

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. IPR2024-00785
U.S. Patent No. 10,407,026

PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 10,407,026

TABLE OF CONTENTS

I.	Preliminary Statement	1
II.	Precise Relief Requested	2
III.	The '026 Patent.....	3
A.	Disclosure.....	3
B.	File History.....	7
C.	The '026 patent's claims are entitled to an effective filing date of no earlier than October 25, 2013	8
1.	Legal requirement for determining entitlement to priority to prior-filed application	9
2.	No application preceding continuation-in-part application US 14/063,638 discloses "electronic key[s]"	10
IV.	Overview of Prior Art.....	11
V.	Level of Ordinary Skill.....	16
VI.	Claim Construction.....	16
VII.	Claims 1-20 Are Unpatentable Over the Prior Art.....	16
A.	Ground 1a: Zaid anticipates claims 1-7, 11-12, 14, and 18-20.....	17
	Ground 1b: Zaid renders obvious claims 1-7, 11-12, 14, and 18-20.....	17
1.	Independent Claim 1	17
2.	Claim 2.....	37
3.	Claim 3.....	39
4.	Claim 4.....	40
5.	Claim 5.....	41
6.	Claim 6.....	43

7.	Claim 7	46
8.	Claim 11	47
9.	Claim 12	48
10.	Claim 14	49
11.	Claim 18	50
12.	Claim 19	51
13.	Claim 20	52
B.	Ground 2: Zaid in view of Patenaude renders obvious claim 10	53
1.	Claim 10	54
C.	Ground 3: Zaid in view of Gilbertson renders obvious claim 13	57
1.	Claim 13	58
D.	Ground 4: Zaid in view of Kleve renders obvious claim 15	63
1.	Claim 15	65
VIII.	Grounds for Standing	69
IX.	The Board Should Not Exercise Discretion to Deny Institution	69
A.	The <i>Fintiv</i> Factors Do Not Warrant Denial	69
B.	The <i>Becton, Dickinson</i> Factors Do Not Warrant Denial	71
X.	Mandatory Notices	72
A.	Real Party-in-Interest Under 37 C.F.R. § 42.8(b)(1)	72
B.	Related Matters Under 37 C.F.R. § 42.8(b)(2)	72
C.	Lead and Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)	73
D.	Service Information Under 37 C.F.R. § 42.8(b)(4)	74
XI.	Conclusion	74

LIST OF EXHIBITS

Exhibit	Description
Ex. 1001	U.S. Patent No. 10,407,026 to <i>Penilla</i> et al.
Ex. 1002	Prosecution File History for U.S. Patent No. 10,407,026.
Ex. 1003	Curriculum Vitae of Dr. Kevin Almeroth.
Ex. 1004	Declaration of Dr. Kevin Almeroth.
Ex. 1005	U.S. Patent Pub. No. 2011/0112969 to Sam Zaid et al.
Ex. 1006	U.S. Patent Pub. No. 2014/0129053 to Robert Bruce Kleve et al.
Ex. 1007	U.S. Patent Application Pub. No. 2006/0136106 A1 by Russell A. Patenaude et al.
Ex. 1008	U.S. Patent Pub. No. 2013/0113602 to Matthew R. Gilbertson 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	District of Columbia Department of Motor Vehicles, <i>Medical Restrictions</i> , Retrieved from: https://web.archive.org/web/20101110064942/http://dmv.dc.gov/serv/medical/medicalRestrictions.shtm (Nov. 10, 2010).
Ex. 1016	Florida Department of Highway Safety and Motor Vehicles, <i>Licensing Requirements for Teens – Graduated Driver Licensing</i> , Retrieved from: https://web.archive.org/web/20101216053738/http://flhsmv.gov/ddl/teendriv.html#learner (Dec. 16, 2010).

Exhibit	Description
Ex. 1017	D. Alfred Owens and Michael Sivak, <i>The Role of Reduced Visibility in Nighttime Road Fatalities</i> , Retrieved from: https://deepblue.lib.umich.edu/bitstream/handle/2027.42/49541/UMTRI-93-33.pdf?sequence= (Nov. 1993).
Ex. 1018	Bob D’Avello and Jim Van Bosch, <i>Portable and Embedded Wireless Devices as Conduits for Telematics Applications</i> (Oct. 2002).
Ex. 1019	Mike Spencer et al., <i>Network Security: Private Communications in a Public World</i> (2002).
Ex. 1020	Jacqui Cheng, <i>OpenTable’s iPhone app makes reservations a breeze</i> (Nov. 17, 2008).
Ex. 1021	Order Granting Request For Ex Parte Reexamination, Reexamination Control No. 90/019,456, Patent No. 11,738,659 (April 15, 2024).
Ex. 1022	<i>Login</i> , Facebook Developers (May 4, 2013).
Ex. 1023	<i>Using the signed_request Parameter</i> , Facebook Developers (April 15, 2013).
Ex. 1024	<i>Email Permissions</i> , Facebook Developers (March 17, 2013).
Ex. 1025	<i>Mercedes-Benz mbraceBy Hughes Telematics, Inc.</i> , iTunes App Store, last updated Aug. 24, 2010, screenshots 2-4, retrieved from: https://web.archive.org/web/20110265054805/http://itunes.apple.com/us/app/mercedes-benz-mbrace/id335276900?mt=8b .
Ex. 1026	<i>Mercedes-Benz mbraceBy Hughes Telematics, Inc.</i> , iTunes App Store, last updated Aug. 24, 2010, screenshots 1-2, retrieved from: https://web.archive.org/web/20110265054805/http://itunes.apple.com/us/app/mercedes-benz-mbrace/id335276900?mt=8b .
Ex. 1027	Reserved.
Ex. 1028	Reserved.
Ex. 1029	Text Comparison of U.S. Patent Application No. 13/452,882 to U.S. Patent Application No. 14/063,638.

