

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

TOYOTA MOTOR CORP. AND KIA CORPORATION,
Petitioners,

v.

EMERGING AUTOMOTIVE LLC,
Patent Owner.

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

PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 11,104,245

TABLE OF CONTENTS

LIST OF EXHIBITS.....	v
I. Preliminary Statement	1
II. Precise Relief Requested	2
III. The '245 Patent.....	3
A. Disclosure.....	3
B. File History.....	6
C. Priority Date	6
1. Legal standard.....	7
2. The pre-October 2013 applications do not disclose “electronic key[s]”	8
IV. The Prior Art.....	9
A. <i>Kleve</i> (Ex.1005).....	9
B. <i>Zaid</i> (Ex.1008).....	11
C. <i>Mottla</i> (Ex.1006) and <i>Goudy</i> (Ex.1007)	13
V. Level of Ordinary Skill.....	13
VI. Claim Construction.....	14
VII. Claims 1-8, 11-18 Are Unpatentable Over the Prior Art	14
A. Ground 1: <i>Kleve</i> and <i>Mottla</i> Render Obvious Claims 1-8, 11-18.....	14
1. Combination of <i>Kleve</i> and <i>Mottla</i>	14
2. Independent Claim 1	15
3. Claim 2.....	25
4. Claim 3	26

5.	Claim 4.....	28
6.	Claim 5.....	30
7.	Claim 6.....	32
8.	Claim 7.....	32
9.	Claim 8.....	33
10.	Claim 11.....	34
11.	Claim 12.....	34
12.	Claim 13.....	35
13.	Claim 14.....	35
14.	Claim 15.....	36
15.	Claim 16.....	37
16.	Claim 17.....	37
17.	Claim 18.....	38
B.	Ground 2: Kleve, Mottla, and Goudy Render Obvious Claims 9-10.....	39
1.	Combination of Kleve, Mottla, and Goudy.....	39
2.	Claim 9.....	40
3.	Claim 10.....	41
C.	Ground 3: Zaid, Kleve, and Mottla Render Obvious Claims 1-8, 11-18.....	42
1.	Combination of Zaid, Kleve, and Mottla.....	42
2.	Independent Claim 1.....	43
3.	Claim 2.....	59
4.	Claim 3.....	60

5.	Claim 4.....	62
6.	Claim 5.....	63
7.	Claim 6.....	64
8.	Claim 7.....	66
9.	Claim 8.....	67
10.	Claim 11.....	68
11.	Claim 12.....	70
12.	Claim 13.....	70
13.	Claim 14.....	70
14.	Claim 15.....	71
15.	Claim 16.....	73
16.	Claim 17.....	74
17.	Claim 18.....	74
D.	Ground 4: Zaid, Kleve, Mottla, and Goudy Render Obvious	
	Claim 10.....	76
1.	Combination of Zaid, Kleve, Mottla, and Goudy.....	76
2.	Claim 9.....	76
3.	Claim 10.....	78
VIII.	Grounds for Standing.....	78
IX.	Mandatory Notices.....	78
A.	Real Party-in-Interest Under 37 C.F.R. § 42.8(b)(1).....	78
B.	Related Matters Under 37 C.F.R. § 42.8(b)(2).....	79
C.	Lead and Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3).....	83

D. Service Information Under 37 C.F.R. § 42.8(b)(4).....84

X. Conclusion84

LIST OF EXHIBITS

Exhibit	Description
Ex.1001	U.S. Patent No. 11,104,245 to <i>Penilla</i> et al.
Ex.1002	Prosecution File History for U.S. Patent No. 11,104,245
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 Robert Bruce Kleve et al.
Ex.1006	U.S. Patent Pub. No. 2011/0060480 to Lesley Mottla et al.
Ex.1007	U.S. Patent Pub. No. 2005/0038573 to Roy Goudy
Ex.1008	U.S. Patent Pub. No. 2011/0112969 to Sam Zaid et al.
Ex.1009	Prosecution File History for U.S. Patent No. 11,738,659
Ex.1010	U.S. Patent Application No. 61/478,436
Ex.1011	U.S. Patent Application No. 61/745,729
Ex.1012	U.S. Patent Application No. 13/452,882
Ex.1013	U.S. Patent Application No. 13/842,158
Ex.1014	U.S. Patent Application No. 14/063,638
Ex.1015	Claim Construction Order in <i>Emerging Automotive LLC v. Kia Corporation et al.</i> , No. 2:23-cv-00437 (E.D. Tex. Sept. 22, 2023)
Ex.1016	Plaintiff's Opposition to Defendants' Motion for Summary Judgement Regarding Effective Filing Dates in <i>Emerging Automotive LLC v. Kia Corporation et al.</i> , No. 2:23-cv-00437 (E.D. Tex. May 5, 2025)
Ex.1017	Wayback Machine archive of www.broadcom.com/products/applications/Automotive from Jan. 19, 2012

Exhibit	Description
Ex.1018	Datasheet for Broadcom BCM4325
Ex.1019	Final Rejection filed in Reexamination No. 90/019,456 (U.S. Pat. No. 11,738,659)

LIST OF CHALLENGED CLAIMS

Claim	Limitation
1[pre]	A vehicle, comprising,
1[a]	an on-board computer of the vehicle;
1[b]	a first system of the vehicle interfaced with the on-board computer of the vehicle for enabling unlocking of the vehicle;
1[c]	a second system of the vehicle interfaced with the on-board computer of the vehicle for enabling starting of the vehicle for use of the vehicle; and
1[d]	communications circuitry of the vehicle interfaced with the on-board computer of the vehicle, the communications circuitry is configured to process program instructions to enable communication with a server and to enable communication with a mobile device;
1[e]	wherein the communications circuitry of the vehicle is configured to receive coded data from the mobile device for unlocking and use of the vehicle,
1[f]	the coded data from the mobile device including a unique access code received by the mobile device from the server,
1[g]	wherein the unique access code is associated with privileges set via the server responsive to a restriction set by an administrator of the vehicle, the restriction is associated with a mode of allowed use of the vehicle, and privileges are for the unique access code,
1[h]	and a camera of the vehicle is used for capturing video of an area that includes the vehicle during a period of time in which the unique access code is to be active, such that actions taken by a user using an electronic key (e-key) is recorded;

1[i]	wherein the unique access code functioning for the e-key ¹ that is managed via one or more graphical user interface inputs rendered on a screen of the mobile device.
2	The vehicle of claim 1, wherein the vehicle is configured to receive information from the server to authenticate the coded data received from the mobile device to activate the e-key.
3[a]	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,
3[b]	each request is associated with a unique access code generated by the server, such that each unique access code is associated with a user account having respective privileges assigned by the administrator of the vehicle that enables assigning or use of e-keys to use the vehicle,
3[c]	wherein one unique access code is active at a particular time when using e-keys.
4	The vehicle of claim 1, wherein said vehicle is identified as available for sharing and is discoverable via an application based on a geographic location of the vehicle.

¹ Petitioner notes that, as allowed, this limitation recited “the unique access code functioning *as an electronic key* (e-key) that is managed via one or more graphical user interface inputs rendered on a screen of the mobile device.” Ex. 1002, 114. Whether the claim is interpreted as allowed (“as an electronic key”), or as issued (“for the e-key”), the limitation is rendered obvious by *Mottla*.

5	The vehicle of claim 1, wherein an application accessed by said mobile device is configured to enable finding a geolocation of said vehicle and enables requesting use of said vehicle to receive said unique access code.
6	The vehicle of claim 1, wherein an application accessed by said mobile device is configured to enable sending instructions to said server to enable sharing said vehicle with the user to enable use of the e-key or another e-key on said vehicle, wherein the e-key has functions enabled via graphical user interfaces of the application of the mobile device.
7	The vehicle of claim 1, wherein the unique access code is obtained by the mobile device responsive to a computer requesting assignment of the e-key to the mobile device, the assignment being enabled when the assignment is by an owner of said vehicle or the administrator of said vehicle.
8[a]	The vehicle of claim 7, wherein the vehicle is a sharable vehicle, and said privileges are defined for each sharing session of the vehicle,
8[b]	wherein the on-board computer collects use data of the vehicle while the e-key is active for use of the vehicle, the collected data being saved to the server.
9	The vehicle of claim 1, wherein the mode of allowed use of the vehicle includes limits on use of vehicle interfaces for safety during driving of the vehicle.
10	The vehicle of claim 1, wherein the mode of allowed use of the vehicle includes disabling of controls of vehicle interfaces.
11	The vehicle of claim 1, wherein the mode of allowed use of the vehicle 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 said restriction is detected.
12	The vehicle of claim 1, wherein the mode of allowed use of the vehicle is programmed to cause generation of a notification to the administrator when a violation of the restriction is detected.

13	The vehicle of claim 12, wherein 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.
14	The vehicle of claim 1, wherein the mode of allowed use of the vehicle is configured to cause generation of a notification on a display of the vehicle identifying the restriction when detected.
15	The vehicle of claim 1, wherein the server is part of a cloud processing system and the cloud processing system is configured to manage user accounts and manage use of said e-key.
16	The vehicle of claim 1, wherein said restriction is for a geolocation.
17	The vehicle of claim 1, wherein said restriction enables access to specific vehicle areas that include one or more of vehicle door operation, or trunk operation.
18	The vehicle of claim 1, wherein the mode of allowed use is to enable access to a trunk of the vehicle, and the mode is associated with instructions to notify the administrator or an owner of the vehicle when said trunk is accessed using the e-key.

I. Preliminary Statement

Toyota Motor Corporation and Kia Corporation request IPR of all claims of U.S. Patent No. 11,104,245, assigned to Emerging Automotive LLC (“EA”).

The ’245 patent discloses that “access [to a 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.” 10:31-33. “[T]he 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.,...amount of time the e-keys will be valid (or else expire)), and requesting that e-keys be sent to the recipient.” *Id.*, 10:33-42.

The ’245 Patent’s claims are similar to U.S. Patent Nos. 9,365,188 and 11,738,659, which Petitioners challenged based on a prior art reference *Kleve* (*see* IPR2024-00981 (Paper 10) and IPR2024-01167 (Paper 14)). The ’245 Patent’s claims are also similar to U.S. Patent No. 10,407,026, the primary difference being the addition of a camera for capturing video while an e-key is used (Ex.1002, 228-29, 249). *Kleve* discloses this limitation too. *See infra* §VII.A.2.1[h].

This Petition raises two primary grounds: *Kleve*, like IPR Nos. 2024-00981 and 2024-01167, and *Zaid*, tracking the Examiner’s arguments during prosecution

and arguments raised in the '026 Patent IPR², but adding *Kleve* regarding the “camera” limitation that mistakenly led to allowance.

II. Precise Relief Requested

Petitioners request review and cancellation of claims 1-18 based on the following art and grounds.

References
<i>Kleve</i> (Ex.1005), U.S. Patent Pub. No. 2014/0129053 (filed Nov. 7, 2012) (§§ 102(a)(2) or pre-AIA § 102(e)).
<i>Mottla</i> (Ex.1006), U.S. Pat. Pub. No. 2011/0060480 (filed June 8, 2010, published Mar. 10, 2011) (§§ 102(a)(1), (2) or pre-AIA § 102(a), (b), (e))
<i>Goudy</i> (Ex.1007), U.S. Pat. Pub. No. 2005/0038573 (filed Aug. 11, 2003, published Feb. 17, 2005) ((§§ 102(a)(1), (2) or pre-AIA § 102(a), (b), (e))

² See IPR2024-00785. There, the Board initially denied institution because a limitation was not shown in *Zaid. Id.*, Paper No. 11. On rehearing, the Board agreed that *Zaid* did disclose the purportedly missing limitation. *Id.*, Paper No. 13, 8-9. Nevertheless, the Board denied institution based on *Fintiv. Id.*, 10-16.

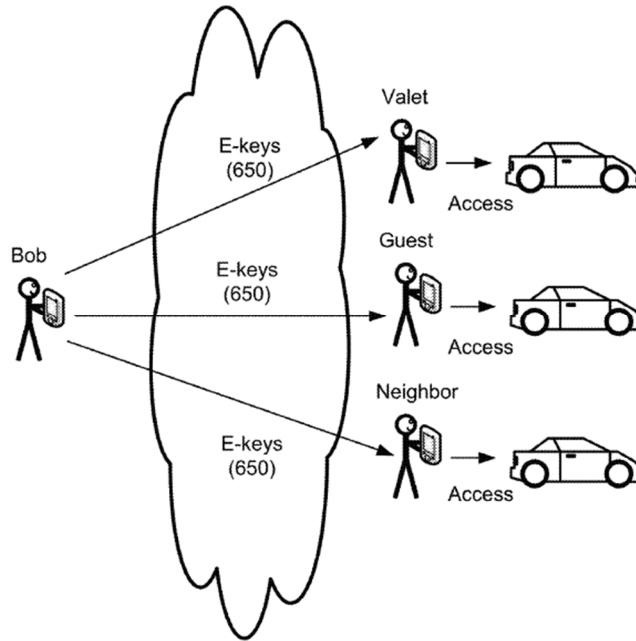
References
<p><i>Zaid</i> (Ex.1008), U.S. Patent Pub. No. 2011/0112969 (filed Oct. 28, 2010, published May 12, 2011) (§§ 102(a)(1), (2) or pre-AIA §§ 102(a), 102(b), 102(e)).</p>

Ground	Basis	Reference(s)	Claims
1	§103	<i>Kleve, Mottla</i>	1-8, 11-18
2	§103	<i>Kleve, Mottla, Goudy</i>	9, 10
3	§103	<i>Zaid, Kleve, Mottla</i>	1-8, 11-18
4	§103	<i>Zaid, Kleve, Mottla, Goudy</i>	9, 10

III. The '245 Patent

A. Disclosure

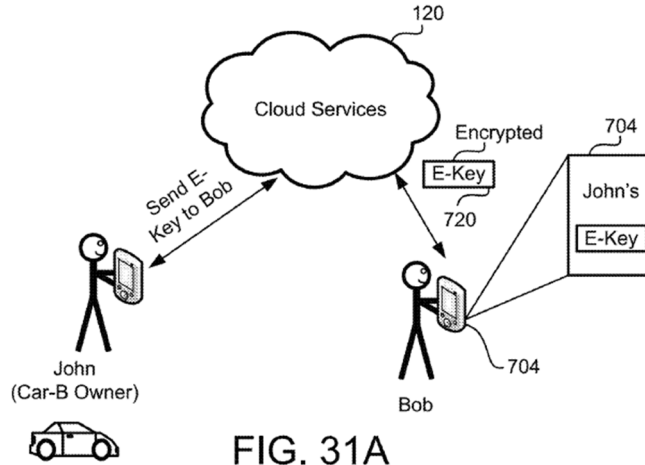
The '245 Patent describes a vehicle owner assigning an e-key to a user. Ex.1001 43:26-40. In Fig. 29, vehicle owner shares electronic keys 650 with “valet,” “guest,” and “neighbor.” *Id.*, 43:26-28. “[E]ach e-key...will include a unique access code or substantially unique access code.” *Id.*, 43:41-42. “The unique generation of access codes enables each electronic keyed [sic] to be different for each user and each e-key can expire at any time set by a requesting user.” *Id.*, 43:49-53.



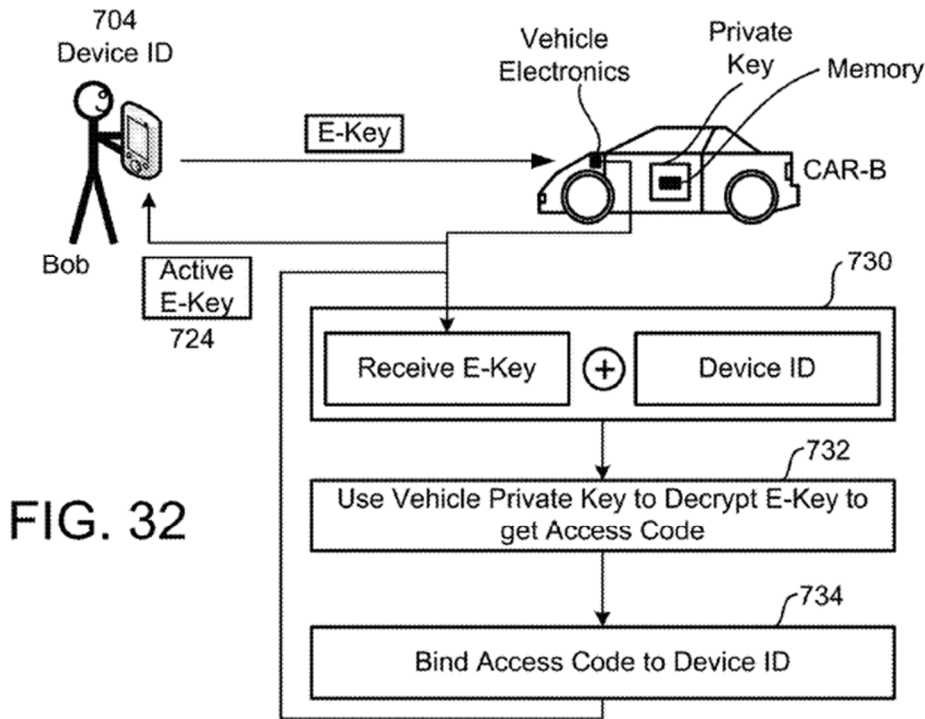
'245 Patent, Fig. 29.

