

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

---

**BEFORE THE PATENT TRIAL AND APPEAL BOARD**

---

KIA CORP.,  
TOYOTA MOTOR CORP.,  
Petitioners,

v.

EMERGING AUTOMOTIVE LLC,  
Patent Owner.

---

Case No. IPR2024-01167

U.S. Patent No. 11,738,659

---

**PETITION FOR *INTER PARTES* REVIEW  
OF U.S. PATENT NO. 11,738,659**

## TABLE OF CONTENTS

|      |                                                                                |    |
|------|--------------------------------------------------------------------------------|----|
| I.   | Introduction .....                                                             | 1  |
| II.  | Grounds .....                                                                  | 2  |
| III. | The '659 Patent .....                                                          | 2  |
| A.   | File History .....                                                             | 4  |
| B.   | Priority Date.....                                                             | 5  |
| 1.   | Legal standard .....                                                           | 7  |
| 2.   | The pre-October 2013 applications do not disclose<br>“electronic key[s]” ..... | 7  |
| IV.  | Level of Ordinary Skill .....                                                  | 8  |
| V.   | Claim Construction .....                                                       | 9  |
| VI.  | Claims 1-21 Are Unpatentable Over the Prior Art .....                          | 9  |
| A.   | Ground 1: Kleve and Hatton render obvious claims 1 and 3-21 .....              | 9  |
| 1.   | Kleve (U.S. Patent Pub. No. 2014/0129053).....                                 | 9  |
| 2.   | Hatton (U.S. Patent No. 9,002,536).....                                        | 11 |
| 3.   | Motivation to Combine.....                                                     | 12 |
| 4.   | Independent Claim 1.....                                                       | 14 |
| 5.   | Claim 3 .....                                                                  | 22 |
| 6.   | Claim 4 .....                                                                  | 23 |
| 7.   | Claim 5 .....                                                                  | 25 |
| 8.   | Claim 6 .....                                                                  | 25 |
| 9.   | Claim 7 .....                                                                  | 26 |
| 10.  | Claim 8 .....                                                                  | 26 |
| 11.  | Claim 9 .....                                                                  | 27 |

|     |                                                                                       |    |
|-----|---------------------------------------------------------------------------------------|----|
| 12. | Claim 10 .....                                                                        | 28 |
| 13. | Independent Claim 11.....                                                             | 28 |
| 14. | Claim 12 .....                                                                        | 30 |
| 15. | Claim 13 .....                                                                        | 31 |
| 16. | Claim 14 .....                                                                        | 33 |
| 17. | Claim 15 .....                                                                        | 33 |
| 18. | Claim 16 .....                                                                        | 34 |
| 19. | Claim 17 .....                                                                        | 34 |
| 20. | Independent Claim 18.....                                                             | 35 |
| 21. | Claim 19 .....                                                                        | 35 |
| 22. | Claim 20 .....                                                                        | 36 |
| 23. | Claim 21 .....                                                                        | 36 |
| B.  | Ground 2: Kleve, Hatton, and Sekiyama render obvious claim 2 .....                    | 36 |
| 1.  | Sekiyama (Japanese Laid Open Patent Application<br>Publication No. 2010-126949) ..... | 36 |
| 2.  | Motivation to Combine.....                                                            | 37 |
| 3.  | Claim 2 .....                                                                         | 38 |
| C.  | Ground 3: Mikan anticipates or renders obvious claims 1-3, 5,<br>and 8-10 .....       | 39 |
| 1.  | Mikan (U.S. Patent Pub. No. 2008/0150683).....                                        | 39 |
| 2.  | Independent Claim 1.....                                                              | 40 |
| 3.  | Claim 2 .....                                                                         | 46 |
| 4.  | Claim 3 .....                                                                         | 46 |
| 5.  | Claim 5 .....                                                                         | 47 |

|     |                                                                          |    |
|-----|--------------------------------------------------------------------------|----|
| 6.  | Claim 8 .....                                                            | 48 |
| 7.  | Claim 9 .....                                                            | 48 |
| 8.  | Claim 10 .....                                                           | 49 |
| D.  | Ground 4: Mikan and Xiao render obvious claims 4, 11-18, and 20-21 ..... | 49 |
| 1.  | Xiao (U.S. Patent No. 8,737,913).....                                    | 50 |
| 2.  | Motivation to Combine.....                                               | 50 |
| 3.  | Claim 4 .....                                                            | 52 |
| 4.  | Independent Claim 11.....                                                | 57 |
| 5.  | Claim 12 .....                                                           | 58 |
| 6.  | Claim 13 .....                                                           | 59 |
| 7.  | Claim 14 .....                                                           | 61 |
| 8.  | Claim 15 .....                                                           | 61 |
| 9.  | Claim 16 .....                                                           | 62 |
| 10. | Claim 17 .....                                                           | 62 |
| 11. | Independent Claim 18.....                                                | 62 |
| 12. | Claim 20 .....                                                           | 63 |
| 13. | Claim 21 .....                                                           | 63 |
| E.  | Ground 5: Mikan and Sekiyama render obvious claims 6-7 .....             | 63 |
| 1.  | Motivation to Combine.....                                               | 63 |
| 2.  | Claim 6 .....                                                            | 65 |
| 3.  | Claim 7 .....                                                            | 66 |
| F.  | Ground 6: Mikan, Xiao, and Sekiyama render obvious claim 19.....         | 67 |
| 1.  | Motivation to Combine.....                                               | 67 |

|       |                                                                   |    |
|-------|-------------------------------------------------------------------|----|
| 2.    | Claim 19 .....                                                    | 67 |
| VII.  | The Board Should Not Exercise Discretion to Deny Institution..... | 68 |
| A.    | <i>Fintiv</i> Factors .....                                       | 68 |
| B.    | 35 U.S.C. §325(d) .....                                           | 70 |
| VIII. | Standing .....                                                    | 71 |
| IX.   | Mandatory Notices.....                                            | 71 |
| A.    | Real Party-in-Interest Under 37 C.F.R. §42.8(b)(1) .....          | 71 |
| B.    | Related Matters Under 37 C.F.R. §42.8(b)(2) .....                 | 71 |
| C.    | Lead and Back-Up Counsel Under 37 C.F.R. §42.8(b)(3) .....        | 75 |
| D.    | Payment of Fees.....                                              | 76 |

## LIST OF EXHIBITS

| <b>Exhibit</b> | <b>Description</b>                                                            |
|----------------|-------------------------------------------------------------------------------|
| Ex. 1001       | U.S. Patent No. 11,738,659 to <i>Penilla</i> et al.                           |
| Ex. 1002       | Prosecution File History for U.S. Patent No. 11,738,659.                      |
| Ex. 1003       | Curriculum Vitae of Dr. Kevin Almeroth.                                       |
| Ex. 1004       | Declaration of Dr. Kevin Almeroth.                                            |
| Ex. 1005       | U.S. Patent Pub. No. 2014/0129053 to Kleve et al.                             |
| Ex. 1006       | Japanese Laid Open Patent Application Publication No. 2010-126949 to Sekiyama |

| <b>Exhibit</b> | <b>Description</b>                                                                                                              |
|----------------|---------------------------------------------------------------------------------------------------------------------------------|
| Ex. 1007       | U.S. Patent Pub. No. 2008/0150683 to Mikan et al.                                                                               |
| Ex. 1008       | U.S. Patent No. 9,002,536 to Hatton                                                                                             |
| Ex. 1009       | U.S. Patent No. 7,868,736 to Fukushima et al.                                                                                   |
| Ex. 1010       | U.S. Patent No. 8,737,913 to Xiao et al.                                                                                        |
| Ex. 1011       | U.S. Patent Application No. 61/478,436                                                                                          |
| Ex. 1012       | U.S. Patent Application No. 61/745,729                                                                                          |
| Ex. 1013       | U.S. Patent Application No. 13/452,882                                                                                          |
| Ex. 1014       | U.S. Patent Application No. 13/842,158                                                                                          |
| Ex. 1015       | U.S. Patent Application No. 14/063,638                                                                                          |
| Ex. 1016       | U.S. Patent Application No. 15/344,566                                                                                          |
| Ex. 1017       | U.S. Patent Application No. 15/180,306                                                                                          |
| Ex. 1018       | U.S. Patent Application No. 14/303,442                                                                                          |
| Ex. 1019       | U.S. Patent Application No. 16/653,958                                                                                          |
| Ex. 1020       | U.S. Patent Application No. 15/854,241                                                                                          |
| Ex. 1021       | U.S. Patent Application No. 15/607,418                                                                                          |
| Ex. 1022       | Text Comparison of U.S. Pat. App. No. 13/842,158 to U.S. Pat. App. No. 14/063,638                                               |
| Ex. 1023       | Order Granting Request For Ex Parte Reexamination, Reexamination Control No. 90/019,456, Patent No. 11,738,659 (April 15, 2024) |
| Ex. 1024       | Docket Control Order in <i>Emerging Automotive LLC v. Kia Corp.</i> , No. 2:23-CV-00437-JRG (E.D. Tex.) (Feb. 6, 2024)          |

### LIST OF CHALLENGED CLAIMS

| <b>Claim</b> | <b>Limitation</b>                                                                                                                                                                                                                                                                                            |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1[pre]       | A sub-system of a vehicle, the vehicle having an on-board computer interfaced with the sub-system for processing instructions to enable use of an electronic key (eKey), the sub-system comprising:                                                                                                          |
| 1[a]         | memory associated with the on-board computer of the vehicle having program instructions for instructing unlocking and starting of the vehicle; and                                                                                                                                                           |
| 1[b]         | communications circuitry of the vehicle interfaced with the on-board computer of the vehicle and the sub-system, the communications circuitry is configured to process program instructions to enable communication with a server,                                                                           |
| 1[c]         | the communications circuitry includes wireless communication circuitry for enabling local connection with a mobile device, the mobile device is configured to use the eKey for said unlocking and said starting the vehicle;                                                                                 |
| 1[d]         | wherein the wireless communications circuitry of the vehicle is configured to receive coded data from the mobile device when using the eKey, the coded data enables functions of said eKey for said unlocking and use of the vehicle, the coded data is associated to the eKey for use by the mobile device, |
| 1[e]         | and the coded data includes privilege settings associated with the eKey for limiting types of use of the vehicle when using the eKey with the vehicle;                                                                                                                                                       |
| 1[f]         | wherein use of the vehicle using the eKey is tracked to identify and log actions taken using the vehicle while the eKey is used.                                                                                                                                                                             |
|              |                                                                                                                                                                                                                                                                                                              |
| 2            | The sub-system of the vehicle of claim 1, wherein said privileges function as restrictions that enable access to specific                                                                                                                                                                                    |

| <b>Claim</b> | <b>Limitation</b>                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              | vehicle areas that include one or more of vehicle door operation, or trunk operation.                                                                                                                                                                                                                                                                                                                                                                         |
|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 3            | The sub-system of the vehicle of claim 1, wherein the vehicle is configured to receive or securely store information from the server to perform authentication or verification that the coded data received from the mobile device should activate the eKey.                                                                                                                                                                                                  |
|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 4            | The sub-system of the vehicle of claim 1, wherein the communications circuitry of the vehicle is configured to receive one or more additional requests from other mobile devices to use the vehicle, each request is associated with coded data generated by the server, such that each coded data is associated with a user account having privileges assigned by an administrator of the vehicle that enables assigning or use of eKeys to use the vehicle. |
|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 5            | The sub-system of the vehicle of claim 1, wherein the wireless communication circuitry is associated with an NFC standard or a radio frequency standard for said local connection between the mobile device and the vehicle.                                                                                                                                                                                                                                  |
|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 6            | The sub-system of the vehicle of claim 1, wherein an application associated with said mobile device is configured to enable sharing of said eKey with a recipient user having a recipient mobile device, the sharing is enabled via a message initiated from said mobile device.                                                                                                                                                                              |
|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 7            | The sub-system of the vehicle of claim 1, wherein the coded data is processed securely by the mobile device responsive to                                                                                                                                                                                                                                                                                                                                     |

| <b>Claim</b> | <b>Limitation</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              | registering the e-Key to the mobile device, the registering being enabled by an owner of said vehicle or an administrator of said vehicle.                                                                                                                                                                                                                                                                                                                                                                                                               |
|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 8            | The sub-system of the vehicle of claim 1, wherein a mode of allowed use of the vehicle using the eKey is configured to monitor said use of the vehicle, and said on-board computer is configured to transmit one or more notifications when a violation of a restriction is detected.                                                                                                                                                                                                                                                                    |
|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 9            | The sub-system of the vehicle of claim 1, wherein the tracked use of the vehicle is configured to identify a violation, and the violation is associated with one or more of driving too fast, or driving out of an area, or accelerating too fast, or stopping too fast, or parking too close to a structure or other vehicle, or coming in contact with a structure or another vehicle, or slamming a door of the vehicle, or turning on a radio, or texting while driving, or interfacing with vehicle controls while driving, or two or more thereof. |
|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 10           | The sub-system of the vehicle of claim 1, wherein the tracked use of the vehicle is configured to identify a violation, and the violation is associated with exceeding a speed limit, or time limit, or an area limit.                                                                                                                                                                                                                                                                                                                                   |
|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 11[pre]      | A system of a vehicle, the vehicle having an on-board computer for processing and communicating with the system for use of an electronic key (eKey), the system comprising:                                                                                                                                                                                                                                                                                                                                                                              |
| 11[a]        | memory associated with the on-board computer of the vehicle having program instructions for controlling unlocking and starting of the vehicle; and                                                                                                                                                                                                                                                                                                                                                                                                       |

| <b>Claim</b> | <b>Limitation</b>                                                                                                                                                                                                                                                           |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11[b]        | communications circuitry of the vehicle interfaced with the on-board computer of the vehicle,                                                                                                                                                                               |
| 11[c]        | the communications circuitry includes wireless communication circuitry for enabling local connection with a mobile device, the mobile device is configured to use the eKey for said unlocking and said starting of the vehicle;                                             |
| 11[d]        | wherein the wireless communications circuitry of the vehicle is configured to receive coded data from the mobile device, the coded data is unique for said eKey,                                                                                                            |
| 11[e]        | and the coded data includes privilege settings set for limiting types of use of the vehicle when using the vehicle via the eKey;                                                                                                                                            |
| 11[f]        | wherein the eKey is associated with a user account, the user account is accessible via a user interface of an application executed by the mobile device, the eKey when active enables said unlocking of the vehicle and said starting of the vehicle.                       |
|              |                                                                                                                                                                                                                                                                             |
| 12           | The system of a vehicle as recited in claim 11, wherein a server is configured for communication with the application executed by the mobile device, the server is one of a plurality of servers, and one of said servers is associated with a manufacturer of the vehicle. |
|              |                                                                                                                                                                                                                                                                             |
| 13[a]        | The system of a vehicle as recited in claim 11, wherein the eKey is securely generated on the mobile device, and                                                                                                                                                            |
| 13[b]        | wherein a server associated with a manufacturer of the vehicle is configured to communicate with the application, the application further being associated with a manufacturer of the vehicle.                                                                              |
|              |                                                                                                                                                                                                                                                                             |

| <b>Claim</b> | <b>Limitation</b>                                                                                                                                                                                                               |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 14           | The system of a vehicle as recited in claim 11, wherein said on-board computer includes logic for processing encryption operations of said eKey in coordination with logic of said mobile device.                               |
|              |                                                                                                                                                                                                                                 |
| 15           | The system of a vehicle as recited in claim 14, wherein said encryption operations use secure public/private key pair encryption operations.                                                                                    |
|              |                                                                                                                                                                                                                                 |
| 16           | The system of a vehicle as recited in claim 11, wherein said wireless communication circuitry facilitates one or more of Bluetooth, near field communication (NFC), WiFi, or radio communication.                               |
|              |                                                                                                                                                                                                                                 |
| 17           | The system of a vehicle as recited in claim 11, wherein said eKey is validated and securely bound to the mobile device to prevent unauthorized transfers of the ekey.                                                           |
|              |                                                                                                                                                                                                                                 |
| 18[pre]      | A vehicle having an on-board computer for processing and communicating an electronic key (eKey), the vehicle comprising:                                                                                                        |
| 18[a]        | memory associated with the on-board computer of the vehicle having program instructions for controlling unlocking and starting of the vehicle; and                                                                              |
| 18[b]        | communications circuitry of the vehicle interfaced with the on-board computer of the vehicle,                                                                                                                                   |
| 18[c]        | the communications circuitry includes wireless communication circuitry for enabling local connection with a mobile device, the mobile device is configured to use the eKey for said unlocking and said starting of the vehicle; |

| <b>Claim</b> | <b>Limitation</b>                                                                                                                                                                                                                                                                                                       |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 18[d]        | wherein the wireless communications circuitry of the vehicle is configured to receive coded data from the mobile device, the coded data is unique for said eKey to be used via the mobile device, and                                                                                                                   |
| 18[e]        | the coded data includes privilege settings for use of the vehicle when using the eKey with the vehicle;                                                                                                                                                                                                                 |
| 18[f]        | wherein the eKey is associated with a user account, the user account is accessible via a user interface of an application executed by the mobile device, the eKey when active enables said unlocking of the vehicle and said starting of the vehicle.                                                                   |
|              |                                                                                                                                                                                                                                                                                                                         |
| 19           | The vehicle of claim 18, wherein the privilege settings being unrestricted for an owner of the vehicle and restricted for a shared user of the vehicle, the shared user of the vehicle receives a shared eKey responsive to said owner of the vehicle causing the shared eKey to be sent for shared use of the vehicle. |
|              |                                                                                                                                                                                                                                                                                                                         |
| 20[a]        | The vehicle of claim 18, wherein the eKey is securely generated on the mobile device, and                                                                                                                                                                                                                               |
| 20[b]        | wherein a server associated with a manufacturer of the vehicle is configured to communicate with the application, the application further being associated with a manufacturer of the vehicle.                                                                                                                          |
|              |                                                                                                                                                                                                                                                                                                                         |
| 21           | The vehicle of claim 18, wherein encryption operations are associated with use of said eKey, and said encryption operations use public/private key pair encryption, and wherein said wireless communication circuitry uses one or                                                                                       |

| Claim | Limitation                                                                             |
|-------|----------------------------------------------------------------------------------------|
|       | more of Bluetooth, or near field communication (NFC), or WiFi, or radio communication. |

## **I. INTRODUCTION**

The '659 patent relates to vehicle access using electronic keys that allow an owner to monitor the use of the vehicle. It discloses that “access [to the vehicle] can be by way of electronic keys (*e.g.*, e-keys), which can be sent by a vehicle owner/admin to some person or entity.” EX1001, 6:1-3. For example, “the user-owner of the vehicle can assign a valet with access to the vehicle by going on an application (App or website) on a computing device (*e.g.*, mobile or non-mobile device), identifying the recipient, identifying a mode for communicating with the recipient (*e.g.*, text, email, message, notification, etc.), selecting the amount of privileges (*e.g.*, what type of access, speed limits, geographic restrictions, amount of time the e-keys will be valid (or else expire)), and requesting that e-keys be sent to the recipient.” *Id.*, 6:3-12. A “history database” may “include information regarding the use of the vehicle when the vehicle was controlled under a specific user account.” *Id.*, 39:5-9.

