturer association and telemetry reporting within the same client-server/VCS pattern. Implementing Xiao’s manufacturer-associated server simply hosts the existing account/permission records (as taught by Kleve) and

exposes status calls to the app (as taught by Xiao), without redesign. *See* EX1004, Fig. 1; EX1008, Fig. 1; EX1010, 4:46–56. Xiao’s OEM hosting and telemetry operate as drop-in backend services within the same client–server/VCS pattern (cellular/PAN links, authenticated exchanges), requiring no architectural redesign.

122. With Xiao, the combined system (i) uses servers associated with the vehicle manufacturer; (ii) communicates over cellular/PAN; and (iii) allows the recipient device to access vehicle status such as battery charge level—while Sekiyama enforces function/time limits and Kleve/Hatton provide term capture and secure app/VCS operation. *See* EX1010, 6:49–63, 7:35–55; EX1005, ¶¶[0007]–[0008], [0034]; EX1004, ¶¶[0036]–[0039], [0062]–[0063]; EX1008, 7:11–56, 13:24–27. In my opinion, this is a routine, predictable integration of well-understood backend elements, with a reasonable expectation of success.

**(d) Technical compatibility and routine implementation**

123. All four references operate in the same field—vehicle e-key services built around a mobile app, a backend server, and a VCS/onboard controller. EX1004 (Kleve), ¶¶[0021]–[0036], [0039], [0048]–[0049]; EX1005 (Sekiyama), ¶¶[0007]–[0008], [0034]–[0040]; EX1008 (Hatton), 1:6–8; EX1010 (Xiao), Abstract.

124. They use standard communication links (cellular, Bluetooth/PAN) and conventional data flows (app ↔ server; app ↔ VCS). EX1004, ¶¶[0035], [0057], [0060], [0063]; EX1008, 7:11–60; EX1010, 3:46–54, Fig. 4.

125. In my opinion, the combinations require straightforward software integration (UI elements, API calls, and encryption that the art already uses) and predictably improve security, manageability, and user experience.

**(e) Reasonable expectation of success**

126. In my opinion, a POSITA would have had a reasonable expectation of success integrating these references because each teaches known elements performing their conventional roles within a shared client-server/VCS ecosystem, with minimal redesign or incompatibility:

- **Server/device workflow and routing:** Sekiyama contemplates issuance by a center server and device-side use of a restricted/duplicate key, with the owner terminal sending the issuance request and the server returning the key for use on the recipient device—*i.e.*, split processing across phone and server with server-routed communications. EX1005, ¶¶[0032]–[0040].
- **Agreement capture and delivery flow:** Kleve provides the app/website workflow to establish terms (user profiles, term exchange) and then deliver the virtual key to the recipient device, fitting the same phone ↔ server ↔ VCS pattern. EX1004, ¶¶[0036]–[0039], [0048]–[0049], [0062]–[0063].
- **Secure mobile ↔ VCS exchanges:** Hatton supplies app-mediated encrypted communications, device recognition, and PIN-gated key use in a Ford VCS topology indistinguishable from Kleve’s, confirming drop-in compatibility of

secure exchanges. EX1008, 7:11–56, 13:24–27, 15:37–41; *compare* EX1008, Fig. 1, *with* EX1004, Fig. 1. A POSITA would therefore expect success whether secure key material is generated server-side (as in Sekiyama’s issuance of key information used for ECU authentication, EX1005, ¶¶[0015], [0036]) or device-side (as in Hatton’s PIN-associated mobile key, EX1008, 7:11–56, 15:37–41), because both rely on standard encryption and credential verification at the vehicle ECU.

- **Account/telemetry backend:** Xiao teaches account-centric backends that “may be associated with an automobile company,” with mobile ↔ server and PAN/cellular links, and status/health reporting to the device (*e.g.*, battery charge level), which align with the same communication layers used in the above references. EX1010, 3:12–20, 3:46–54, 4:33–36, 4:46–56, 6:49–63, 7:35–55, 12:8–13.

127. In my opinion, implementing the combination uses standard interfaces (*e.g.*, app UI to capture terms; API calls for issuance and acknowledgments; existing encrypted mobile ↔ VCS channels; account tables for identities/permissions; telematics/status endpoints), all within conventional VCS and server architectures—a routine engineering task yielding predictable results.

128. Taken together, these references teach interoperable, conventional components such that a POSITA would have a reasonable expectation of success

implementing either server-side or device-side secure key generation within the combined system. *See* EX1005, ¶¶[0015], [0036]; EX1008, 7:11–56, 15:37–41).

**6. Claim 1**

**a. 1[pre] – “A method for sharing electronic keys (e-keys)”**

129. To the extent the preamble is limiting, in my opinion, the Sekiyama + Kleve + Hatton + Xiao combination (hereafter “the combined system”) discloses *a method for sharing electronic keys (e-keys)*. Sekiyama teaches an “electronic key system” in which the “server 20 of the management center” performs “issuance of electronic keys.” EX1005, ¶[0021]. The electronic key system can issue a “master key,” which “allows all functions of the vehicle 40 to be executed without restrictions,” as well as “restricted *duplicate* electronic keys,” which “allows only a subset of the plurality of functions.” *Id.*, ¶[0012] (emphasis added). The restricted duplicate keys are “lent out ... to others,” indicating that they are *shared* keys. *Id.*, ¶¶[0051], [0048] (“[I]t becomes possible to lend a duplicate electronic key to another person while resolving the security problems involved.”). In the combined system, Sekiyama and Kleve supply the familiar owner–recipient transaction flow and delivery mechanics for sharing, Hatton supplies the app-mediated secure handling used when the recipient device presents/uses the shared key with the VCS, and Xiao supplies the account/server context typical of manufacturer-associated backends.

See EX1004, ¶¶[0036]–[0039], [0062]–[0063]; EX1005, ¶¶[0025]–[0027], [0031]–[0040]; EX1008, 7:11–56, 15:37–41; EX1010, 3:12–20, 4:33–36, 12:8–13.

- b. **1[a] – “processing a request to share an electronic key (e-key) of a vehicle with a recipient device, the request to share the e-key being received responsive to a message being sent to the recipient device from a sharing device;”**

130. In my opinion, in the combined system, Sekiyama teaches “*processing a request to share an electronic key (e-key) of a vehicle with a recipient device*” where an owner’s device requests the issuance of a restricted key for use by a recipient device. Specifically, Sekiyama teaches that “portable telephone A 10” (*i.e.*, a *sharing device*) issues “a restricted duplicate electronic key issuance *request*” to the “management center.” EX1005, ¶[0035] (emphasis added). In response, the restricted key is sent for use by “portable telephone B 30” (*i.e.*, a *recipient device*) to allow access to a vehicle. *Id.*, ¶¶[0038]–[0039].

131. Further, as expressly taught by Kleve, it would have been obvious in the combined system for the server to send the key to the recipient device (EX1004, ¶¶[0062]–[0063] (describing the owner entering information into a server to “set up a virtual key,” which is “sent in an encrypted message ... to the Temporary User’s nomadic device,” *i.e.*, a *recipient device*)). . As discussed in §5(a), a POSITA would have implemented server-to-recipient issuance as part of the combined system as a

routine client-server integration yielding predictable results. See EX1004, ¶¶[0062]–[0063]; EX1005, ¶¶[0035], [0038]–[0039]..