Exhibit	Description
Ex. 1030	U.S. Patent No. 11,738,659.
Ex. 1031	U.S. Patent Publication 2014/0156111 to Ehrman (“Ehrman”).
Ex. 1032	U.S. Patent Application No. 15/344,566.
Ex. 1033	U.S. Patent Application No. 15/180,306.
Ex. 1034	U.S. Patent Application No. 14/303,442.
Ex. 1035	Budget Rent-a-Car Common Questions (Dec. 2, 2010).
Ex. 1036	Docket Control Order.
Ex. 1037	Plaintiff Emerging Automotive LLC’s Disclosure of Asserted Claims and Infringement Contentions Against Toyota Defendants.
Ex. 1038	Text Comparison of U.S. Patent Application No. 13/842,158 to U.S. Patent Application No. 14/063,638.
Ex. 1039	9/3/2015 Response to Office Action, App. No. 14/063,638.

I. Preliminary Statement

Petitioners Toyota Motor Corporation and Kia Corporation request IPR of claims 1-7, 10-15, and 18-20 of U.S. Patent No. 10,407,026, purportedly assigned to Emerging Automotive LLC (“EA”).

The patent relates to providing limited access to a vehicle via electronic keys associated with privileges. It discloses that “access [to the vehicle] can be by way of electronic keys (e.g., e-keys), which can be sent by a vehicle owner/admin to some person or entity.” ’026 Patent at 10:23-25. For example, “the user-owner of the vehicle can assign a valet with access to the vehicle by going on an application (App or website) on a computing device (e.g., mobile or non-mobile device), identifying the recipient, identifying a mode for communicating with the recipient (e.g., text, email, message, notification, etc.), selecting the amount of privileges (e.g., what type of access, speed limits, geographic restrictions, amount of time the e-keys will be valid (or else expire)), and requesting that e-keys be sent to the recipient.” *Id.*, 10:25-34. The electronic key provides limited vehicle access privileges, defined remotely. The ’026 describes privileges including the “amount of time the e-keys will be valid (or else expire)[.]” *Id.*, 5:64-66.

But, such vehicle access systems were well-known prior to the ’026 patent’s effective filing date, October 25, 2013. For example, *Zaid* was filed nearly three years earlier. *Zaid* disclosed the same concept of unique electronic keys (e.g., e-

keys) on mobile devices providing vehicle access, where e-keys are associated with privileges. *Zaid*'s system provides privileges to access and start the vehicle for specified amounts of time, just like the privileges disclosed in the '026 patent. Accordingly, the Board should institute IPR and cancel the challenged claims.

I. Precise Relief Requested

Petitioner requests review and cancellation of the challenged claims based on the following prior art and grounds. As explained in Section III.C., the '026 patent claims are entitled to an effective filing date of no earlier than October 25, 2013. Petitioner notes the prior art status of the references under both AIA and pre-AIA law to account for the possibility of EA arguing for an earlier priority date.

Prior Art References
<i>Zaid</i> (Ex. 1005), 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)).
<i>Kleve</i> (Ex. 1006), U.S. Patent Pub. No. 2014/0129053, filed Nov. 7, 2012, and published May 8, 2014 (§§ 102(a)(2) or pre-AIA § 102(e)).
<i>Patenaude</i> (Ex. 1007), U.S. Patent App. Pub. No. 2006/0136106, filed Dec. 22, 2004, and published Jun. 22, 2006 (§§ 102(a)(1), (2) or pre-AIA § 102(a), (b), (e)).

Prior Art References	
<i>Gilbertson</i> (Ex. 1008), U.S. Patent Pub. No. 2013/0113602, filed Nov. 5, 2012, published May 9, 2013, (§§ 102(a)(1), (2) or pre-AIA §§ 102(a), 102(e)).	