But such vehicle access and monitoring systems were prolific by the earliest priority date to which the '659 patent is potentially entitled, October 25, 2013. For example, Kleve and Hatton, relied upon in Grounds 1 and 2, are both Ford patents that describe the same or a substantially similar system in which owners and renters create website accounts for short-term vehicle rentals using “virtual keys,” which enable the owners to place use restrictions (*e.g.*, speed, position, load weight) and monitor the restricted parameters—thereby rendering obvious the purported

invention of the '659 patent.

Similarly, Mikan and Xiao, relied upon in Grounds 3-6, both relate to systems for securely operating a vehicle using an electronic key embedded in a wireless device (*e.g.*, a mobile phone). Mikan's system enables generation of a limited-functionality secondary electronic key restricting access to certain functionalities and modes of operation, and allows the owner to monitor vehicle use (*e.g.*, based on location or speed). Xiao additionally discloses associating electronic keys with user profiles, applicable to claims 11-21. Mikan thus anticipates several of the challenged claims, and renders obvious the remaining claims in combination with Xiao.

## **II. GROUNDS**

Petitioners request review and cancellation of the challenged claims based on the following grounds.

| <b>Ground</b> | <b>Basis</b> | <b>Reference(s)</b>     | <b>Claims</b>   |
|---------------|--------------|-------------------------|-----------------|
| 1             | 103          | Kleve, Hatton           | 1, 3-21         |
| 2             | 103          | Kleve, Hatton, Sekiyama | 2               |
| 3             | 102/103      | Mikan                   | 1-3, 5, 8-10    |
| 4             | 103          | Mikan, Xiao             | 4, 11-18, 20-21 |
| 5             | 103          | Mikan, Sekiyama         | 6-7             |
| 6             | 103          | Mikan, Xiao, Sekiyama   | 19              |

## **III. THE '659 PATENT**

The '659 patent describes vehicle electronics operating in conjunction with cloud services to provide vehicle access using a mobile device as an electronic key. EX1001, Abstract, 12:28-30, 22:44-49. The vehicle owner may generate and assign

electronic keys, each associated with a unique encrypted code, to different users. *Id.*, 43:37-39, 43:52-58, 44:53-57, Fig. 29.

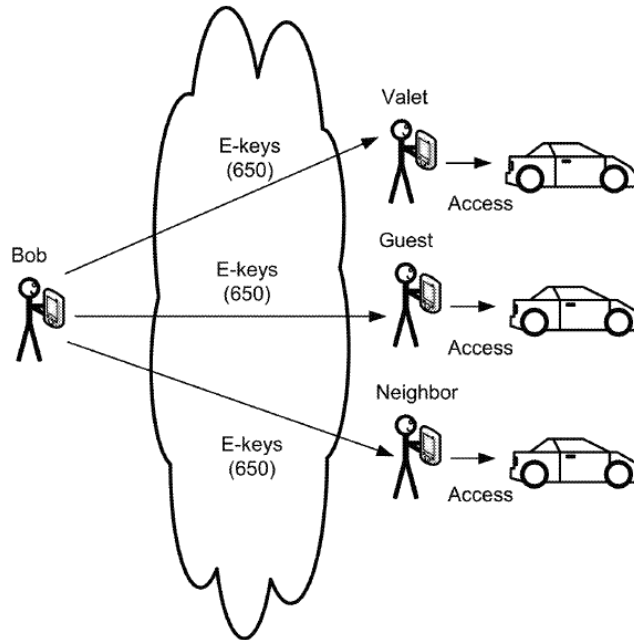
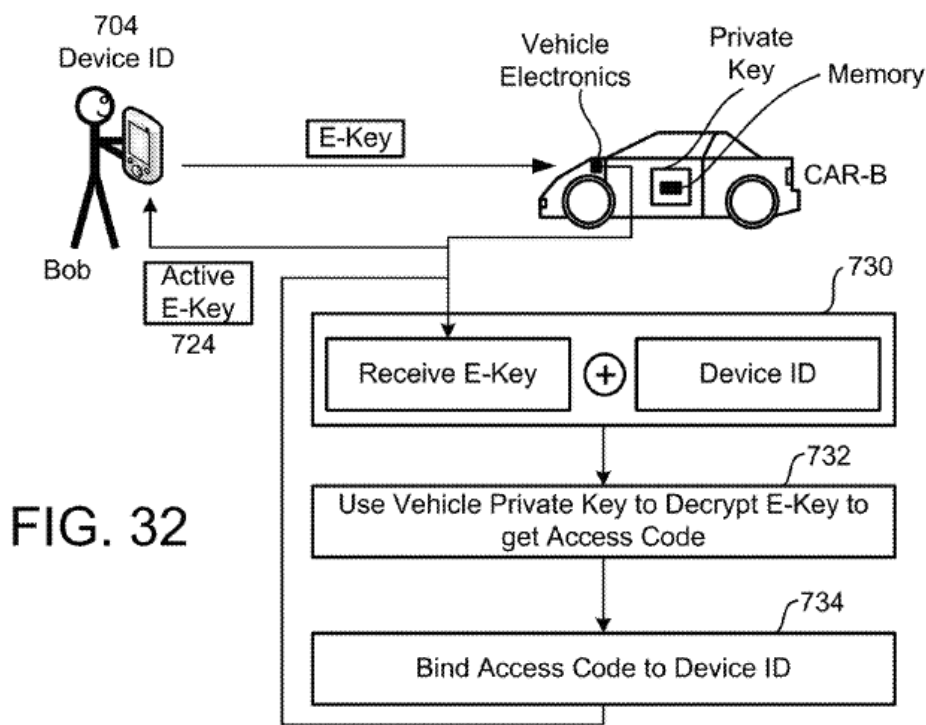


FIG. 29

Each electronic key may then be associated with the recipient's mobile device and used to access the vehicle, using a private key stored in the vehicle to decrypt and activate the electronic key. *Id.*, 44:63-45:27, Fig. 32.



Electronic keys may also have different “privileges” that determine, *e.g.*, the “type of access, speed limits, geographic restrictions, [and] amount of time the e-keys will be valid.” *Id.*, 44:39-48, 45:27-29.

#### A. File History

The application leading to the ’659 patent was filed August 30, 2021, as the latest in a long string of applications beginning with a provisional application on April 22, 2011. EX1002, 62-63. One of the two inventors, Mr. Albert Penilla, was also the prosecuting attorney. *Id.*, 7, 11.

The Examiner initially rejected all claims based primarily on U.S. Patent Pub. 2011/0112969 (“Zaid”). *Id.*, 178-196. Applicant amended the independent claims to require the “coded data” for the electronic key include “privilege settings” that

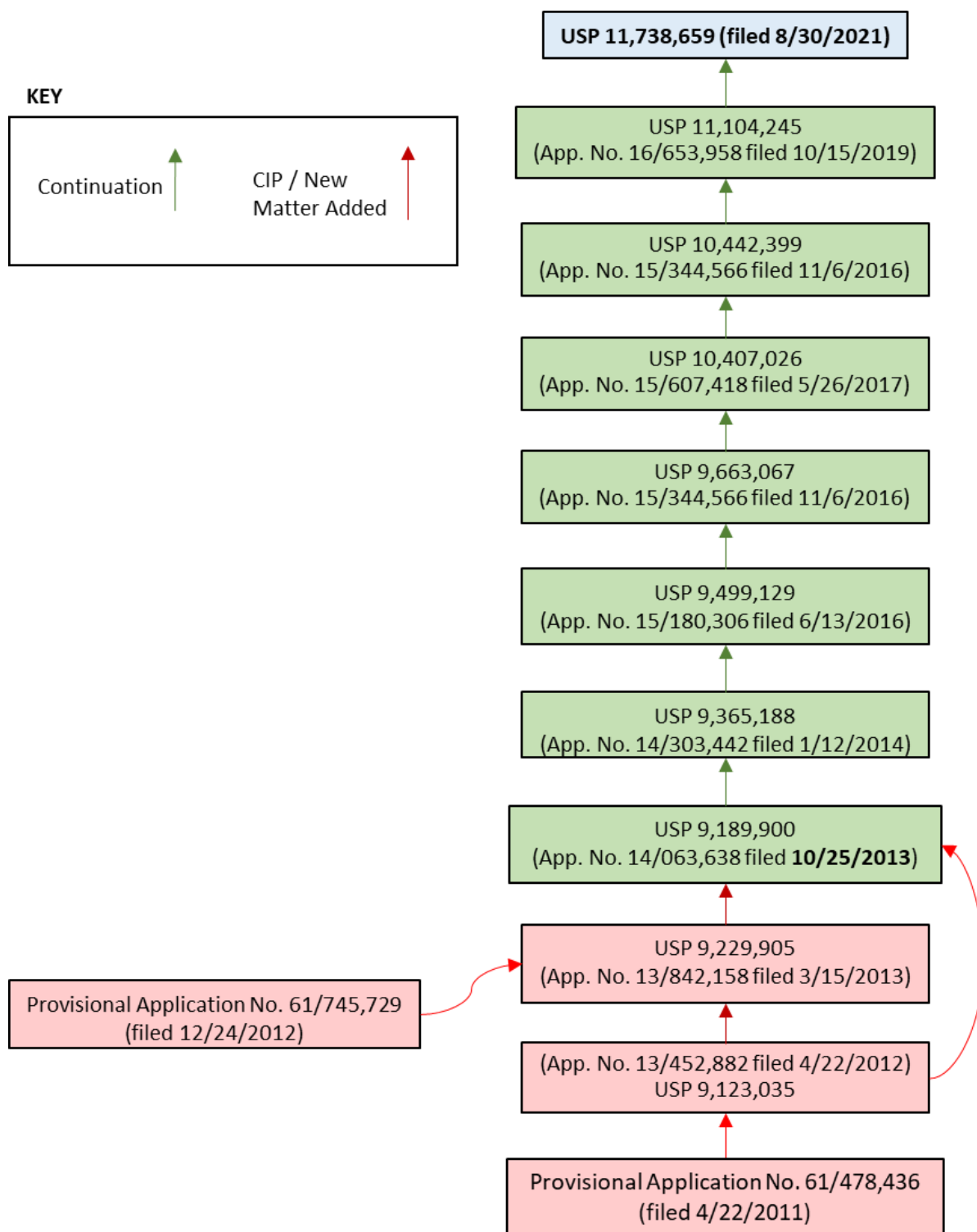
“limit[] types of use of the vehicle.” *Id.*, 333-338. Applicant argued Zaid’s electronic key only “control[s] the ‘time’ for the reservation” and otherwise provides “unlimited” vehicle use. *Id.*, 339.

The Examiner then rejected the amended claims based on Zaid in combination with U.S. Patent Pub. No. 2005/0203752 (“Shinada”), noting Shinada teaches “restrictions to limit the usage of the vehicle.” *Id.*, 352. In response, Applicant argued that Shinada is “not related to what is claimed” because its electronic key is not used by a mobile device, and its restrictions on use are defined in a rental contract. *Id.*, 511-512. But Applicant did not explain why a POSITA would not or could not have applied Shinada’s restrictions on use to Zaid’s electronic key system. *See id.* Applicant also amended the claims to recite “wireless communication circuitry” and using the mobile device to unlock and start the vehicle, and argued that these limitations are not taught by Zaid and Shinada. *Id.*, 504-510, 512. Applicant did not address Zaid’s disclosures—cited by the Examiner—of a “wireless communication device” that allows “opening the vehicle door, and/or allowing engine to be turned on by user.” *Id.*, 350 (quoting Zaid). Nevertheless, the Examiner issued a notice of allowance in response to the amendment. *Id.*, 519-522.

## **B. Priority Date**

The ’659 patent claims priority to several applications, illustrated below.

*Inter Partes Review*  
U.S. Patent No. 11,738,659



The '638 application, a continuation-in-part filed on October 25, 2013, first introduces the description of “e-keys.” Accordingly, the '659 patent claims, which

all recite electronic keys, are not entitled to a filing date before October 25, 2013. Kleve and Hatton (relied upon in Ground 1) are prior art under the October 25, 2013 priority date. Sekiyama, Mikan, and Xiao (relied upon in Grounds 2-6) are prior art even under the earliest provisional application to which the '659 patent purports to claim priority.

### **1. Legal standard**

A claim is only entitled to the benefit of an earlier filed U.S. application if the earlier filed application discloses the subject matter of the claims. 35 U.S.C. §120; *see also D Three Enters., LLC v. SunModo Corp.*, 890 F.3d 1042, 1046-47 (Fed. Cir. 2018). To satisfy that requirement, the earlier filed application must “reasonably convey[] to those skilled in the art that the inventor had possession of” the claimed subject matter. *Ariad Pharms., Inc. v. Eli Lilly & Co.*, 598 F.3d 1336, 1351 (Fed. Cir. 2010). Evaluation of adequate written description “requires an objective inquiry into the four corners of the specification from the perspective of a person of ordinary skill in the art.” *Id.* A description cannot “merely render[] the invention obvious.” *Id.*, 1352.

### **2. The pre-October 2013 applications do not disclose “electronic key[s]”**

The claims recite systems for requesting, generating, transmitting and using electronic keys (“eKeys”) for vehicle access. However, none of the earlier applications disclose “eKeys” or anything similar to an eKey.

The '638 Application, filed October 25, 2013, introduced a significant amount of new material directed to e-keys. EX1022; EX1004, ¶¶70-75. For example, Figures 17-35 and their descriptions discuss the requesting, generating, transmission, and use of e-keys. EX1015, 105, 122-28; EX1004, ¶¶72.

The earlier applications did not include these disclosures, or any other disclosures relating to eKeys, and a POSITA would have understood that control of the vehicles in these applications did not use eKeys. EX1004, ¶¶75. 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. EX1014, Abstract. The '882 Application and provisionals are directed to electric vehicle charging. EX1013, Abstract; EX1011-EX1012. Thus, a POSITA would not have considered the Applicant to be in possession of the claimed subject matter. EX1004, ¶¶79.

In granting a recent third-party *ex parte* reexamination request, the Patent Office considered the priority date of the '659 Patent. Specifically, the Patent Office determined that the '436 Provisional Application “appears to lack support for several limitations ... includ[ing] for example an ‘eKey’.” EX1023, 4 n.1. Petitioners agree.

#### **IV. LEVEL OF ORDINARY SKILL**

A POSITA would have had at least a four-year undergraduate degree in electrical engineering, automotive engineering, or a closely related field and at least two years of experience in the field of access control systems, vehicle electronics,

and/or cryptography. More education can supplement practical experience and vice versa. EX1004, ¶85. Petitioners' expert exceeded this by 2013. *Id.* ¶6.

## **V. CLAIM CONSTRUCTION**

Claims only need to be construed to the extent necessary to resolve a controversy. No terms need construction because the claims read on the prior art identified below under any construction consistent with *Phillips*. The claim terms should thus be given their plain and ordinary meaning under *Phillips*. EX1004, ¶¶89-90.