132. ***“the request to share the e-key being received responsive to a message being sent to the recipient device from a sharing device”***: As explained in Ground 2 (§112), *the ’715 patent’s specification does not explain how the e-key request is responsive to a message sent from the sharing device to the recipient device*. And while PO may argue that the overall flow “implies” such coupling or that a POSITA would infer missing app internals, the specification itself never links a recipient-bound message to the server’s receipt/processing of the request. The specification describes that “the app on the user’s mobile device can request that a message be sent to the recipient, so that the recipient can receive the e-keys and be granted access to the vehicle,” and particularly that the recipient receives “instructions for obtaining/validating/using the e-keys.” EX1001, 5:11–19. *That is, the ’715 patent describes a way for the owner to message a recipient that the e-key is available. However, the ’715 patent generally describes that the owner requests the issuance of the e-key without any reference to such a message. Id.*, 42:10–11 (“Bob [the owner] can request that keys be sent to the valet”), 42:35–37 (“FIG. 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.”), 43:37–46 (“[T]he user-owner of the vehicle can assign a valet with access to the vehicle by going on an application (App or website)

... and requesting that the e-keys be sent to the recipient.”), 43:47–51 (“[A] user, John ... is able to communicate and send e-keys to another user (Bob). In this example, the sending of e-keys will include the sending of the request to a server”), 44:51–54 (“[T]he request is associated with the user account making the request. The user account will be John’s account, which will have predefined information associated with the vehicles that John is able to assign e-keys for.”), 45:37–43 (“[A] request is sent by John ... to send e-keys to Bob.”).<sup>3</sup>

133. Thus, while the ’715 patent describes the owner providing a message to the recipient, it does not disclose a causal relationship between that message and the sending of a request by the owner (or the recipient) or the processing thereof. To the extent PO asserts that this claim limitation “responsive to” requires a direct causal connection between a message being sent to a recipient and the issuance/processing of a request (i.e., the server receives/processes the request because of the recipient-bound message), the claim fails written description and enablement support and is invalid under 35 U.S.C. §112(a) (see Ground 2 (§112)).

<sup>3</sup> The ’715 patent provides an example where “the recipient may directly request e-keys,” but does not provide any disclosure in that example of the recipient’s request being responsive to receiving a message from an owner’s device. EX1001, 48:57–59.

134. Regardless of PO's §112 position, and even under a non-causal reading, the combined system renders this limitation obvious. Kleve describes that, prior to the request for an e-key, the owner and recipient "have already ... both agreed to the rental agreement." EX1004, ¶[0062]. Kleve explains that the agreement of terms involves the owner and recipient messaging each other. For example, Kleve describes that the owner can deliver to the recipient a "standard rental agreement form" or a "custom form based on the type of use the Temporary user [recipient] is requesting to use the vehicle for." EX1004, ¶[0038]. In Kleve, the recipient's acceptance/return of the terms precedes the owner's submission of those agreed terms to the server, which then sets up the key—so the recipient-facing message(s) function as the trigger for the owner/server request flow. EX1004, ¶¶[0038], [0062]). Once that owner request exists, Sekiyama supplies the downstream mechanics: the center server generates key information according to owner-set restriction items and issues a restricted duplicate key for the recipient device; the vehicle ECU authenticates and controls use based on that key information. EX1005, ¶¶[0034]–[0036], [0038]–[0040], [0015]. A POSITA would, from this end-to-end flow in the combined system—owner↔recipient messaging (Kleve) followed by server-side processing and issuance (Sekiyama)—understand that the processing is "responsive to" the message in ordinary client-server e-key workflows. See EX1004, ¶¶[0038], [0062]; EX1005, ¶¶[0034]–[0039].

135. As discussed in §5(a) above, in my opinion, a POSITA would have found it obvious to incorporate these teachings into the combined system.

**c. 1[b] – “determining that the request to share the e-key was associated with a registered owner e-key;”**

136. In my opinion, in the combined system, Sekiyama teaches that the server determines that the request to share originates from, and therefore is associated with, the owner’s device, *i.e.*, ***a registered owner e-key***. Specifically, Sekiyama teaches that “portable telephone A 10,” the owner’s device, “functions as a master key that allows all functions of the vehicle 40 to be executed without restrictions.” EX1005, ¶[0012].

137. Sekiyama further teaches that “portable telephone A 10 performs a restricted duplicate electronic key issuance request” that is sent to the server. *Id.*, ¶[0035]. In response to that request, the server “issues an electronic key that functions as a restricted duplicate electronic key,” with restrictions set “according to the restriction items that were set on the portable telephone A 10,” *i.e.*, ***a registered owner e-key***. *Id.*, ¶[0036]. In other words, because the server issues a specific restricted key in accordance with the specific restrictions set by the ***registered owner e-key***, the server has determined the request is associated with that registered owner e-key.

138. Kleve discloses that the owner “may set up a user profile” on the server (e.g., via website/nomadic device) including vehicle-identifying information (make/model/year). EX1004, ¶[0037]. In my opinion, a POSITA would understand that this profile creation is the server-side *registration* step—i.e., creation of an authenticated owner account linked to the vehicle(s)—because subsequent actions (including sharing) are performed while logged in under the owner’s credentials. Accordingly, when the owner submits the sharing request while authenticated, the server determines that the request is associated with the owner’s registered credentials/e-key. This is consistent with Sekiyama’s server issuing a restricted key “according to” restriction items set from the owner’s master key (EX1005, ¶[0036]) and with Xiao’s account/credential model (mobile ID, authentication data, permissions) that ties requests to a registered account/e-key. EX1010, 4:33–36; 12:8–12. Motivation to incorporate Kleve’s server-hosted owner profile/account—and Xiao’s account/credential framework for binding sharing requests to a registered owner e-key—is discussed in §5 (Motivation to Combine).

**(d) 1[c] – “processing instructions to enable the e-key to be securely generated for use by the recipient device; and”**

139. *“processing instructions”*: In my opinion, in the combined system, Sekiyama discloses a “center server” which performs various operations, including through the use of an “electronic key issuance unit 21.” *See, e.g.*, EX1005, ¶[0021].

A POSITA would understand that a server performs operations by processing instructions, specifically, server program code and firmware that comprises of instructions that are executed by a processor. Sekiyama expressly identifies server 20's "electronic key issuance unit 21" as the module that processes the owner's request and performs issuance. *Id.*, ¶¶[0021], [0035]–[0036].