In Fig. 31A, vehicle owner utilizes cloud server 120 to send an encrypted e-key to a guest. “[T]he server will generate an access code for the vehicle” (*id.*, 44:43-45), which “will then be encrypted by the server and then sent as encrypted e-keys 722³ to Bob’s device 704.” *Id.*, 44:45-48.

³ “Encrypted e-keys 722” is likely a typo referring to encrypted e-keys 720.



'245 Patent, Fig. 31A.



...

704

In Fig. 32 the e-key is associated with the guest's device seeking to utilize the e-key. At 732, "the vehicle private key is used to decrypt the e-keys to get access to an access code." *Id.*, 45:11-12. At 734, "[t]he access code is then sent as

activated e-keys 724 back to Bob’s device 704,” allowing Bob’s device to access the vehicle. *Id.*, 45:15-19. The unique access code “can be ... [an] incremental number generator, or any other generation device that can generate codes that are unique or substantially unique.” *Id.*, 45:58-61.

B. File History

The ’245 Patent was originally filed on October 15, 2019, as the latest in a string of applications beginning with a provisional on April 22, 2011. Ex.1002, 516.

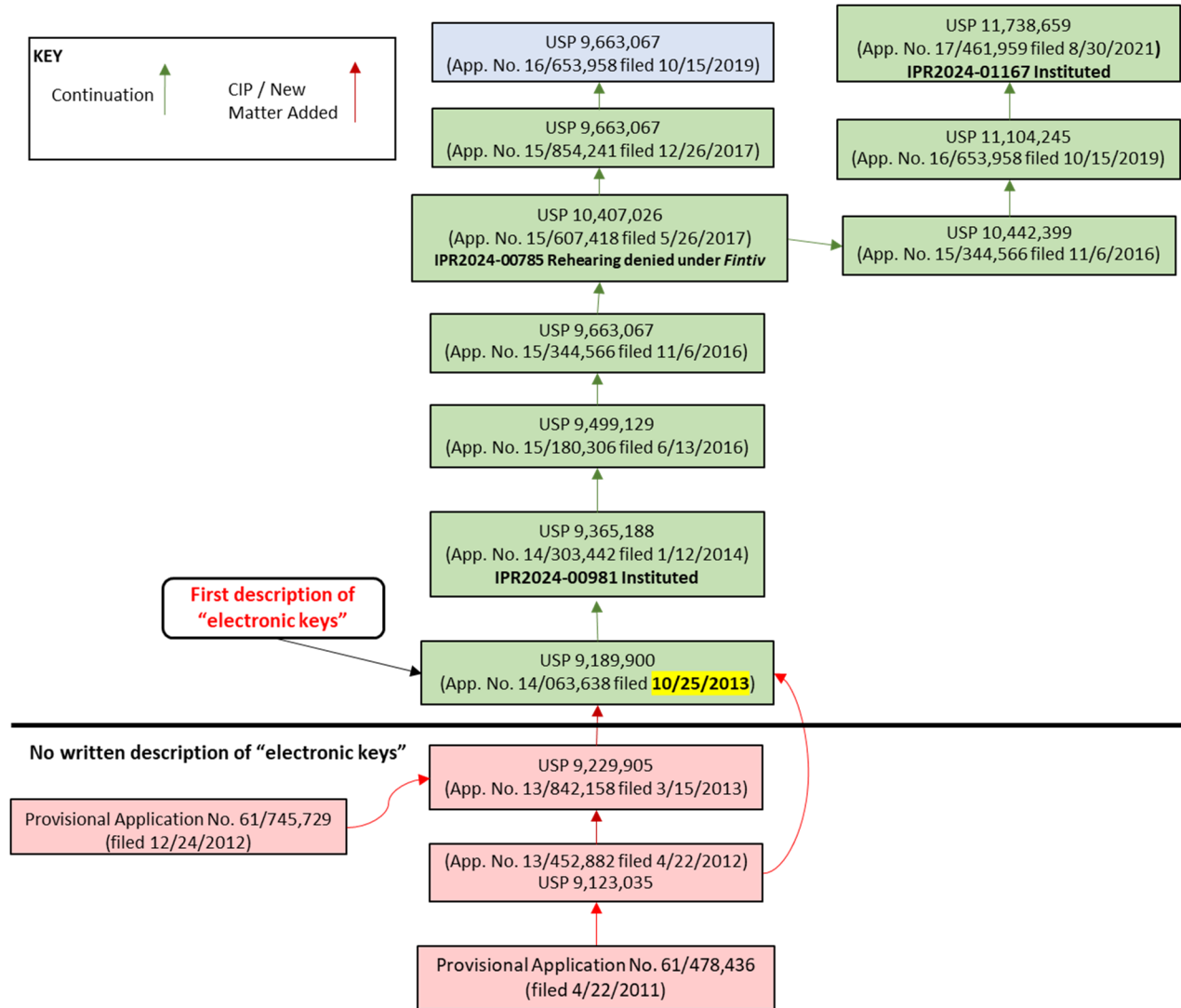
All claims were rejected for nonstatutory double patenting over, among others, U.S. Patent No. 10,407,026 (*see* IPR2024-00785), and as obvious over U.S. Patent Publication No. 2011/0112969 (“*Zaid*”) in view of U.S. Patent Publication No. 2011/0060480 (“*Mottla*”). *Id.*, 383-85; Exs. 1006, 1008.

In response, Applicants amended some claims and included 11 new claims, including claim 16 requiring a camera. *Id.*, 361-63. The Examiner indicated that new claim 16 would be allowable if rewritten in independent form. *Id.*, 249. After further rejections, Applicants cancelled claim 1 and amended all claims to depend from claim 16. *Id.*, 110-16, 230-31. The Examiner then allowed the claims, *id.*, 8, without considering *Kleve*.

C. Priority Date

The ’245 patent claims priority to several applications, illustrated below.

Inter Partes Review
U.S. Patent No. 11,104,245



The '638 application, a continuation-in-part filed on October 25, 2013, first introduces "e-keys." Accordingly, the '245 patent claims, which all recite electronic keys, are not entitled to a filing date before October 25, 2013. *Kleve* is prior art under the October 25, 2013 priority date. *Mottla*, *Zaid*, and *Goudy* are prior art even under the earliest provisional application to which the '245 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 an “electronic key,” a “unique access code” functioning for the “e-key,” and an “e-key” managed by a GUI on a mobile device. However, no earlier application discloses “e-keys” or anything similar.

The ’638 Application, filed October 25, 2013, introduced new material directed to e-keys. Ex.1014. Almeroth, ¶64. Figs. 17-35 and descriptions discuss electronic keys and unique access codes. Ex.1014, [0051], [0188], [0233]-[0269]; Ex. 1004, ¶64.

The earlier applications did not include these disclosures, or any other disclosures relating to e-keys, and a POSITA would have understood that control of

the vehicles in these applications did not use e-keys. Almeroth, ¶¶67-70. The '158 Application is directed to sending vehicle user profiles from a server to a mobile device defining vehicle settings. Ex.1014, Abstract. The '882 Application and provisionals are directed to EV charging. Ex.1013, Abstract; Exs.1011-1012. Thus, a POSITA would not have considered the Applicant to be in possession of the e-key subject matter. Almeroth, ¶71.

In a recent third-party *ex parte* reexamination request, the Office considered the priority date of the '659 Patent. The Office determined that “[t]he claims of the ['659 Patent] include subject matter first introduced in the '638 application and are therefore being examined with a benefit date no earlier than 10/25/2013.” Ex.1019,

3. Petitioners agree.

IV. The Prior Art

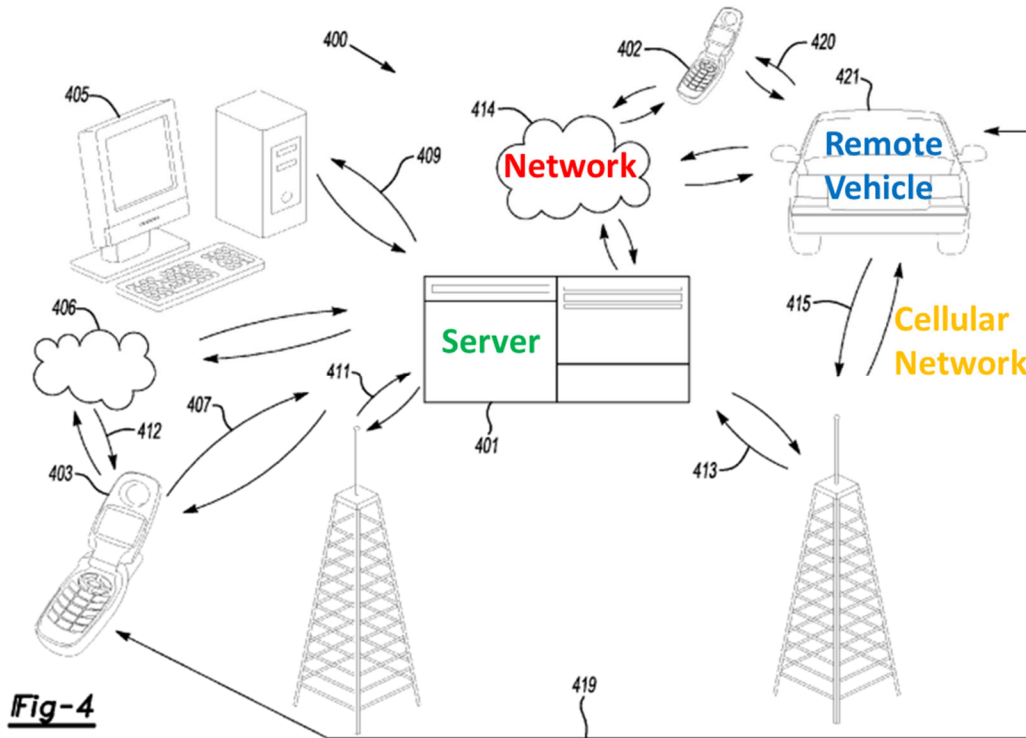
In an IPR regarding a parent to the '245 patent, Patent Owner did not dispute that *Kleve*, *Zaid*, or *Mottla* were prior art. *See* IPR2024-00981 (Paper No. 16).

A. *Kleve* (Ex.1005)

Kleve describes a short-term vehicle rental system. Through website accounts, Vehicle Owners (VO) and Temporary Users (TU) negotiate conditional rental agreements. TU provides identifying information to the VO who submits it to the server to generate a time-limited virtual key. The virtual key is sent to TU's

device and the vehicle to allow access. *Kleve*, Fig. 2, step 210, [0036] (“distribut[e] a virtual key to [TU]...”).

Kleve discloses in-vehicle wireless communication circuitry for server communications. *Kleve*, [0057], [0060].



Kleve, Fig. 4 (annotated).

Kleve continuously monitors the TU. *Kleve*, [0041-42]. Monitoring includes a “dashboard camera” [0079] to record the user while using the virtual key. *Id.*, [0073] (“[D]uring the rental term the VCS may monitor the Temporary User’s utilization of the vehicle...For example, the system may monitor that the actual authorized renter is the one driving the vehicle with the use of an interior viewing camera[.]”).

Kleve provides various illustrations of its shared vehicle system. Fig. 1 describes a block diagram of the main VCS and its interactions with the network. [0021]. Fig. 2 illustrates the general steps involved in renting a vehicle via *Kleve*'s rental micro-business. [0036]. Fig. 3 illustrates a vehicle with additional monitoring and control features in the same rental micro-business. [0046]. Fig. 4 illustrates the communication pathways between users, owners, server, and vehicle. [0056]. Fig. 5 illustrates a further addition to the micro-rental business where the vehicle is accessed via a "keyless transaction." [0062]. Fig. 6 illustrates the system for distributing virtual keys to a vehicle and a nomadic device. [0069]. Fig. 7 illustrates the functionality on the VCS as the vehicle monitors rental usage. [0075]. Figs. 8 and 9 illustrate the rental process interactions from VO and TU's perspective, respectively. [0081, 0086]. All disclosures describe *Kleve*'s shared vehicle system.

B. *Zaid* (Ex.1008)

Zaid discloses a car sharing system where renters use mobile devices to find, unlock, and start vehicles. Ex.1005 (*Zaid*), [0067-69]. The mobile device receives an e-key from a server and sends an encrypted vehicle reservation to the vehicle for access and use. *Id.*, [0070].

Zaid **vehicle** has a "vehicle access kit." *Zaid*, [0075], [0085]. It receives a vehicle reservation from a user's **wireless communication device**, e.g.,

smartphone. *Id.*, [0082], [0135]. The wireless communication device

communicates via a **cloud network** with a server (**yellow**). *Id.*, [0075-76].

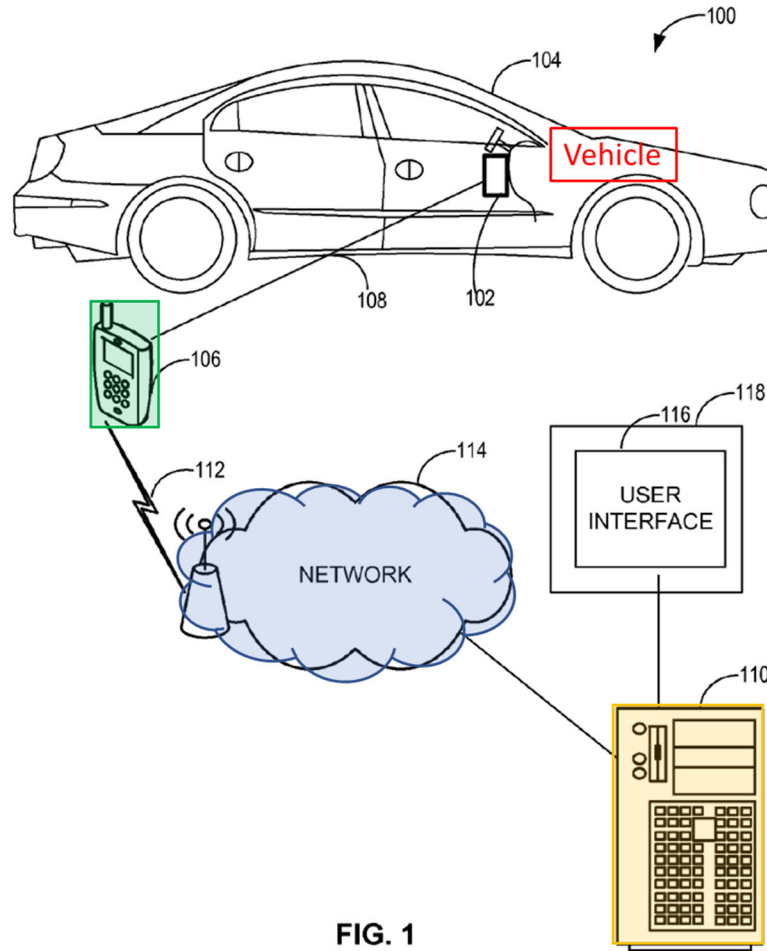


FIG. 1

Zaid, Fig. 1 (annotated).

Zaid's server interacts with vehicles to provide rental options. *Zaid*, [0079-80]. Customers make vehicle reservations, which are communicated to the server, processed into vehicle reservations, and encrypted. *Id.*, [0076], [0099], [0125]. The server sends the reservation to the vehicle. *Id.*, [0128]. The vehicle access

component decrypts the request and permits the customer to unlock and start for a specific time. *Id.*, [0129-31]. When the time elapses, access is withdrawn. *Id.*

In *Zaid*, “communications, including vehicle reservation communications, ...includes [sic] a unique increment for each message to avoid repeat message attack. In various embodiments, the unique increment is in the form of a counter and/or time stamp that indicate the uniqueness of the message to avoid a repeat message attack.” *Id.*, [0081]. Thus, each vehicle reservation is uniquely identified.

Zaid was discussed extensively during prosecution of the '245 Patent. §III.B. The Examiner found that *Zaid* disclosed all limitations of claim 1 other than the camera, which *Kleve* discloses, and the user interface, which *Mottla* discloses. The Examiner also found that *Zaid* disclosed many dependent limitations.

C. *Mottla* (Ex.1006) and *Goudy* (Ex.1007)

Motta (Ex.1006) and *Goudy* (Ex.1007) demonstrate well-known elements of electronic systems, namely, determining user interfaces (*Mottla*) and limiting access to infotainment systems (*Goudy*). *Mottla*, [0044]; *Goudy*, [0008-11].

V. Level of Ordinary Skill

A skilled artisan 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. Petitioners' expert exceeded this by 2013. Ex.1004, ¶84-87.