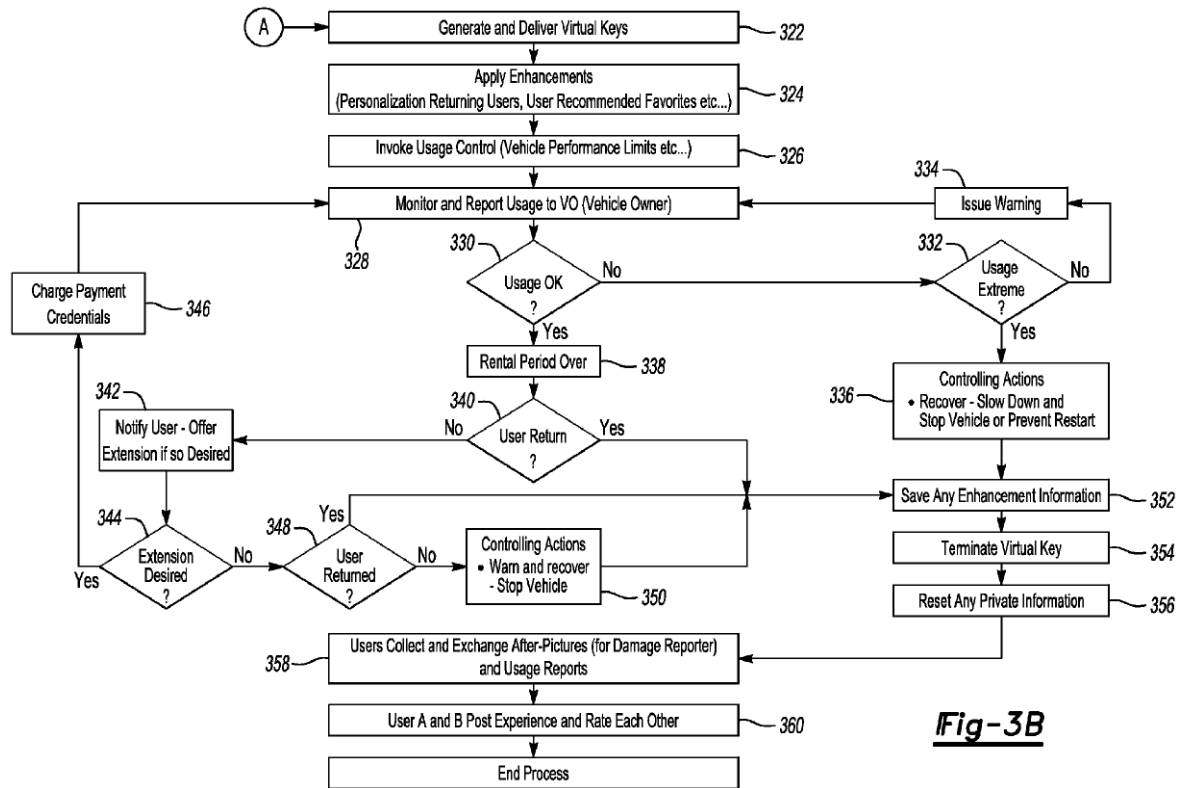
## **VI. CLAIMS 1-21 ARE UNPATENTABLE OVER THE PRIOR ART**

### **A. Ground 1: Kleve and Hatton render obvious claims 1 and 3-21**

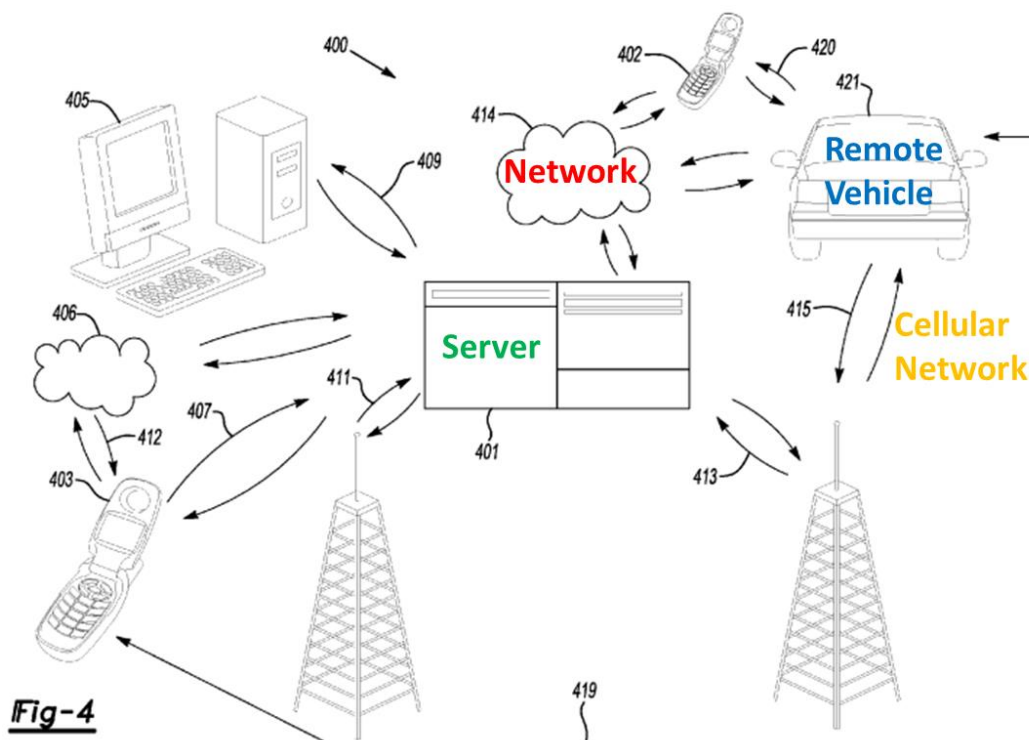
#### **1. Kleve (U.S. Patent Pub. No. 2014/0129053)**

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

Kleve is a Ford patent directed to a rental car system where vehicle owners and temporary users create website accounts for short-term vehicle rentals. EX1005, Abstract, [0036], [0056]. Once rental terms are agreed to, a server may transmit a “virtual key” to the temporary user’s mobile device, which can be used to unlock and operate the vehicle. *Id.*, [0036]-[0049], Fig. 3B.



Kleve's vehicle includes a "vehicle computing system" that communicates wirelessly with a "server," either directly or via a user's mobile device (*e.g.*, using a Bluetooth connection to the user's mobile device to access a wireless network), as illustrated in Figure 4, annotated below. EX1005, [0035], [0057], [0060].



The vehicle owner may impose restrictions on usage (*e.g.*, based on speed or location). EX1005, [0040]. Kleve's system then monitors the vehicle while it is in use by the temporary user and notifies the owner if restrictions are violated. *Id.*, [0051]-[0052].

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

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

Hatton is another Ford patent that describes an “electronic key system and a vehicle computing system for managing a vehicle electronic key.” EX1008, 1:6-8. Hatton discloses the same vehicle computing system as used by Kleve. *Compare* EX1005, Fig. 1, *with* EX1008, Fig. 1. Hatton teaches that a “mobile device 124 may

be configured using a software application to communicate with the VCS,” using encrypted data to control the vehicle. EX1008, 7:11-45. Hatton also teaches that the encrypted data may be used to securely generate an electronic key on the mobile device, such as by a user “typing a pin number on the [software] application [on the mobile device],” and associating the pin number “as the primary or secondary key.” EX1008, 15:37-41. The virtual key and encrypted data can then be communicated between the mobile device and the VCS using “wireless communication technologies.” *Id.*, 7:56-60.

### **3. Motivation to Combine**

A POSITA would have been motivated to apply Hatton’s teachings to Kleve’s rental car system and would have had a reasonable expectation of success. EX1004, ¶¶109-115.

Kleve, Hatton, and the ’659 patent are all analogous art because they are directed to the same field of electronic key systems. *See* EX1001, Abstract; EX1005, [0044]-[0045]; EX1008, 1:6-8; EX1004, ¶115.

There were well-known benefits of using encrypted data for wireless communications. EX1004, ¶110. Wireless communications (*e.g.*, Bluetooth and WiFi) that send messages over radio waves may be intercepted by unauthorized third parties. Encrypted communications ensure that only an authorized receiver can view the contents of the messages. For electronic key systems, encrypted communications would be particularly effective to prevent unauthorized access to the vehicle.

Associating encrypted data with specific electronic keys would further facilitate an owner's monitoring and control of vehicle use by individual users.

Enabling the mobile device to securely generate and communicate encrypted data associated with a virtual key, and to include use restrictions within the encrypted data, would have also simplified and facilitated use of the virtual key for end users, while protecting an owner's control over vehicle access and use. EX1004, ¶¶110-112. Using a mobile device to securely generate the virtual key and send it as encrypted data directly to the vehicle enables an owner or temporary user to distribute, activate, and use a virtual key even when the vehicle and mobile device cannot connect to a remote server (*e.g.*, in areas with poor cell or wireless reception), and without the need for additional hardware or manual identity verification by the user. And by encrypting both the virtual key and use restriction information, a temporary user cannot tamper with the system to circumvent use restrictions, or grant unauthorized access to third parties. A POSITA would have also been motivated to bind the virtual key to the receiving user's mobile device (*e.g.*, by associating the virtual key with an identifier unique to the mobile device) to prevent unauthorized distribution to third parties. *Id.*, ¶111.

A POSITA would have been particularly motivated to look to Hatton's teachings to improve Kleve because both Kleve and Hatton are Ford references directed to similar electronic key systems for use in a vehicle. EX1004, ¶113. For example, both Kleve and Hatton describe an identical architecture for a computing

system within a vehicle (the “VCS” in both references) and a “vehicle rental” business using that system. EX1005, [0021]-[0036], Fig. 1; EX1008, 2:54-5:53, Fig. 1.

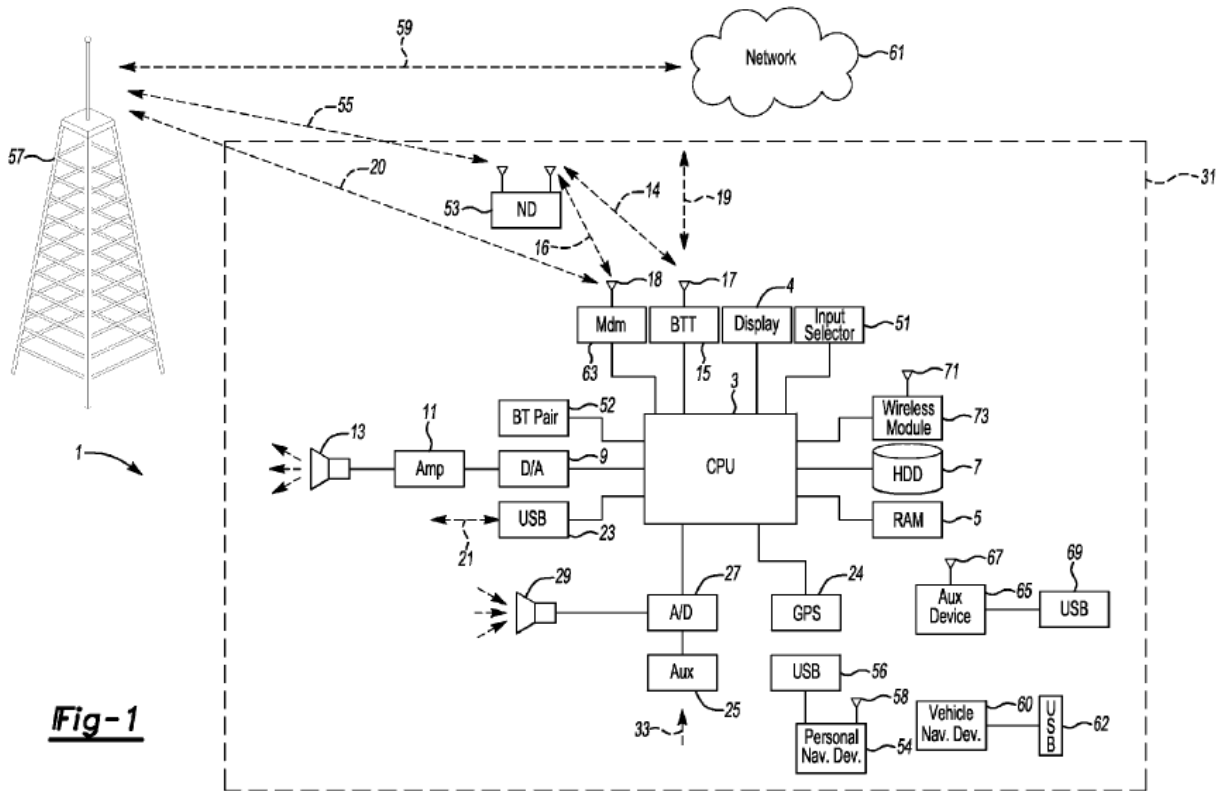
Finally, a POSITA would have had a reasonable expectation of success in apply Hatton’s teachings relating to encryption in Kleve’s system Kleve already uses its wireless communications circuitry for encrypted communications (*e.g.*, with a server). EX1005, [0063]. Configuring the wireless communications circuitry to additionally receive encrypted messages associated with a virtual key and including use restriction information directly from a mobile device would have been a straightforward and routine application of well-known techniques in wireless communications and encryption. EX1004, ¶114. Further, it would have been obvious to a POSITA to use one of several standard, well-known encryption techniques (such as public/private key encryption) to implement the encryption schemes described by Kleve and Hatton, and a POSITA would have been capable of implementing such encryption techniques within those systems. *Id.*

#### **4. Independent Claim 1**

##### **1[pre]**

To the extent the preamble is limiting, Kleve discloses it. EX1004, ¶¶116-119.

Kleve discloses a vehicle computing system (“VCS,” depicted below in Fig. 1). EX1005, [0021]-[0022], [0071], Fig. 1.

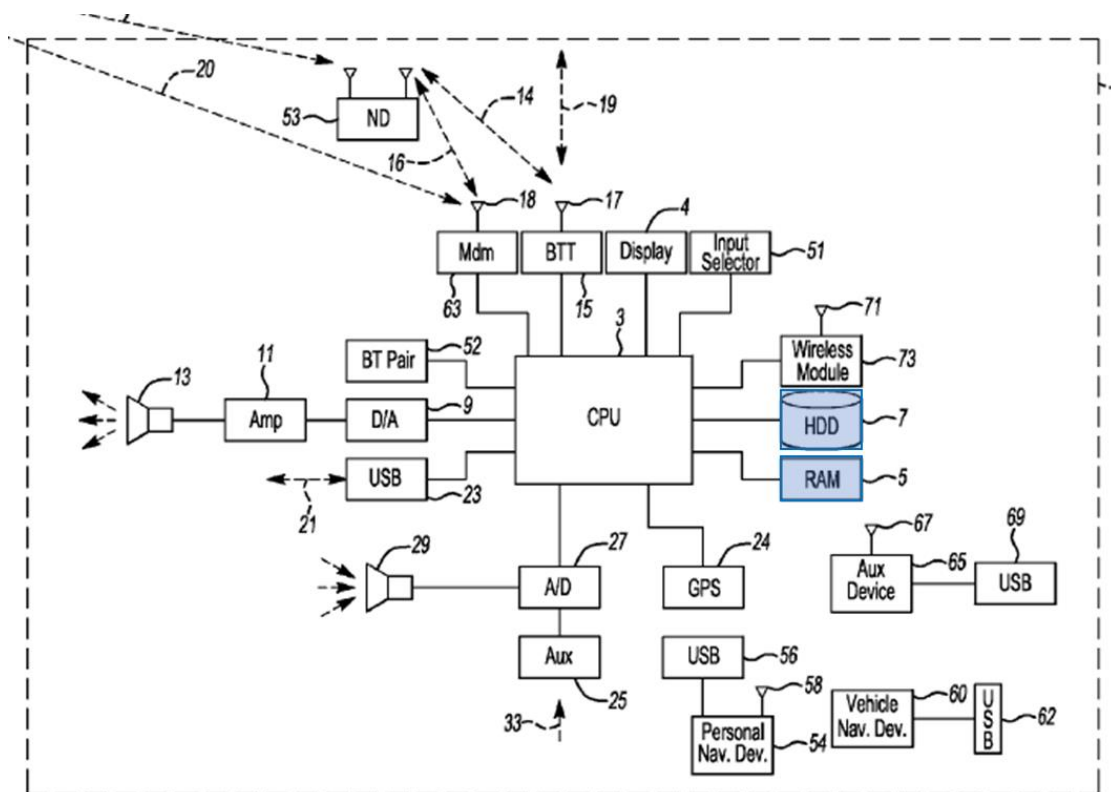


Kleve's VCS comprises "a processor 3" "[p]rovided within the vehicle" (i.e., an **on-board computer**) that "controls at least some portion of the operation of the vehicle-based computing system" and "allows onboard processing of commands and routines." *Id.*, [0022]; *see also id.*, [0035]. The VCS interfaces with "numerous of the vehicle components and auxiliary components [i.e., **sub-systems of the vehicle**]" via a vehicle network. *Id.*, [0023].

Kleve discloses that the VCS and its processor enable the use of a "virtual key." EX1005, [0039] ("The virtual key may also be sent to the vehicle configuring the VCS to enable the keyless drive system for the appropriate Temporary User during a given rental period."), [0048], [0063], [0067], [0071]-[0074].

**1[a]**

Kleve discloses memory associated with the VCS processor. See EX1005, Fig. 1 (annotated below); EX1004, ¶¶120-123.

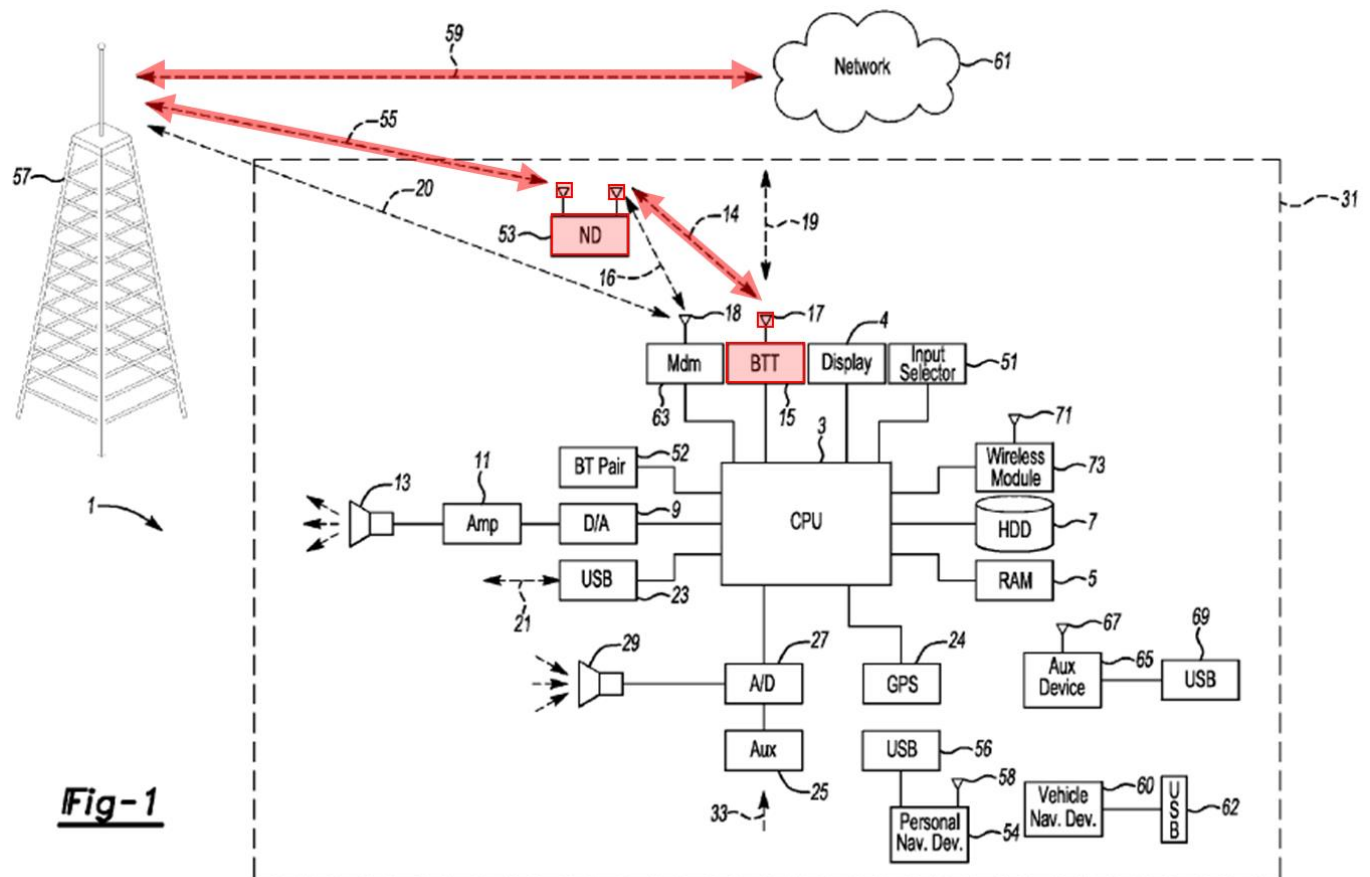


Kleve's memory includes random access memory (RAM) and a hard disk drive (HDD) or flash memory (both depicted in blue, above). EX1005, [0022]. This memory is used to store data. *Id.*, [0031].