140. ***“enable the e-key to be securely generated”***: Sekiyama teaches that the recipient's e-key is ***securely generated***. In particular, when the restricted key is generated, the server generates “key information . . . according to the restriction items that were set” by the owner. *Id.*, ¶[0036]. Such “key information” is used by the vehicle to “authenticate[] the electronic key by comparing the encrypted data stored in the [vehicle's] storage unit with the key information read from the portable telephone 10, 30.” *Id.*, ¶[0015]. Specifically, the “key information” allows the system to “determine[] whether the electronic key is a key that allows execution of functions of the vehicle 40.” *Id.* In other words, Sekiyama describes that e-keys are generated with “key information” that matches encrypted information stored on the vehicle to authenticate the key—thereby ensuring that the key was securely generated. A POSITA would recognize this as the standard encryption/authentication model in vehicle ECUs (key information generated per owner-set restrictions and later verified against encrypted vehicle data), consistent with §5(e). *Id.*, ¶¶[0015], [0036]. Likewise, as discussed above, Kleve teaches user

accounts and a mobile/website flow that captures terms and delivers a virtual key. Kleve describes its communications, in one embodiment, as employing Bluetooth. The Bluetooth standard as it existed prior to the priority date included BR/EDR secure simple pairing, a secure communication. (EX1029 (Bluetooth Core Specification v4.0) at page 85; see also pages 85-92).<sup>4</sup> Indeed, Bluetooth states that the goal of secure simple pairing is to “protect[] against passive eavesdropping and protect against man-in-the middle (MITM) attacks (active eavesdropping).” *Id.* A person of ordinary skill in the art would thus understand that Kleve’s discussion of

<sup>4</sup> In my opinion, the Bluetooth standard, and the Bluetooth specification, are both very well known in the industry. Bluetooth.com is the well-known repository for versions of the Bluetooth standard. The Bluetooth standard (Bluetooth Core Specification v4.0) attached at EX1029 was downloaded from the Bluetooth.com archive at <https://www.bluetooth.com/specifications/archived-specifications/> and <https://www.bluetooth.com/specifications/specs/core-specification-4-0/>. A POSITA familiar with the standard would understand that the date printed on the front of the standard, June 30, 2010, is reliable and indicates the document was publicly available at least on that date, and a POSITA, having deep understanding of the Bluetooth standard, would have been readily able to locate and search the standard.

Bluetooth was “secure.” Thus, in the combination, the communications from the server to the car, including from the mobile device, are “secure.”

141. Additionally, Hatton also teaches secure on-device generation and use of an electronic key by a mobile app—the user enters a PIN and the system associates that PIN as a primary/secondary key, with encrypted data used for device recognition and start/unlock—which a POSITA would have combined with Sekiyama to meet this limitation. EX1008, 7:11-56, 13:24-27, 15:37-41. A POSITA would have had a reasonable expectation of success implementing either server-side (Sekiyama) or device-side (Hatton) secure key generation for the reasons explained in §5(e).

142. “*e-key ... for use by the recipient device*”: Sekiyama teaches that the “restricted duplicate electronic key” is delivered to “portable telephone B 30” (*i.e. recipient device*). EX1005, ¶[0038]. The key is “use[d][by] ... the duplicate key user B [by] ... transmit[ting] the key information to ... [a vehicle’s] electronic key ECU 41,” which controls the vehicle, such as “locking/unlocking” and “start[ing] the engine ... based on the recognized key information.” *Id.*, ¶[0039]-[0040].

**(e) 1[d] – “saving information regarding the e-key with a server associated with a manufacturer of the vehicle;”**

143. “*saving information regarding the e-key with a server*”: In my opinion, in the combined system, Sekiyama teaches that the server receives, maintains, and saves “key *information*” regarding the restricted key, such as “the

functions that will be usable with the restricted duplicate electronic key” and “the expiration” of the key. *Id.*, ¶¶[0034], [0036], [0025] (“Information related to the subset of functions that was set is outputted to the center server 20.”).<sup>5</sup> In my opinion, a POSITA would understand that issuing and enforcing a restricted, expiring e-key requires the server to persist that key information at least through the access period so it can be used for authentication and expiration checks.

144. In addition, during operation of the restricted key, the server “periodically” requests and the vehicle “transmits a vehicle status related signal to the center server.” EX1005, ¶¶[0041]–[0042]. Such information can be “check[ed]” by the owner’s device “at any time” via request. *Id.*, ¶¶[0043]–[0044]. Thus, Sekiyama’s disclosure of periodic uploads and on-demand owner queries indicates that the server stores status/usage information related to the active e-key, i.e., “saving information regarding the e-key.” In my opinion, a POSITA would recognize this as routine server-side management of e-key records (e.g., key parameters and active-use status) to support validation, expiration, and owner visibility; the claim does not require any particular schema, and implementing such storage would have been

<sup>5</sup> In my opinion, a POSITA would understand that “outputted to the center server 20” means the server stores the e-key information (*i.e.*, persists the key information for later authentication and expiration checks).

conventional. Moreover, a POSITA would have understood that storage and management methods for saving information regarding e-keys with a server follow conventional server implementation practices and would have been routine. *Id.*

145. “*server associated with a manufacturer of the vehicle*”: As an initial matter, I have been informed that the phrase “associated with a manufacturer of the vehicle” is nonfunctional descriptive material and therefore is not entitled to patentable weight under the printed matter doctrine, because “it claims the content of information” (i.e., who operates the server) and lacks any “functional relationship” to the server.<sup>6</sup> Who owns/operates the server does not alter the server’s structure or the method’s operation. Nor does characterizing manufacturer operation as “improving reliability/security” supply the missing functional tie—those are at most asserted advantages of *who* hosts the same server functions, not a change to *how* the claimed saving/processing occurs. Even if this phrase is accorded patentable weight, the limitation is also met—or obvious—on the merits, as set out below.

146. In my opinion, a POSITA would have understood that Sekiyama’s server is *associated with a manufacturer of the vehicle*. Sekiyama is a Japanese patent application invented by employees of Toyota Motor Corp. and assigned to

<sup>6</sup> To the extent the Examiner relied on this phrase in allowing the claims, I have been informed that the Examiner erred in according the phrase patentable weight.

Toyota Motor Corp. EX1005. Accordingly, a POSITA would have recognized that the “center server” described in Sekiyama was a server associated with the manufacturer of the vehicle, as the “electronic key system” described in Sekiyama would have been understood to have been developed for use by Toyota and its vehicles. And even if PO argues Sekiyama lacks an explicit statement of OEM hosting, that only underscores why the claim, if given weight, remains obvious: choosing an OEM-operated server is one of a finite set of routine hosting options (OEM, telematics provider, carrier, third-party) with predictable, generic benefits and no change to the underlying key-saving functionality.

147. It further would have been an obvious option to host Sekiyama’s server functions on a server operated by (or on behalf of) the vehicle manufacturer. Multiple contemporaneous references teach manufacturer-associated servers for e-key services. Xiao explains that its wireless automobile key service servers “may be associated with an automobile company.” EX1010, 3:12–20; *see also id.*, 3:46–54, 4:46–56, 12:8–12, 16:48–54.<sup>7</sup> Thus, a POSITA would have found it obvious to

<sup>7</sup> As noted above, in the relevant period, OEM-hosted cloud servers and account-based provisioning for mobile/vehicle services were conventional. *See, e.g.*, Harris (OEM server provisioning/authentication, EX1009, ¶[0038]) and Cazanans (cloud

implement Sekiyama’s saving of e-key information on a manufacturer-associated server as one of a finite, predictable set of options for the owner/operator of the server (*e.g.*, vehicle manufacturer, telematics provider, carrier, third-party) with no change to functionality and with a reasonable expectation of success. A POSITA would have been motivated to select the OEM-associated option taught by Xiao because it centralizes account/permission management, integrates with OEM telematics/ECU support workflows, and improves auditability and lifecycle controls (*e.g.*, credential resets, expiration enforcement)—all without altering Sekiyama’s key-saving/processing operations (EX1010, 3:12–21; 3:46–54; 12:8–13). This is a routine hosting choice in the same client–server/VCS architecture, yielding predictable results with a reasonable expectation of success (see §5(e)).