VI. Claim Construction

The District Court construed “electronic key”/“eKey”/“e-key” as “electronic data that enables one or more functions of the vehicle.” Ex.1015. Claims only need to be construed to the extent necessary, and no other terms need construction here.

VII. Claims 1-8, 11-18 Are Unpatentable Over the Prior Art

A. Ground 1: *Kleve* and *Mottla* Render Obvious Claims 1-8, 11-18

1. Combination of *Kleve* and *Mottla*

Kleve discloses nearly all limitations, other than the graphical user interface (1[i]), but that was shown in *Mottla* and would have been obvious to combine with *Kleve*. Both are analogous art to the '245 patent because the references are from the same field of endeavor (electronic key systems); and/or (2) are reasonably pertinent to the problem faced by the inventor (controlling vehicle systems to provide added functionality and improve user experience). *Compare* '245 Patent, 2:23-29 *with* Ex.1005 [0007] and Ex.1006 [0033].

Kleve's “vehicle rental micro-business” utilizes “a “virtual key” for “enabl[ing] the keyless drive system for the appropriate Temporary User during a given rental period.” *Kleve*, [0036], [0039]. *Mottla* discloses a graphical user interface for a car sharing system where users choose vehicles by clicking icons on a map, then reserve the vehicles for time periods, and receive an electronic key on

their mobile device. *Mottla*, [0029]. Both implement e-keys via a mobile device for conveying shared vehicle access. It would have been obvious to combine *Kleve* with the graphical user interface of *Mottla*. Almeroth at ¶¶102-105.

2. Independent Claim 1

1[preamble]: “A vehicle, comprising,”

Kleve discloses a vehicle. *Kleve*, [0056], Fig. 4. Accordingly, *Kleve* discloses the preamble. Almeroth, ¶106.

1[a]: “an on-board computer of the vehicle;”

Kleve’s vehicle includes an on-board computer, a “vehicle based computing system (VCS).” *Kleve*, [0021], Fig. 1. VCS is a computer with a processor that is “provided within the vehicle.” *Id.*, [0022].

Accordingly, *Kleve* discloses this limitation. Almeroth, ¶¶107-08.

1[b]: “a first system of the vehicle interfaced with the on-board computer of the vehicle for enabling unlocking of the vehicle;”

Kleve’s vehicle includes a first system, an unlocking system, for enabling unlocking the vehicle interfaced with the VCS. *Kleve* discloses that when a Temporary User “arrives at the vehicle within the scheduled rental time” they enter a virtual key. *Kleve*, [0070] “One method [for entering the key] may include having the Temporary User scan their finger with the use of a fingerprint scanner integrated with the VCS to validate authorization to access the vehicle.” *Id.* *Kleve*

discloses that after using the virtual key to access the vehicle via the VCS, “the Temporary User may again input the same identifying credentials to unlock and drive.” *Id.*, [0071]. Because the VCS is used to validate the user “to access the vehicle” and “unlock,” the first system for enabling unlocking is interfaced with the VCS. *Id.*, [0070-71].

Accordingly, *Kleve* discloses this limitation. Almeroth, ¶¶109-10.

1[c]: “a second system of the vehicle interfaced with the on-board computer of the vehicle for enabling starting of the vehicle for use of the vehicle; and”

Kleve’s vehicle includes a second system, a starting system, interfaced VCS for enabling starting the vehicle. After using the virtual key via the VCS, “the Temporary User may again input the same identifying credentials to unlock and drive.” *Kleve*, [0071]. Because the VCS permits the user to *drive* the vehicle, the system for starting the vehicle is interfaced with the VCS.

Accordingly, *Kleve* discloses this limitation. Almeroth, ¶¶111-12.

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

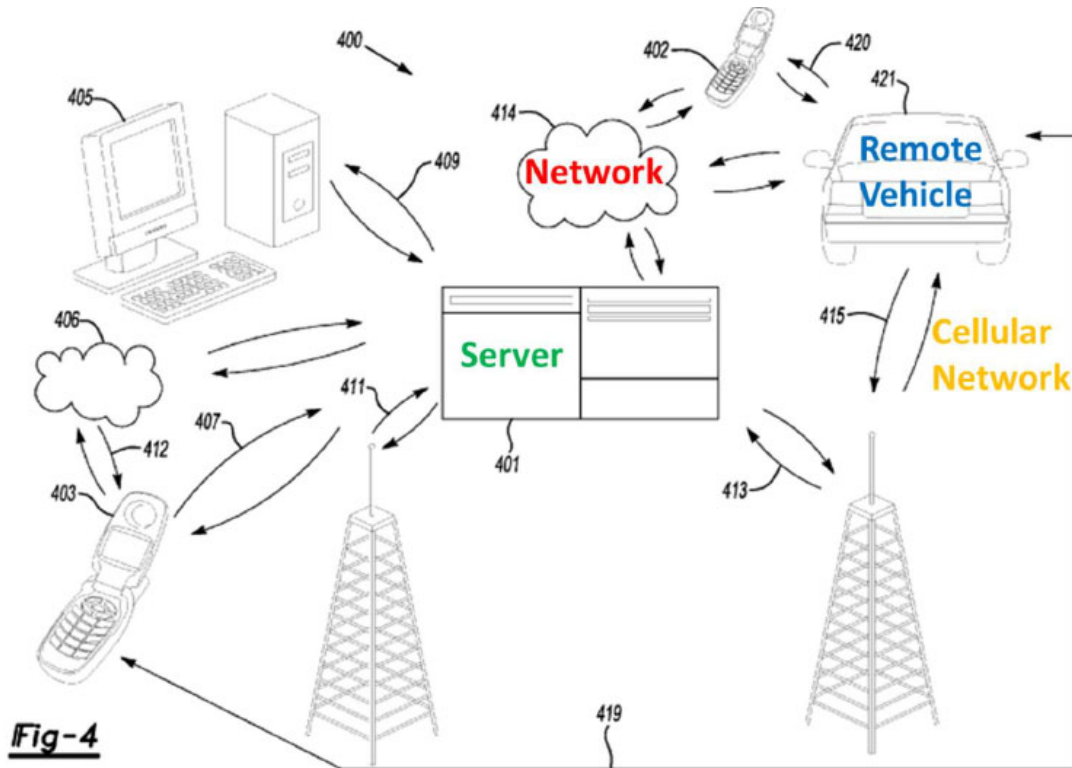
Kleve’s vehicle includes communications circuitry including Bluetooth, Wi-Fi, cellular, and a matrix barcode scanner. *Kleve*, [0061], [0066]. For example, *Kleve*’s vehicle is “outfitted with a communication transceiver, such as, but not

limited to, a BLUETOOTH transceiver.” *Id.*, [0061], [0027]. This transceiver is configured to process program instructions to enable communication with a mobile device such as a “temporary user nomadic device 402” via a wireless connection 420. *Id.*, [0025-27] (“Pairing a nomadic device 53 and the Bluetooth transceiver can be instructed through a button 52[.]”) [0029] (“modem application software may access an embedded module or firmware on the Bluetooth transceiver to complete wireless communication with a remote Bluetooth transceiver (such as that found in a nomadic device”), [0061].

Kleve’s vehicle includes a communication transceiver for cellular or Wi-Fi (*Kleve*, [0061]) configured to process program instructions to enable communication with a server such as “server(s) 401” via a cellular network 415. *Kleve*, [0028], [0060] (Wi-Fi module used as relay to send data to server).

Figure 1 illustrates BT transceiver 15, cellular communications transceiver modem 63, Wi-Fi router 73 all interfaced with the CPU 3 of VCS 1. *See Kleve*, Fig. 1.

These components are illustrated in Figure 4, showing communication between vehicle and mobile device, and between vehicle and server.



Kleve's vehicle also includes a matrix barcode scanner processing instructions to enable communication by reading the barcode (“communicating”) with the mobile device. *Kleve*, [0044], [0066]. Because the barcode is “recognized by the VCS,” the barcode scanner is interfaced with the on-board computer. *Id.* [0044].

Accordingly, *Kleve* discloses this limitation. Almeroth, ¶¶113-119.

1[e]: “wherein the communications circuitry of the vehicle is configured to receive coded data from the mobile device for unlocking and use of the vehicle,”

Kleve's communication circuitry receives coded data from the mobile device for unlocking and use of the vehicle. When *Kleve*'s Temporary User "arrives at the vehicle within the scheduled rental time" they enter a virtual key. *Kleve*, [0036], [0039], [0070]. *Kleve* discloses that the virtual key may be a "matrix barcode" (i.e., coded data) that can be transmitted from the mobile device to the vehicle's VCS for authorization via the matrix barcode scanner, and therefore for unlocking and use of the vehicle. *Id.*, [0037], [0044] ("The [Temporary User's] smart phone may be used to communicate the matrix barcode information to the vehicle rental micro-business system directly... Once the Temporary User has the matrix barcode scanned by the vehicle, the smart phone may be able to connect with the VCS and be used to enter and enable the vehicle drive away event.").

Accordingly, *Kleve* discloses this limitation. Almeroth, ¶¶120-21.

**1[f]: the coded data from the mobile device including
a unique access code received by the mobile device
from the server,"**

Kleve's matrix barcode includes a unique access code received by the mobile device from the server. *Kleve*'s a server 634, part of a "micro-business administrative system," is "used to communicate between a vehicle Owner nomadic device 601, a Temporary User nomadic device 611, and a vehicle computing system 621." *Kleve*, [0069]. The Vehicle Owner uses server 634 to generate the matrix barcode. *Id.* The server then sends the matrix barcode to the

Temporary User’s nomadic device, where it may be used as the virtual key to access and use the vehicle. *Id.* (“At step 616, the virtual key is generated and sent to the Temporary User.”); *see also id.*, [0044]. The matrix barcode, i.e., coded data, encodes a unique access code within the two-dimensional matrix. *See* Fig. 5.

Almeroth, ¶122. *Kleve* describes the matrix barcode as a type of “unique Temporary User identification” because, like a fingerprint or photo ID, the matrix barcode contains or encodes unique information (i.e., a unique access code) that is used by the vehicle to ensure that the intended TU is being given access to the vehicle. *Kleve*, [0069].



Accordingly, *Kleve* discloses this limitation. Almeroth, ¶123.

1[g]: “wherein the unique access code is associated with privileges set via the server responsive to a restriction set by an administrator of the vehicle, the restriction is associated with a mode of allowed use of the vehicle, and privileges are for the unique access code,”

Kleve’s unique access code, encoded within the virtual key as a matrix barcode, is associated with privileges, such as privileges to unlock and drive a vehicle during a time of use. *Kleve*, [0039] (virtual key enables “keyless drive system...during a given rental period”). Each virtual key is tied to a time of use

and so the privileges are for the unique access code. *Id.*, [0039], [0069]. The privileges are set via the server responsive to a restriction set by an administrator of the vehicle. *Id.*, [0037] (owner sets when vehicle is “available for rent”); [0040] (“Owner may have access to control usage of the vehicle being rented...”).

The restriction is associated with a mode of allowed use, because while the rental is underway “braking, steering, throttle, and accelerator pedal positions” are monitored to ensure that the driver is staying within a normal driving mode. *Id.*, [0042], [0053].

Accordingly, *Kleve* discloses this limitation. Almeroth, ¶¶124-26.

1[h]: “and a camera of the vehicle is used for capturing video of an area that includes the vehicle during a period of time in which the unique access code is to be active, such that actions taken by a user using an electronic key (e-key) is recorded;”

Kleve’s vehicle includes a camera for capturing video of the vehicle during a time in which the unique access code is active, such that actions taken by a user using the electronic key are recorded. *Kleve*’s vehicle has an “interior viewing camera” recording monitoring information that would be “sent to the vehicle owner...if the [temporary user] exceed[s] or violate[s] a restriction limit.” *Kleve*, [0073], [0076] (“continuous monitoring” via “camera system” which “start[s] and end[s] when the ignition key is turned on and off,” [0077]). *Kleve*’s camera includes a “dashboard camera” to “continue to check to see if continued usage of

the vehicle is acceptable based on [collected data].” *Id.*, [0079]. Data is collected while the unique access code is active, because it occurs while the Temporary User uses the vehicle, i.e., the time when the unique access code is active. *Id.*, [0079], [0080].

Accordingly, *Kleve* discloses this limitation. Almeroth, ¶¶127-28.

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

Kleve’s Fig. 9 “illustrat[es]...a temporary user *interface* with a vehicle rental authorization system.” *Kleve*, [0019], Fig. 9. The flowchart illustrates how the temporary user sets up a profile, expresses interest in a vehicle, and accepts rental terms, so they can “begin keyless vehicle rental authorization process” (step 924) which includes receiving a barcode matrix with the unique access code to unlock and use the vehicle. *Kleve*, [0044], [0090], Fig. 9. Almeroth, ¶129.

It would have been obvious to combine *Kleve* with *Mottla*’s graphical user interface (GUI) on a mobile screen to manage an e-key for accessing a vehicle.

Mottla’s Fig. 5 discloses a mobile GUI for reserving a vehicle. Almeroth, ¶130-32.

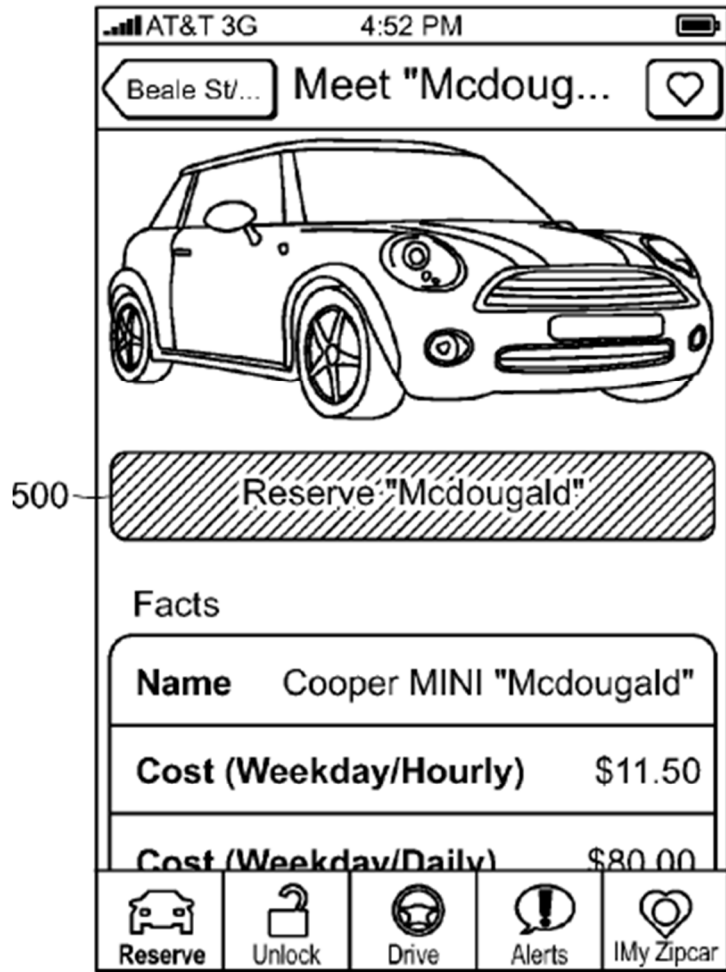


FIG. 5

Mottla's Fig. 12 shows a mobile GUI for accessing a vehicle.

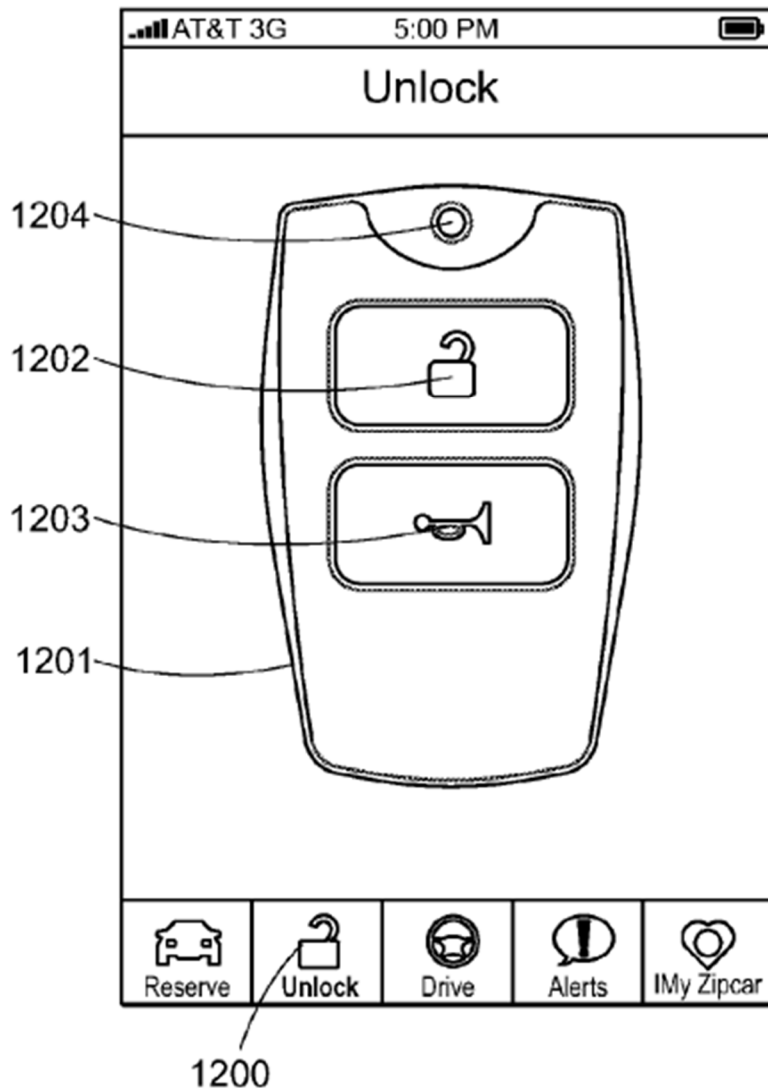


FIG. 12

Kleve's "user interface" would have motivated a POSITA to look to the art for examples of user interfaces in similar references, like *Mottla*. Almeroth, ¶132. A POSITA would have been motivated to incorporate *Mottla*'s GUI into *Kleve* by the benefits of a user-friendly GUI, as on-demand unlocking via icon gives the user better control over vehicle access, and using an unlock icon (instead of text) is

more user-friendly. *Id.* A POSITA would have also been motivated to allow the Temporary User on-demand locking control instead of requiring a virtual key scan—that would allow a Temporary User to use the unlock icon after the virtual key has been scanned and authorized, providing a better user experience while maintaining security. *Id.*, ##. A POSITA would have a reasonable expectation of success because GUIs were standard and implementation was within a POSITA’s capabilities. *Id.* *Kleve*, *Mottla*, and the ’245 patent are all electronic key systems.