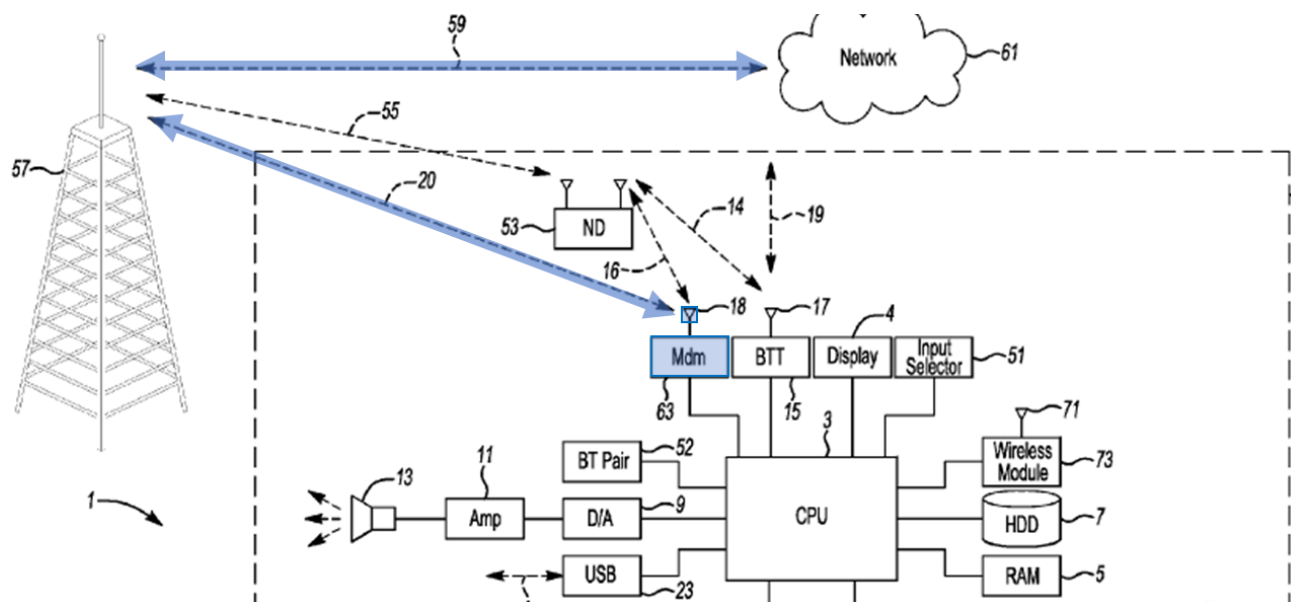
Kleve’s processor executes instructions stored at a “storage medium [*i.e.*, **memory**] that “enable a vehicle rental transaction” by “activat[ing] [*i.e.*, **starting**] the vehicle during a prescribed rental period” and, “enabl[ing] a keyless drive-away.” *Id.*, [0009]; *see also id.*, [0071] (describing use of a virtual key to “**unlock** and drive”).

1[b]

Kleve discloses multiple communications circuits interfaced with its on-board computer and sub-systems for communicating with a server located on a cloud network. EX1004, ¶¶124-129. For example, Kleve's VCS may use a "BLUETOOTH transceiver 15 to communicate 17 with a user's nomadic device 53 (e.g., cell phone, smart phone...)," which in turn communicates "with a network 61 outside the vehicle 31." EX1005, [0025]; *see also id.*, [0029]-[0030] (describing other communication protocols, such as WiFi), Fig. 1 (annotated below).



Kleve's VCS may also communicate directly with a wireless network using "an onboard modem 63 having antenna 18" or a "vehicle based wireless router" such as a "WiFi ... transceiver." *Id.*, [0028], [0030], [0034], Fig. 1 (annotated below).



In both examples, Kleve's communications circuitry interfaces directly with Kleve's processor, and indirectly through the processor with other vehicle sub-systems, as shown in Figure 1. A POSITA would have understood that Kleve's communications circuitry (*e.g.*, modem, 63, Bluetooth transceiver 15, or wireless router 73) processes program instructions to communicate using the disclosed communications protocols (*e.g.*, Bluetooth or WiFi). EX1004, ¶128.

The VCS communicates with a "centralized system," such as "a server system" via the network 61. *Id.*, [0057]. The server "may route an incoming signal from a nomadic device (ND) 403 to the appropriate remote vehicle to enable a

Temporary User keyless access and drive away capabilities of the Owner's vehicle."

*Id.*

**1[c]**

Kleve's communications circuitry includes wireless communication circuitry (*e.g.*, modem 63, Bluetooth transceiver 15, and wireless router 73), which enable local connection to a mobile device. See Limitation 1[b]; EX1005, [0025]; EX1004, ¶129. Kleve's mobile device is configured to use a virtual key (**eKey**) to "unlock and drive" (which entails starting) the vehicle. See Limitation 1[a]; EX1005, [0009], [0071]; EX1004, ¶130.

**1[d]**

Kleve discloses that a virtual key is wirelessly communicated to the vehicle using encrypted data (**coded data**). EX1004, ¶¶131-137. For example, Kleve teaches that a virtual key may be sent "in an encrypted message" to "the VCS." EX1005, [0063].

It would have been obvious to a POSITA to also use Kleve's wireless communications circuitry to receive encrypted data associated to a virtual key directly from the mobile device to enable unlocking and use of the vehicle. EX1004, ¶134.

For example, Hatton teaches a "mobile device 124 may be configured using a software application to communicate with the VCS." EX1008, 7:21-23. Communication between the mobile device and the vehicle may use "wireless

communication technologies including, but not limited to Bluetooth, WiFi, cellular, and/or near field communication.” *Id.*, 7:56-60. The vehicle “may recognize the mobile device associated to a user using ... mobile device transmitted encrypted data.” *Id.*, 7:49-56. The encrypted data is associated to a particular electronic key. *Id.*, 7:33-45. Once configured as an electronic key, the mobile device may be used to “start[] the vehicle” and “unlock[]/lock[] doors.” *Id.*, 13:24-27.

A POSITA would have been motivated to use Kleve’s wireless communications circuitry to receive encrypted wireless communications associated to an electronic key for enabling virtual key unlock and drive functionality, as described in Hatton, because it would simplify activation and use of the virtual key while preventing unauthorized access to the vehicle. *See* Section VI.A.3.

Kleve also independently discloses this limitation. EX1004, ¶¶132-133. For example, Kleve discloses using a “matrix barcode (ex. two-dimensional code) [*i.e.*, **coded data**] ... as the virtual key.” EX1005, [0044]. A “smart phone may be used to communicate the matrix barcode information” using an optical scanner (**wireless communication**), allowing the user to “enter and enable the vehicle drive away event.” *Id.*; *see also id.*, [0045], [0071].

### 1[e]

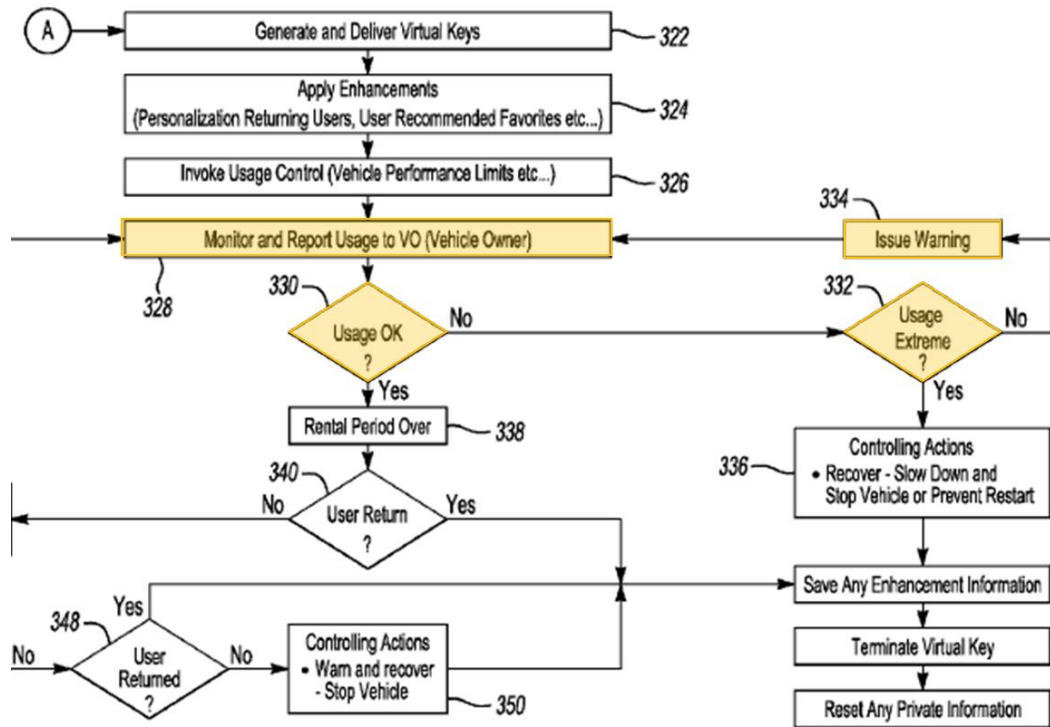
Kleve discloses that the virtual key, represented as encrypted data, includes privilege settings that limit types of use of the vehicle. EX1004, ¶¶138-140. For example, the vehicle’s “Owner” “may set user restrictions ... based on ... parameters

including, but not limited to, speed, global position coordinates, or load weight restrictions.” EX1005, [0040]. The restrictions may be set in accordance with the types of use intended by the owner and temporary user. *Id.*, [0083] (owner may review rental request “based on what the Temporary User is looking to use the vehicle for (*e.g.*, without limitation, for towing, hauling or errands)”), [0076] (VCS may monitor for “unauthorized objects or cargo ... and/or an unauthorized trailer tow”).

It would have been obvious to a POSITA to include the use restrictions within the encrypted data associated with the virtual key in order to prevent tampering by a temporary user. *See* Section VI.A.3.

### **1[f]**

Kleve discloses monitoring (**tracking**) use of the vehicle to identify and record (**log**) actions taken by a temporary user using a virtual key. EX1004, ¶¶141-142, 160-165. For example, Kleve discloses “restrictions” that “may be monitored and if a restriction exceeds a limit the Temporary User and Owner may be notified.” EX1005, [0040]. The monitoring steps are illustrated in more detail in Fig. 3B, annotated below.



After a virtual key is delivered to the vehicle (VCS) and the temporary user (step 322), “Usage Control ([e.g., ]Vehicle Performance Limits)” may be invoked (step 326). *Id.*, [0051]. Use of the vehicle is monitored and reported to the owner (step 328). *Id.*, [0052]. Usage data (“location, speed, and driving behavior”) may be “record[ed].” *Id.*; *see also id.*, [0076] (monitoring for unauthorized uses).

## 5. Claim 3

Kleve’s VCS may receive and store a virtual key received as “an encrypted message” from the server. *See* Limitation 1[d]; EX1005, [0063].

It would have been obvious to a POSITA to use encrypted data sent from the server to authenticate and activate a virtual key based on encrypted data received from the mobile device. EX1004, ¶147-148. For example, Hatton teaches the VCS

uses encrypted data received from the mobile device to “recognize the mobile device” and “allow[] the vehicle to start the engine.” EX1008, 7:18-20, 7:49-56; *see also* Limitation 1[d]. Hatton’s VCS stores the encrypted virtual key information from the server in a look-up table associating encrypted data with authorized electronic keys. *Id.*, 7:33-45. The VCS “recognize[s] [*i.e.*, **authenticates**] the mobile device associated to a user using ... the mobile device transmitted encrypted data.” *Id.*, 7:52-56.

A POSITA would have been motivated to use the encrypted data received from the server to authenticate a user’s virtual key based on encrypted data received from a mobile device, as described in Hatton, because it would simplify activation and use of the virtual key and prevent temporary users from tampering with the virtual key. *See* Section VI.A.3.

Kleve also independently teaches that the VCS may “compare” a temporary user’s identification information (e.g., a “matrix barcode”) with a “previously sent virtual key,” sent as an encrypted message via the server, “to determine authorization.” EX1005, [0063], [0068], [0071]; EX1004, ¶¶141-146. Kleve also describes using “remote credential verification at the vehicle ... by the VCS, using a server” to “verify” an access request from a temporary user with a virtual key. EX1005, [0048]-[0049]. Once the temporary user is authorized, the user may use the virtual key to operate and drive the vehicle. *Id.*, [0059].

## 6. Claim 4

Kleve discloses that its VCS receives additional requests (comprising coded data associated with a user account and received from the server) to use the vehicle from other users (and their associated mobile devices), via the VCS communication circuitry. EX1004, ¶¶149-152. For example, Kleve’s “vehicle rental authorization system” allows owners and administrators to rent vehicles to multiple potential temporary users. EX1005, [0087]. “Temporary Users” may “select[] [a] vehicle to rent” from a list of owners and vehicles. *Id.*, [0081]-[0082] (emphasis added). A POSITA would have thus understood the rental system may receive multiple requests for the same vehicle from different temporary users over different rental periods, and that each request comprises the same type of information (*i.e.*, coded data generated by the server and associated with a user profile), and is received via the VCS’s communication circuitry. EX1004, ¶149-150; *see also* Limitations 1[b]-1[e]. Hatton confirms that Kleve’s VCS stores encrypted data for multiple electronic keys, each associated with a different mobile device. EX1008, 7:33-45, 7:52-56.

Kleve explains that each rental request may be accepted or denied by the owner responsible for administering the vehicle and may include terms negotiated between the owner and the temporary users. *Id.*, [0082]-[0084]. The terms include “vehicle restriction limits initially set by the Owner at the beginning of the rental term.” EX1005, [0043]; *see also id.*, [0084], [0089]. The temporary users have user profiles (**accounts**) on the vehicle rental system, allowing a temporary user to be associated with a virtual key and its associated restrictions (**privileges**). *Id.*, [0062],

[0069]. After an agreement is reached, “the system may generate a virtual key to distribute to the Temporary User and VCS.” *Id.*, [0039].

## **7. Claim 5**

It would have been obvious in view of Hatton to use wireless communications, including near field communication (NFC) and radio frequency standards (*e.g.*, Bluetooth and WiFi), to receive encrypted data from the mobile device in Kleve’s system. *See* Limitation 1[d]; EX1004, ¶153; EX1008, 7:56-60.

## **8. Claim 6**

Kleve discloses a “rental microbusiness” implemented as a “smart phone application” that enables sharing virtual keys. EX1005, [0036]. 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.* Distribution is enabled by the owner using the smartphone application to send messages agreeing to rental terms and generating the virtual key. *Id.*, [0039], [0047]-[0048], [0051], [0069]; EX1004, ¶¶154, 156.

It would have been obvious to a POSITA that the smartphone application may also be used to enable multiple authorized temporary users to share virtual keys with each other. EX1004, ¶155. A POSITA would have been motivated to allow such sharing to facilitate rentals to groups (*e.g.*, families, travel groups) where multiple members may use the vehicle. *Id.* A POSITA could implement such sharing using

the same or similar software used to enable an owner to distribute virtual keys to temporary users. *Id.*

### 9. Claim 7

Kleve discloses that a “virtual key may be sent in an encrypted message to the [] Temporary User’s nomadic device.” EX1005, [0063]; *see also* Limitation 1[d]. Encrypting the data renders its processing at the mobile device secure. EX1004, ¶157.

Kleve further discloses that the delivery of a virtual key to the temporary user (via the encrypted message) occurs after (and is responsive to) “identification of the Temporary User with an accepted agreement and payments made,” which is enabled by the owner agreeing to the terms of the rental and generating a virtual key specific to the temporary user. EX1005, [0048], [0069]; EX1004, ¶158. Kleve also discloses that the virtual key may be registered to the temporary user’s device only after “remote credential verification at the vehicle,” which “may be done by the VCS, using a server, or allowing the Owner to verify the Temporary User’s request,” *e.g.*, using a “credential verification password.” EX1005, [0049]; *see also id.*, [0070]; EX1004, ¶159. After verification, the temporary user’s mobile device may process the encrypted data to pair with the VCS. EX1005, [0072].