**(f) 1[e] – “wherein the e-key is enabled for said use on the vehicle by the recipient device.”**

148. In the combined system, Sekiyama teaches that the “restricted duplicate electronic key” is delivered to “portable telephone B 30” (*i.e.*, *recipient device*). EX1005, ¶[0038]. The key is “use[d] [by] ... the duplicate key user B [by] ...

accounts storing user/vehicle identifiers and policies, EX1011, 6:27–34, 12:13–30, 15:4–33). These references are cited as background corroboration of industry practice; the limitations at issue are satisfied by Xiao.

transmit[ting] the key information to ... [a vehicle's] electronic key ECU 41," which controls the vehicle, such as "locking/unlocking" and "start[ing] the engine ... based on the recognized key information." *Id.*, ¶¶[0039]–[0040]. A POSITA would recognize this enablement/use as the standard ECU authentication flow (comparing key information to encrypted vehicle data, *id.*, ¶[0015]), making implementation feasible and predictable in the combined system, as discussed in §5(e).

**7. Claim 2 – The method of claim 1, wherein the request to share the e-key includes a setting to assign a privilege level for use of the vehicle when used via the e-key, the privilege level provides one or more conditions of use of the vehicle.**

149. In my opinion, in the combined system, Sekiyama teaches that key request includes various "restriction items," *i.e.*, ***settings to assign a privilege level for use of the vehicle***. Specifically, Sekiyama teaches that the owner's device "sets restriction items for the restricted duplicate electronic key," which are then sent with the request. *Id.*, ¶¶[0034]–[0036], Fig. 3 (indicating that the restrictions are set by the owner device).

150. The "restriction items" provide for ***conditions of use of the vehicle***, specifically a "subset of functions[] of the vehicle 40 that can be utilized with the restricted duplicate electronic key." *Id.*, ¶[0025]. Such functions include "locking and unlocking of the door lock, permission to start the engine, locking and unlocking of the trunk, locking and unlocking of the console compartment, permission to use

the on-board unit functioning as a car navigation device, permission to use the on-board unit functioning as a communication device capable of sending and receiving email,” and “conditions for using those functions (for example, usage time).” *Id.*, ¶[0016]–[0017] (internal quotation marks omitted).

8. **Claim 3 – The method of claim 2, wherein the one or more conditions of use defined via the privilege level is one of a geographic restriction for where the vehicle is allowed to be used, or a speed restriction, or an occupancy restriction, or a time frame of use, or an expiration-time of use, or unlocking of the vehicle, or driving of the vehicle, or combinations of two or more thereof.**

151. As discussed above for claim 2, in the combined system, Sekiyama teaches *conditions of use* that include a “conditions for using those functions (for example, usage time)” (*i.e.*, *time frame of use, or an expiration-time of use*), “locking and unlocking of the door lock,” and “permission to start the engine.” *Id.*, ¶¶[0016]–[0017] (internal quotation marks omitted).

9. **Claim 4 – The method of claim 1, wherein the request is enabled via an application executed via the sharing device, the application provided by said manufacturer of the vehicle to enable initiation of sharing of the e-key, the application is associated with an owner account for the vehicle.**

152. In my opinion, the plain meaning of “application” to a POSITA at the time of the patent is software instructions to perform a particular task. Accordingly, a POSITA would understand that, in the combined system, Sekiyama’s teachings of

an owner's device (*i.e.*, **sharing device**) issuing the sharing of an e-key is performed by an application on the device.

153. In addition, Kleve discloses an application for requesting an e-key that is associated with an owner account. For example, Kleve discloses a “rental microbusiness” implemented as a “smart phone application” that an Owner uses to log into and manage a user profile (owner account) and to initiate sharing/distribution of virtual keys from the sharing device. EX1004, ¶¶[0036] (smartphone application is used to manage “assets and/or user profile”), [0037] (Owner “may set up a user profile ... that is stored in a database”), [0047]. In Kleve's system, “an Owner and Temporary User may use [the smartphone application] to manage their assets and/or user profile,” including to “distribut[e] a virtual key to the Temporary User.” *Id.*, ¶[0036]. Kleve further explains that the Owner, through the application and/or website user interface tied to the owner profile, initiates sharing by entering the Temporary User's credentials and causing the system to “set up a virtual key,” which is then delivered to the recipient. *Id.*, ¶¶[0039], [0062]–[0063], [0047]–[0048], [0051], [0069] (generation/delivery flow). Thus, the “request is enabled via an application executed via the sharing device,” and the application is “associated with an owner account for the vehicle.” As discussed above, a POSITA would have found it obvious to incorporate these teachings into Sekiyama.

154. A POSITA would have understood—and it would have been obvious—that the software application may be developed by and/or associated with a vehicle manufacturer. Sekiyama is a patent invented by and assigned to Toyota Motor Corp. Accordingly, the recited software application functions of the owner’s device would have been developed by Toyota and therefore associated with a vehicle manufacturer. Furthermore, Hatton expressly discloses a Ford VCS/SYNC architecture, explaining that a “software application 212 ... may be an application that was developed and/or associated with the vehicle manufacturer,” and that the app communicates with the VCS to perform key functions (recognition, start/unlock). EX1008, 12:46–51; *see also id.*, 7:11–45, 7:49–60, 13:24–27. A POSITA would have been motivated to incorporate Hatton’s manufacturer-associated app flows into the combined system to leverage existing VCS security/usability features (PIN-gated access, device recognition, encrypted exchanges) and to align the owner’s mobile app with OEM back-end services—an ordinary fit in the same client-server/VCS architecture with predictable results (*see* §5(b); §5(e)).

155. Further, as with claim 1[d], the phrase “the application provided by said manufacturer of the vehicle” merely identifies the source of the software and is non-functional descriptive material. *See* claim 1[d]. Who supplies the app does not alter the structure or operation of the claimed method.

- 10. Claim 5 – The method of claim 1, wherein responsive to said request, the e-key is generated, the generation of the e-key includes one or more processes executed by the server associated with the manufacturer of the vehicle, one or more processes executed by one or more additional server, one or more processes executed by the recipient device, one or more processes executed by a computer, or a combination of two or more thereof.**

156. As discussed above for claim 1, in the combined system, Sekiyama teaches that in response to the key request, a server *associated with the manufacturer of the vehicle* (to the extent that limitation has patentable weight) executes a process for generating an e-key. EX1005, ¶¶[0036]–[0037], Fig. 3. The generation of the e-key further includes delivery to the recipient device, which likewise involves a process executed by the recipient device, specifically its “electronic key reception unit.” *Id.*, ¶¶[0028], [0038].