Accordingly, *Kleve* in view of *Mottla* renders obvious this limitation.

Almeroth, ¶133.

3. Claim 2

2: “The vehicle of claim 1, wherein the vehicle is configured to receive information from the server to authenticate the coded data received from the mobile device to activate the e-key.”

Kleve’s vehicle receives information from the server to authenticate the coded data, or verify the virtual key, received from the mobile device to activate the e-key. *Kleve*, [0058-59], Fig. 6, [0062] (“The virtual key may be sent to the vehicle allowing Temporary User access to the Owner’s vehicle.”). The vehicle receives information from the server to “allow[] Temporary User’s access” by decoding the unique access code embedded in the barcode which is received from the mobile device. *Id.*, [0062, 0067]. *Kleve*’s server 634 “communicate[s] between a vehicle Owner nomadic device 601, a Temporary User nomadic device 611, and

a vehicle computing system 621.” *Id.*, [0069]. The Vehicle Owner uses server 634 to generate the virtual key which could be a matrix barcode. *Id.* The server then sends the matrix barcode to the Temporary User’s device, (*Id.*, Fig. 6, Step 616) where it is used to access and use the vehicle because the vehicle has received information from the server to decode the coded data in the barcode matrix. *Id.* (“Temporary User may enter/send [the matrix barcode] to the vehicle when ready to begin the rental term.”).

Accordingly, *Kleve* discloses this limitation. Almeroth, ¶¶134-35.

4. Claim 3

3[a]: “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,”

Kleve’s communication circuitry receives additional requests from other mobile devices to use the vehicle because *Kleve* provides a vehicle sharing platform . *Kleve*, [0036] (“vehicle rental micro-business 200”). Users provide their own mobile device and make additional requests to use the vehicle. *Id.*, [0054], [0082], [0087], Fig. 9, element 906 (matching “Temporary Users”).

Accordingly, *Kleve* discloses this limitation. Almeroth, ¶¶136-37.

3[b]: “each request is associated with a unique access code generated by the server, such that each unique access code is associated with a user account having respective privileges assigned by the administrator of

the vehicle that enables assigning or use of e-keys to use the vehicle,”

Each of *Kleve*'s requests is associated with a unique access code embedded in a virtual key that can be expressed as a matrix barcode. *Kleve*, [0044], [0069]. Each unique access code is associated with a user account, the Temporary User. *Id.*, [0037], [0059] (“server(s) 401 may respond [to a request] by transmitting an authorization code to both the Temporary User’s nomadic device 402 and to the vehicle control system...”). The unique access code is associated with the rental period, which provides the respective privileges assigned by the Vehicle Owner, the vehicle administrator. *Id.*, [0039]. This enables assigning e-keys to use the vehicle.

Accordingly, *Kleve* discloses this limitation. Almeroth, ¶¶138-39.

3[c]: “wherein one unique access code is active at a particular time when using e-keys.”

Kleve discloses that one unique access code is active at a particular time because *Kleve* provides access to vehicles in a “vehicle rental micro-business.” *Kleve*, [0002], [0047]. This permits temporary users to make time-limited shared vehicle rentals. *Id.*, [0047]. The claim does not require that *only* one code is active, but that one code is active.

Kleve's virtual key includes a unique access code that is active during the rental period because it provides access during the rental period. *Id.*, [0039] (“The

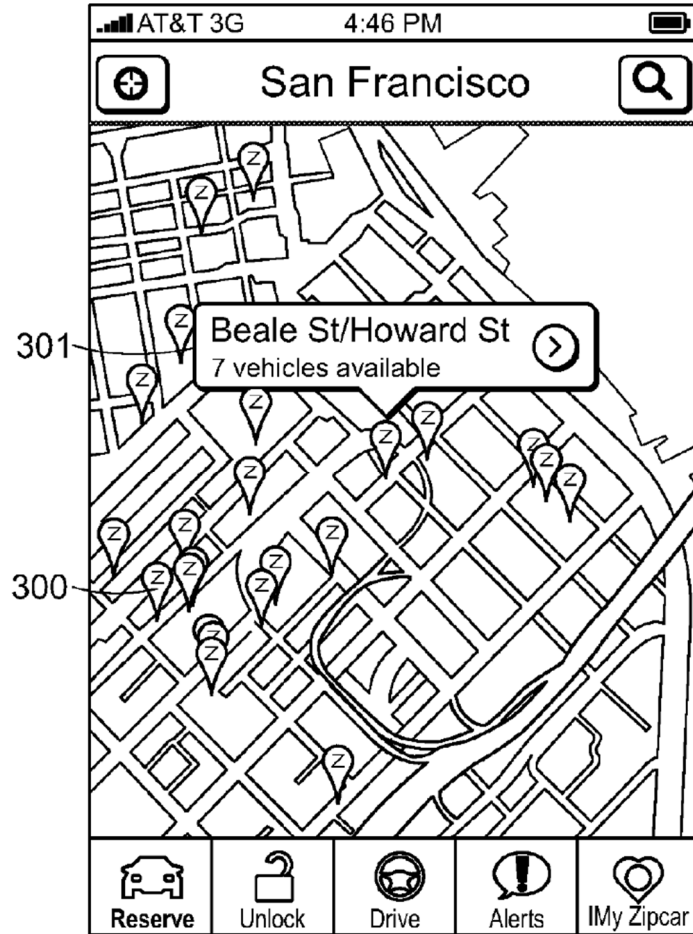
virtual key may...enable the keyless drive system for the appropriate Temporary User during a given rental period.”). *Kleve*’s VO “may enter in vehicle authorization credentials based on information received by the Temporary User to set up the virtual key.” *Id.*, [0062]. Because information received by the TU is utilized to generate the virtual key, and the key is for the TU to use, it is unique to the user. *Kleve*, [0039], 0069]. Almeroth, ¶141.

Accordingly, *Kleve* discloses this limitation. Almeroth, ¶142.

5. Claim 4

“The vehicle of claim 1, wherein said vehicle is identified as available for sharing and is discoverable via an application based on a geographic location of the vehicle.”

Kleve’s vehicles can be identified on an application as available for sharing based on geographic location. *Kleve*, [0086-87] (“Temporary User [can] be matched with a vehicle based on location” via a “smart phone”), [0036] (“smart phone application”), [0047]. Further, *Mottla* shows available vehicles based on location, and it would have been obvious to combine with *Kleve*. *Mottla*’s Fig. 3 shows vehicles available for sharing, discoverable via an application based on location. In Figure 3, vehicles are shown as “Z” pins in San Francisco.



A POSITA would have been motivated to combine *Motta*'s map of available vehicle locations with *Kleve*'s micro-rental business because the map display improves user experience by making it easier to identify near-by vehicles.

Almeroth, ¶144-45. *Kleve* discloses that the TU utilizes a website to “brows[e] the database of available vehicles to rent[.]” *Kleve*, [0047]. Vehicle *location* (tracked via *Kleve*'s continuous monitoring) would be an obvious datapoint to provide to users. A POSITA would have a reasonable expectation of success in such a

combination because GPS tracking for the purposes of including a location in a database would have been well within the capabilities of a POSITA. *Id.*

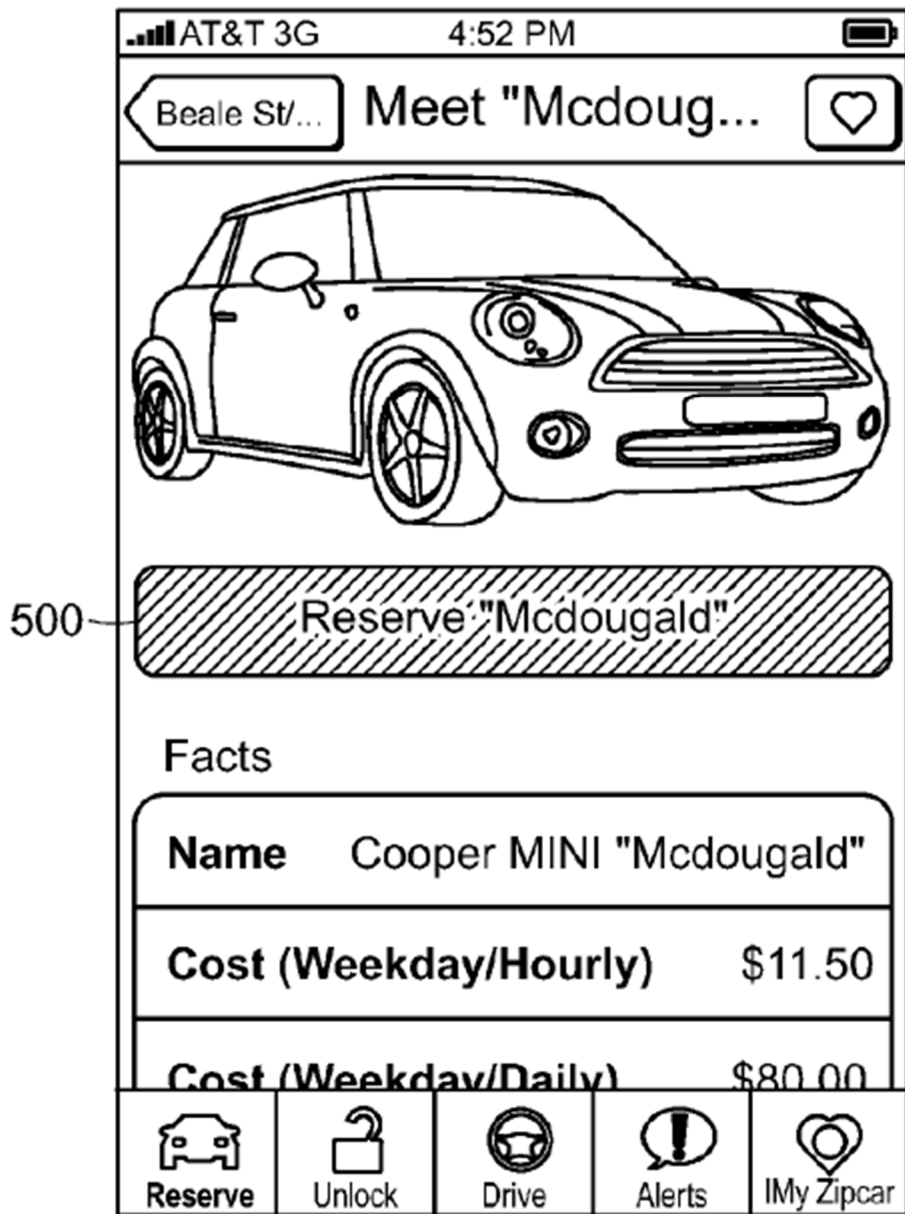
Accordingly, *Kleve* alone or in view of *Mottla* discloses or renders obvious this limitation. Almeroth, ¶146.

6. Claim 5

“The vehicle of claim 1, wherein an application accessed by said mobile device is configured to enable finding a geolocation of said vehicle and enables requesting use of said vehicle to receive said unique access code.”

Like claim 4, *Kleve* discloses using a “smart phone application.” *Kleve*, [0036]. TU locates a vehicle to request use via the unique access code. *Kleve*, [0087], Fig. 9, Step 906 (matching “by location”). Further, *Mottla* discloses an application accessed by the requester’s mobile device for finding a vehicle’s geolocation and to enable requesting vehicle use by receiving the unique access code. *Mottla* includes the ability to “Reserve” (i.e., request use of the vehicle) in Fig. 5. A POSITA would have found it obvious to combine *Mottla*’s request to use in *Kleve*’s application, as in claim 4. A POSITA would further have been motivated to combine *Mottla*’s “reserve” button to request use of the vehicle to receive an access code because it provides a user-friendly example of a GUI for selecting and requesting access to vehicles on a map. Almeroth, ¶147.

A POSITA would have had a reasonable expectation of success in combining the “reserve” button since adding simple UI elements to a smartphone app was well within the abilities of a POSITA. *Id.*



Accordingly, *Kleve* alone or in view of *Mottla* discloses or renders obvious this limitation. *Almeroth*, ¶148.

7. Claim 6

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

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

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

8. Claim 7

“The vehicle of claim 1, wherein the unique access code is obtained by the mobile device responsive to a computer requesting assignment of the e-key to the mobile device, the assignment being enabled when the assignment is by an owner of said vehicle or the administrator of said vehicle.”

Kleve's unique access code may be embedded in a matrix barcode for vehicle access. *Kleve*, [0044] (“matrix barcode...used as the virtual key”). This

unique access code is obtained by the mobile device responsive to a computer requesting assignment of the e-key to the mobile device because *Kleve*'s server assigns the matrix barcode with its unique access code to the mobile device. *Id.*, Fig. 6 (step 616).

This assignment can be enabled after VO approves a rental request. *See Kleve*, [0089]. When VO approves and the parties agree, the e-key is enabled and sent to a mobile device. *Id.*, [0085].

Accordingly, *Kleve* discloses this limitation. Almeroth, ¶¶151-53.

9. Claim 8

8[a]: “The vehicle of claim 7, wherein the vehicle is a sharable vehicle, and said privileges are defined for each sharing session of the vehicle,”

Kleve's vehicle is shareable. *Kleve*, [0044] (a “rental micro-business”). Privileges for time limited access to use the vehicle are defined for each sharing session. *Id.*, [0039] (virtual key permits vehicle to be driven “for the appropriate Temporary User during a given rental period”).

Accordingly, *Kleve* discloses this limitation. Almeroth, ¶¶154-55.

8[b]: wherein the on-board computer collects use data of the vehicle while the e-key is active for use of the vehicle, the collected data being saved to the server.

Kleve continuously monitors TU while using the vehicle with the virtual key. During rental, vehicle “control parameters” are “monitor[ed]” to determine

whether a “restriction” is exceeded. *Kleve*, [0040], [0053]. Monitored behaviors may be saved to the server. *Id.*, [0076] (“The continuous monitoring of the Temporary User’s behavior during the rental period may be transmitted to the server.”).

Accordingly, *Kleve* discloses this limitation. Almeroth, ¶¶156-57.

10. Claim 11

“The vehicle of claim 1, wherein the mode of allowed use of the vehicle 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 said restriction is detected.”

Kleve continuously monitors the vehicle during a rental mode of allowed use. *Kleve*, [0053], [0076]. Monitoring “may be transmitted to the server.” *Id.* *Kleve*’s VCS transmits notifications when restriction violations are detected. *Id.*, [0053] (“[T]he system may send a message to issue a warning to the Temporary User notifying of unauthorized usage of the vehicle.”); *see id.*, [0040].

Accordingly, *Kleve* discloses this limitation. Almeroth, ¶¶158-59.

11. Claim 12

“The vehicle of claim 1, wherein the mode of allowed use of the vehicle is programmed to cause generation of a notification to the administrator when a violation of the restriction is detected.

Kleve’s rental mode of allowed use is programmed to generate notifications to the administrator when restriction violations are detected. *Kleve*, [0053] (“The

VCS may monitor and detect the Temporary User exceeding a restriction limit and may notify the Owner ...”); [0073]. A POSITA would have understood that the VO is an “administrator” because VO administrates the rental system by choosing when their vehicle will be made available and which TUs will be approved to rent. Almeroth, ¶160 (citing *Kleve*, [0003]-[0004], [0037]-[0040]).

Accordingly, *Kleve* discloses this limitation. Almeroth, ¶161.