### 10. Claim 8

Kleve discloses that restrictions on types of use (**a mode of allowed use of the vehicle**) are configured to monitor use of the vehicle, and the VCS is configured

to send notifications when restrictions are violated. EX1004, ¶¶160-161. Kleve's monitoring of restrictions is illustrated in Figure 3B and its accompanying disclosure. See Limitation 1[f]. Kleve further discloses "the **VCS may monitor that a restriction threshold has been violated**," and "the system may **send an issue warning** to the vehicle display information center" and "**send a message** to issue a warning to the Temporary User." EX1005, [0053]. The VCS also sends vehicle user data to the Owner, along with notifications "if a restriction exceeds a limit." *Id.*, [0040], [0078] (describing "driver behavior" monitored by the VCS and "transmitted ... to the vehicle owner's nomadic device").

## 11. Claim 9

Kleve discloses monitoring use of the vehicle to identify violations of restrictions on use. See Limitation 1[f]; Claim 8.

Kleve further teaches that violations may include driving too fast, driving out of an area, accelerating too fast, stopping too fast, or coming in contact with a structure or another vehicle. See, e.g., EX1005, [0041] ("driving to restricted areas"), [0078] (describing monitoring "vehicle speed, acceleration force, wheel speed, breaking, steering, vehicle weight, throttle and pedal position," e.g., "driving the vehicle at excessive vehicle speeds"), [0079] (describing notifications that "the Temporary User has been in an accident or near miss based on airbag deployment, accelerometer data, and/or anti-lock brake information"); EX1004, ¶¶162-163.

## **12. Claim 10**

Kleve discloses identifying violations of restrictions on use. *See* Claims 8-9. The violations may be of speed limits, time limits, and area limits. *See* EX1005, [0040] (“speed” and “global position coordinates”), [0041] (“driving to restricted areas”), [0043] (time limit), [0075] (speed limit), [0078] (“vehicle speed, acceleration force, wheel speed”); EX1004, ¶¶164-165.

## **13. Independent Claim 11**

Limitations 11[pre]-11[c] and 11[e] of Claim 11 are substantively the same as the corresponding limitations in Claim 1 and are disclosed by Kleve. *See* Limitations 1[pre]-1[c], 1[e], EX1004, ¶166. Limitations 11[d] and 11[f] are addressed below.

### **11[d]**

As described in Limitation 1[d], Kleve and Hatton render obvious that the wireless communications circuitry of the vehicle is configured to receive encrypted (**coded**) data from the mobile device. EX1004, ¶168.

Claim 11[d] additionally requires that the coded data is “unique for said eKey.” Kleve discloses that encrypted data (such as a “matrix barcode”) associated with a virtual key is uniquely generated for each temporary user based on the temporary user’s personal information. EX1005, [0037], [0063]; EX1004, ¶169. Hatton also confirms that Kleve’s VCS separately stores unique encrypted data for each authorized key, and it would have been obvious to do so for the reasons discussed above. EX1008, 7:33-45.

**11[f]**

Kleve discloses that a temporary user may create a user profile (**user account**) to be associated with virtual keys for that user. EX1004, ¶¶170-172. For example, Kleve teaches that a temporary user may “set[] up a user profile that is saved in a database within the vehicle rental authorization system.” EX1005, [0086]; *see also id.* [0037] (the “Temporary User may set up a user profile ... to include ... matrix barcode (ex. two-dimensional code), ... or other types of unique Temporary User identification to validate and pay for the rental service.”). The user accesses the vehicle rental authorization system by logging into the temporary user’s profile. *Id.*, [0047]; *see also id.*, [0063] (describing the use of “Temporary User Identification,” including the user’s “mobile web login IDs and password,” as or in addition to the virtual key). The system may then “generate and deliver virtual keys to the Temporary User.” *Id.*, [0048]. The virtual keys are associated with the temporary user’s profile and use information from that profile to verify the temporary user’s credentials when using the virtual key. *Id.*, [0037], [0063].

Kleve further discloses that the user profile is accessible via a user interface of a smart phone application. EX1004, ¶171; EX1005, [0036] (“The vehicle rental micro-business 200 may include a website, smart phone application or other nomadic device that an Owner and Temporary User may use to manage their assets and/or user profile.”).

Kleve discloses that the virtual key enables unlocking and starting the vehicle. EX1004, ¶172. For example, Kleve teaches that after the vehicle determines that a virtual key is authorized, the Temporary User may use the virtual key to “unlock and drive.” *Id.*, [0071].

#### **14. Claim 12**

Kleve discloses an application on a mobile device that communicates with a server. EX1004, ¶¶173-176. For example, Kleve discloses a “centralized system” that is a “server system that includes processing capability for incoming nomadic device [*i.e.*, mobile device] signals designated to interact with a remote vehicle.” EX1005, [0057]. The server “may route an incoming signal from a nomadic device (ND) 403 to the appropriate remote vehicle to enable a Temporary User keyless access and drive away capabilities.” *Id.*

Kleve further discloses that the server may be one of a plurality of servers. For example, Kleve’s server system may include at least an “automated call server and/or web host,” each of which may be operated as a separate server. EX1005, [0057]; EX1004, ¶174.

Claim 12 additionally requires that one of the servers “is associated with a manufacturer of the vehicle.” That limitation is not entitled to any 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. *Praxair Distribution, Inc. v. Mallinckrodt Hosp. Prods. IP Ltd.*, 890 F.3d 1024,

1031-32 (Fed. Cir. 2018). The owner of the server would not change the underlying functionality and implementation of the system. EX1004, ¶175. Regardless, a POSITA would have understood, and it would have been obvious that the server may be associated with a manufacturer of the vehicle because Kleve is a Ford patent, and thus the disclosed system would have been developed for use by Ford. *Id.*, ¶176. Contemporaneous references confirm that electronic key systems including servers operated by vehicle manufacturers were well known by the time of the '659 patent. *See, e.g.*, EX1010, 11:15-31, 16:6-18 (describing an “automobile service server” and “automobile web service server” “associated with an automobile company”).

## 15. Claim 13

### 13[a]

It would have been obvious to a POSITA to securely generate the virtual key on the mobile device. EX1004, ¶¶177-178. Kleve expressly teaches that the “exemplary processes” described therein “may be executed by a computing system in communication with a vehicle computing system,” which may include a “cellular telephone,” or “a server.” EX1005, [0035]. Kleve teaches that in different embodiments, “particular components ... may perform particular portions of a process depending on the particular implementation of the system,” and that “[o]ne of ordinary skill in the art will understand when it is *in*appropriate” to use a particular component. *Id.* (emphasis added). Here, a POSITA would understand that there is no reason why Kleve’s virtual key generation could not be performed on the mobile

device rather than the server. EX1004, ¶178. As noted above, Kleve expressly confirms this is an obvious design choice; however, a POSITA would also have been motivated to enable virtual key generation on the mobile device to allow owners to generate and distribute virtual keys when they cannot access the server. *See* Section VI.A.3.

### **13[b]**

Kleve discloses and renders obvious a software application on a mobile device that communicates with a server. *See* Claim 12; EX1004, ¶¶179-181. To the extent the server being associated with a manufacturer of the vehicle is afforded any patentable weight, Kleve renders that limitation obvious. *See id.*

Claim 13 additionally requires that the application is “associated with a manufacturer of the vehicle.” That limitation is not entitled to any patentable weight under the printed matter doctrine for the same reason as the corresponding server limitation in claim 12, *i.e.*, because the supplier of the application would not change its functionality or implementation. *See* Claim 12; *Praxair*, 890 F.3d at 1031-32; EX1004, ¶¶175, 180. Regardless, a POSITA would have understood, and it would have been obvious that the software application may be associated with a manufacturer of the vehicle because Kleve is a Ford patent, and thus the disclosed software application would have been developed for use by Ford. EX1004, ¶181. Hatton further confirms that the Ford system described in Kleve may make use of a

“software application 212” that “may be an application that was developed and/or associated with the vehicle manufacturer.” EX1008, 12:46-51.

**16. Claim 14**

Kleve and Hatton render obvious that the VCS includes logic for processing encryption operations of a virtual key in coordination with logic of a mobile device. EX1004, ¶182. Kleve teaches that a virtual key may be sent “in an encrypted message” to “the VCS, Temporary User’s nomadic device, and/or vehicle Owners nomadic device.” *See* Limitation 1[d]; EX1005, [0063]. It also would have been obvious to a POSITA to use Kleve’s wireless communication circuitry to receive encrypted data directly from the mobile device. *See* Limitation 1[d]. Kleve’s VCS and mobile device would thus necessarily be capable of processing encryption operations in a coordinated manner in order to decrypt the encrypted messages and authenticate and verify the virtual key. EX1004, ¶182.

**17. Claim 15**

Kleve discloses encryption operations. *See* Claim 14. It would have been obvious to a POSITA that the encryption operations may use public/private key pair encryption 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 Kleve’s system. EX1004, ¶¶183-184. Contemporaneous references confirm that public/private key

pair encryption was well-known years before the '659 patent, including in electronic key systems for vehicles. *See, e.g.*, EX1009, 15:34-51, EX1004, ¶185.

**18. Claim 16**

Kleve and Hatton render obvious wireless communication circuitry using Bluetooth, NFC, WiFi, and radio communication. *See* Claim 5; EX1004, ¶186.

**19. Claim 17**

Kleve discloses associating a virtual key with a temporary user and the Temporary User's associated mobile device. *See* Limitation 11[f]. It would have been obvious to a POSITA to further bind the virtual key to the mobile device to prevent unauthorized transfers. EX1004, ¶¶187-189. For example, Hatton teaches that configuring a mobile device to operate as an electronic key may require configuring a "mobile device application ... to the user's mobile device," and receiving "vehicle security codes" at the mobile device. EX1008, 14:61-15:6. In addition, Hatton teaches that configuring the mobile device as an electronic key may require additional validation steps, such as "plac[ing] [the mobile device] in a backup slot before transmission of codes." *Id.*, 13:14-18; EX1004, ¶188.

A POSITA would have been motivated to configure Kleve's system to bind a virtual key to a mobile device in order to prevent unauthorized access to the vehicle. *See* Section VI.A.3.

## **20. Independent Claim 18**

Independent Claim 18 is substantively the same as Independent Claim 11 for the purposes of validity and is rendered obvious by Kleve and Hatton for at least the same reasons as Independent Claim 11. *See* Claim 11; EX1004, ¶190.

## **21. Claim 19**

Kleve discloses that privilege settings may be restricted for a shared user of a vehicle by the owner. EX1004, ¶¶191-192. For example, Kleve discloses that an Owner “may set user restrictions by use of the website or nomadic device ... based on, but not limited to, the owner’s selection of parameters including, but not limited to, speed, global position coordinates, or load weight restrictions.” EX1005, [0040]; *see also id.*, [0043] (“vehicle restriction limits [are] initially set by the Owner at the beginning of the rental term”). Kleve further discloses that a virtual key may provide a different “driver status signal” to indicate whether the key corresponds to the owner or a temporary user, and that “vehicle functionality may be restricted or limited” only when “the driver is the Temporary User.” *Id.*, [0045].

Kleve further discloses that the shared virtual key is received in response to the Owner causing the virtual key to be sent. EX1004, ¶192. For example, Kleve discloses that that a virtual key is generated and distributed to the temporary user only after the user “pays the appropriate amount and signs a consent agreement” with the Owner. *Id.*, [0039]; *see also id.* Fig. 6 (embodiment where generating and sending the virtual key occurs at the owner’s mobile device). Kleve’s system may

additionally use “remote credential verification,” which can add a requirement for a server or “the Owner to verify the Temporary User’s request” when the temporary user attempts to access the vehicle. *Id.*, [0049].

**22. Claim 20**

Kleve and Hatton render obvious the additional limitations of Claim 20. *See* Claim 13; EX1004, ¶193.

**23. Claim 21**

Kleve and Hatton render obvious the additional limitations of Claim 21. *See* Claims 14-16; EX1004, ¶194.

**B. Ground 2: Kleve, Hatton, and Sekiyama render obvious claim 2**

**1. Sekiyama (Japanese Laid Open Patent Application  
Publication No. 2010-126949)**

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

Sekiyama is a Toyota patent that describes an “electronic key system that allows restrictions on functions that can be executed with a duplicate electronic key.” EX1006, 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). Sekiyama also teaches that an electronic key may be sent from a first mobile device (*e.g.*, “portable telephone A”) to a second

mobile device (*e.g.*, “portable telephone B”) via a series of messages initiated by the first mobile device. EX1006, [0011], [0032]-[0039].

## **2. Motivation to Combine**

A POSITA would have been motivated to apply Sekiyama’s teachings of restricting access to the door locks and trunk of a vehicle to Kleve’s rental car system and would have had a reasonable expectation of success. EX1004, ¶¶195-199.

Kleve, Hatton, Sekiyama, and the ’659 patent are all analogous art because they are directed to the same field of electronic key systems. *See* VI.A.3 (discussing Kleve, Hatton, and ’659 patent); EX1006, [0005]; EX1004, ¶199.

There were clear benefits to adding vehicle access restrictions as taught by Sekiyama to Kleve’s vehicle rental system. EX1004, ¶196. For example, such restrictions would have provided vehicle owners with more control over the use of their vehicle by a temporary user. As discussed in Ground 1, Kleve already discloses using a virtual key to apply restrictions on the use of the vehicle by a Temporary User. By adding additional restrictions, such as restrictions on access to the door lock and trunk, an owner would have been provided more flexibility in providing access to the vehicle for different uses and to different types of temporary users. In addition, because Kleve’s system is already designed to provide access to and control over vehicle sub-systems, it would have been a mere design choice to separately enable a virtual key to restrict door lock or trunk access.

Sekiyama also provides an express motivation to combine the references. EX1004, ¶197. Sekiyama explains that in scenarios where non-owners are given access to a vehicle (*e.g.*, “valet parking”), “lending a dedicated key to another person could pose a security risk.” EX1006, [0004]. Sekiyama describes that its invention solves that problem by “allow[ing] restrictions on the functions that can be executed with a duplicate electronic key.” *Id.*, [0005]. The function restrictions include “locking and unlocking of the door lock” and “locking and unlocking of the trunk.” *Id.*, [0018].

Finally, a POSITA using Kleve’s virtual keys to restrict access to the door lock or trunk of the vehicle would have had a reasonable expectation of success, because Kleve already discloses applying restrictions on use to the virtual key, and using the virtual key to control sub-systems of the vehicle. EX1005, [0023], [0040]. Adding an additional option to restrict access to the door lock or trunk of the vehicle would have been a straightforward and routine application of the same techniques used to otherwise implement sub-system control and use restrictions within Kleve’s system. EX1004, ¶198.

### **3. Claim 2**

Kleve and Hatton render obvious Claim 1, as discussed in Ground 1.

It would have been obvious to a POSITA to configure Kleve’s virtual keys and restrictions on use to control access to the door lock and trunk of a vehicle, as taught by Sekiyama. EX1004, ¶¶201-202. Sekiyama teaches an “electronic key

system” that enables “a subset of functions” while disabling “other functions.” EX1006, [0008]. For example, the system may enable “a function of locking/unlocking a door lock of a vehicle” but disable “unlocking the trunk.” *Id.*; *see also id.*, [0018].

A POSITA would have been motivated to apply Sekiyama’s teachings regarding restricting duplicate key access to vehicle functions such as the door lock and trunk to Kleve’s vehicle rental system, because it would provide the vehicle owner with more control over the use of the vehicle, and thus offer more flexibility in providing access to the vehicle to temporary users. *See* Section VI.B.2.

**C. Ground 3: Mikan anticipates or renders obvious claims 1-3, 5, and 8-10**

**1. Mikan (U.S. Patent Pub. No. 2008/0150683)**

Mikan was filed on December 21, 2006, and published on June 26, 2008. It is thus prior art under at least §102(a)(1), or pre-AIA §§102(a)-(b).

Mikan is directed to the use of “wireless devices for providing secure operation of a vehicle.” EX1007, Abstract. The system may include multiple keys, which may be “electronic keys” that are “embedded in a wireless device such as a cellular telephone or Personal Digital Assistant.” *Id.*, [0050]. A “vehicle operation policy” may assign specific “vehicle operation features” (*e.g.*, “unlocking a door,” “opening a trunk,” or “engaging an ignition”) that are accessible to different electronic keys. *Id.*, [0049], [0051].

Mikan's system includes a "control unit 202" that is "in communication with wireless network 207" using well known wireless communication techniques, such as WiFi. *Id.*, [0052]. The control unit may also "interface with vehicle 201" to "control vehicle functions and ... sense operation of vehicle 201." *Id.*, [0053]. For example, the control unit may "lock and unlock the vehicle doors" or "sense vehicle speed and the status of the ignition." *Id.*

Mikan's system also includes local and master databases that maintain information about vehicles, keys, and operation policies associated with different vehicles and keys. *Id.*, [0051], [0054]. The control unit may employ the vehicle operation policies to "block and/or limit operation of vehicle 201 ... when an access request does not conform with vehicle operation policy." *Id.*, [0077].

## 2. Independent Claim 1

### 1[pre]

To the extent the preamble is limiting, Mikan discloses it. EX1004, ¶¶204-207. Mikan discloses a vehicle with a "control unit," which may be "any combination of hardware and/or software," including "an onboard computer." EX1007, [0051]. A POSITA would understand a computer, such as Mikan's control unit, processes instructions to perform different functions. EX1004, ¶206.

Mikan's control unit "is in operative communication with vehicle 201." EX1007, [0051]. For example, Mikan's control unit "may interface with vehicle 201" to "control vehicle functions" or "sense operation of vehicle 201." *Id.*, [0053].

Mikan's control unit may also "be in communication with wireless network 207," such as a cellular network or a WiFi network. *Id.*, [0052]. In general, "any aspect [*i.e.*, **sub-system**] of the vehicle that may be controlled by an electrical signal may be controlled by control unit 202, and [any] aspect of the vehicle operation that may be sensed and converted to an electronic signal may be sensed by control unit 202." *Id.*, [0053]. Every "aspect of the control, use, or functionality of the vehicle" may be controlled by "one or more vehicle subsystems ... in operative communication with" the control unit. *Id.*, [0060].