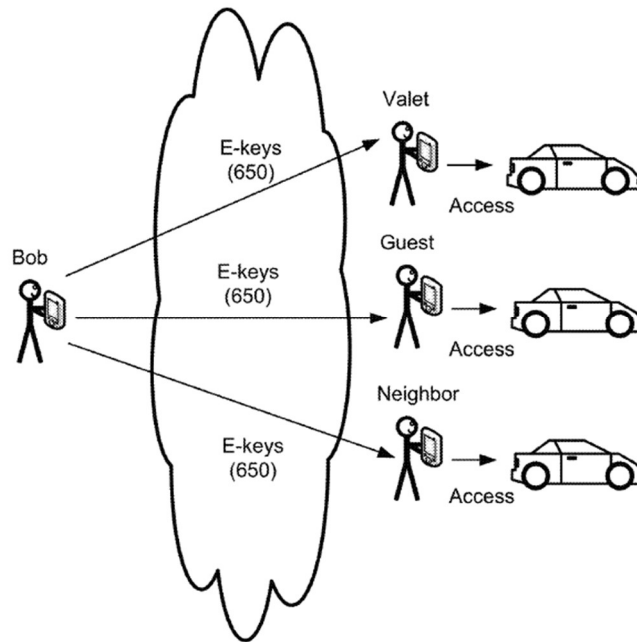
Grounds of Unpatentability	
1a	<i>Zaid</i> anticipates 1-7, 11-12, 14, and 18-20 under Section 102.
1b	<i>Zaid</i> renders obvious claims 1-7, 11-12, 14, and 18-20 under Section 103.
2	<i>Zaid</i> and <i>Patenaude</i> render obvious claim 10 under Section 103.
3	<i>Zaid</i> and <i>Gilbertson</i> render obvious claim 13 under Section 103.
4	<i>Zaid</i> and <i>Kleve</i> render obvious claim 15 under Section 103.

II. The '026 Patent

A. Disclosure

The specification describes a system where a vehicle owner assigns an electronic key to a user. '026 Patent, 43:23-37. In Figure 29, vehicle owner Bob shares electronic keys 650 with users “valet,” “guest,” and “neighbor”. *Id.*, 43:23-25. The specification explains that “[e]ach e-key, in one embodiment, will include a unique access code or substantially unique access code.” '026 Patent, 43:38-39. “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.*, 43:46-50.



'026 Patent, Fig.29.

In Figure 31A, vehicle owner John utilizes the cloud server 120 to send an encrypted ekey to guest user Bob. In this embodiment, “the server will generate an access code for the vehicle” (*id.*, 44:40-41), which “will then be encrypted by the server and then sent as encrypted e-keys 722¹ to Bob’s device 704.” *Id.*, 44:41-43.

¹ Reference to “encrypted e-keys 722” is likely a typo and should refer to encrypted e-keys 720.

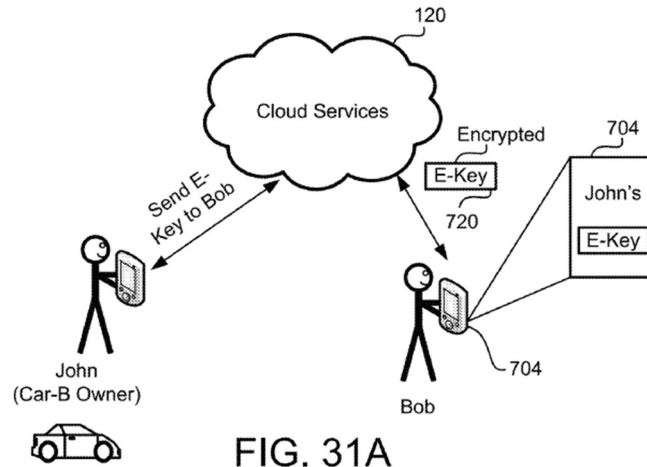


FIG. 31A

'026 Patent, Fig.31A.

In Figure 32, user Bob “will transfer the encrypted e-keys 720 to the vehicle that belongs to John (car-B). . . The vehicle will receive the encrypted e-keys and the device ID of Bob’s device 704. The vehicle will hold a private key to unlock and un-encrypt the encrypted e-keys 720.” *Id.*, 44:49-58.