12. Claim 13

“The vehicle of claim 12, wherein 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.”

Kleve’s violations include driving too fast or out of an area. *Kleve*, [0073] (“speed limits,” “No-Go Zones”).

Accordingly, *Kleve* discloses this limitation. Almeroth, ¶¶162-63.

13. Claim 14

“The vehicle of claim 1, wherein the mode of allowed use of the vehicle is configured to cause generation of a notification on a display of the vehicle identifying the restriction when detected.”

Kleve’s mode of allowed use, during a rental period, includes a vehicle configured to generate notifications on a vehicle display identifying the restriction

when detected. *Kleve*'s VO may impose geographic limitations and "may be notified by the system and the vehicle may enter a remedial actions limiting vehicle speed." *Kleve*, [0041]. *Kleve* notifies the TU regarding violations "at the display information center, instrument cluster..." *Id.*, [0053]. Thus the notification is provided on the vehicle display identifying the restriction when detected. Accordingly, *Kleve* discloses this limitation. Almeroth, ¶¶164-65.

14. Claim 15

"The vehicle of claim 1, wherein the server is part of a cloud processing system and the cloud processing system is configured to manage user accounts and manage use of said e-key."

Kleve's server is part of a cloud processing system. *Kleve*'s server communication "is relayed through a network 406 (e.g., without limitation cloud computing...)." *Kleve*, [0056]. *Kleve*'s "centralized system is a server system that includes processing capability for incoming nomadic device signals designated to interact with a remote vehicle 421." *Id.*, [0057]. Thus, *Kleve*'s server is part of a cloud processing system.

Kleve's server is configured to manage user accounts and e-key use. *Kleve*'s VO and TU "create[] a user profile submitted through a website," and VO may "set[] up a deposit account, for example a paypal account." *Kleve*, [0046]. The user profile is a user account. *Kleve*'s server also manages the electronic key for accessing the vehicle. *Kleve*, [0048], step 616, [0059] (server may provide "an

authorization code”). Kleve’s “the server(s) 401 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.*, [0057]. Thus, the server manages use of the key to access the vehicle.

Accordingly, *Kleve* discloses this limitation. Almeroth, ¶¶166-68.

15. Claim 16

“The vehicle of claim 1, wherein said restriction is for a geolocation.”

Kleve’s restriction can include geolocation because the VO can set the location where the vehicle may be used, i.e., a geolocation. *Kleve*, [0040] (“restrictions may be based on...global position coordinates”). *Kleve* discloses a “restricted area” as an exemplary restriction. *Id.*, [0041]; *see also* [0051] (restrictions for “destination location”), [0052] [0073], [0075].

Accordingly, *Kleve* discloses this limitation. Almeroth, ¶¶169-70.

16. Claim 17

“The vehicle of claim 1, wherein said restriction enables access to specific vehicle areas that include one or more of vehicle door operation, or trunk operation.”

Kleve’s restrictions are permitted times when the vehicle is available for rental wherein access is enabled for specific areas of the vehicle including “unlock[ing]” vehicle doors. *Kleve*, [0071] (“For the duration of the rental term,

the Temporary User may again input the same identifying credentials to unlock and drive.”).

Accordingly, *Kleve* discloses this limitation. Almeroth, ¶¶171-72.

17. Claim 18

“The vehicle of claim 1, wherein the mode of allowed use is to enable access to a trunk of the vehicle, and the mode is associated with instructions to notify the administrator or an owner of the vehicle when said trunk is accessed using the e-key.”

It would have been obvious to a POSITA for *Kleve*’s rental mode of allowed use to enable trunk access and notify VO when the truck is accessed. *Kleve* describes unlocking doors, which would be trivially extended to unlocking the trunk. Almeroth, ¶173. A POSITA would have been motivated to combine *Kleve*’s system for door unlocking access with *Mottla*’s system providing trunk access because TUs would have appreciated the added convenience of trunk access via the application and because trunk access is typically provided by traditional key fobs. It would have been obvious to a POSITA to extend *Kleve*’s functionality to the trunk. *Mottla* discloses controlling vehicle functions including “opening a trunk.” *Mottla*, claims 1 (“control a function”) and 2 (“function is...opening a trunk”). Almeroth, ¶173. A POSITA would have had a reasonable expectation of success in permitting access to unlock the trunk because similar signals and vehicle

systems would be utilized to unlock the trunk as would be utilized to unlock the doors. *Id.*

A POSITA would have been further motivated to extend *Kleve*'s system for notifying the VO when the doors are opened to also notify the VO when the trunk is opened because access to the trunk essentially provides the same level of access to the vehicle as opening a door. Almeroth, ¶175. *Kleve*'s vehicle "transmit[s] confirmation back to the vehicle Owner 512 through a telecommunications network notifying that the Temporary User entered the vehicle..." *Kleve*, [0068]. A POSITA would have found it obvious that if *Kleve* included trunk access as modified by *Mottla*, then VO would also be notified if the trunk is accessed. A POSITA would have had a reasonable expectation of success in this modification because the same signals and vehicle systems would be used to send notifications about the trunk being opened as would be utilized to send notifications about doors being unlocked.

Accordingly, *Kleve* alone or in view of *Mottla* discloses or renders obvious this limitation. Almeroth, ¶176.

B. Ground 2: Kleve, Mottla, and Goudy Render Obvious Claims 9-10

1. Combination of Kleve, Mottla, and Goudy

It would have been obvious to combine *Goudy* with *Kleve* and *Mottla*, because *Kleve* discloses methods for remotely monitoring and limiting

functionality of a shared vehicle, for example if the shared user is observed to be using a vehicle excessively. *Kleve*, [0078]. A POSITA would have been motivated to look for ways to improve safety and avoid driver distractions for drivers using shared vehicles via electronic keys. *Goudy*'s limitations on use of the infotainment system are consistent with the kinds of limitations that a vehicle owner might seek to impose on their shared vehicle users. Almeroth, ¶177. Specifically, *Goudy* describes a function where a vehicle user interface is disabled to reduce “the probability of vehicle crashes due to distractions caused by the driver operating communication/multimedia devices while driving.” *Goudy*, [0001], [0016]-[0017].

As described in Ground 1, *Kleve*, *Mottla*, and the '245 patent are all from the same field of endeavor (electronic key systems). *Kleve* and *Mottla* are reasonably pertinent to the problem faced by the inventor of the '245 patent (controlling vehicle systems to provide added functionality and improve user experience). *Goudy* reasonably pertains to this same problem. Almeroth, ¶178.

2. Claim 9

The Office already determined that *Goudy* teaches this limitation. *Goudy* discloses “disabl[ing] at least one infotainment device under certain conditions relative to the current driving environment of the user.” *Goudy*, Abstract. *Goudy* explains that a “risk level” can prompt a “disable signal [] generated to disable []

infotainment devices” such as a “navigation system” comprising an “interface.”

Id., [0018]-[0019]; [0023]; Fig. 1, element 16.

It would have been obvious to a POSITA to combine *Kleve* and *Mottla* with *Goudy* such that the system “disable[s] at least one infotainment device” during high-risk scenarios under the rental mode of use. Almeroth, ¶180. A POSITA would have been motivated to make the combination to promote safer driving. *Id.* *Goudy* explains that “if a distraction occurs...safety can be jeopardized.” *Goudy*, [0003]. A POSITA would have understood that disabling distractions during high-risk scenarios helps the driver focus on the road, thus improving safety. Almeroth, Almeroth, ¶1805.

Accordingly, the combination of *Kleve*, *Mottla* and *Goudy* renders obvious this limitation. Almeroth, ¶181.

3. Claim 10

The combination of *Kleve* and *Mottla* discloses a mode of allowed use that includes disabling vehicle interface controls. When giving a user access to a vehicle that is not their own, a POSITA would have understood that the user should not have full access to every feature of the vehicle (or to certain features at certain times) for safety. This same understanding would have motivated a POSITA to look to *Goudy*. Almeroth, ¶182.

It would have been obvious to combine *Kleve* with *Goudy* which discloses disabling multimedia system controls, which are a vehicle interface. The Examiner found, and Applicants did not rebut, that *Goudy* discloses claim 10. Ex.1002, 131. The Examiner stated: “in the same field of vehicle, *Goudy* teaches a vehicle [that] has a function to disable the vehicle’s infotainment device. See abstract, ‘The present invention is operative to disable at least one infotainment device under certain conditions relative to the current driving environment of the user.’” *Id.* The Examiner further stated that it would have been obvious to a POSITA to modify *Zaid*’s vehicle “with a function to disable the vehicle’s infotainment system while driving to improve safety.” *Id.* The same motivation applies to modify *Kleve*’s vehicle. A Vehicle Owner would not want the infotainment system to distract a young driver and so might want to remotely disable controls. Almeroth, ¶183. A POSITA would have had a reasonable expectation of success in the combination because *Kleve* and *Mottla* already disclose the requisite hardware, including a navigation/infotainment interface and a means for monitoring usage of the vehicle and determining a risk level. *Id.*

Accordingly, *Kleve* in view of *Goudy* renders obvious this limitation.

Almeroth, ¶184.

C. Ground 3: Zaid, Kleve, and Mottla Render Obvious Claims 1-8, 11-18

1. Combination of Zaid, Kleve, and Mottla

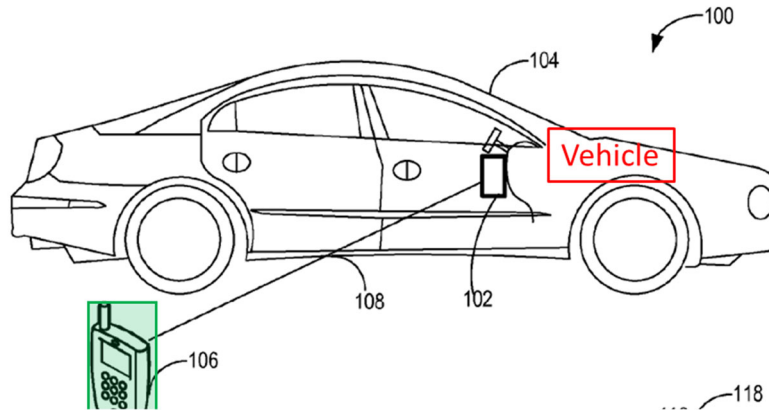
Zaid, Mottla, and Kleve are analogous to the claimed invention of the '245 patent because they are from the same field of endeavor (electronic key systems); and/or (2) are reasonably pertinent to the problem faced by the inventor (controlling vehicle systems to provide added functionality and improve user experience). Compare '245 Patent, Title, with *Zaid*, [0090], *Kleve*, [0039], and *Mottla*, [0033]. *Zaid* discloses “a system 100 for vehicle access control” via an electronic key including “a vehicle access component 102 configured to provide access to a vehicle 104 when a vehicle reservation is received from a wireless communication device 106 via a communication link 108.” *Zaid*, [0075]. *Kleve* discloses a “vehicle rental micro-business” utilizing “a “virtual key” for “enabl[ing] the keyless drive system for the appropriate Temporary User during a given rental period.” *Kleve*, [0036], [0039]. *Mottla* discloses a “method for using a mobile device 100 to gain access to, or identify the location of, a vehicle 104.” *Mottla*, [0033]. *Zaid, Kleve, and Mottla* recognize the benefit of implementing an e-key via a mobile device for conveying vehicle access to shared vehicles. It would have been obvious to combine *Zaid, Kleve, and Mottla*, which discloses the claim limitations below. Almeroth, ¶¶185-86.

2. Independent Claim 1

1[preamble]:

The Office determined that Zaid's "vehicle 104" discloses this limitation.

Ex.1002, 122.



Zaid, Fig. 1 (annotated).

Accordingly, *Zaid* discloses the preamble. Almeroth, ¶¶187-89.

1[a]:

The Office determined Zaid's "ECU 308" discloses this limitation. Ex.1002, 122.

Zaid's vehicle includes **electronic control units 308**, which are "embedded system[s] that control[] one or more subsystems in a motor vehicle." *Zaid*, [0035].

A POSITA would have understood an ECU to be a "computer." Almeroth, ¶191.

Zaid's vehicle access kit 200 includes a **microprocessor 224**, another example of an "on-board computer of the vehicle." *Zaid*, [0100]-[0101], Fig. 2, [0083]. Microprocessor 224 utilizes memory to "store various computer instructions." *Id.*, [0101]. The vehicle access kit is "coupled to the vehicle[.]" *Id.*, [0083].

Accordingly, *Zaid* discloses or renders obvious this limitation. Almeroth, ¶¶192-93.

1[b]:

The Office determined that *Zaid*'s "vehicle access control component 206" discloses this limitation. Ex.1002, 122.

Zaid's **vehicle access control component 206** "provides access to the vehicle by...*unlocking the vehicle door*" and "includes the capability to actuate (e.g., lock, *unlock*, start engine...) vehicle functions." *Zaid*, [0090]; *see also id.*, [0091] ("the vehicle access control component 206 includes a *physical adaptor* connected to the vehicle bus of a vehicle so that it is capable of actuating car functions (e.g., *unlock doors*, start engine)").

Zaid's vehicle access control component 206 is "interfaced with the on-board computer" by virtue of its "physical adaptor connected to the vehicle bus." *Zaid*, [0091]. *Zaid*'s figure 3 depicts "interfacing" the "vehicle access kit" with the vehicle. "[M]icroprocessor 224 unit (MPU) [is] connected to the vehicle bus adapter" (*Id.*, [0100]) and ECU 308 interfaces with the vehicle access kit via the vehicle bus and adapter (*id.*, Fig. 3).

Zaid's "**vehicle actuators 310**" enable unlocking. *Zaid*, [0123], Fig. 3. *Zaid*'s ECU 308 interfaces with vehicle access kit 302, via a vehicle bus 306 and adapter 304, such that microprocessor 224 "accepts commands (e.g., unlock doors,

start engine, and/or other commands)[.]” *Id.*, [0100]; *see also id.*, [0037]-[0038], [0046], [0059], [0062] (“[h]ardware components commonly installed in a vehicle, generally includ[e]...[a] hardware interface to the vehicle control bus and *primary ECU for...trigger[ing] vehicle actuators (e.g., Door locks)*”).

A POSITA would have recognized that *Zaid*’s figure 2 and 3 disclosures emphasize different aspects of *Zaid*’s vehicle sharing system and should be read together. Almeroth, ¶198 (citing *Zaid*, [0006]-[0007]). It further would have been obvious to a POSITA to combine *Zaid*’s “vehicle access kit for providing vehicle access” (Fig. 2) with its “interfacing of a vehicle access kit with a vehicle” (Fig. 3) such that the vehicle access kit can actuate the vehicle’s “door locks” and “engine starter.” A POSITA would have made this combination because the vehicle access kit must be “interfaced” with the vehicle to actuate vehicle functions. *Id.*, ¶199 (citing *Zaid*, [0037], [0062], [0123]). A POSITA would have reasonably expected success because *Zaid* provides technical details for “interfacing of a vehicle access kit with a vehicle.” *Id.* (citing *Zaid*, [0007]).

Accordingly, *Zaid* discloses or renders obvious this limitation. Almeroth, ¶¶194-200.

1[c]:

The Office determined that *Zaid*’s “vehicle access control component 206” discloses this limitation. Ex.1002, 122-23.

Zaid's **vehicle access control component 206** “provides access to the vehicle by...*allowing for starting* of the vehicle engine” and “includes the capability to actuate (e.g., lock, unlock, *start engine*...) vehicle functions.” *Zaid*, [0090]; *see also id.*, [0091] (“the vehicle access control component 206 includes a *physical adaptor* connected to the vehicle bus of a vehicle so that it is capable of actuating car functions (e.g., unlock doors, *start engine*)”).

Zaid's vehicle access control component 206 is “interfaced with the on-board computer” via its “physical adaptor connected to the vehicle bus.” *Zaid*, [0091]. *Zaid*'s “microprocessor 224 unit (MPU) [is] connected to the vehicle bus adapter” (*id.*, [0100]) and ECU 308 interfaces with vehicle access kit 302 via a vehicle bus 306 and adapter 304 (*Id.*, Fig. 3).

Zaid's “**vehicle actuators 310**” enable starting. *Zaid*, [0123], Fig. 3. ECU 308 interfaces with vehicle access kit 302 via vehicle bus 306 and adapter 304, such that microprocessor 224 “accepts commands (e.g., unlock doors, *start engine*, and/or other commands).” *Id.*, [0100]; *see also id.*, [0037]-[0038], [0046], [0059], [0062]. *Zaid*'s “vehicle access kit is thus connected to the engine control unit (ECU) 308 of the vehicle, which is in turn connected to various vehicle *actuators 310* (e.g., ... *engine starter*).” *Id.*, [0123]. *Zaid*'s vehicle actuators include door lock actuators (e.g., “door locks”) and an engine start actuator (e.g., “engine starter”). Almeroth, ¶204.

Zaid discloses or renders obvious this limitation. Almeroth, ¶¶201-06.