- 11. Claim 6 – The method of claim 1, further comprising, encrypting the e-key, the e-key being encrypted using public/private key pairs that are generated and used for security in communication.**

157. In the combined system, Sekiyama teaches that the e-key is authenticated by comparing it to “the encrypted data stored” on the vehicle. *Id.*, ¶[0015]. A POSITA would have therefore understood that the e-key is likewise encrypted in order to match that information to the stored encrypted data.

158. This limitation also would have been obvious in view of Hatton, which teaches the use of encrypted communications in an e-key system to prevent

unauthorized access to the vehicle and to recognize the authorized mobile device. EX1008, 9:50–63; *see also id.*, 7:33–45, 7:49–56. As discussed above, prior to the filing date Bluetooth employed secure simple pairing. One specific implementation of this was the use of “Elliptic Curve Diffie Hellman (ECDH) public key cryptography.” EX1029, at page 85; *see also* pages 85-92.

159. It would have been obvious to a POSITA that the encryption operations may use public/private key pairs because public/private key pair encryption was a well-known and widely used encryption technique well before October 2013, and a POSITA would have been capable of implementing public/private key pair encryption in Sekiyama’s system. Contemporaneous references confirm that public/private key pair encryption was well-known years before the ’715 patent, including in electronic key systems for vehicles. *See, e.g.*, EX1020 (Fukushima), 15:34–51 (explaining public/private key–pair encryption for securing vehicle communications).

**12. Claim 7 – The method of claim 1, further comprising, receiving a deactivation request, the deactivation request is used to disable the e-key for use by the recipient device on the vehicle.**

160. In the combined system, Sekiyama teaches that when the restricted key’s “usage period has ended,” the vehicle’s “electronic key ECU” disables the e-key—specifically, “settings are changed to disable use of the subset of functions that

was usable with the restricted duplicate electronic key.” EX1005, ¶[0045]. A POSITA would have understood that the ECU sends a *deactivation request* to the vehicle systems to disable those functions. A POSITA would have understood that the disablement occurs in response to received control signal/request within the vehicle system when the expiration condition is met (*i.e.*, a deactivation request internal to the ECU/vehicle network that is used to disable the key).

161. In addition, as part of the disabling of the e-key, the ECU “transmits a signal (usage end data) [to the server] notifying that the usage period of the restricted duplicate electronic key has ended,” and that message is used to complete the deactivation flow (*e.g.*, terminate active connections/permissions). *Id.* In the combined system, that “usage end” notification constitutes a deactivation request used to disable the e-key (server- and vehicle-side).

162. Further, even beyond expiration-driven disablement, it would have been obvious to include an explicit deactivation command (owner/server-initiated) delivered via the app/UI: Hatton provides the manufacturer-associated mobile app and secure VCS command path (PIN/device recognition/encrypted exchanges), and Kleve provides the owner account/UI through which access is granted and can likewise be withdrawn. A POSITA would have implemented an app-triggered “disable/revoke” operation as a routine complement to the time-based disablement disclosed in Sekiyama, yielding predictable results. *See* §5(b); §5(e); EX1008, 7:11–

56, 12:46–51, 13:24–27, 15:37–41; EX1004, ¶¶[0036]–[0039], [0047], [0062]–[0063].

13. **Claim 8 – The method of claim 1, wherein the message to share and enable the e-key for the recipient device is communicated over a network, the communication enables processing by one or more servers or devices, and said one or more servers or devices include a server associated with the sharing device or the recipient device, and the server associated with the manufacturer of the vehicle.**

163. *“wherein the message to share and enable the e-key for the recipient device is communicated over a network”*: In the combined system, Sekiyama teaches that the server is “connected to a network” which is involved with the “issuance of electronic keys.” EX1005, ¶[0021]. The owner’s device likewise has “network connection functions.” *Id.*, ¶[0024]. A POSITA would therefore understand that the request for an e-key is communicated over a network. Similarly, the recipient device also has “network connection functions,” and a POSITA would have understood that the reception of the e-key is performed using those network connections. *Id.*, ¶¶[0028], [0031] (“Examples of the means of communication going from portable telephone A 10 to portable telephone B 30 include Bluetooth, ... email attachments, and the like.”).

164. In addition, as discussed above for limitation 1[a], it would have been obvious in view of Kleve for the owner and recipient device to message each other to enable the e-key. Kleve discloses that such communications are performed over

a network. Specifically, Kleve states that rental agreement terms are exchanged and agreed-to by the owner and recipient device via a “website using smart phones or a smart phone application.” EX1004, ¶[0047]. A POSITA would understand that access to a website involves network communications. *Id.* (“Acceptance may be sent back to the Owner over the wireless network.”).

165. “*the communication enables processing by one or more servers or devices*”: See Claim 5.

166. “*include a server associated with the sharing device or the recipient device*”: As discussed above for claim 1, the owner’s device (*i.e.*, *sharing device*) connects to and sends a request to a server. The server is therefore *associated* with that device.

167. “*the server associated with the manufacturer of the vehicle.*” See limitation 1[d]. As noted with respect to claim 1[d], the phrase “associated with the manufacturer of the vehicle” merely identifies the source of a server and is non-functional descriptive material not entitled to patentable weight under the printed-matter doctrine; who operates the server does not change the method’s structure or operation. In any event, a POSITA would have understood the server to be manufacturer-associated in typical deployments: Sekiyama is invented by/assigned to Toyota and describes OEM-integrated key/ECU functions (EX1005, ¶[0014]–

[0015], [0039]–[0040]), and contemporaneous art expressly teaches manufacturer-associated servers (Xiao, EX1010, 3:12–20).

- 14. Claim 9 – The method of claim 1, wherein the recipient device is identified by one or more of an email address, a phone number, a text message, a message address, a notification, a link, a web address, a social network address, or combination of two or more thereof.**