Mikan's control unit also enables use of electronic keys. For example, Mikan's vehicle may have one or more "key 205A-C" that "communicate[s] directly with control unit 202." EX1007, [0051]. "Keys 205A-C may be electronic keys," including "embedded in a wireless device such as a cellular telephone or Personal Digital Assistant (PDA)." *Id.*, [0050]. The control unit enforces a "vehicle operation policy" associated with a particular electronic key. *Id.*, [0076]-[0077]. For example, depending on its associated policy, an electronic key may be operable to "unlock[] a door, open[] a trunk, open[] a glove box, engag[e] an ignition, direct[] the vehicle from a first geographic location to a second geographic location, and accelerat[e] the vehicle." *Id.*, [0060], [0073]-[0074].

### **1[a]**

Mikan discloses that memory is associated with the control unit. EX1004, ¶¶208-210. For example, the control unit "may be in operative communication with

local database 203,” which “may be resident within vehicle 203.” EX1007, [0051]. “Local database 203 may be any software system or device suitable for storing and retrieving data records,” *i.e.*, memory. *Id.*

Mikan’s local database stores “vehicle operation policies” comprising “access control rules” which may be used to control, *inter alia*, unlock and starting of a vehicle. EX1007, [0060]-[0061]. For example, each vehicle operation policy may have an access control rule associated with one or more “vehicle operation features.” *Id.*, [0060]. These vehicle operation features include “unlocking a door” and “engaging an ignition.” *Id.* A POSITA would understand that the access control rules are or comprise program instructions. EX1004, ¶210.

### **1[b]**

Mikan discloses that its control unit (**on-board computer**) and associated sub-systems interface with communications circuitry for communicating with a server. EX1004, ¶¶211-215. For example, Mikan’s control unit communicates with a server via a wireless network. *See* EX1007, [0052] (“Control unit 202 may be in communication with wireless network 207,” which “may host master database 208 and application 209”), [0055] (“[M]aster application 209 may be software resident on a server platform.”). A POSITA would have understood that Mikan’s system includes communications circuitry interfacing with the control unit to enable communication with the wireless network, and that such communication would involve processing program instructions to communicate with the server. EX1004,

¶¶212-213. Mikan’s vehicle sub-systems interface directly with and are sensed and controlled by the control unit, and thus interface at least indirectly with the communications circuitry via the control unit. *Id.*, ¶¶214-215; *see also* EX1007, [0060] (“one or more vehicle subsystems that control one or more ... vehicle operation features may be in operative communication with [the] wireless vehicle security system”).

### 1[c]

Mikan discloses its control unit communicates with a wireless network via wireless communication circuitry. *See* Limitation 1[b]. Mikan further discloses that its wireless communication circuitry connects locally to a mobile device. EX1004, ¶¶216-217. For example, Mikan discloses “electronic keys” that “may be embedded in a wireless device such as a cellular telephone or Personal Digital Assistant (PDA).” EX1007, [0050]. “[K]ey 205A-C and control unit 202 may communicate directly via a radio frequency transmission” (**wireless communications**). *Id.*, [0051]. In addition, each electronic key (*e.g.*, an electronic key embedded in a mobile device) has an associated “vehicle operation policy,” which may enable it to be used to, *inter alia*, “unlock[] a door” or “engag[e] an ignition” of the vehicle. *Id.*, [0073]-[0074], [0076]-[0077].

### 1[d]

Mikan discloses wireless communication circuitry. *See* Limitation 1[c]. Mikan further teaches its wireless communications circuitry receives coded data

associated to an electronic key from a mobile device. EX1004, ¶¶218-219. For example, when “a user attempt[s] to access or operate vehicle 201 with a key 205A-C,” the control unit initiates an authentication process. EX1007, [0070]. As part of the authentication process, a “[s]ecure identifier 407 may be received ... at control unit 202.” *Id.*; *see also id.*, [0067]. The secure identifier comprises coded data, such as “a digital signature associated with a key,” which may be “the product of a public key encryption system.” *Id.*, [0059].

Authenticating the electronic key using the secure identifier enables the key to perform vehicle functions, such as unlocking and using the vehicle. EX1004, ¶219. For example, after the electronic key has been authenticated, the control unit may retrieve a “vehicle operation policy ... based on authenticated key 205A-C,” which enables the use of certain “vehicle operation features,” including “unlocking a door” and “engaging an ignition.” EX1007, [0060]-[0061], [0072].

### **1[e]**

Mikan discloses that the coded data associated with an electronic key includes privilege settings that limit the types of use of the vehicle. EX1004, ¶¶220-223. For example, Mikan teaches that electronic keys may be linked to vehicle operation policies. EX1007, [0060]-[0061], [0076]-[0077]. As part of the electronic key authentication process, the vehicle receives the vehicle operation policy associated with the authenticated key. *Id.*, [0072].

It would have been obvious to a POSITA to transmit the vehicle operation policy as additional coded data along with Mikan's secure identifier. EX1004, ¶221. A POSITA would have been motivated to do so to prevent a secondary user from tampering with the use restrictions associated with an electronic key. A POSITA would have had a reasonable expectation of success because the vehicle operation policy could be encoded and transmitted using the same encryption and wireless communication techniques already implemented and used to transmit Mikan's secure identifier, and a POSITA would have been capable of applying these techniques to encode and transmit Mikan's vehicle operation policy. *Id.*, ¶222.

Mikan's vehicle operation policy limits the types of use of the vehicle by the particular electronic key. For example, a vehicle operation policy may control whether an electronic key may be used to “unlock[] a door, open[] a trunk, open[] a glove box, engag[e] an ignition, direct[] the vehicle from a first geographic location to a second geographic location, and accelerat[e] the vehicle.” EX1007, [0060], [0073]-[0074]. A POSITA would have understood that limiting access to different vehicle functions serves to limit the types of use of the vehicle. EX1004, ¶223. For example, a secondary key intended for use as a valet key (*i.e.*, to temporarily park the vehicle on behalf of the owner) may be limited to valet use by restricting access to the trunk, to accelerating the vehicle over a certain speed, or to directing the vehicle to a geographic location beyond a specified range. *Id.*

Mikan discloses the wireless vehicle security system “enable[s] a user to ... monitor [*i.e.*, **track**]” use of the vehicle. EX1007, [0056]; EX1004, ¶224. For example, when the user of the electronic key initiates an access request (*e.g.*, to unlock a door, engage the ignition, accelerate the vehicle, or take other actions using the vehicle), the control unit determines whether “the access request is consistent with the retrieved vehicle operation policy,” and may “notify a user or a system by signaling an indication of whether an access request conformed with the retrieved vehicle operation policy.” EX1007, [0073]-[0075]. The notification process may include “appending a text string to a log file.” *Id.*, [0075].

### 3.     **Claim 2**

Mikan discloses that vehicle operation policies may be used to restrict access to vehicle areas, including door and trunk operation. EX1004, ¶225. For example, Mikan teaches that a “vehicle operation policy” “enables the use of certain “vehicle operation features,” including “unlocking a door” and “opening a trunk.” EX1007, [0060]-[0061], [0073]. The vehicle operation policies are used to process an “access request” from the holder of an electronic key, determine whether the request is “inconsistent” with a vehicle operation policy, and, if it is, “block and/or limit the operation of the vehicle.” EX1007, [0063], [0073]-[0074].

### 4.     **Claim 3**

Mikan discloses receiving and securely storing information from a server to authenticate coded data for activating an electronic key. EX1004, ¶¶226-228.

Mikan's vehicle includes a "local database" that "may regularly poll [a] master database ... to maintain consistent data." EX1007, [0054]. The master database may be "integrated" with an application that is "resident on a server platform." *Id.*, [0055]. The "local database 203 and master database 208 may communicate an update to the other after a record change." *Id.*, [0054].

The information stored at the local database and received and updated from the master database includes a "key set ... representing a collection of keys." *Id.*, [0058]-[0059]. The "key set" may include a "secure ID check," which is used in conjunction with the key's secure identifier to authenticate the key. *Id.*, [0059]. The secure ID check may verify coded data received from a mobile device, such as a digital signature. *Id.*, [0071] ("Control unit 202 may authenticate key 205A-C via secure ID check 315. ... The authentication may include verifying a digital signature and timestamp, for example."), [0065]-[0067] (describing the mobile device sending the secure identifier to the vehicle to authenticate an electronic key).

## **5. Claim 5**

Mikan discloses wireless communication circuitry that communicates with a mobile device. *See* Limitations 1[c]-1[d]. Mikan also teaches wireless communication over a radio frequency standard. EX1004, ¶¶229-230. For example, Mikan discloses that "key 205A-C and control unit 202 may communicate directly via a radio frequency transmission." EX1007, [0051].

Mikan also teaches that a “wireless device 400 equipped for use as a key 205A-C” may include a “vehicle access module” that “may communicate with vehicle 201 ... via any wireless protocol suitable for the transmission of data,” including “Bluetooth protocol, WiFi, RF-ID, cellular, and the like,” all of which are radio frequency standards. *Id.*, [0067]; EX1004, ¶230. In order to communicate with the wireless device, Mikan’s vehicle necessarily also includes wireless communication circuitry implementing the same wireless communication protocols as the wireless device. EX1004, ¶230.

## 6. Claim 8

Mikan discloses that according to a vehicle operation policy (**a mode of allowed use of the vehicle using the eKey**), the status of the vehicle is “monitor[ed]” to “confirm[] its conformance with vehicle operation policy 311 associated with the key 205A-C that is currently in use.” EX1007, [0076]; *see also* EX1004, ¶231. If a feature “being monitored no longer conforms with vehicle operation policy 311,” the control unit may initiate a “notification” or “enforcement action,” which may include “sending an electronic message,” such as “e-mail” or “a text message via Short Message Service.” EX1007, [0075]-[0078].

## 7. Claim 9

Mikan discloses monitoring (**tracking**) use of the vehicle to identify violations of a vehicle operation policy. *See* Limitation 1[f], Claim 8. Mikan further teaches that access control rules in a vehicle operation policy may establish

restrictions on use of the vehicle, including “a maximum acceleration for the vehicle, ... a geographic range within which the vehicle may be operated,” and other limits, such as maximum speed. EX1007, [0060] (“For illustration, access control rule 317 may indicate ... that the vehicle may not be operated above 65 miles per hour.”); EX1004, ¶233.

The control unit may identify and track violations of the access control rules. EX1004, ¶232. For example, “where vehicle operation policy 311 includes setting a maximum speed for the operation of vehicle 201, monitoring continuously checks the speed of vehicle 201 and compares it to the maximum imposed by vehicle operation policy 311,” and “[i]f vehicle 201’s speed exceeds that defined by policy 311, notification and/or enforcement action may be taken.” EX1007, [0076].

## **8. Claim 10**

Mikan discloses identifying violations of a vehicle operation policy. *See* Claims 8, 9. Mikan teaches the access control rules may include setting speed limits, time limits, and area limits. *E.g.*, EX1007, [0060] (“For example, access control rule 317 may establish ... a **range of time** within which the vehicle may be operated, [or] a **geographic range** within which the vehicle may be operated.”), [0061] (describing a rule “that limits the maximum speed to 35 miles per hour”); *see also* EX1004, ¶235.

## **D. Ground 4: Mikan and Xiao render obvious claims 4, 11-18, and**

**20-21**

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

Xiao was filed on December 22, 2010, and published on June 28, 2012. It is thus prior art under at least §102(a)(1), or pre-AIA §§102(a)-(b).

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.

**2. Motivation to Combine**

A POSITA would have been motivated to apply Xiao’s teachings relating to user accounts to Mikan’s electronic key system and would have had a reasonable expectation of success. *See* EX1004, ¶¶237-241.

Mikan, Xiao, and the ’659 patent are all analogous art because they are directed to the same field of electronic key systems. *See* EX1001, Abstract; EX1007, Abstract; EX1010, Abstract; EX1004, ¶241.

There were well-known benefits to requiring users to create accounts to store information for wireless and mobile-based systems, including electronic key systems. EX1004, ¶¶238-239. For example, one critical concern with electronic key systems is ensuring that only authorized users have access to a vehicle and that an electronic key is not improperly used by unauthorized third parties. Requiring users to register an account in order to use an electronic key thus promotes accountability and allows owners and system administrators to verify the identities of users before they are provided with an electronic key, and identify users who are violating the platform's policies, or an owner's use restrictions.

In addition, Mikan's system describes using a database to track a large number of vehicles, keys, and vehicle policies. Organizing, tracking, searching, and retrieving such information is greatly facilitated by associating accounts with individual users, and linking specific vehicles, keys, and vehicle operation policies with those user accounts. EX1004, ¶239. For example, a particular owner may choose to define a vehicle operation policy that applies to multiple ones of that owner's vehicles. The addition of user accounts may enable the owner to define the vehicle operation policy once and then apply it to all vehicles associated with the owner's account, as opposed to creating separate identical vehicle operation policies for each vehicle.

Finally, a POSITA adding user accounts to Mikan's electronic key system would have had a reasonable expectation of success. EX1004, ¶240. By the time of

the '659 patent, there were countless online services that required users to register accounts, and that stored information about users, user preferences, and user devices within those accounts. Adding user accounts to Mikan's system would have been a straightforward and routine application of well-known and conventional software and user interface techniques, such as those used to support user accounts in many other internet and mobile products and services.

### **3. Claim 4**

Mikan anticipates or renders obvious Claim 1, as discussed in Ground 3.

Mikan further discloses that multiple electronic keys, corresponding to multiple mobile devices, may be associated with a vehicle, and each may generate requests to use the vehicle. EX1004, ¶¶242-244. For example, Mikan's control unit may be "in operative communication with [a plurality of] keys 205A-C." EX1007, [0050]. These keys may be "electronic keys ... embedded in a wireless device." *Id.*, [0049]. In one example, illustrated in Figure 2 and reproduced below, keys 205A and 205B are both incorporated into different mobile devices:

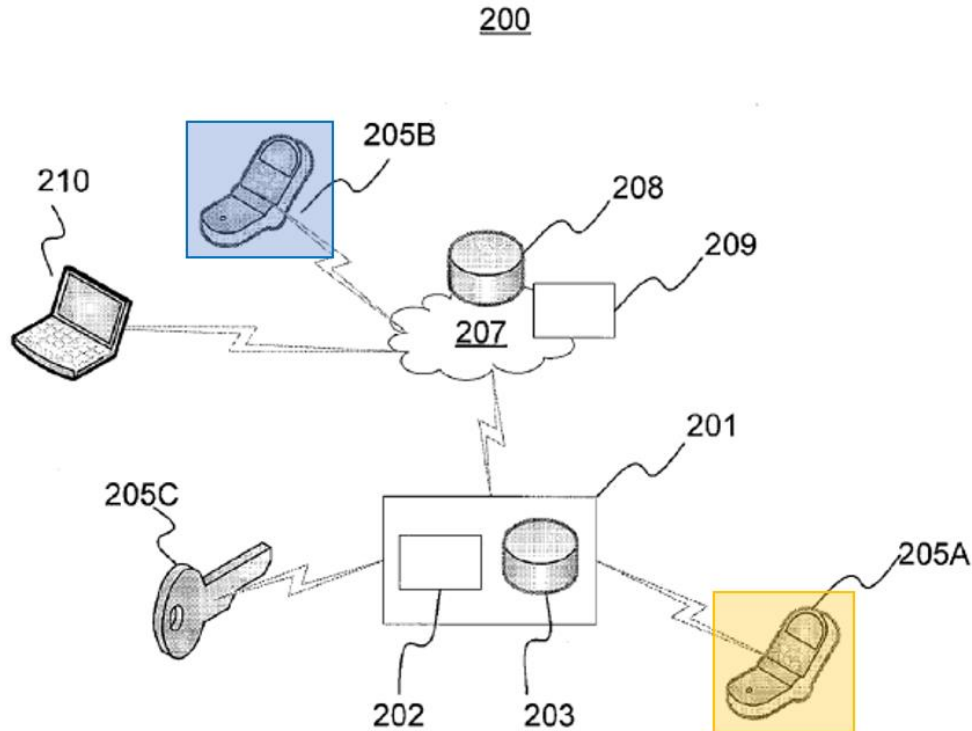


FIG. 2

EX1007, Fig. 2.

Each electronic key and its corresponding requests are associated with a different secure ID check (*e.g.*, a digital signature), which is used to authenticate the key and associate it with its corresponding vehicle operation policy (*i.e.*, **privileges**). EX1004, ¶¶243-244. For example, in one embodiment, Mikan's vehicle has an associated key set that is maintained in the master database at the server, and mirrored (*i.e.*, **received** and **stored**) by the local database at the vehicle. EX1007, [0058] ("Master database 200 may include any number of vehicle records 302. ...