1[d]:

The Office determined that *Zaid*'s "wireless device communication interface 202" discloses this limitation. Ex.1002, 123.

Zaid's wireless device **communication interface 202**, in vehicle access kit, interfaces with microprocessor 224 and ECU 308 via "vehicle bus." *Zaid*, [0100], [0037].

Communication interface 202 is programmable to communicate with (1) cloud system server and (2) mobile device. Communication interface 202 communicates with the "central server [] sitting on [the] data network" (the server of the cloud system) and a "wireless communication device" (mobile device). *Zaid*, [0076], [0099], [0125]-[0126], [0130]. Communications interface 202 receives a vehicle reservation from a server. *Id.*, [0126]-[0128] ("server...communicates the vehicle reservation to a wireless communication device... [then] the reservation is forwarded from the wireless communication device to the vehicle access kit."). Communications interface 202 also "includes a short-range wireless interface (e.g., Bluetooth and/or WiFi)." *Id.*, [0087]. A POSITA would have understood *Zaid*'s "wireless interface" to comprise a standard "Automotive 802.11 Wireless LAN Solution[]" such as Broadcom's BCM4325. Almeroth, ¶209; *see also* Exs.1017-18.

Zaid's communications interface 202 is programmed with pairing or network details to connect, illustrating *programmability*. *Id.*, (citing *Zaid*, [0087]).

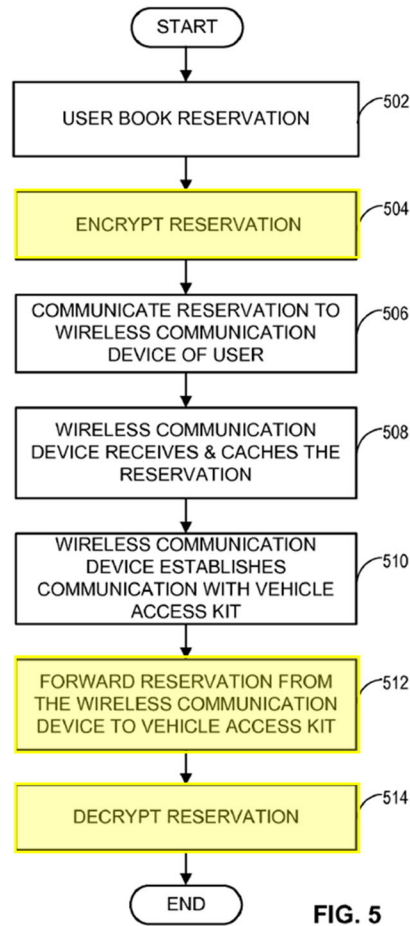
Accordingly, *Zaid* discloses or renders obvious this limitation. Almeroth, ¶¶207-212.

1[e]:

The Office determined that *Zaid*'s "vehicle reservation" is "coded data" per this limitation. Ex.1002, 123. In IPR2024-00758, the Board agreed on rehearing that *Zaid* discloses "the vehicle receives a request from a mobile device that unlocks the vehicle as required by claim 1[e]⁴." IPR2024-00758, Paper 13.

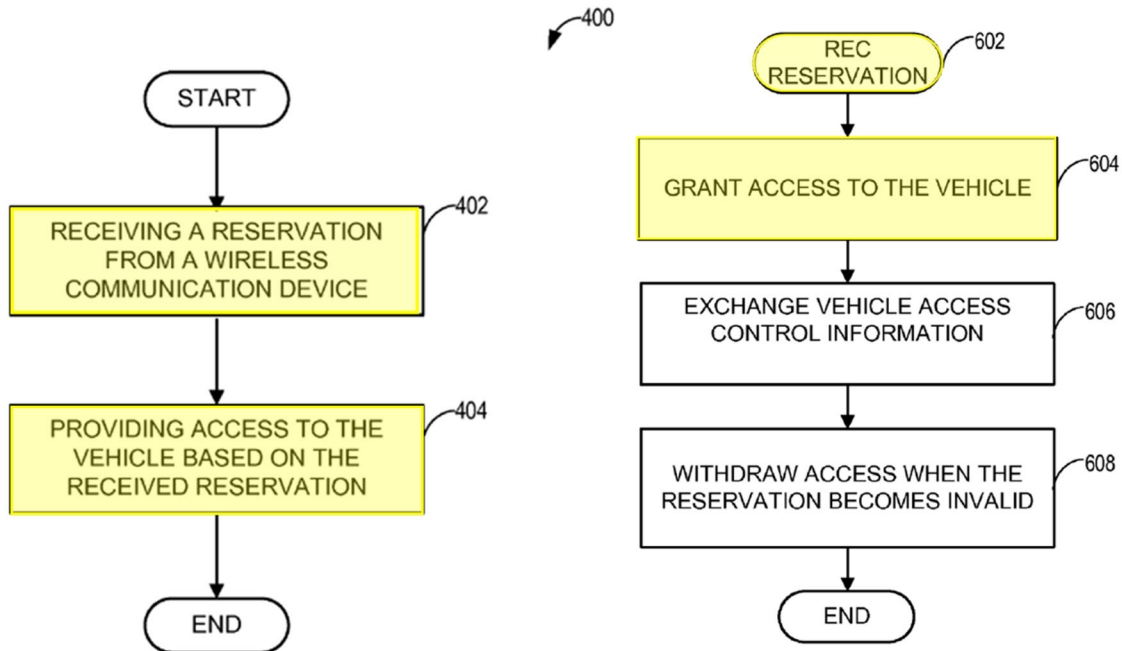
Zaid's vehicle access kit receives unlocking requests via communication interface 202. Unlocking requests are referred to as **encrypted "vehicle reservations,"** generated by the server and encrypted before being sent to the user's "wireless communication device." *Zaid*, [0126] ("server...communicates the vehicle reservation to a wireless communication device"). *Compare with* '245 Patent, 46:32-35 ("Cloud services 120 can generate the unique access code which *is then encrypted* in a message and *sent as encrypted e-keys* 720 to the recipient[.]). *Zaid*'s "wireless communication device" then "forward[s] [the encrypted] reservation...to [the] vehicle access kit." *Zaid*, Fig. 5; [0128].

⁴ Limitation 1[e] in the -0758 IPR substantively matches '245 Patent limitation 1[e].



Zaid, Fig. 5 (annotated)

Zaid's vehicle access kit receives encrypted vehicle reservations, via communication interface 202, before being decrypted. *Id.*, [0128], Fig 5.



Zaid, Fig. 4 (left), Fig. 6 (right) (annotated).

On receipt, the reservation is decrypted, and the user is granted access. Zaid, [0067] (“access to the vehicle is provided when a vehicle reservation is received”), [0124], [0129], Fig. 4, Fig. 6. Zaid explains that “granting access includes opening the vehicle door, and/or allowing engine to be turned on by user.” *Id.*, [0129]; see also *id.*, [0090] (“a vehicle access control component 206 [] provides access to the vehicle by for example unlocking the vehicle door”).

Therefore, Zaid’s “communication interface 202” is configured to receive an encrypted “vehicle reservation” from the “wireless communication device” for unlocking and use of the vehicle (comprising the vehicle reservation that provides access and “allowing engine to be turned on by user”).

Accordingly, Zaid discloses this limitation. Almeroth, ¶¶213-218.

1[f]:

The Office determined that *Zaid*'s "server transmits the unique access code to the user's wireless device and then the user's wireless device transmits the unique access code to the vehicle to unlock and to operate the vehicle." Ex.1002, 387.

Zaid's vehicle receives an encrypted vehicle reservation, from the server via mobile device. Within the encrypted vehicle reservation exists the decrypted **vehicle reservation**, i.e., a unique access code. *Zaid*'s vehicle decrypts coded data to retrieve the vehicle reservation, *Zaid*, [0125], which was generated by the server and encrypted after the reservation was booked. *Zaid*, Fig. 5; [0125]-[0126], [0128].

Zaid's vehicle reservation comprises a unique increment, rendering reservations unique. *Zaid*, [0130] ("each message...such as a vehicle reservation and updates includes a unique increment.") *see also* '245 Patent, 45:58-60 (unique access code can include an "incremental number" generated by a "incremental number generator"). Almeroth, ¶221. *Zaid*'s reservation also provides vehicle access. *Zaid*, [0129] ("[T]he vehicle reservation is *decrypted* and authenticated at the vehicle access control system. At 604, *vehicle access is granted.*").

Zaid's encrypted vehicle reservation also falls within the '245 Patent's description. *See* '245 Patent, 45:58-61 ("The unique access code can be generated

by...any other generation device that can generate codes that are unique or substantially unique.”), 46:32-35 (“Cloud services 120 can generate the unique access code which *is then encrypted* in a message and sent as encrypted e-keys 720 to the recipient[.]”).

Accordingly, *Zaid* discloses or renders obvious this limitation. Almeroth, ¶¶219-23.

1[g]:

Despite ultimately determining that this limitation is disclosed, the Examiner opined that *Zaid* “fails to expressly teach the server is configured to set operational restrictions[.]” Ex.1002, 120, 125. But the Examiner misinterpreted the claims, which do not require “operational restrictions,” and the Examiner overlooked *Zaid*’s privileges that limit (1) vehicle access and (2) use for a period of time, which affect vehicle “operation.” *Zaid*, [0069].

The Office determined that “it would have been obvious to a [POSITA] to modify *Zaid*’s vehicle access system to allow an authorized individual to set limitations or restrictions on the usage of the vehicle to improve vehicle security and to prevent unauthorized usage.” *Id.*, 125-26.

Zaid’s updated vehicle reservation limits the time that a user can access and use the vehicle, i.e., driving privileges, which is responsive to a restriction set by a vehicle owner. *Zaid*’s vehicle reservation “includes...a specified time period”

(*Zaid*, [0069]) during which a user is “allow[ed] the start of vehicle engine, and/or allowing actuation of various other vehicle functions” (*id.*, [0068], [0015], [0090], [0100]). Because the vehicle reservation includes the access and use privileges, the vehicle reservation is necessarily “associated with privileges...and privileges are for the unique access code.” Almeroth, ¶225.

Zaid’s access and use privileges are set via the server responsive to a restriction set by a vehicle administrator. *Zaid*’s vehicle owner can “*update the server(s)* (e.g., online vehicle reservation system) of various vehicle related information *such as vehicle availability and vehicle location...used by the backend vehicle sharing system to register the vehicle as available for sharing.*” *Zaid*, [0079]. Thus, the vehicle owner restricts vehicle availability to particular times. Almeroth, ¶226. Once the user identifies a vehicle, “[t]he vehicle reservation is booked at the server” subject to the owner’s restrictions. *Zaid*, [0080], [0125]. The reservation is then encrypted and distributed to the mobile device and vehicle. Accordingly, *Zaid*’s time-limited access and use privileges are set via *Zaid*’s central server responsive to the selected time period being within the vehicle owner’s identification of availability. Almeroth, ¶226.

Zaid’s restriction is “associated with” a mode of allowed use as a vehicle rental because “the vehicle reservation becomes invalid at the end of the vehicle reservation period.” *Id.*, [0131]. Almeroth, ¶227. The specification does not define

“modes of allowed use.” *But see* ’245 Patent, 2:2-3 (“mode of transport”), 3:51-53 (“the request to generate the e-key is received from...a rental car operator”), 26:41-43 (“the vehicle may be...a rented vehicle”).

Accordingly, *Zaid* discloses this limitation. Almeroth, ¶228.

1[h]:

The Office identified only this limitation as comprising allowable subject matter. *Zaid* discloses a camera. *Zaid*, [0092]. *Kleve* explicitly discloses capturing video that includes the vehicle. *See* Ground 1 at §VII.A.2.[1h].

A POSITA would have been motivated to combine *Zaid*’s system with *Kleve*’s camera to give the owner “better control over” the renter and allow the “owner to keep tabs” on the vehicle, “giv[ing] the vehicle owner an increased level” of security and control. Almeroth, ¶230 (citing *Zaid*, [0072], [0097], [0114]). *Zaid* recites these concerns, which would have motivated a POSITA to look to *Kleve*, describing methods for “additional security” and “continued control” for shared vehicles. *Kleve*, [0049], [0043]. A POSITA would have appreciated *Kleve*’s camera for verifying identity and “monitoring” driver behavior to detect violations for “remedial actions.” *See Kleve*, [0073] (camera generates “monitoring information”), [0076] (monitoring detects “unauthorized driving behavior, unauthorized driver”), [0042] (“in-vehicle cabin activities”), [0053] (“remedial actions”). A POSITA reviewing *Kleve*’s camera would have had a

reasonable expectation of success since *Zaid* describes monitoring vehicle usage and developing a “driver profile.” *Zaid*, [0097]-[0099], [0134]. The only modification to *Zaid* would be facing *Zaid*’s camera at the driver and initiating recording, both described in *Kleve*. *Kleve*, [0042], [0066], [0072]. This would have been well within a POSITA’s skill. Almeroth, ¶230.

Accordingly, the combination of *Zaid* and *Kleve* renders obvious this limitation. Almeroth, ¶231.

1[i]:

The Office determined that (1) “the unique access code functioning as an electronic key (ekey) that is managed by the mobile device” is disclosed in *Zaid*, (2) “one or more graphical user interface inputs rendered on a screen of the mobile device” is disclosed in *Mottla* via its “vehicle remote entry application,” and (3) that “it would have been obvious to a [POSITA] to modify *Zaid*’s wireless device with a vehicle remote entry application to provide visual graphics of the vehicle fob [as in *Mottla*] to conveniently control the vehicle.” Ex.1002, 124-25.

Mottla’s Fig. 5 discloses a GUI for reserving a vehicle.

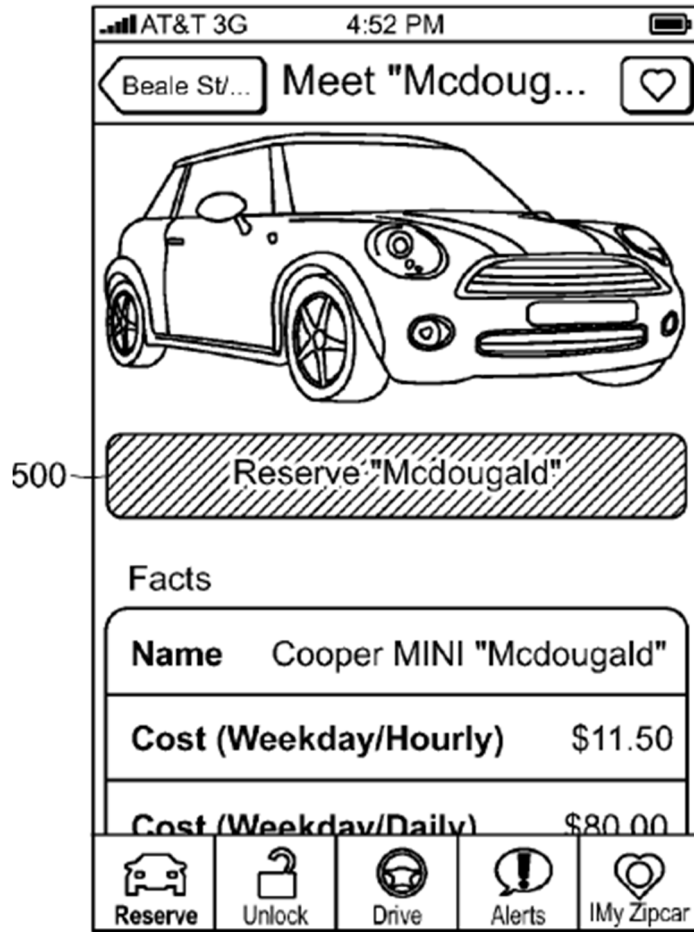


FIG. 5

Mottla's Fig. 12 shows a mobile device GUI for utilizing an electronic key to access a shared vehicle.