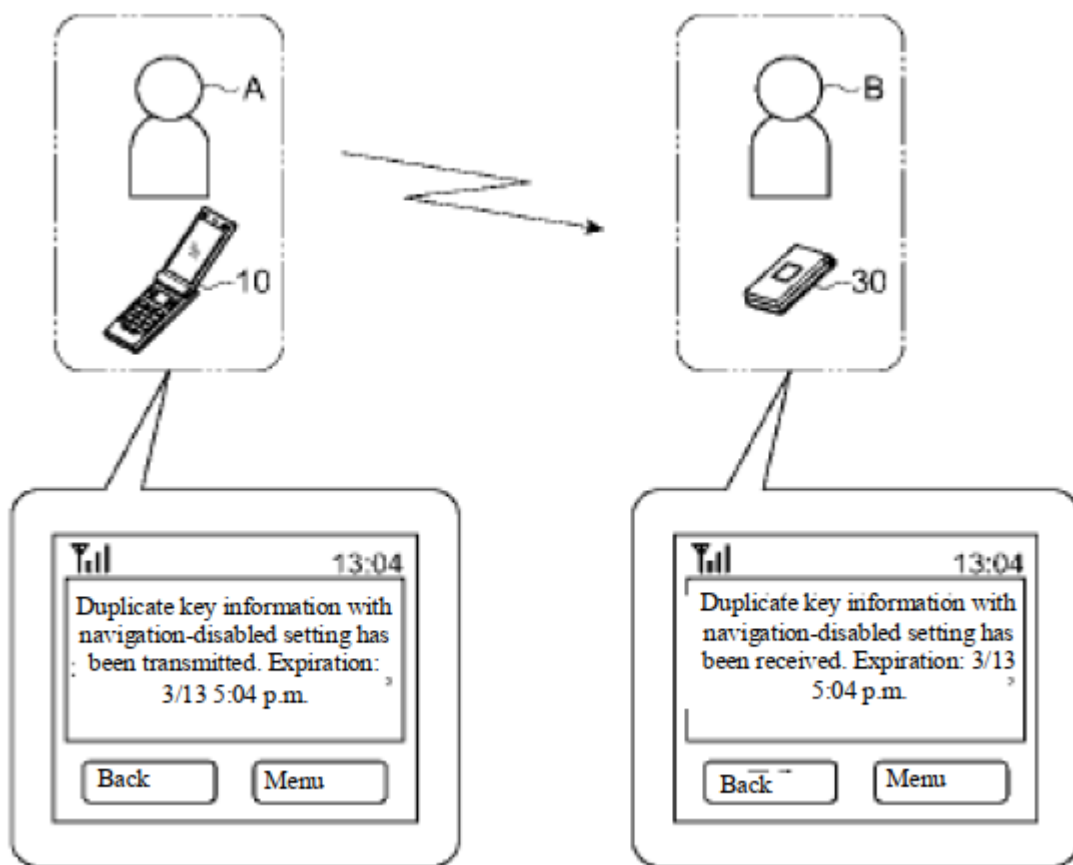
168. In the combined system, Sekiyama discloses that the *recipient device* is a “portable telephone” with “calling functions,” which a POSITA would understand is identified by a *phone number*. EX1005, ¶[0028]. In addition, the recipient device has “email sending and receiving functions” and is therefore identified by *an email address*. *Id.*

- 15. Claim 10 – The method of claim 1, wherein an application provided by a manufacturer of the vehicle includes a graphical user interface for registering the registered owner e-key for the vehicle and sharing of the e-key with one or more recipient devices.**

169. “*application provided by a manufacturer of the vehicle*”: See Claim 4.

170. “*graphical user interface for registering the registered owner e-key for the vehicle*”: See limitation 1[b]. Kleve’s “website” used to register the owner’s user profile is a *graphical user interface for registering the registered owner*. As discussed above, a POSITA would have found it obvious to combine Kleve’s user profile system with Sekiyama’s issuance of master keys to register the master key.

171. “*graphical user interface for ... sharing of the e-key with one or more recipient devices*”: Sekiyama teaches a graphical user interface for *sharing of the e-key with one or more recipient devices*. In particular, Sekiyama discloses, and depicts in Figure 2, a graphical user interface (“GUI”) “when the restricted duplicate electronic key has been transmitted from owner A to borrower B.” EX1005, ¶[0047].



172. Sekiyama also teaches that the e-key can be shared as an “email attachment,” which a POSITA would have understood involves graphical user interfaces. *See id.*, ¶[0031].

16. **Claim 11 – The method of claim 1, wherein the e-key enabled for use on the vehicle using the recipient device enables unlocking and starting the vehicle when the recipient device uses the e-key with the vehicle, and the e-key is associated with at least one privilege associated with a type of operation use of the vehicle.**

173. See Claims 2 and 3; EX1005, ¶[0049] (“[T]he subset of functions that become usable with the restricted duplicate electronic key can be set to only the function of locking/unlocking the door lock of the vehicle and the function of starting the drive source of the vehicle”). The restricted e-key can also be associated with a *at least one privilege associated with a type of operation use* such as “permission to use the on-board unit functioning as a communication device capable of sending and receiving email.” EX1005, ¶[0017] (internal quotation marks omitted). Using a vehicle to send/receive email is a privilege associated with a *type of operation use* where the vehicle operates as a communication device.

174. In addition, Klevé teaches that the owner and temporary user can agree to various *privileges associated with a type of operation use*, such as “speed, global position coordinates, or load weight restrictions.” EX1004, ¶[0040]. Klevé provides an example where the temporary user may wish to operate the vehicle to “move furniture,” and thus can agree with the owner on a privilege that defines “what can and cannot be transported.” *Id.*, ¶[0038].

**17. Claim 12**

- (a) 12[pre] – A system for enabling use and sharing of an electronic key (e-key) for a vehicle, comprising:**

175. *See* limitation 1[pre].

- (b) 12[a] – a server associated with a manufacturer of the vehicle, the server is configured to interface with an application provided by the manufacturer of the vehicle, the application provides access to data and logic for enabling sending a request to share the e-key for the vehicle with a recipient device;**

176. *“a server associated with a manufacturer of the vehicle”*: *See* limitation 1[d]. Further, I am informed that “associated with/provided by the manufacturer” merely identifies source and is non-functional descriptive material not entitled to patentable weight; who operates or supplies the server/app does not change the system’s structure or operation.

177. *“the server is configured to interface with an application provided by the manufacturer of the vehicle, the application provides access to data and logic for enabling sending a request to share the e-key for the vehicle with a recipient device”*: *See* Claim 4.

- (c) **12[b] – the request to share is configured to be initiated by a message originating from the recipient device, and responsive to the request, processing the request to securely generate the e-key;**

178. *See* limitations 1[a] and 1[c]. As discussed above for limitation 1[a], in the combined system, Sekiyama in view of Kleve renders obvious an e-key request that is initiated by communications between the owner and recipient device involving agreement to rental terms.

- (d) **12[c] – the server associated with the manufacturer of the vehicle assisting in enabling the e-key for use on the vehicle by the recipient device.**

179. *“the server associated with the manufacturer of the vehicle”*: *See* limitation 1[d]. Further, *“associated with the manufacturer”* merely identifies source and is non-functional descriptive material not entitled to patentable weight.

180. *“assisting in enabling the e-key for use on the vehicle by the recipient device”*: *see* limitation 1[c].

- 18. Claim 13 – The system of claim 12, wherein the request to share the e-key includes enabling a setting to apply a privilege level for use of the vehicle via the e-key, the privilege level provides one or more conditions of use of the vehicle via the e-key.**

181. *See* Claim 2.

- 19. Claim 14 – The system of claim 12, wherein the e-key is encrypted, and wherein encryption uses a public/private process for security.**

182. *See* Claim 6.

**20. Claim 15 – The system of claim 12, wherein the application includes a selectable option for disabling the e-key from use by the recipient device on the vehicle.**

183. *See* Claim 7.

**21. Claim 16 – The system of claim 12, wherein the e-key enabled for use on the vehicle using the recipient device enables unlocking and starting the vehicle when the recipient device uses the e-key with the vehicle, and the e-key is associated with at least one privilege associated with a type of operational use of the vehicle.**

184. *See* Claim 11.