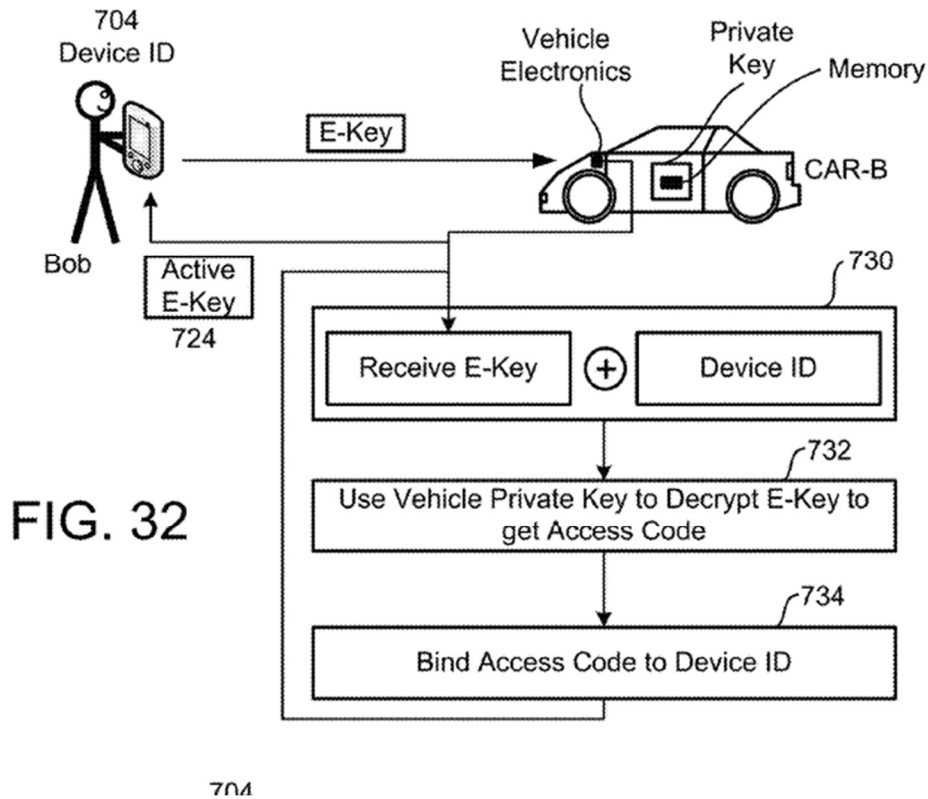


Figure 32 describes the e-key being associated with the device of the user seeking to utilize the e-key. In step 730, the encrypted ekey is “associated” with the mobile device. *Id.*, 44:63-65. In step 732, “the vehicle private key is used to decrypt the e-keys to get access to an access code.” *Id.*, 45:7-8. And in step 734, “[t]he access code is then sent as activated e-keys 724 back to Bob’s device 704,” allowing Bob’s device to access the vehicle. *Id.*, 45:11-15. The unique access code “can be generated by a number generator, and [sic] alphanumeric random generator, in [sic] incremental number generator, or any other generation device that can generate codes that are unique or substantially unique.” *Id.*, 45:52-55.

The specification also discloses that “electronic keys for each user can be

associated with a different expiration time.” *Id.*, 43:36-37; *see also* 38:50-51 (privileges for “use[] during specific periods of time”), 50:37-39 (“the privileges can be assigned by selecting . . . time durations[.]”). In the example above, once Bob receives the ekey from the server as John requested, “Bob’s device 704 can now access the vehicle in accordance with the time-bound privileges set by John, the owner of the vehicle.” *Id.*, 45:13-15.

B. File History

The application leading to the ’026 Patent was filed with 20 claims on May 26, 2017, as the latest in a long string of continuations and continuations-in-part beginning with a provisional application on April 22, 2011. Ex. 1002, 74. Four days after filing, an Information Disclosure Statement was filed containing 357 US patents and publications. *Id.*, 136-45. One of two inventors, Mr. Albert S. Penilla, was also the prosecuting attorney. *Id.*, 146.

All initial claims were rejected for nonstatutory double patenting over U.S. Patent No. 9,663,306 and as obvious over U.S. Patent Publication 2014/0156111 to Ehrman (“*Ehrman*”). *Id.*, 171-73; *see also* Ex. 1031.

Applicants made no amendments in response to the rejection but instead filed a terminal disclaimer and argued against the *Ehrman* obviousness rejection. Ex. 1002, 209. Applicants distinguished the claimed “unique access code” with associated privileges from *Ehrman*’s vehicle ID and password combination by