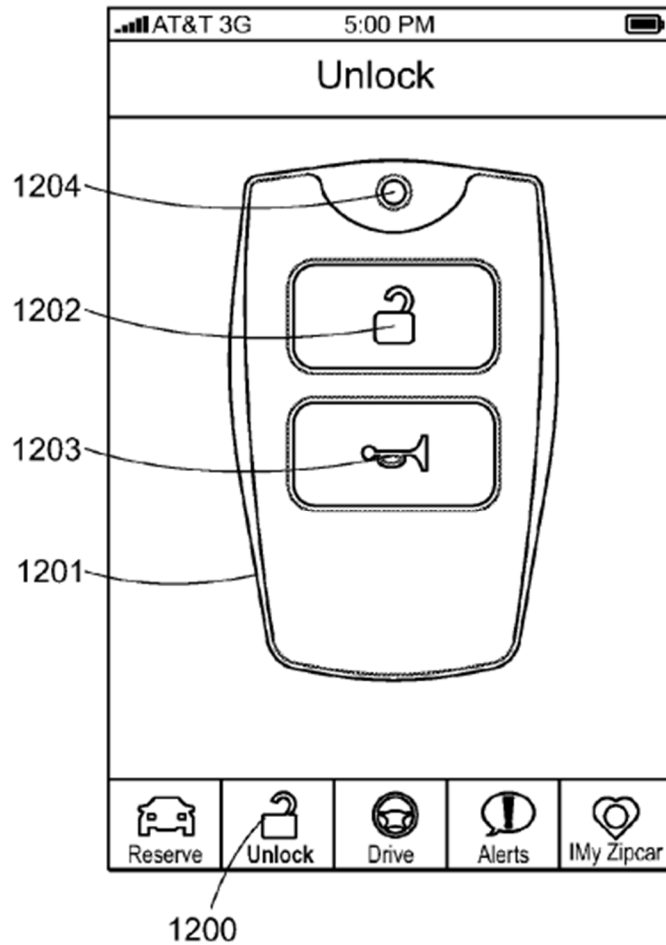


FIG. 12

A POSITA would have been motivated to combine *Zaid*'s device with *Mottla*'s GUI such that *Zaid*'s wireless device provides graphics for vehicle control. Ex.1002, 125, 130; Almeroth, ¶235. A POSITA would be motivated by the benefits of a user-friendly GUI, as unlocking via icon gives better control over vehicle access and is more user-friendly. *Id.* A POSITA would have also been motivated to allow app-based locking/unlocking instead of scanning the virtual key—providing a better user experience while maintaining security. *Id.* A POSITA would have a reasonable

expectation of success because GUI icons were standard and implementation was within a POSITA's capabilities. *Id.*

Accordingly, the combination of *Zaid* and *Mottla* renders obvious this limitation. Almeroth, ¶236.

3. Claim 2

The Office determined that *Zaid* discloses “exchang[ing] vehicle access information with the server to determine whether the access information is valid.” Ex.1002, 126.

Zaid's messages are “encrypted using a public key” and “decrypted using [a] private key.” *Zaid*, [0099]. *Zaid's* “vehicle reservation is encrypted” by the sever “in a first layer of encryption using a public key of the wireless communication device” and in a “second layer of encryption encrypted using a public key of the vehicle access kit.” *Id.*, [0125], [0128]. Upon receipt, the wireless communication device decrypts “the first layer of encryption...using a private key of the wireless communication device.” *Id.*, [0125]. The wireless communication device then sends the vehicle reservation to the vehicle access kit, **which decrypts “[t]he second layer of encryption...using a private key of the vehicle access kit.”** *Id.*

Zaid's “the vehicle access control system...receive[s] a server update...from the wireless communication device. In various embodiments, the server update includes a new private key.” *Zaid*, [0081] (emphasis added). A POSITA

understood that decryption verifies authenticity and, after decryption, the e-key is activated. Almeroth, ¶239.

Accordingly, *Zaid* discloses this limitation. Almeroth, ¶¶237-40.

4. Claim 3

3[a]:

The Office determined that “[i]t is inherent that the vehicle access component 102 is configured to receive reservation from different wireless device users.” Ex.1002, 126.

Zaid’s communications interface receives reservations from other devices. Almeroth, ¶242. *Zaid* discloses a *sharing* service where anyone sends requests to reserve vehicles. *See, e.g., Zaid*, [0077] (“retrieving a list of nearby vehicles”), [0016], [0095] (“*one or more reservations*”), [0134] (“*all the drivers* of a particular vehicle”), claim 34 (“one *or more* vehicle users”).

A POSITA would have understood that car sharing users would, using their wireless communication devices, book reservations at the server, which would be transmitted to a vehicle. Almeroth, ¶243.

3[b]:

The Office determined that *Zaid*’s “reservation is unique to the user who made the reservation” and “the server reserves the vehicle for a specific period of

time and access to the vehicle is only valid during that specific time.” Ex.1002, 126-27.

As in 1[e], each vehicle reservation in *Zaid* is associated with an encrypted unique access code generated by the server and is associated with privileges for time-limited vehicle access and use.

Zaid's vehicle reservation is associated with a user account, which has privileges assigned by a vehicle administrator that enables assigning or use of e-keys to use the vehicle. *Zaid*'s reservations can be “booked through one or more social networking websites[.]” *Zaid*, [0072]. There, the user “***must first log into the social networking website,***” which connects the user to their account and then requests a time-limited vehicle reservation. *Id.* Upon the vehicle owner (administrator) accepting the request, the user account is assigned time-limited privileges. *Id.* *Zaid* tracks “driving history” and “reputation,” so the vehicle reservation and unique access code are associated with a user account. *Id.* User tracking allows the vehicle owner to “have better control over the type of user the owner is lending/sharing/renting vehicle to.” *Id.* A POSITA would have understood that, to enable renter tracking, the vehicle reservation must be associated with the renter's account. Almeroth, ¶247. By making reservations through a social media account, *Zaid* discloses associating vehicle reservation and unique access code with a renter. *Id.*

Zaid teaches that the vehicle owner assigns privileges and enables assigning or use of e-keys by defining times the system can assign keys. *Zaid*, [0077] (owner can “advertise or announce when the vehicle will be available for sharing...”). *Zaid* “allows a vehicle user and owner to dynamically send out a vehicle request and/or update the server(s) (e.g., online vehicle reservation system) of various vehicle related information such as vehicle availability and vehicle location.” *Id.*, [0079]. The owner enables the requested duration for vehicle access and use. Almeroth, ¶248.

3[c]:

Zaid's access code is active at a particular time when using e-keys. The claim does not require that *only* one code is active, but that one code is active. *Zaid*'s encrypted vehicle reservation “provides access to the vehicle,” indicating that the encrypted vehicle reservation is “active at a particular time when using e-keys.” *Zaid*, [0090]. Almeroth, ¶249.

Accordingly, *Zaid* discloses these limitations. Almeroth, ¶250.

5. Claim 4

The Office determined that *Zaid* discloses this limitation. Ex.1002, 127 (citing *Zaid*, [0077]-[0078]).

Zaid's vehicle is advertised as available for sharing and is discoverable based on location. *Zaid*'s application shows vehicles and locations. *Zaid*, [0077]

("[T]he wireless communication device includes a vehicle reservation application...that enables a vehicle user (e.g., renter and owner) to communicate with backend server(s) (e.g., an online vehicle reservation system) to (a) ***advertise or announce the location of the vehicle...***" *Zaid* discloses that a user may "retriev[e] a list of nearby vehicles available for sharing," including location. *Id.*

Accordingly, *Zaid* discloses this limitation. Almeroth, ¶¶251-52.

6. Claim 5

The Office determined that *Zaid*'s "wireless device has an application to provide the location and availability of the vehicles." Ex.1002, 127 (citing *Zaid*, [0077] ("e.g., an iPhone or Droid application"), [0078]).

First, *Zaid*'s application "enables a vehicle user...[to] advertise or announce the location of the vehicle." *Zaid*, [0077]. Using this, the prospective renter "retriev[es] a list of nearby vehicles available[.]" *Id.*; *see also* claim 31 ("server configured to advertise a vehicle reservation using a social network site, wherein the advertised vehicle reservation includes geolocation information").

Second, the user requests the vehicle via user interface on their wireless communication device. *Zaid*, [0125] ("At 502, a vehicle reservation is booked. In various embodiments, ***the vehicle reservation is booked by a user at a central server via a user interface*** displayed on a computing device.... [T]he computing device is ***the same wireless communication device the reservation is sent to.***"),

[0072] (“the reservation is booked through one or more social networking websites”).

It would have been obvious to a POSITA to implement *Zaid*'s vehicle reservation application to enable geolocation (*id.*, [0077]) and requesting use of the vehicle (*id.*, [0125]) such that users only need one application. Almeroth, ¶257. This would have been a simple addition to the reservation functionality that simplifies the user experience, and would have been desirable to minimize user downloads and confusion and maximize ease of use by providing both features in a single application. A POSITA would have had a reasonable expectation of success in doing so since *Zaid* provides location and reservation as functionalities available via mobile device; combining them into one application would not change how they are programmed. *Id.* A POSITA at the relevant time would have been motivated to make this combination to simplify access to the shared vehicles. *Id.* (citing *Zaid*, [0077], [0125]).

Accordingly, *Zaid* discloses or renders obvious this limitation. Almeroth, ¶258.

7. Claim 6

The Office determined that *Zaid*'s “user reserves the vehicle from the server” (citing *Zaid*, [0080]) and that, in an obvious combination, *Mottla*'s “e-key has functions enabled via the [GUI]” (citing *Mottla*, Fig. 12). Ex.1002, 127-28.

Zaid's vehicle reservation application is configured to enable sending instructions to the central server to share the vehicle with a user to enable use of the electronic key on said vehicle. *Zaid*, [0077]. The vehicle reservation application enables "communicat[ion] with backend server(s)" to permit vehicle "sharing." *Zaid*, [0077]. The vehicle reservation is "booked at the server 110 via a user interface" and then the vehicle reservation is sent to the vehicle, via the mobile device, for providing access and usage via an electronic key. *Id.*, [0080]. As explained above, it would have been obvious to a POSITA at the relevant time to implement *Zaid*'s vehicle reservation application to enable both geolocation (*id.*, [0077]) and requesting use of the vehicle (*id.*, [0125]) such that users only need to install one application. Almeroth, ¶¶260, 257. *Zaid* further explains that the mobile device generally includes "a rich visual interface." *Zaid*, [0026].

Mottla discloses that the e-key has functions enabled via GUI. Ex.1002, 127-28; *see supra* §VII.C.2 1[i]. *Mottla*'s Fig. 12 shows a mobile GUI for utilizing an e-key to access a vehicle.

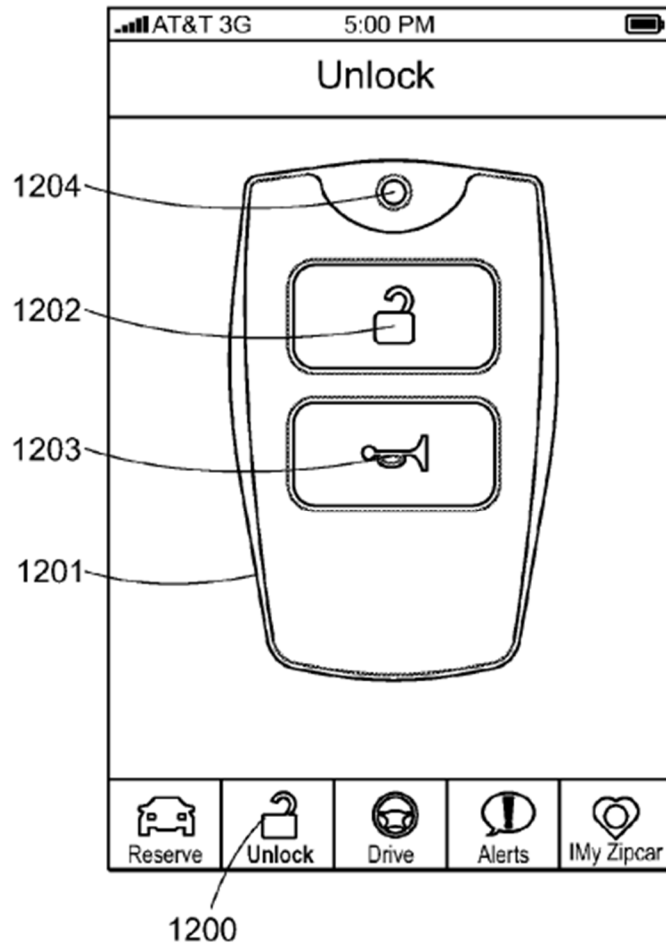


FIG. 12

A POSITA would have been motivated to combine *Zaid*'s wireless device with *Mottla*'s vehicle remote entry application, implementing the same features that *Zaid* already discloses within its "application" and "user interface," such that *Zaid*'s wireless device provides graphics to control the vehicle, for all the reasons discussed in 1[i]. Ex.1002, 125; Almeroth, ¶¶261-63.

Accordingly, *Zaid* combined with *Mottla* renders obvious this limitation.

Almeroth, ¶264.

8. Claim 7

The Office determined that *Zaid*'s "computing device 118 reserves the vehicle and the reservation is transmitted to the mobile device via the server" and "the rental server 110 enabled the reservation of the vehicle to the user of the wireless device 106." Ex.1002, 128 (citing *Zaid*, Fig. 1, [0080]).

As in 1[g], *Zaid*'s encrypted vehicle reservation is obtained by the wireless communication device responsive to the server encrypting the vehicle reservation with the wireless communication device's public key. *Zaid*, [0125]-[0126]. *Zaid* explains that generation and encryption of the vehicle reservation by the server is enabled by the vehicle owner assigning the vehicle with availability. *Id.*, [0077].

Accordingly, *Zaid* discloses this limitation. Almeroth, ¶¶265-67.

9. Claim 8

8[a]:

The Office determined that *Zaid*'s "the vehicle is a shared vehicle" (citing *Zaid*, [0002]), "privileges are defined for each sharing session" (citing *Zaid*, Fig. 6, [0131]). Ex.1002, 128.

Zaid discloses a vehicle *sharing* service. *See, e.g., Zaid*, [0077] ("vehicles available for sharing"), [0016], [0095], [0134], claim 34 ("one *or more* vehicle users"). *Zaid*'s service is "attractive to customers who make only occasional use of a vehicle." *Id.*, [0002]. A POSITA would have understood that each customer has a unique vehicle reservation with unique time-restricted privileges. Almeroth, ¶269.

Specifically, usage of *Zaid*'s vehicle is limited to individual "reservations" (i.e., sharing sessions) with specific time-constrained privileges for access and use.

Zaid, [0069].

8[b]:

The Office determined that *Zaid*'s "vehicle collects trip information and reports to the server." Ex.1002, 128-29 (citing *Zaid*, [0130]).

Zaid describes monitoring vehicle usage and developing a "driver profile" while the vehicle reservations are active. *Zaid*, [0095] (monitoring "during one or more reservations"), [0097] ("location tracking system"), [0098] ("vehicle sensor readout unit"), [0099] ("vehicle usage data reporting unit 222 configured to report and communicate back to a central server"), [0134]. "[T]rip information (e.g., location information, traffic information, emergency information, and/or accident information) is reported to a central server." *Id.*, [0130].

Accordingly, *Zaid* discloses these limitations. Almeroth, ¶¶271-73.

10. Claim 11

Kleve continuously monitors the vehicle during the rental mode of use. *Kleve*, [0053], [0076]. Monitoring "may be transmitted to the server." *Id.* *Kleve*'s VCS transmits a notification to the user when violations are detected. *Kleve*, [0053] ("[T]he system may send a message to issue a warning to the Temporary User notifying of unauthorized usage of the vehicle."), [0040].

It would have been obvious to combine *Zaid*, *Mottla*, and *Kleve* to incorporate *Kleve*'s notifications into the combined system. Almeroth, ¶276. *Zaid*'s vehicle reports "trip information," including vehicle location and "usage information," to "a central server" during the rental mode of use. *Zaid*, [0130]. A POSITA would have found it obvious to include within this "trip information" a notification when a violation of a restriction is identified, as disclosed in *Kleve*, so the vehicle owner can ultimately be notified. A POSITA would have made this combination to give the owner "better control over" the renter and to allow the "owner to keep tabs" on the vehicle, "giv[ing] the vehicle owner an increased level" of security and control. *Id.*, [0072], [0097], [0114]. *Zaid* explicitly recites these concerns, which would have motivated a POSITA to look to *Kleve*, describing several methods for "additional security" and "continued control" in the context of vehicle sharing systems. *Kleve*, [0049], [0043]. A POSITA would have had a reasonable expectation of success in implementing the combination as *Kleve* already discloses vehicle and server hardware. The only modification to *Zaid*'s existing system would have been implementing a notification in software at the vehicle, as is described in *Kleve*. This would have been well within the skill of a POSITA at the time. Almeroth, ¶276.

Accordingly, the combination of *Zaid* and *Kleve* renders obvious this limitation. Almeroth, ¶277.

11. Claim 12

Kleve discloses this limitation. *See supra* §VII.A.13. It would have been obvious to combine *Zaid*, *Mottla*, and *Kleve* to incorporate *Kleve*'s notification features into the combined system for the same reasons discussed in Ground 3, claim 11, above. *See supra* §VII.C.10.

Accordingly, the combination of *Zaid* and *Kleve* discloses or renders obvious this limitation. Almeroth, ¶¶278-79.

12. Claim 13

Kleve discloses this limitation. *See supra* §VII.A.14; *Kleve*, [0073]. It would have been obvious to combine *Zaid*, *Mottla*, and *Kleve* to incorporate *Kleve*'s speed and geographical notifications into the combined system, such that *Zaid*'s vehicle reports *Kleve*'s “speed limit[]” and “No-Go Zone[]” violations to *Zaid*'s “central server” during the rental mode of use, for the same reasons discussed in Ground 3, claim 11, above. *See supra* §VII.C.10.

Accordingly, the combination of *Zaid* and *Kleve* renders obvious this limitation. Almeroth, ¶¶280-81.