In one embodiment, vehicle record 302 may include key set 310 ... [which] may include data representing a collection of keys 205A-C.”), [0059] (“Local database 303 may include vehicle ID 301, [and] key set 310 .... Vehicle ID 301 in local database 303 may map directly to that in master database 300.”), [0084] (“[L]ocal database 203 and master database 208 may synchronize. ... In one embodiment, consistency may be achieved by making the data of local database 203 mirror that of corresponding vehicle record 302.”). Figure 3, reproduced and annotated below, shows the contents of the databases, including vehicle records (yellow), key sets (red), secure ID checks (blue), and key/policy mappings (purple):

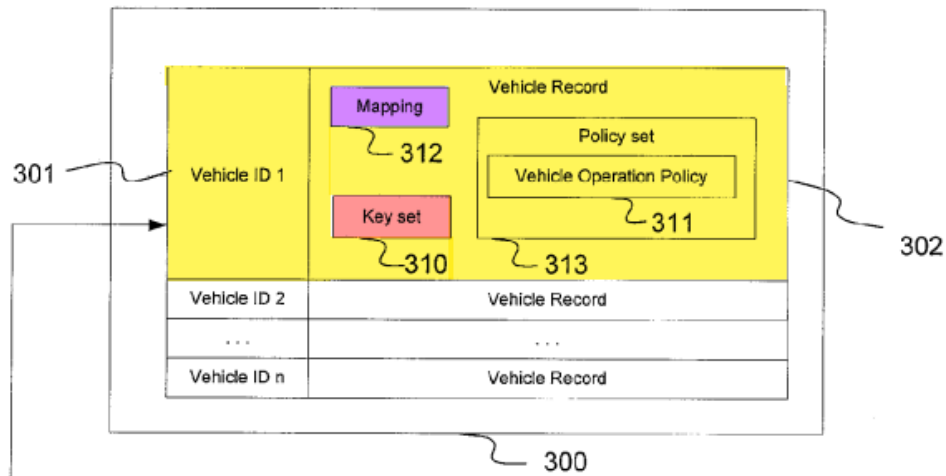


FIG. 3A

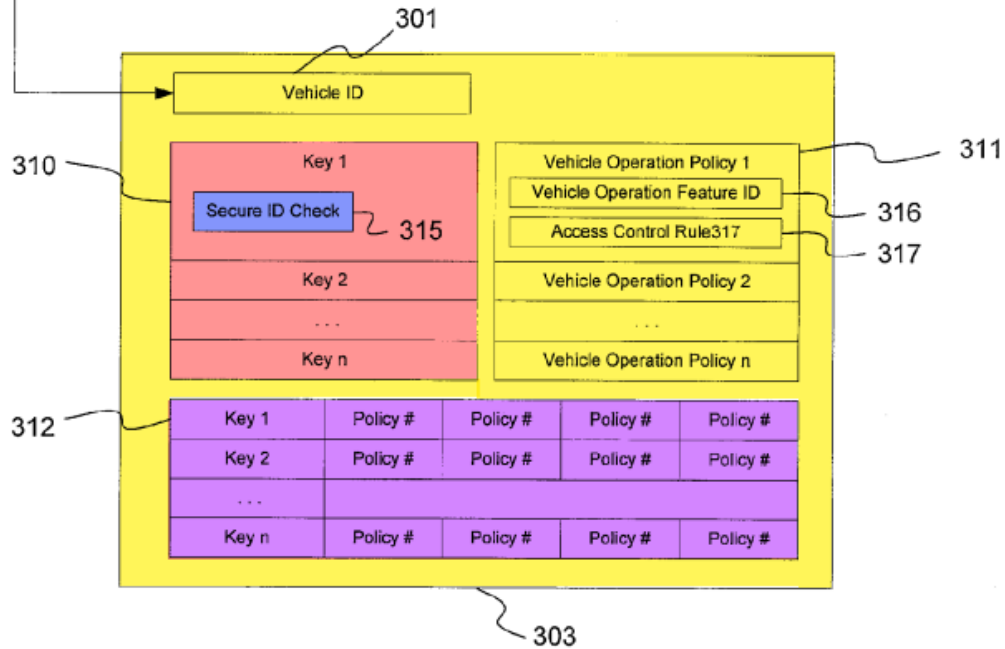


FIG. 3B

Each key within the key set (shown in red) may have an associated secure ID check (shown in blue), such as a digital signature (**coded data**) associated with the key, which is used to authenticate a key when used by a user. EX1007, [0059], [0071]; *see also* Ground 3, Claim 3. Each key is also mapped to one or more vehicle

operation policies (mappings shown in purple), which define a set of access privileges assigned to that key. *Id.*, [0060]-[0061]. The contents of the database, including the access rules associated with the vehicle operation policies, may be set and updated by an owner or administrator via a computer or mobile device. *Id.*, [0056] (“[C]omputer 210 and key 205B may provide a user interface with wireless vehicle security system 200 to enable a user to manage and monitor system 200. For example, where key 205B is part of a mobile telephone, the user of the mobile telephone may use the mobile telephone to send updates to master database 208 via master application 209.”), [0080] (“The update request may have originated at a computing device, such as a wireless telephone, a computer 210, ... [or] key 205B .... The update request may include ... a[n] access control rule.”).

It would have been obvious to a POSITA in view of Xiao to assign privileges to a user account associated with an electronic key, rather than directly to electronic key. EX1004, ¶¶248-249. For example, Xiao discloses that “the owner or operator [of a vehicle] must have an account with the system 100 to take advantage of the disclosed wireless automobile key security service.” EX1010, 3:23-25. The account may include information about the user’s “**automobile permissions information** 616.” *Id.*, 12:8-13.

A POSITA would have been motivated to add user accounts to Mikan’s system and assign privileges to those user accounts in order to better organize and track information about users, vehicles, and electronic keys. *See* Section VI.D.2.

#### **4. Independent Claim 11**

Limitations 11[pre]-11[c] and 11[e] of Claim 11 are substantively the same as the corresponding limitations in Claim 1 and are disclosed by Mikan. *See* Ground 3, Limitations 1[pre]-1[c], 1[e]. Limitations 11[d] and 11[f] are addressed below.

##### **11[d]**

Mikan discloses that the wireless communications circuitry of the vehicle is configured to receive coded data (*e.g.*, a digital signature) from the mobile device as part of a secure ID check. *See* Ground 3, Limitation 1[d]. Mikan further discloses that each electronic key has its own associated digital signature, which would be unique to that key. *See* Claim 4; *see also* EX1004, ¶253.

##### **11[f]**

Mikan discloses a “security application” on a mobile device equipped for use as an electronic key. EX1007, [0067]. The security application “may provide a user with customizable features that may be presented by user interface module 402.” *Id.* The user interface module allows users to submit “requests ... such as an update request and an access request.” *Id.*, [0063]. The security application and user interface thus enable a user to access and update information on the server corresponding to electronic keys that the user is permitted to access and/or update. *Id.*, [0080]-[0082]; EX1004, ¶254-257. Mikan further discloses that the electronic key may be used to unlock and start the vehicle. *See* Ground 3, Limitation 1[d].

It would have been obvious to a POSITA in view of Xiao that information about the electronic keys and related privileges available to a user may be organized as a user account accessible by the security application. EX1004, ¶256. For example, Xiao discloses “the owner or operator [of a vehicle] must have an account with the system 100 to take advantage of the disclosed wireless automobile key security service.” EX1010, 3:23-25. The 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 discloses that a user account may be accessed from a “wireless automobile key service page” that may be part of an “automobile key service application” and “displayed to an automobile operator using mobile device 110.” *Id.*, 16:48-54.

A POSITA would have been motivated to add user accounts as taught by Xiao to Mikan’s system in order to improve security and accountability and to organize and track information about vehicles and electronic keys. *See* Section VI.D.2.

## **5. Claim 12**

Mikan discloses an application on the mobile device that communicates with a server. EX1004, ¶¶258-260. For example, Mikan’s wireless device includes a “security application” and “user interface module” that operate to receive user-initiated update requests and access requests, and a “wireless communications module” that communicates the requests via a wireless network. EX1007, [0063]-

[0064], [0067]. The update and access requests are received by a master application, which may be hosted on a server platform. *Id.*, [0055] (“Master application 209 ... may be software resident on a server platform.”), [0080]-[0082] (“[M]a[s]ter application 209 may receive an update request ... [that] originated at a computing device such as a wireless telephone.”). The master application may itself include one or more servers, such as an HTTP server. *Id.*, [0055].

As discussed above, the “manufacturer” limitation of Claim 12 is not entitled to any patentable weight under the printed matter doctrine. *See* Ground 1, Claim 12. Regardless, it would have been obvious to a POSITA that servers within the server platform may be associated with a manufacturer of the vehicle because vehicle manufacturers typically supply customers with keys and related services. EX1004, ¶260. Xiao confirms that electronic key systems including servers operated by a vehicle manufacturer were well known by the time of the ’659 patent. *See, e.g.*, EX1010, 3:12-20, 3:46-54, 4:46-56 (describing an “automobile service server” and “automobile web service server” that “may be associated with an automobile company”).

## 6. Claim 13

### 13[a]

Mikan discloses securely generating an electronic key on the mobile device. EX1004, ¶261. For example, Mikan teaches that the mobile device may include a “security application” with “software relating to the management of secure

identifiers,” and “may perform cryptographic functions related to the secure identifier, an authentication process, or cryptographic key generation.” EX1007, [0067]. A POSITA would have understood that the cryptographic key generation function of the security application includes generating an electronic key, because the secure identifier is used to “authenticate wireless device 400 as a key.” EX1007, [0065], EX1004, ¶261.

### **13[b]**

Mikan discloses a software application on a mobile device that communicates with a server. *See* Claim 12. To the extent the server being associated with a manufacturer of the vehicle is afforded any patentable weight, Mikan renders that limitation obvious. *See id.*

As discussed above, the additional “manufacturer” limitation of Claim 13 is also not entitled to any patentable weight under the printed matter doctrine. *See* Ground 1, Claim 13. Regardless, it would have been obvious to a POSITA that the software application may be associated with the manufacturer of the vehicle because vehicle manufacturers typically supply customers with keys and related services. EX1004, ¶264. Contemporaneous references (such as Hatton) further confirm that it was well-known at the time of the ’659 patent that a software application for an electronic key system may be “developed and/or associated with the vehicle manufacturer.” EX1008, 12:46-51.

**7. Claim 14**

Mikan discloses that its control unit (**on-board computer**) processes encryption operations of an electronic key in coordination with logic of a mobile device. EX1004, ¶265. For example, Mikan teaches that a key may be authenticated via a secure ID check. EX1007, [0071]. Information relating to the secure ID check is stored at the local database of the vehicle, and a secure identifier associated with the electronic key is stored in the memory of the mobile device. *Id.*, [0059], [0065]. The secure identifier may be a “digital signature,” such as “the product of a public key encryption system,” and the security application on the mobile device includes logic to “perform cryptographic functions related to the secure identifier, [or] authentication process.” *Id.*, [0065], [0067]. The control unit on the vehicle receives the secure identifier and uses the secure identifier and the secure ID check to authenticate the electronic key, including by “verifying a digital signature and timestamp.” *Id.*, [0071]. A POSITA would have understood that when the secure identifier is a digital signature using a public key encryption system, the control unit would also need to perform encryption operations using the same encryption scheme as part of the authentication process. EX1004, ¶266.

**8. Claim 15**

Mikan discloses encryption operations using secure public/private key pair encryption operations. EX1004, ¶267. Mikan discloses authenticating an electronic key based on a digital signature, which may be the “product of a public key

encryption system.” *See* Claim 14; EX1007, [0065]. Public key encryption refers to a known encryption technique that uses public/private key pairs for encryption and decryption. EX1004, ¶267.

### **9. Claim 16**

Mikan discloses wireless communication circuitry using Bluetooth, WiFi, and other radio communication. *See* Ground 3, Claim 5.

### **10. Claim 17**

Mikan discloses a “security application” that may be used to validate and securely bind an electronic key to a mobile device. EX1004, ¶269. For example, Mikan’s security application is used to “manage secure identifiers” and “perform cryptographic functions related to the secure identifier, an authentication process, or cryptographic key generation.” EX1007, [0067]. Mikan further teaches that the secure identifier “may authenticate [*i.e.*, **validate**] wireless device 400 as a key.” *Id.*, [0065]. When the secure identifier is a digital signature, it may be “a digital signature associated with the wireless device.” *Id.* If the digital signature is associated with the wireless device, the associated key would necessarily be bound to the mobile device with which the digital signature is associated. EX1004, ¶269.

### **11. Independent Claim 18**

Independent Claim 18 is substantively the same as Independent Claim 11 for the purposes of validity and is rendered obvious by Mikan and Xiao for at least the same reasons as Independent Claim 11. *See* Claim 11.

**12. Claim 20**

Mikan and Xiao render obvious the additional limitations of Claim 20. *See* Claim 13.

**13. Claim 21**

Mikan and Xiao render obvious the additional limitations of Claim 21. *See* Claims 14-16.

**E. Ground 5: Mikan and Sekiyama render obvious claims 6-7**

**1. Motivation to Combine**

A POSITA would have been motivated to apply Sekiyama's teachings relating to registration and sharing of electronic keys to Mikan's electronic key system and would have had a reasonable expectation of success. EX1004, ¶¶274-276.

Mikan, Sekiyama, and the '659 patent are all analogous art because they are directed to the same field of electronic key systems. *See* EX1001, Abstract; EX1007, Abstract; EX1006, [0005]; EX1004, ¶276.

Mikan already requires using wireless communications to transmit electronic keys between a mobile device and the vehicle. *See* Ground 3, Limitations 1[c]-1[d]. Further enabling the mobile device to register an electronic key and transmit it to a secondary mobile device would have simplified and facilitated distributing an electronic key to an authorized user. EX1004, ¶274. In particular, allowing the owner to register the electronic key using his or her mobile device simplifies generation of

the electronic key for the owner, as a singular interface can be used both to generate and transmit the electronic key. In addition, by sending the electronic key as a secure communication from one mobile device to a second mobile device, an electronic key can be shared even if the mobile device and the vehicle cannot connect to a remote server (*e.g.*, Mikan's master database and master application), such as in areas with poor cellular service or wireless reception. For example, the owner may register a secondary key in advance of an anticipated use and then share the electronic key with a recipient (such as a valet) at a later time, when communication with a server may not be possible.

Finally, a POSITA using Mikan's mobile device to securely register and share electronic key information with other mobile devices would have had a reasonable expectation of success, because Mikan's mobile devices are already configured to generate, send, receive electronic key information to and from external sources (*e.g.*, the vehicle's control unit). EX1004, ¶275. Configuring the mobile device to perform registration of the electronic key information (*e.g.*, by generating it using the security application on the mobile device and storing it in the master database) and then send or receive it to or from other mobile devices would have been a straightforward and routine application of the technology already implemented within Mikan's system, using conventional software programming. *Id.*

## 2. Claim 6

Mikan discloses that a plurality of electronic keys may be incorporated into mobile devices for use with a vehicle. *See* Ground 4, Claim 4. Mikan further discloses that a first key may be a master key with an access control rule “that enables all vehicle operation features,” while a second key may have “limited functionality.” EX1007, [0061]. Mikan also teaches that the mobile device may include a “security application” used to “manage secure identifiers” and “perform cryptographic functions related to the secure identifier, an authentication process, or cryptographic key generation.” *Id.*, [0067].

It would have been obvious to a POSITA in view of Sekiyama that Mikan’s security application may be used to share electronic key information with an authorized mobile device, in addition to sharing electronic key information with the vehicle. EX1004, ¶¶278-279. For example, Sekiyama discloses that “key information [may] be transmitted from portable telephone A (first terminal) 10, which functions as a master key, to portable telephone B (second terminal) 30, which functions as a duplicate electronic key.” EX1006, [0011]. Sekiyama’s key sharing functionality is enabled by a series of messages, initiated by the mobile device functioning as a master key, between the mobile device and a management center, and the mobile device and the recipient mobile device. *Id.*, [0032]-[0039]. The mobile device sends a connection request to a management center, along with messages to indicate the restricted uses to be enabled for the duplicate key, in order

to generate the duplicate key. *Id.*, [0034]-[0037]. The mobile device then “transmits the received electronic key to portable telephone B” by “send[ing] the key information for the restricted duplicate electronic key to portable telephone B.” *Id.*, [0038].

A POSITA would have been motivated to configure Mikan’s mobile device to share electronic key information with a recipient mobile device in order to facilitate transmission of secondary electronic keys. *See* Section VI.E.1.

### **3. Claim 7**

Mikan discloses that coded data, *e.g.*, a “secure identifier,” is processed securely at Mikan’s mobile device, *e.g.*, by a “security application” performing “cryptographic functions.” EX1007, [0057]; *see also* Ground 3, Limitation 1[d].

It would have been obvious to a POSITA in view of Sekiyama that Mikan’s security application may also be used by a vehicle owner to register an electronic key, and that a mobile device may process the “secure identifier” using its local security application. EX1004, ¶¶280-282. For example, Sekiyama teaches that before an electronic key is transmitted from an owner to a recipient, the owner must first initiate and enable registration of the electronic key at a “management center” by “set[ting] restriction items for the restricted duplicate key” and sending a “restricted duplicate electronic key issuance request” to the server. EX1006, [0034]-[0035]. After the electronic key has been issued, the owner’s mobile device “transmits the electronic key to portable telephone B [the recipient user’s device].”

*Id.*, [0038]. When the newly registered electronic key is received, it would be processed securely, *e.g.*, at Mikan’s security application.

A POSITA would have been motivated to configure Mikan’s mobile device to enable registration of electronic keys by the owner and secure sharing of registered electronic keys with secondary users. *See* Section VI.E.1,

**F. Ground 6: Mikan, Xiao, and Sekiyama render obvious claim 19**

**1. Motivation to Combine**

Ground 6 relies on Xiao only insofar as claim 19 depends from claim 18, where Xiao is cited in Ground 4.

A POSITA would have been further motivated to apply Sekiyama’s teachings relating to registration and sharing of electronic keys to Mikan’s electronic key system, as described in Ground 5, and would have had a reasonable expectation of success. *See* Section VI.E.1; EX1004, ¶¶283-284.

**2. Claim 19**

Mikan discloses that a plurality of electronic keys may be incorporated into mobile devices for use with a vehicle. *See* Ground 4, Claim 4; EX1004, ¶286; EX1007, [0049]-[0050], [0058]-[0061], Fig. 3. Mikan also teaches that a first key may be a master key with an access control rule “that enables all vehicle operation features” (*i.e.*, privilege settings being unrestricted) while a second key may have “limited functionality” (*i.e.*, privilege settings being restricted). EX1007, [0061]; EX1004, ¶285.

It would have been obvious to a POSITA in view of Sekiyama that Mikan's security application may be used to share electronic key information with an authorized mobile device, such that a shared user will receive a shared electronic key in response to the owner sending the shared key. EX1004, ¶¶287-288. For example, Sekiyama teaches that "key information [may] be transmitted from portable telephone A (first terminal) 10, which functions as a master key, to portable telephone B (second terminal) 30, which functions as a duplicate electronic key." EX1006, [0011]. Sekiyama also teaches that before an electronic key is transmitted from an owner to a recipient, the owner must first initiate and enable registration of the electronic key at a "management center" by "set[ting] restriction items for the restricted duplicate key" and sending a "restricted duplicate electronic key issuance request" to the server. EX1006, [0034]-[0035]. After the electronic key has been issued, the owner's mobile device "transmits the electronic key to portable telephone B [the recipient user's device]." *Id.*, [0038].