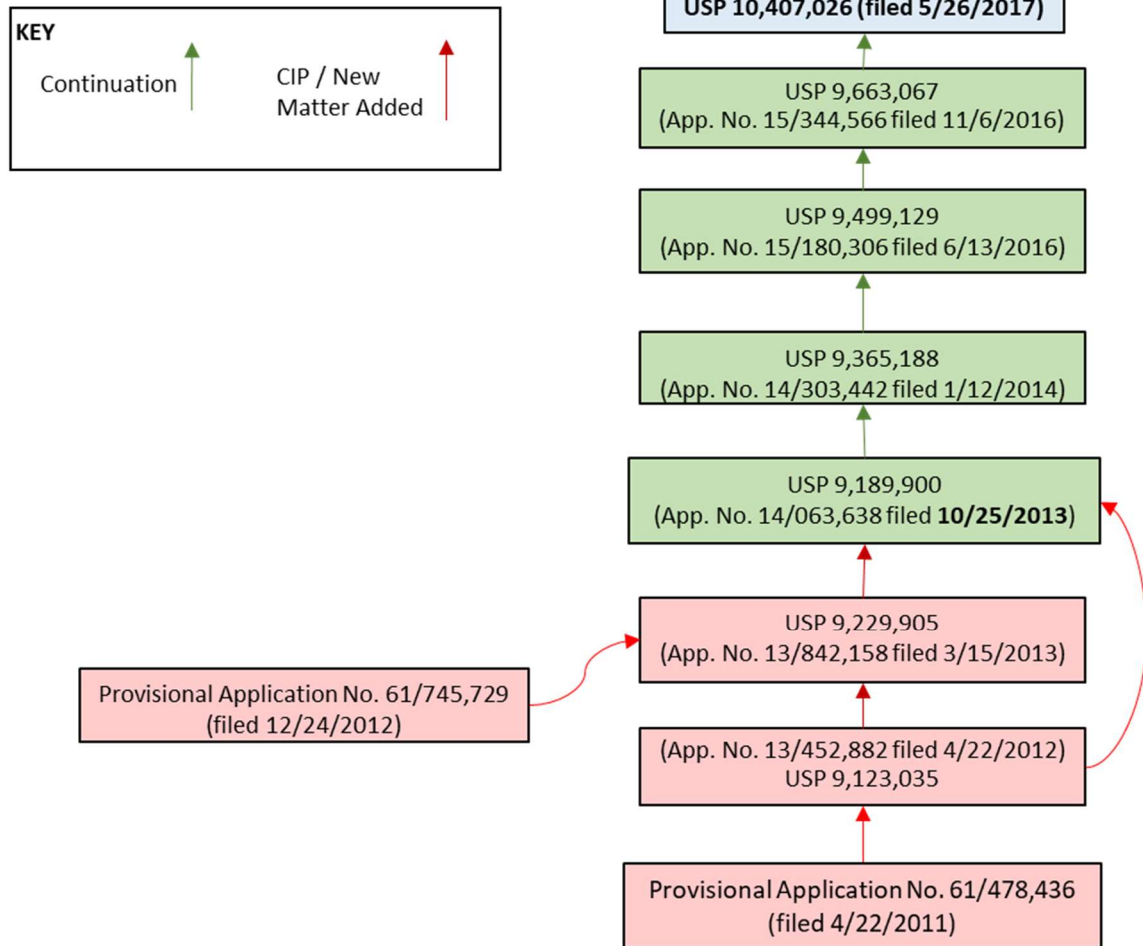
arguing that *Ehrman*'s "VID is unique to the car, not something that is unique to access," as in the claimed unique access code. Ex. 1031, ¶[0052]; Ex. 1002, 207. Applicants also pointed out that "Ehrman does not teach that privileges are defined for the unique access code." *Id.* While *Ehrman* discloses a rental agreement, which would include a time period, Applicants argued "nothing is discussed [in Ehrman] on how the [rental] agreement is related to the claimed unique access code." *Id.*

In response, the Examiner issued a Notice of Allowance noting that the prior art did not teach the limitations of claim 1. *Id.*, 218.

C. The '026 patent's claims are entitled to an effective filing date of no earlier than October 25, 2013

The application leading to the '026 Patent claims priority to U.S. Application Nos. 15/344,566, 15/180,306, 14/303,442, 13/452,882, 14/063,638, 13/824,158, 61/478,436, and 61/745,729 (Ex. Nos. 1032-1034, 1012, 1014, 1013, 1010, 1011, respectively). Several of these are continuations-in-part, which include new subject matter, as illustrated in the graphic below.

Inter Partes Review
U.S. Patent No. 10,407,026



The '026 patent's claims are not entitled to a filing date before October 25, 2013, because none of the applications before then describe the “e-key” subject matter.

1. Legal requirement for determining entitlement to priority to prior-filed application

Under 35 U.S.C. § 120, a claim is not entitled to the benefit of an earlier filed U.S. application unless the subject matter of the claim is disclosed in the manner provided by 35 U.S.C. § 112 in the earlier filed application. *See, e.g., D Three Enters., LLC v. SunModo Corp.*, 890 F.3d 1042, 1046-47 (Fed. Cir. 2018).

To comply with the written description requirement under 35 U.S.C. § 112, an application must “reasonably convey [] to those skilled in the art that the inventor had possession of” and “actually invented” the claimed subject matter. *Ariad Pharms., Inc. v. Eli Lilly & Co.*, 598 F.3d 1336, 1351 (Fed. Cir. 2010) (en banc). The test for adequate written description support “requires an objective inquiry into the four corners of the specification from the perspective of a person of ordinary skill in the art.” *Id.* “It is the disclosures of the applications that count.” *Lockwood v. Am. Airlines, Inc.*, 107 F.3d 1565, 1571-72 (Fed. Cir. 1997). “[T]he disclosure must describe the claimed invention with all its limitations.” *Tronzo v. Biomet, Inc.*, 156 F.3d 1154, 1158 (Fed. Cir. 1998).

**2. No application preceding continuation-in-part application
US 14/063,638 discloses “electronic key[s]”**

None of U.S. Application Nos. 61/478,436, 13/452,882, 61/745,729 or 13/842,158 (Ex. 1010-13) discloses “electronic key[s],” “ekey[s],” or anything similar.