13. Claim 14

Kleve discloses this limitation. *See supra* §VII.A.15. It would have been obvious to combine *Zaid*, *Mottla*, and *Kleve* to incorporate *Kleve*'s notifications “at

the display information center, instrument cluster, and/or other driver display device” (*Kleve*, [0053]) into the combined system. Almeroth, ¶283.

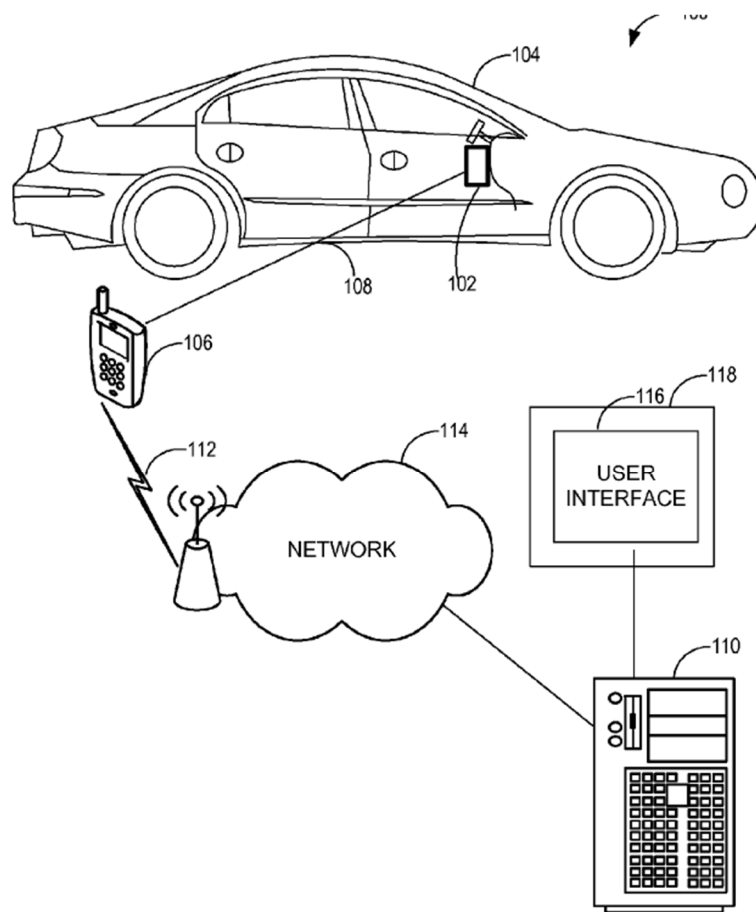
Zaid’s vehicle records “trip information,” including vehicle location and “usage information,” during the rental mode of allowed use. *Zaid*, [0130]. A POSITA would have found it obvious to use this “trip information” to identify a violation of a restriction for the purpose of displaying a notifications in the vehicle, as disclosed in *Kleve*. Almeroth, ¶283 (citing *Kleve*, [0053]). This would promote careful and conscientious use of the vehicle by the user. *Id.* A POSITA would have had a reasonable expectation of success in implementing the combination as *Kleve* already discloses vehicle hardware. The only modification to *Zaid*’s existing system would have been implementing a notification in software at the vehicle, as is described in *Kleve*. This would have been well within the skill of a POSITA at the time. *Id.*

Accordingly, the combination of *Zaid* and *Kleve* renders obvious this limitation. Almeroth, ¶284.

14. Claim 15

The Office determined that *Zaid*’s “user reserves the vehicle through the server and the server generates the access key.” Ex.1002, 129 (citing *Zaid*, Fig. 1, Fig. 5). *See, e.g., Zaid*, [0125] (“the vehicle reservation is booked by a user at a central server”), [0126] (“a central server managing vehicle reservation

communicates the vehicle reservation to a wireless communication device of a vehicle user”), [0130] (“trip information...is reported to a central server.”) (“an update (e.g., server update) to the vehicle access control from the wireless communication device is received from the central server.”), Fig. 1. *Zaid*’s “user must first log into the social networking website before he/she can view the advertisement and make reservation,” indicating that a cloud processing system is managing the user social media accounts. *Zaid*, [0072]; Almeroth, ¶285.



Zaid, Fig. 1.

Zaid's server is part of a cloud processing system. *See* Fig. 1, reproduced above (showing "Network" in cloud).

Accordingly, *Zaid* discloses or renders obvious this limitation. Almeroth, ¶¶286-87.

15. Claim 16

Kleve discloses this feature. *See supra* §VII.A.17. It would have been obvious to combine *Zaid*, *Mottla*, and *Kleve* to incorporate *Kleve*'s geolocation restriction into the combined system such that *Zaid*'s vehicle rental is subject to a geographic restriction set by the owner. Almeroth, ¶289. The combined system would allow the owner to set an allowed area of use (in addition to setting the vehicle's availability, as already disclosed in *Zaid*), giving the owner "better control over" the renter and providing "the vehicle owner [with] an increased level" of security and control. *Zaid*, [0072], [0097], [0114]. *Zaid* explicitly recites these concerns, which would have motivated a POSITA to look to *Kleve*, describing several methods for "additional security" and "continued control" in the context of vehicle sharing systems. *Kleve*, [0049], [0043]. A POSITA would have had a reasonable expectation of success in implementing the combination as *Zaid*'s system already includes a restriction based on availability and "dynamically update[ing] vehicle location" such that the vehicle location can be "announce[d]" in the "vehicle reservation application." *Zaid*, [0078]-[0079]. The only

modification to *Zaid*'s existing system would have been implementing Kleve's "approved ... area" (*Kleve*, [0076]) in software at *Zaid*'s vehicle reservation server such that the access and usage privileges associated with any vehicle reservation are subject to a "restricted area" set by the owner. This would have been well within the skill of a POSITA at the time. Almeroth, ¶289.

Accordingly, the combination of *Zaid* and *Kleve* render obvious this limitation. Almeroth, ¶290.

16. Claim 17

Zaid's restriction (vehicle availability) enables access to the vehicle via the doors. Specifically, *Zaid* explains that any vehicle reservation is prompted by "the backend vehicle sharing system [] register[ing] the vehicle as available" according to the owner setting the vehicle's availability. *Zaid*, [0079]. Once a reservation is made, subject to the vehicle's availability, a user may then use the reservation to "unlock doors" during the reservation period. *Zaid*, [0052], [0100], Figs. 4, 6.

Accordingly, *Zaid* discloses this limitation. Almeroth, ¶¶291-92.

17. Claim 18

The Office determined that this limitation is disclosed in *Mottla*. In *Mottla* "a mobile phone installed with a vehicle remote entry app [that] is usable by a user to operate the vehicle trunk by touch of the door icon displayed on the screen of

the mobile phone and the remote entry app. The status of the door is reflected in the display of the door icon.” Ex.1002, 130 (citing *Mottla*, Fig. 12, claims 1-2).

As described in claim 11, it would have been obvious to incorporate *Kleve*'s violation notification scheme into the vehicle sharing system of *Zaid* combined with *Mottla*, including *Kleve*'s “transmit[ing] confirmation back to the vehicle Owner 512 through a telecommunications network notifying that the Temporary User has entered the vehicle.” Almeroth, ¶294 (citing *Kleve*, [0068]). *Zaid*'s vehicle and server, performing *Kleve*'s notification scheme, would thus notify the vehicle owner when the vehicle is accessed using the vehicle reservation. *Id.* *Zaid* and *Kleve*, however, do not explicitly disclose that access may be to the vehicle's truck.

Mottla does. See *Mottla*, Fig. 12, claim 1-2. It would have been obvious to incorporate *Mottla*'s functionality for “opening a trunk” such that a user of the combined vehicle reservation system may access the trunk during the rental mode of allowed use. Almeroth, ¶295. Per *Kleve*'s disclosures, the combined system would result in *Zaid*'s “owner” receiving a notification when the trunk is accessed by the user. Specifically, a POSITA would have been motivated to add *Mottla* to the combined system to allow the user usage of additional vehicle functionality. For instance, A POSITA would have understood that airport rentals are a common application for the rental mode of allowed use, and travelers often have luggage

that would intrude on passenger space if trunk access was not enabled for the rental mode of allowed use. *Id.* The combination would have been well within the abilities of a POSITA, as the addition of *Mottla*'s trunk features would require nothing more than software connecting *Mottla*'s "trunk" function to *Kleve*'s notification scheme in the combined system. *Id.*

Accordingly, the combination of *Zaid*, *Kleve*, and *Mottla* renders obvious this limitation. Almeroth, ¶296.

D. Ground 4: Zaid, Kleve, Mottla, and Goudy Render Obvious Claim 10

1. Combination of Zaid, Kleve, Mottla, and Goudy

As in Ground 3, *Zaid*, *Kleve*, *Mottla*, and the '245 patent are all from the same field of endeavor (electronic key systems). *See supra* §VII.C. Further, as described in Ground 3, *Zaid*, *Kleve*, and *Mottla* are reasonably pertinent to the problem faced by the '245 patent inventor (controlling vehicle systems to provide added functionality and improve user experience). *Id.* Likewise, *Goudy* reasonably pertains to this same problem. *Goudy*, [0016]-[0017]. Almeroth, ¶297-98.

2. Claim 9

The Office determined that *Goudy* teaches this limitation and that "it would have been obvious to a [POSITA] to modify *Zaid*'s vehicle with a function to disable the vehicle's infotainment device while driving to improve safety."

Ex.1002, 131 (citing *Goudy*, Abstract).

Goudy “disable[s] at least one infotainment device under certain conditions relative to the current driving environment of the user.” *Goudy*, Abstract. *Goudy* explains that a “risk level” can prompt a “disable signal [] generated to disable [] infotainment devices” such as a “navigation system” comprising an “interface.” *Id.*, [0018]-[0019]; [0023]; Fig. 1, element 16.

It would be obvious to a POSITA to combine *Zaid*, *Mottla*, and *Kleve* with *Goudy* such that the system “disable[s] at least one infotainment device” during high-risk scenarios under the rental mode of use. Almeroth, ¶¶299-301. A POSITA would have been motivated to make the combination to promote safer driving. *Id.* *Goudy* explains that “if a distraction occurs...safety can be jeopardized.” *Goudy*, [0003]. A POSITA would have understood that disabling distractions during high-risk scenarios helps the driver focus on the road, thus improving safety. Almeroth, ¶301. A POSITA would have had a reasonable expectation of success in the combining the infotainment-disabling functionality of *Goudy* with the shared car system of *Kleve* because *Kleve* already provides options for limiting operational characteristics of the vehicle in the form of “remedial measures” and the modifications to further limit the infotainment interface would have been well within the abilities of a POSITA.

Accordingly, the combination of *Zaid*, *Mottla*, *Kleve*, and *Goudy* renders obvious this limitation. Almeroth, ¶302.

3. Claim 10

The Office determined that *Goudy* “teaches a vehicle has a function to disable the vehicle's infotainment device.” Ex.1002, 131 (citing *Goudy*, Abstract).
See supra §VII.D.2.

A POSITA would have understood that *Goudy*'s “disabl[ing] some or all of the functions of the least one infotainment device” would including disabling “controls of vehicle interfaces,” e.g., “navigation system” inputs. Almeroth, ¶¶303-04 (citing *Goudy*, [0023], [0041]). The combination would have been obvious as in claim 9.

Accordingly, the combination of *Zaid*, *Mottla*, *Kleve* and *Goudy* discloses or renders obvious this limitation. Almeroth, ¶305.

VIII. Grounds for Standing

Petitioners certify that the '245 patent is available for IPR and that Petitioners are not barred or estopped from requesting IPR challenging the patent claims on the grounds herein.

IX. Mandatory Notices

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

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

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

To the best of Petitioners’ knowledge, the ’245 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>	2:25-cv-00782	EDTX	August 12, 2025
<i>Emerging Automotive LLC v. Kia Corp. et al.</i>	2:25-cv-00799	EDTX	August 15, 2025

To the best of Petitioners’ knowledge, patents within the ’245 patent’s family are, or have been, involved in the following additional 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	September 20, 2023
<i>Emerging Automotive LLC v. Kia Corp. et al.</i>	2:23-cv-00437	EDTX	September 22, 2023
<i>Toyota Motor Corp. v. Emerging Automotive LLC</i>	IPR2024-00786	PTAB	April 15, 2024
<i>Toyota Motor Corp. v. Emerging Automotive LLC</i>	IPR2024-00814	PTAB	April 25, 2024
<i>Toyota Motor Corp and Kia Corporation v. Emerging Automotive LLC</i>	IPR2024-00785	PTAB	April 23, 2025
<i>Toyota Motor Corp and Kia Corporation v. Emerging Automotive LLC</i>	IPR2024-00981	PTAB	May 29, 2024
<i>Toyota Motor Corp and Kia Corporation v. Emerging Automotive LLC</i>	IPR2024-01167	PTAB	July 15, 2024

To the best of Petitioners’ knowledge, the ’245 patent is related to the

following U.S. applications that had been pending as of the issuance of the '245 patent, and their corresponding issued patents (if applicable):

Application Number	Patent Number	Filing Date
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
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

Inter Partes Review
U.S. Patent No. 11,104,245

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
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

Inter Partes Review
U.S. Patent No. 11,104,245

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	11,734,026	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
16/566,872	11,370,313	9/10/2019
16/732,069	11,270,699	12/31/2019
16/733,233	11,602,994	1/2/2020
16/785,629	11,294,551	2/9/2020
16/788,253	11,396,244	2/11/2020
16/929,083	11,427,101	7/14/2020
16/987,919	11,305,666	8/7/2020
17/088,349	11,889,394	11/3/2020
17/088,535	11,472,310	11/3/2020
17/094,804	11,396,240	11/10/2020
17/182,892	11,731,618	2/23/2021
17/329,935	11,935,013	5/25/2021
17/461,959	11,738,659	8/30/2021

90/019,456		3/25/2024
17/689,921	11,837,231	3/08/2022
17/713,216	12,197,710	4/04/2022
17/873,096	12,337,716	7/25/2022
17/873,119	11,772,502	7/25/2022
17/968,475	11,975,631	10/18/2022
18/076,278		12/6/2022
18/125,448	11,794,601	3/23/2023
18/236,369		8/21/2023
18/236,677	12,330,637	8/22/2023
18/376,409	12,257,914	10/3/2023
18/379,043	12,337,715	10/11/2023
18/427,686		1/30/2024
18/530,125		12/5/2023
19/026,361		1/17/2025
19/012,653		1/7/2025
19/248,175		6/24/2025
19/248,414		6/24/2025

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

Lead Counsel	Back-Up Counsel
<p>Joshua L. Goldberg (Reg. No. 59,369) Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 901 New York Ave NW Washington, DC 20001 Tel: 202-408-4000 Fax: 202-408-4400</p> <p>James M. Glass (Reg. No. 46,729) jimglass@quinnemanuel.com</p> <p>QUINN EMANUEL URQUHART & SULLIVAN, LLP 51 Madison Avenue, 22nd Floor New York, NY 10010 Tel: (212) 849-7000</p>	<p>James R. Barney (Reg. No. 46,539) james.barney@finnegan.com</p> <p>Aidan Skoyles (Reg. No. 61,119) aidan.skoyles@finnegan.com</p> <p>Nicholas Eitsert (Reg. No. 78,843) nicholas.eitsert@finnegan.com</p> <p>Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 901 New York Ave NW Washington, DC 20001 Tel: 202-408-4000 Fax: 202-408-4400</p>

Lead Counsel	Back-Up Counsel
Fax: (212) 849-7100	Quincy Lu (Reg. No. 76,954) quincylu@quinnemanuel.com Joseph Milowic III (Reg. No. 52,034) josephmilowic@quinnemanuel.com QUINN EMANUEL URQUHART & SULLIVAN, LLP 1109 First Avenue, Suite 210 Seattle, WA 98101 Tel: (206) 905-7000 Fax: (206) 905-7100

D. Service Information Under 37 C.F.R. § 42.8(b)(4)

Please address all correspondence to counsel at the addresses above.

Petitioners consent to service by email at the above addresses.

X. Conclusion

Petitioners request that the Board institute *inter partes* review and cancel each challenged claim.

Respectfully submitted,

Dated: October 21, 2025

By: /Joshua L. Goldberg/
Joshua L. Goldberg, Reg. No. 59,369

CERTIFICATION UNDER 37 C.F.R. § 42.24(d)

Pursuant to 37 C.F.R. § 42.24(d), the undersigned hereby certifies that the foregoing Petition contains 13,648 words, excluding parts of this Petition exempted under § 42.24(a), as measured by the word-processing system used to prepare this paper.

Respectfully submitted,

Dated: October 21, 2025

By: /Joshua L. Goldberg/
Joshua L. Goldberg, Reg. No. 59,369

CERTIFICATE OF SERVICE

The undersigned certifies that the foregoing Petition for *Inter Partes* Review, the associated Powers of Attorney, and Exhibits 1001-1019 were served on October 21, 2025, on counsel of record for the subject patent by FedEx Priority Overnight at the addresses below.

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

Dated: October 21, 2025

By: /Daniel E. Doku/
Daniel E. Doku
Senior Litigation Paralegal
FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.