A POSITA would have been motivated to configure Mikan's mobile device to received shared electronic key information in response to the owner sending the shared electronic key. *See* Section VI.E.1.

## **VII. THE BOARD SHOULD NOT EXERCISE DISCRETION TO DENY INSTITUTION**

### **A. *Fintiv* Factors**

PO asserted the '659 patent against Petitioners in the Eastern District of Texas. *See* Section IX.B. The *Fintiv* factors weigh against discretionary denial.

Factor 1 is neutral because a stay has been neither requested nor granted.

Factor 2 does not warrant denial. Trial is set for July 21, 2025, but the trial date is not determinative. *See e.g., NetNut Ltd. v. Bright Data Ltd.*, IPR2021-01492, Paper 12 at 9-16 (PTAB Mar. 21, 2022) (instituting review with trial date six months before FWD deadline).

Factor 3 favors institution. Petitioners filed this petition roughly 9 months after service of the complaint, 5 months after service of infringement contentions, after filing IPRs on four related asserted patents, and roughly 6 weeks after the '659 patent became eligible for IPR. *CoolIT Sys., Inc. v. Asetek Danmark A/S*, IPR2021-01195, Paper 10 at 11-14 (PTAB Dec. 28, 2021) (petitioner acted diligently by filing petition five months after PO identified asserted claims). The district court case is in early stages: claim construction has not begun and will only be completed after the Board's institution decision, and discovery and dispositive motions will conclude even later. EX1024 at 3-5; *Protect Animals with Satellites LLC, v. OnPoint Sys., LLC*, IPR2021-01483, Paper 11 at 14-15 (PTAB Mar. 4, 2022).

Factor 4 favors institution. Review may be instituted without a stipulation as to district court arguments. *See e.g., NetNut*, Paper 12 at 9-16. This Petition also challenges one claim not asserted in the litigation (claim 19), creating nonoverlapping issues. *Apple Inc. v. Neodron, Ltd.*, IPR2020-00778, Paper 10 at 19 (PTAB Sept. 14, 2020) (nonoverlap of two claims supports institution).

Petitioners are defendants in the district court litigation, but this does not warrant denial under Factor 5. *See, e.g., Apple*, Paper 10 at 19-20 (institution despite Petitioner being defendant in district court).

Factor 6 favors institution because the merits of this Petition are strong and materially different from the references considered during prosecution. *See* Section VII.B.

**B. 35 U.S.C. §325(d)**

Discretionary denial under §325(d) is not warranted. None of the references relied upon in the Petition were considered by the Examiner or cited in an IDS.

Mikan is currently cited in a pending *ex parte* reexamination (EPR) filed by Unified Patents, LLC, which is not an RPI, on March 25, 2024. *See* Section IX.B. But the EPR only presents Mikan as a secondary reference in combination with non-overlapping prior art in challenges to 10 of the 21 claims. EX1023, 8. By contrast, the Petition relies on Mikan as an anticipatory or primary obviousness reference challenging every claim; the Office will not consider these grounds in the EPR. And the Petition's grounds based on Kleve do not overlap with the EPR prior art at all. In addition, no office action has issued in the EPR, which weighs against discretionary denial. *Juniper Networks, Inc. v. Monarch Networking Solutions LLC*, IPR2024-00175, Paper 12 at 27-28 (PTAB May 8, 2024).

To the extent the Board determines to exercise its discretion under §325(d), it should stay the EPR rather than deny institution here, as it is empowered to do. *See*

37 C.F.R. §42.122; *see also CBS Interactive Inc. v. Helferich Patent Licensing, LLC*, IPR2013-00033, Paper 15 (PTAB Nov. 6, 2012). Unlike Unified Patents, Petitioners have been accused of infringing the '659 patent and should be provided the opportunity to challenge the claims asserted against them.

## VIII. STANDING

Petitioners certify the '659 patent is available for *inter partes* review and they are not barred or estopped from requesting *inter partes* review.

## IX. MANDATORY NOTICES

### A. Real Party-in-Interest Under 37 C.F.R. §42.8(b)(1)

The real parties-in-interest are Kia Corporation, Kia America Inc., Toyota Motor Corp., Toyota Motor North America, Inc., and Toyota Motor Sales, U.S.A., Inc.

### B. Related Matters Under 37 C.F.R. §42.8(b)(2)

To the best of Petitioner's knowledge, the '659 patent is, or has been, involved in the following district court litigations and Board proceedings.

| Name                                                        | Number        | Court | Filed          |
|-------------------------------------------------------------|---------------|-------|----------------|
| <i>Emerging Automotive LLC v. Toyota Motor Corp. et al.</i> | 2:23-cv-00434 | EDTX  | Sept. 20, 2023 |
| <i>Emerging Automotive LLC v. Kia Corp. et al.</i>          | 2:23-cv-00437 | EDTX  | Sept. 22, 2023 |
| <i>Ex Parte</i> Reexamination of U.S. Pat. No. 11,738,659   | 90/019,456    | USPTO | Mar. 25, 2024  |

On December 13, 2023, the Toyota case and the Kia case were consolidated for pretrial purposes. The Kia case (2:23-cv-00437) is the lead case.

On April 15, 2024, the Office granted third-party Unified Patents, LLC's *ex parte* reexamination request of claims 1-21 of the '659 Patent. See EX1023. Of the references relied upon in this Petition, only Mikan was raised in the *ex parte* reexamination, and on grounds different from those presented herein. Unified Patents, LLC is neither an RPI in this proceeding nor a party in the district court litigations.

To the best of Petitioners' knowledge, the '659 patent is related to the following U.S. applications that had been pending as of the issuance of the '659 patent, and their corresponding issued patents (if applicable):

| <b>Application Number</b> | <b>Patent Number</b> | <b>Filing Date</b> |
|---------------------------|----------------------|--------------------|
| 61/478,436                |                      | 4/22/2011          |
| 13/452,882                | 9,123,035            | 4/22/2012          |
| 13/452,881                | 10,217,160           | 4/22/2012          |
| 61/745,729                |                      | 12/24/2012         |
| 61/757,020                |                      | 1/25/2013          |
| 61/760,003                |                      | 2/1/2013           |
| 61/763,453                |                      | 2/11/2013          |
| 13/784,823                | 9,285,944            | 3/5/2013           |
| 13/797,974                | 9,180,783            | 3/12/2013          |
| 13/797,982                |                      | 3/12/2013          |
| 13/842,158                | 9,229,905            | 3/15/2013          |
| 13/906,335                | 9,104,537            | 5/30/2013          |
| 13/911,072                | 9,809,196            | 6/5/2013           |
| 13/934,215                | 9,581,997            | 7/2/2013           |
| 13/937,202                | 9,346,365            | 7/8/2013           |
| 14/050,314                | 9,171,268            | 10/9/2013          |
| 61/896,007                |                      | 10/25/2013         |
| 14/063,638                | 9,189,900            | 10/25/2013         |
| 14/063,837                | 9,139,091            | 10/25/2013         |
| 14/145,693                | 9,372,607            | 12/31/2013         |
| 14/173,818                | 9,697,733            | 2/6/2014           |
| 14/176,138                | 9,697,503            | 2/9/2014           |

*Inter Partes Review*  
U.S. Patent No. 11,738,659

|            |            |            |
|------------|------------|------------|
| 14/222,670 | 9,348,492  | 3/23/2014  |
| 14/246,145 | 9,229,623  | 4/7/2014   |
| 14/251,537 | 9,230,440  | 4/11/2014  |
| 14/275,569 | 9,467,515  | 5/12/2014  |
| 14/281,892 | 9,545,853  | 5/20/2014  |
| 14/288,356 |            | 5/27/2014  |
| 14/303,442 | 9,365,188  | 6/12/2014  |
| 14/316,559 | 9,371,007  | 6/26/2014  |
| 14/338,636 | 9,648,107  | 7/23/2014  |
| 14/499,039 | 9,536,197  | 9/26/2014  |
| 14/595,186 | 9,177,305  | 1/12/2015  |
| 14/599,541 | 9,177,306  | 1/18/2015  |
| 14/602,256 | 9,129,272  | 1/21/2015  |
| 14/640,004 | 9,423,937  | 3/5/2015   |
| 14/672,038 | 10,286,919 | 3/27/2015  |
| 14/677,341 | 9,778,831  | 4/2/2015   |
| 62/185,578 |            | 6/27/2015  |
| 14/790,409 | 9,215,274  | 7/2/2015   |
| 14/801,803 | 9,193,277  | 7/16/2015  |
| 14/872,404 | 9,335,179  | 10/1/2015  |
| 14/880,970 | 9,579,987  | 10/12/2015 |
| 62/254,858 |            | 11/13/2015 |
| 14/949,883 | 9,493,130  | 11/24/2015 |
| 14/952,911 | 9,288,270  | 11/25/2015 |
| 14/987,755 | 10,218,771 | 1/4/2016   |
| 14/989,100 | 10,839,451 | 1/6/2016   |
| 14/997,429 |            | 1/15/2016  |
| 15/071,120 | 9,426,225  | 3/15/2016  |
| 15/085,094 | 10,286,842 | 3/30/2016  |
| 15/161,373 | 9,434,270  | 5/23/2016  |
| 15/180,306 | 9,499,129  | 6/13/2016  |
| 15/188,971 | 9,815,382  | 6/21/2016  |
| 15/191,506 | 9,597,973  | 6/23/2016  |
| 15/243,933 | 10,286,798 | 8/22/2016  |
| 15/243,948 | 10,225,350 | 8/22/2016  |
| 15/257,016 | 9,718,370  | 9/6/2016   |
| 15/290,430 | 10,223,134 | 10/11/2016 |
| 15/344,566 | 9,663,067  | 11/6/2016  |
| 15/351,422 | 9,672,823  | 11/14/2016 |
| 15/384,314 | 10,411,487 | 12/19/2016 |

*Inter Partes Review*  
U.S. Patent No. 11,738,659

|            |            |            |
|------------|------------|------------|
| 15/387,651 | 10,181,099 | 12/22/2016 |
| 15/404,574 | 10,274,948 | 1/12/2017  |
| 15/420,098 | 10,424,296 | 1/31/2017  |
| 15/444,892 | 10,396,576 | 2/28/2017  |
| 15/444,328 | 10,308,244 | 2/28/2017  |
| 15/463,287 | 9,738,168  | 3/20/2017  |
| 15/469,517 | 9,855,947  | 3/25/2017  |
| 15/469,520 | 9,963,145  | 3/25/2017  |
| 15/470,881 | 10,535,341 | 3/27/2017  |
| 15/607,418 | 10,407,026 | 5/26/2017  |
| 15/615,812 | 9,818,088  | 6/6/2017   |
| 15/657,112 | 9,802,500  | 7/22/2017  |
| 15/683,286 | 9,925,882  | 8/22/2017  |
| 15/696,618 | 9,928,488  | 9/6/2017   |
| 15/714,113 | 10,821,845 | 9/25/2017  |
| 15/723,790 | 9,916,071  | 10/3/2017  |
| 15/786,578 | 10,210,487 | 10/17/2017 |
| 15/787,295 | 10,071,643 | 10/18/2017 |
| 15/787,414 | 10,286,875 | 10/18/2017 |
| 15/787,677 | 10,453,453 | 10/18/2017 |
| 15/787,691 | 10,821,850 | 10/18/2017 |
| 15/788,419 | 10,289,288 | 10/19/2017 |
| 15/841,721 | 10,714,955 | 12/14/2017 |
| 15/854,241 | 10,442,399 | 12/26/2017 |
| 15/859,730 | 10,829,111 | 1/1/2018   |
| 15/927,975 | 10,086,714 | 3/21/2018  |
| 15/928,054 | 10,282,708 | 3/21/2018  |
| 15/972,198 | 10,576,969 | 5/6/2018   |
| 16/150,252 | 10,245,964 | 10/2/2018  |
| 16/280,020 | 11,017,360 | 2/19/2019  |
| 16/285,706 | 10,652,312 | 2/26/2019  |
| 16/290,936 | 10,554,759 | 3/3/2019   |
| 16/293,617 |            | 3/5/2019   |
| 16/405,036 | 11,132,650 | 5/7/2019   |
| 16/409,819 | 11,203,355 | 5/11/2019  |
| 16/411,109 | 10,824,330 | 5/13/2019  |
| 16/411,525 | 10,572,123 | 5/14/2019  |
| 16/552,885 | 11,518,245 | 8/27/2019  |
| 16/566,872 | 11,370,313 | 9/10/2019  |

**C. Lead and Back-Up Counsel Under 37 C.F.R. §42.8(b)(3)**

Petitioner provides the following counsel and service information. Petitioner consents to electronic service the email addresses listed in the table below. Pursuant to 37 C.F.R. §42.10(b), Powers of Attorney accompany this Petition.

| <b>Lead Counsel</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <b>Back-Up Counsel</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| For Kia:<br><br>James M. Glass (Reg. No. 46729)<br>jimglass@quinnemanuel.com<br><br>QUINN EMANUEL URQUHART<br>& SULLIVAN, LLP<br>51 Madison Avenue, 22 <sup>nd</sup> Floor<br>New York, NY 10010<br>Tel: (212) 849-7000<br>Fax: (212) 849-7100<br><br>For Toyota:<br><br>Joshua L. Goldberg (Reg. No. 59,369)<br>joshua.goldberg@finnegan.com<br><br>Finnegan, Henderson, Farabow,<br>Garrett & Dunner, LLP<br>901 New York Ave NW<br>Washington, DC 20001<br>Tel: 202-408-4000<br>Fax: 202-408-4400 | For Kia:<br><br>Quincy Lu (Reg. No. 76,954)<br>quincylu@quinnemanuel.com<br><br>QUINN EMANUEL URQUHART<br>& SULLIVAN, LLP<br>1109 First Avenue, Suite 210<br>Seattle, WA 98101<br>Tel: (206) 905-7000<br>Fax: (206) 905-7100<br><br>Ron Hagiz<br><i>Pro hac vice</i> forthcoming<br>ronhagiz@quinnemanuel.com<br><br>QUINN EMANUEL URQUHART<br>& SULLIVAN, LLP<br>51 Madison Avenue, 22 <sup>nd</sup> Floor<br>New York, NY 10010<br>Tel: (212) 849-7000<br>Fax: (212) 849-7100<br>Email:<br><br>Jeffrey S. Gerchick<br><i>Pro hac vice</i> forthcoming<br>jeffgerchick@quinnemanuel.com<br><br>QUINN EMANUEL URQUHART<br>& SULLIVAN, LLP<br>1300 I Street NW<br>Washington, DC 20005 |

|  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <p>Tel: (202) 538-8000<br/>Fax: (202) 538-8100</p> <p>Brett Watkins (Reg. No. 60,458)<br/>brettwatkins@quinnemanuel.com</p> <p>QUINN EMANUEL URQUHART<br/>&amp; SULLIVAN, LLP<br/>700 Louisiana St., Suite 3900<br/>Houston, TX 77002<br/>Tel: (713) 221-7000<br/>Fax: (713) 221-7100</p> <p>For Toyota:</p> <p>James R. Barney (Reg. No. 46,539)<br/>james.barney@finnegan.com</p> <p>Aidan Skoyles (Reg. No. 61,119)<br/>aidan.skoyles@finnegan.com</p> <p>Nicholas Eitsert (Reg. No. 78,843)<br/>nicholas.eitsert@finnegan.com</p> <p>Finnegan, Henderson, Farabow,<br/>Garrett &amp; Dunner, LLP<br/>901 New York Ave NW<br/>Washington, DC 20001<br/>Tel: 202-408-4000<br/>Fax: 202-408-4400</p> |
|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**D. Payment of Fees**

The undersigned authorizes the Office to charge the fee required for this Petition for *Inter Partes* Review to Deposit Account No. 50-5708. Any additional fees that might be due are also authorized.

Date: July 15, 2024

Respectfully submitted,

By: /s/ James M. Glass  
James M. Glass

*Counsel for Petitioners*

**CERTIFICATE OF COMPLIANCE WITH  
TYPE-VOLUME LIMITATION, TYPEFACE REQUIREMENTS,  
AND TYPE STYLE REQUIREMENTS**

1. This Petition complies with the type-volume limitation of 14,000 words, comprising 13,993 words, as counted using the Microsoft Word software that was used to prepare this paper, excluding the parts exempted by 37 C.F.R. §42.24(a).

2. This Petition complies with the general format requirements of 37 C.F.R. §42.6(a) and has been prepared using Microsoft® Word 2016 in 14-point Times New Roman.

Date: July 15, 2024

By: /s/ James M. Glass  
James M. Glass  
QUINN EMANUEL URQUHART  
& SULLIVAN, LLP  
51 Madison Avenue, 22<sup>nd</sup> Floor  
New York, NY 10010  
Tel: (212) 849-7000  
Fax: (212) 849-7100

*Counsel for Petitioners*

**CERTIFICATE OF SERVICE**

The undersigned certifies that the foregoing Petition for *Inter Partes* Review, the associated Powers of Attorney, and Exhibits 1001-1024 were served on July 15, 2024, on counsel of record for the subject patent by FedEx Priority Overnight at the addresses below.

| Correspondence Address of Record                                                                                   | Litigation Counsel                                                                  |
|--------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| Albert Penilla<br>PENILLA IP, APC - PATENT LAW<br>5619 Scotts Valley Drive<br>SUITE 280<br>Scotts Valley, CA 95066 | Marc Belloli<br>BUNSOW DE MORY LLP<br>701 El Camino Real,<br>Redwood City, CA 94063 |

Date: July 15, 2024

By: /s/ James M. Glass  
James M. Glass  
QUINN EMANUEL URQUHART  
& SULLIVAN, LLP  
51 Madison Avenue, 22<sup>nd</sup> Floor  
New York, NY 10010  
Tel: (212) 849-7000  
Fax: (212) 849-7100

*Counsel for Petitioners*