**22. Claim 17**

**(a) 17[pre] – A method for providing access to a vehicle, comprising:**

185. *See* limitation 1[pre]. Sekiyama discloses that the restricted key *provides access to a vehicle*. EX1005, ¶[0040].

**(b) 17[a] – receiving confirmation of a sharing request being sent for an electronic key (e-key) for use of the vehicle by a recipient device, the sharing request originates responsive to a message transferred by an owner device to the recipient device;**

186. *See* limitation 1[a].

**(c) 17[b] – receiving confirmation of the sharing request from the recipient device;**

187. The '715 specification does not describe the system “receiving confirmation of the sharing request from the recipient device.” Accordingly, this limitation lacks written description and enablement support and renders claim 17

invalid under 35 U.S.C. §112(a) (*see* Ground 2). Even if PO argues that the specification need not recite hardware/protocol details, §112(a) still requires that the specification itself demonstrate possession/enablement of the claimed confirmation step; here, the specification nowhere discloses a recipient-originated confirmation returning to the system.

188. In any event, adding a recipient-side “accept/received” confirmation back to the backend/server is a routine client-server pattern that fits Sekiyama and Kleve’s architecture without changing it. Kleve already provides owner app/website interactions, permits portions of the process to execute on the phone and/or a remote server, and routes device signals via a server system. EX1004, ¶¶[0035] (processes may execute on a cellular telephone and/or a remote computing system), [0057] (server routing signals from a nomadic device), [0039], [0062]–[0063] (key generation/delivery), [0068]–[0071] (time-bounded activation/usage enforcement), [0048]–[0049] (remote credential verification). Messaging acknowledgments over communication networks (*e.g.*, app-to-server “accept” or receipt acks) were widely used and would be applied here for reliability/audit, resend/cancel flows, and coordination with time-bounded activation. A POSITA would have included such a recipient confirmation (*e.g.*, “accept invite,” “key received”) with a reasonable expectation of success using well-understood app-to-server acknowledgments.

- (d) **17[c] – processing data related to the message by a server associated with a manufacturer of the vehicle, said processing data is performed to enable the e-key for use by the recipient device on the vehicle; and**

189. See limitations 1[c] and 1[d]. The e-key request includes *data related to the message* because, as taught by Sekiyama, the request includes vehicle use restrictions/privileges, and as taught by Kleve, such restrictions and privileges are agreed to by the owner and recipient. Thus, the request includes *data related to the message*.

190. As noted with respect to limitation 1[d], “*associated with the manufacturer*” merely identifies source and is non-functional descriptive material not entitled to patentable weight. In any event, manufacturer-associated servers for e-key services were conventional (*see* limitation 1[d]).

- (e) **17[d] – enabling the e-key for use by the recipient device on the vehicle.**

191. See limitation 1[e].

- 23. Claim 18 – The method of claim 17, wherein the e-key is associated with at least one privilege associated with use of the vehicle, the at least one privilege is defined based on a setting associated with the sharing request, and wherein the recipient device is one of a smartphone, or a smartwatch, or smart glasses, or a computer, or a digital assistant, or a key fob, and wherein the e-key is unique for said sharing request and said use by said recipient device.**

192. “*the e-key is associated with at least one privilege ... defined based on a setting associated with the sharing request.*” See Claim 2.

193. “*the recipient device is one of a smartphone ... or a digital assistant*”:

In the combined system, Sekiyama teaches that the recipient device is a “portable telephone” with “email sending and receiving functions,” which at the time of the patent would have been understood to be a *smartphone or digital assistant*. EX1005, ¶[0028].

194. “*the e-key is unique for said sharing request and said use by said recipient device.*” In the combined system, Sekiyama teaches that the owner sets a unique set of restrictions that are sent with the request to generate a unique restricted key for the recipient device. *Id.*, ¶¶[0034]–[0036].

**24. Claim 19 – The method of claim 17, wherein the e-key is caused to be generated by either one of said owner device, the server, the recipient device, a computer, the vehicle, or a combination of two or more thereof.**

195. In the combined system, Sekiyama teaches that the e-key is generated by the server. *Id.*, ¶[0036]. Sekiyama also teaches that the e-key is caused to be generated by the owner device sending a request. *Id.*, ¶[0035].

**25. Claim 20 – The method of claim 17, wherein the e-key is securely generated for the recipient device, and wherein the owner device has an owner e-key that was initially generated for the owner device to enable said sharing request, and the e-key is encrypted, and wherein encryption uses a public/private process for security.**

196. In the combined system, Kleve—alone or in combination with Hatton and/or Sekiyama—discloses and/or renders this claim obvious.

197. “*the e-key is securely generated for the recipient device*” / “*the e-key is encrypted, and wherein encryption uses a public/private process for security.*”

See limitation 1[c] and Claim 6.

198. “*wherein the owner device has an owner e-key that was initially generated for the owner device to enable said sharing request.*” In the combined system, Sekiyama teaches that the owner device “functions as a master key,” *i.e.*, *owner e-key*. EX1005, ¶[0024]. This master key is *initially generated* prior to any request for a “restricted duplicate electronic key.” *Id.*, ¶[0035]. The master key enables the sharing request, because Sekiyama teaches that it is only the owner’s device operating as a master key which can request a “restricted duplicate electronic key.” *Id.* Indeed, a POSITA would understand that the “restricted duplicate electronic key” is a *duplicate* of the master key (in that it allows access to the vehicle), but a restricted version of said key.

**26. Claim 21 – The method of claim 17, wherein the e-key, once enabled, provides access to information via the recipient device regarding a level of charge of a battery of the vehicle for when the vehicle is an electric vehicle (EV).**

199. In the combined system, Sekiyama in view of Xiao renders this claim obvious. Sekiyama provides the enabled e-key sharing/use framework (*see, e.g.*, EX1005, ¶¶[0034]–[0040]). Xiao teaches that the mobile device (the recipient device) can request automobile health information including “battery charge level”

from the vehicle and receive a report transmitted back to the mobile device displaying that charge level (e.g., mobile device 110 requesting/receiving health data such as battery charge level). EX1010, 6:49–63, 7:35–55, 10:1–13, 14:3–11, 19:37–46. A POSITA would have been motivated to integrate Xiao’s telemetry/status reporting (including battery charge level) into Sekiyama’s e-key sharing framework to provide status visibility during temporary access (e.g., monitoring range/charge to coordinate use/return), auditing, and remote diagnostics in the same phone ↔ server ↔ vehicle architecture—a routine combination yielding predictable results (see §5(c); EX1005, ¶¶[0034]–[0040]; EX1010, 6:49–63. Thus, ***“the e-key, once enabled, provides access to information via the recipient device regarding a level of charge of a battery of the vehicle for when the vehicle is an electric vehicle (EV).”***

200. Further, in my opinion, applying Xiao’s “battery charge level” reporting to an EV would have been an obvious, vehicle-agnostic application: in an EV, the reported battery charge level corresponds to the traction-battery state of charge, with no change to the underlying client-vehicle communication or UI logic.