For example, the Patent Office recently considered the effective priority date of descendent Patent No. 11,738,659 (the “’659 Patent) in granting ex-parte reexamination. *See* Ex. 1021 at 4. In the order granting reexamination, the Patent Office stated that, “[t]he disclosure of [U.S. Provisional App. No. 61/478,436] however *appears to lack support* for several limitations . . . include[ing] for

example an ‘eKey’, ‘coded data’, ‘unlocking’ or ‘starting’ of the vehicle and ‘privilege settings’”. *Id.*

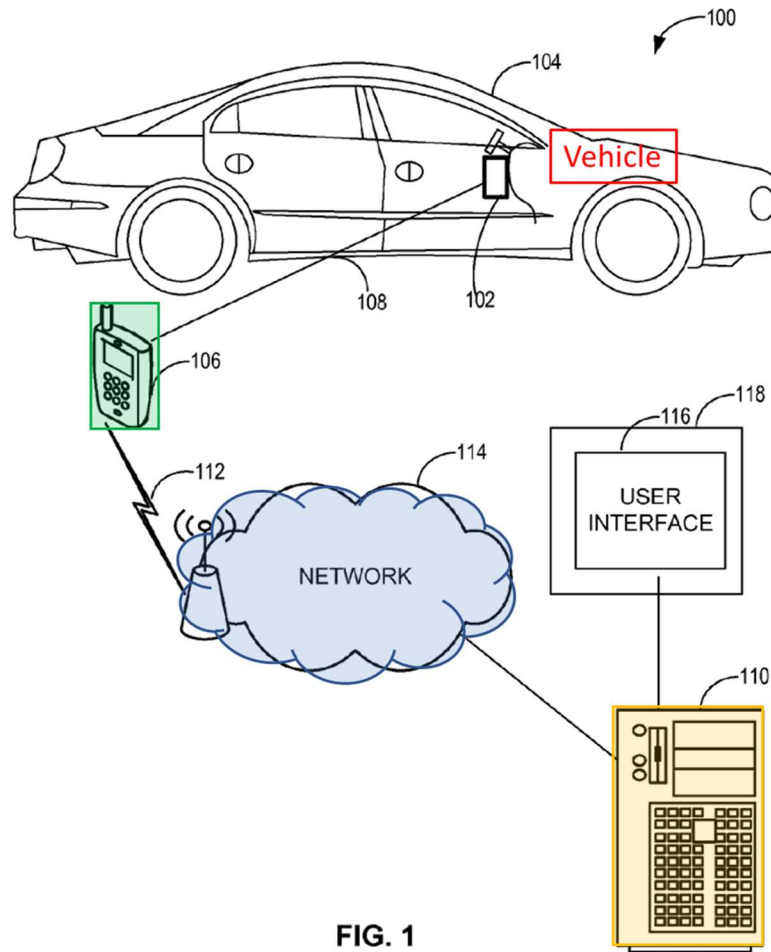
Indeed, the Applicant added new subject matter concerning “e-keys” for the first time on October 25, 2013, via CIP App. No. 14/063,638. *See* Exs. 1029 (generally) (illustrating, in redline, new matter regarding “e-keys” compared to the subject matter of priority App. No. 13/452,882) and 1038, 2-5, 35-50, 53-70 (illustrating, in redline, new matter regarding “e-keys” compared to the subject matter of priority App. No. 13/842,158). Accordingly, the ’638 application is the earliest application possibly supporting “enabling access to use the vehicle via one or more electronic keys,” as required by every claim of the ’026 patent. Almeroth (Ex. 1004), ¶¶[0061]-[0068] (citing Exs. 1010-14, 1032-34, 1038-9).

Accordingly, the ’026 Patent is entitled to an effective filing date of no earlier than October 25, 2013.

III. The Prior Art

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

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



Zaid, Fig.1 (annotated).

Zaid's central server interacts with vehicle access control systems on many vehicles to provide rental options for users across a town or city. *Zaid*, ¶[0080]. In a typical case, a customer uses their wireless communication device 106 to search for vehicles. *Id.*, ¶[0077]. They make a reservation for a vehicle, which is communicated to the central server 110. *Id.*, ¶[0076]. The central server 110 sends an encrypted vehicle reservation to the reserved vehicle via the wireless communication device 106. *Id.* The vehicle access component 102 then decrypts the request and, if authentic, permits the customer to unlock and start the vehicle, but only for the specific time-period requested and paid for. When the time-period elapses, access is withdrawn and the customer can no longer unlock or start the vehicle. *Id.*, ¶[0131].

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

Zaid's vehicle access component can be integrated into a “vehicle access kit,” as in Fig.2 and shown containing electronic components such as a

microprocessor, memory, and a communication interface (WiFi or Bluetooth) for communicating to a remote server via the user's mobile device. *Id.*, Fig.2, ¶[0087]. A long-range communication function can be added to the communication interface to "act as a backup" in case communication via the user's mobile phone is unavailable. *Id.*, ¶[0106].

Zaid was not substantively addressed during the prosecution of the '026 Patent, but *Zaid* was submitted to the Examiner in an IDS containing 357 references. Ex. 1002, 138.

Zaid was cited and discussed by the Examiner during prosecution of a *descendant* continuation application from the '026 patent. Applicant's statements there regarding *Zaid* are relevant to this proceeding. During prosecution of continuation Application No. 17/461,959, which issued as U.S. Patent No. 11,738,659 (also asserted in the below-referenced litigations), the Examiner rejected pending claims as anticipated by *Zaid*. Ex. 1009, 349. The Examiner noted that *Zaid* disclosed a vehicle capable of being unlocked with an ekey received from a mobile device. *Id.*, 357.