**27. Claim 22 – The method of claim 17, wherein the e-key enabled for use on the vehicle using the recipient device enables unlocking and starting the vehicle when the recipient device uses the e-key with the vehicle, and the e-key is associated with at least one privilege associated with a type of operational use of the vehicle.**

201. *See* Claims 2–3 and 11.

**28. Claim 23**

**(a) 23[pre] – A system for enabling use and sharing of an electronic key (e-key) for a vehicle, comprising:**

202. *See* limitations 1[pre] and 12[pre].

**(b) 23[a] – an onboard computer of the vehicle;**

203. In my opinion, in the combined system, Sekiyama teaches that the vehicle includes an “electronic key ECU 41” which “comprises a CPU that performs computation processing.” EX1005, ¶[0014].

- (c) **23[b] – a communications system of the vehicle interfaced with the on-board computer, the on-board computer of the vehicle having program instructions for communication with a server associated with a manufacturer of the vehicle, the server is configured to interface with an application provided by the manufacturer of the vehicle, the application provides a user interface for initiating a request to share the e-key for the vehicle with a recipient device, the request to share is configured to be initiated using a message communicated to the recipient device, and responsive to the request, processing the request to enable generation of the e-key for use on the vehicle by the recipient device.**

204. *“a communications system of the vehicle interfaced with the on-board computer, the on-board computer ... having program instructions for communication with a server”*: In my opinion, in the combined system, Sekiyama teaches that the ECU 41 “is configured to be capable of communicating with portable telephones 10, 30, as well as with a center server 20 of a management center that performs issuance of electronic keys.” *Id.*, ¶[0014].

205. *“server associated with a manufacturer of the vehicle”*: See limitation 1[d]. Furthermore, I am informed that *associated with a manufacturer* is non-functional descriptive material not entitled to patentable weight. Even if this phrase is accorded patentable weight, in my opinion, the limitation is also met—or obvious—on the merits for the reasons set out in §6(e) (see 1[d]).

206. *“the server is configured to interface with an application provided by the manufacturer of the vehicle.”* See Claim 4. Further, “provided by the manufacturer” is non-functional descriptive material for printed-matter purposes.

207. *“the application provides a user interface for initiating a request to share the e-key for the vehicle with a recipient device.”* See Claims 4 and 10.

208. *“the request to share is configured to be initiated using a message communicated to the recipient device.”* See limitation 1[a].

209. *“and responsive to the request, processing the request to enable generation of the e-key for use on the vehicle by the recipient device.”* See limitations 1[a], 1[e].

**29. Claim 24 – The system of claim 23, wherein the e-key enabled for use on the vehicle using the recipient device enables unlocking and starting the vehicle when the recipient device uses the e-key with the vehicle, and the e-key is associated with at least one privilege associated with a type of operational use of the vehicle.**

210. See Claims 2–3 and 11.

**B. Ground 2: Claims 1–11, 17–24 lack written description and enablement support**

211. I am informed that to satisfy the written description requirement under 35 U.S.C. §112, the specification must fully support the claimed subject matter and must describe an invention so as to “reasonably convey[] to those skilled in the art that the inventor had possession of the claimed subject matter as of the filing date.”

I have been informed that the purpose of the written description requirement is to ensure that a patent's claims “do[] not overreach the scope of the inventor’s contribution to the field of art as described in the patent specification.” The specification must describe the claimed features—not merely render them obvious.

**1. What the ’715 specification discloses (request to cloud/server; server-to-recipient delivery; optional notification)**

212. The specification describes a sharing flow in which a user (*e.g.*, the owner) sends a request to cloud/server infrastructure identifying the recipient and privileges; the server generates and encrypts the e-key and sends it to the recipient device; the recipient then uses the e-key with the vehicle. *See, e.g.*, EX1001, 5:11–19 (“[T]he app on the user’s mobile device can request that a message be sent to the recipient ... [with] instructions for obtaining/validating/using the e-keys.”), Figs. 26–35 (ops. 741–745) and accompanying text (cloud receives the request; generates a unique access code; encrypts with the vehicle’s public key; sends encrypted e-keys to the recipient device, which the recipient then uses with the vehicle). These passages describe an optional message/notification or link that provides instructions or launches an app/webpage to complete activation. In my opinion, they do not describe (i) a message to the recipient that causes the server to receive or process a share request, nor (ii) the system receiving acknowledgment that a sharing request was sent or receiving acknowledgment from the recipient device. To the extent the

claims require such causation or acknowledgments, in my opinion, the specification is silent on any mechanism, protocol, or architecture to implement them.

213. Against that backdrop, several claim limitations add procedural steps and causal couplings that the specification never describes. In my opinion, those new requirements lack written description in the specification. In my opinion, the absence of any teaching on how to implement these causation/acknowledgment flows would require a POSITA to devise and integrate unclaimed messaging and backend protocols without guidance.

**2. No support for “message-caused” initiation of the sharing request (claims 1 and 23 (and their dependents))**

214. Claim 1[a] requires “processing a request to share ... the request ... being received responsive to a message being sent to the recipient device from a sharing device.”

215. Claim 23[b] likewise requires that “the request to share is configured to be initiated using a message communicated to the recipient device.”

216. In my opinion, the specification never describes a message to the recipient that causes the server to receive/process the share request or that initiates the request. The only “message” described is a notification/instructional message to help the recipient obtain/activate an already-issued e-key. In my opinion, in *See* EX1001, 5:11–19, Figs. 26–35 (ops. 741–745). There is no disclosure of any causal

coupling between sending a message to the recipient and the server's receipt/processing of a share request. Accordingly, in my opinion, independent claim 1 lacks written description and enablement, and its dependent claims 2–11 fall with it. For the same reason, claim 23 (and dependent claim 24) lack §112(a) support to the extent they require initiation of the share request “using a message communicated to the recipient device.”

**3. No support for “confirmation” events (independent claim 17 and dependents)**

217. Claim 17[a] requires “receiving confirmation of a sharing request being sent” for an e-key.

218. Claim 17[b] requires “receiving confirmation of the sharing request from the recipient device.”

219. In my opinion, the written description contains no disclosure of (i) the system receiving a confirmation that a sharing request was sent, or (ii) the system receiving a confirmation from the recipient device. The depicted flow simply assumes the server sends the e-key to the recipient, with no two-way acknowledgment path and no recipient-originated confirmation back to the server. See EX1001, Figs. 26–35 (ops. 741–745) and accompanying text. Even if PO argues the specification need not recite hardware/protocol details or that known messaging systems make confirmations readily implementable by a POSITA, §112(a) still

requires that the specification itself demonstrate possession of the claimed confirmation steps; here, it nowhere discloses a recipient-originated or “request-sent” confirmation returning to the system. Accordingly, in my opinion, independent claim 17 lacks written description and enablement, and dependent claims 18–22 fall with it.

### **VIII. Secondary Considerations of Non-Obviousness**

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

221. 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.

222. 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 '715 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 '715 patent of which I am aware.

223. 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.

224. 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.

## **IX. Conclusion**

225. For the reasons set forth above, I believe claims 1-24 of the '715 patent are unpatentable in view of the prior art and claims 1-11 and 17-24 are unpatentable for lack of written description and enablement. 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.

226. 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: October 21, 2025

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