In response to the rejection, Applicants did not dispute that *Zaid* discloses wireless transfer of a unique, encrypted reservation from a mobile device to a vehicle where the reservation is decrypted to unlock and enable starting the vehicle for a specified period of time. *Id.*, 511.

To overcome the rejection, Applicants amended the pending claims of the continuation application to require that transmissions to the vehicle for unlocking and use include “coded data including [sic] privilege settings for additionally limiting *types of use* of the vehicle when using the ekey with the vehicle.” Ex. 1009, 333 (emphasis added). Applicants argued that in *Zaid* “[u]pon access of the vehicle the use is unlimited – once decrypted. ¶69 [citing *Zaid* publication] . . . In fact, nothing is discussed by *Zaid* regarding a unique access code that includes privilege settings set ***for additionally limiting types of use*** of the vehicle when using the ekey with the vehicle.” *Id.*, 339 (bold italics added). Thus, Applicants distinguished a privilege setting a period of time for vehicle use (disclosed in *Zaid*) from a privilege that further limits a “*type of use*” (allegedly not disclosed in *Zaid*). Applicants thus tacitly admitted that *Zaid* discloses an ekey associated with a privilege for use but argued it did not disclose the newly-narrowed privilege limitation requiring a privilege limiting the “type of use.”

As a result of the amendments, the ’659 patent claims require “privilege settings associated with the eKey for ***limiting types of use*** of the vehicle[.]” Ex. 1030, ’659 Patent, claim 1 (emphasis added). The ’026 patent claims, in contrast, merely require “the unique access code is associated with privileges for use of the vehicle,” and that the ekey “enable unlocking of the vehicle and enable starting of

the vehicle . . . consistent with the privileges of the unique access code.” ’026

Patent, claim 1.

The remaining cited references, *Patenaude* (Ex. 1007), *Gilbertson* (Ex. 1008), and *Kleve* (Ex. 1006), demonstrate other well-known elements of electronic systems present in the art, namely, determining learned settings (*Patenaude*, claim 10), deactivating access to an electronic key (*Gilbertson*, claim 13), and sending notifications to vehicles in the event of a privilege violation (*Kleve*, claim 15).

IV. 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 (“Almeroth”), ¶¶[0069]-[0075].

V. Claim Construction

Claims only need to be construed to the extent necessary to resolve a controversy. No terms need construction because the claims read on the prior art identified below under any construction consistent with *Phillips*.

VI. Claims 1-20 Are Unpatentable Over the Prior Art

A. Ground 1a: Zaid anticipates claims 1-7, 11-12, 14, and 18-20

Ground 1b: Zaid renders obvious claims 1-7, 11-12, 14, and 18-20

1. Independent Claim 1

1[preamble]: “A vehicle configured to communicate with a server of a cloud system to enable access to use the vehicle via one or more electronic keys, comprising,”

Zaid discloses a **vehicle 104** in communication with a server 110 (**yellow**) belonging to a cloud system or **network 114** for enabling access to use the vehicle via an electronic key from a **wireless communication device 106**. *Zaid*, Fig.1. Almeroth, ¶[0085].

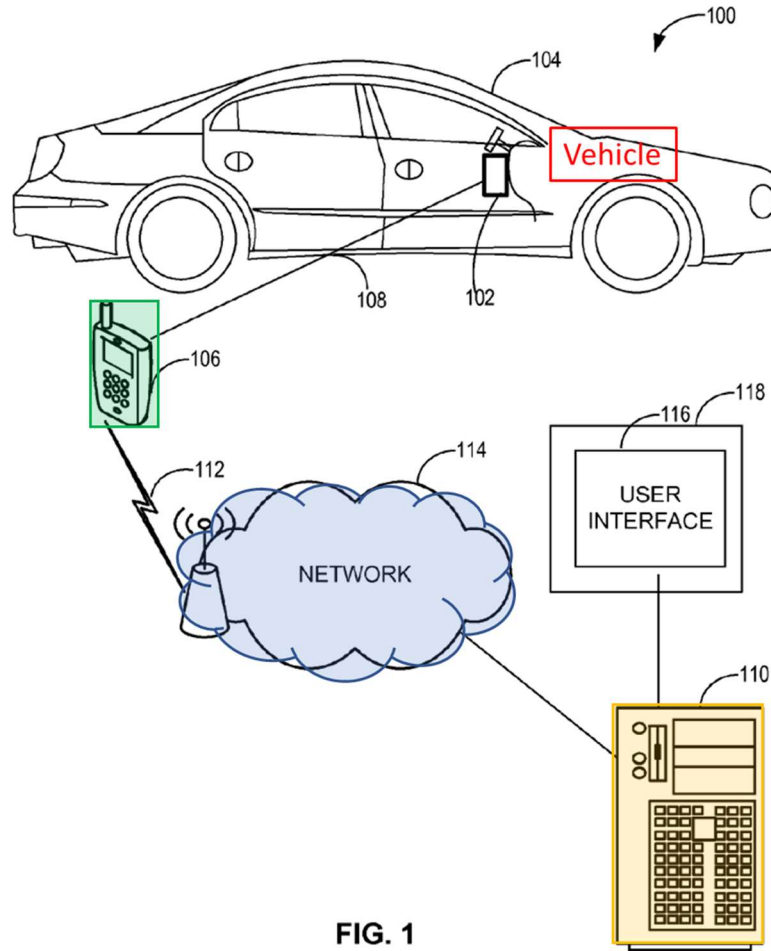


FIG. 1

Zaid, Fig.1 (annotated).

Zaid's electronic key is part of a "vehicle access control service[]" for "provid[ing] access to a vehicle . . . when a vehicle reservation is received from [a] wireless communication device." *Zaid*, Abstract, ¶[0067]. The server generates and transmits a vehicle reservation (i.e. an electronic key) to the wireless communication device 106, e.g., a "smart phone," which passes the request to a "vehicle access component" in the vehicle to enable access. *Id.*, ¶¶[0075]-[0076].

The vehicle reservation therefore provides electronic access to use the vehicle via an electronic key.

To enable access, *Zaid*'s vehicle communicates with the wireless communication device and with the server of network 114, which Fig.1 shows is a cloud system. Vehicle-server communication in *Zaid* is used for encryption/decryption purposes. *Id.*, ¶¶[0070], [0099], [0125]-[0128], [0133], claims 10-13. For example, to allow for decryption of the vehicle reservation, *Zaid*'s server sends a private key to the vehicle. *Id.*, ¶[0130] ("the server update includes a new private key for vehicle access control"). Vehicle-to-server communication is transmitted via the user's wireless communication device, but the vehicle may also include a mobile communication radio (e.g., GSM radio) to act as a backup when the user's wireless communication device is not available. *Id.*, ¶[0106] (vehicle can include "long-range mobile communication radio/interface . . . for wireless communication to a vehicle reservation or sharing system"); *see also id.* claims 7-8. The mobile communication radio provides a route for direct vehicle-to-server communications. *Id.*

Zaid's system is functionally identical to the '026 patent specification. Both send a request to a server ('026 Patent, 44:37-39; *compare Zaid*, ¶[0080]), send an "access code" from server to user device ('026 Patent, 44:41-44; *compare Zaid*, ¶[0126]), transmit an access code from user device to vehicle ('026 Patent, 44:49-

51; *compare Zaid*, ¶[0128]), decrypt the access code using a private key from the server ('026 Patent, 44:55-58, 47:52-54; *compare Zaid*, ¶[0128]), and send the decrypted access code back to user device from vehicle for enabling vehicle access ('026 Patent, 45:11-15; *compare Zaid*, ¶[0129]). Accordingly, *Zaid* discloses the preamble of claim 1. Almeroth, ¶¶[0088]-[0090].

1[a]: “electronics of the vehicle;”

Zaid's vehicle includes electronics, e.g., a microprocessor 224 and memory 226, in the vehicle access kit 200. *Zaid*, ¶¶[0100]-[0101], Fig.2; *see also id.*, ¶[0083]. The microprocessor 206 utilizes memory 226 to “store various computer instructions to be executed by the microprocessor[.]” *Id.*, ¶[0101]. The vehicle access kit, containing the microprocessor and memory, is “coupled to the vehicle[.]” *Id.*, ¶[0083].

Accordingly, *Zaid* discloses this limitation of claim 1. Almeroth, ¶[0092].

1[b]: “a subsystem of the vehicle for enabling unlocking of the vehicle, the subsystem being interfaced with the electronics;”

Zaid's vehicle includes part of an electronic control unit 308, and vehicle actuators 310 to enable unlocking the vehicle. *Zaid*, ¶[0123], Fig.3. *Zaid* provides a definition of ECU “Electronic Control Unit” as “any embedded system that controls one or more subsystems in a motor vehicle. Modern motor vehicles have up to 80 ECU's and often the [sic] collectively referred to as the ECU.” *Id.*,

¶[0035]. The component of the ECU 308 which enables unlocking is part of the claimed unlocking “subsystem” in limitation 1[b].

ECU 308 interfaces with the vehicle access kit 302, including the microprocessor 224 and memory 226, via a vehicle bus 306 and adapter 304. *Id.*, Fig.3. *Zaid* discloses that microprocessor 224 “accepts commands (e.g., unlock doors, start engine, and/or other commands) . . . and instructs the vehicle bus to actuate the corresponding car function.” *Id.*, ¶[0100]. *Zaid* discloses that the vehicle bus used to interface between the microprocessor and other vehicle components is typically a CAN-bus or LIN-bus. *Id.*, ¶¶[0037]-[0038], [0046] (describing “central ECU” and “door lock[s]” as being controlled via the LIN bus interface).

Zaid also discloses that “[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). This typically leverages SAE standards such as CAN-bus and/or LIN-bus.” *Id.*, ¶¶[0058], [0062].

Accordingly, *Zaid* discloses this limitation of claim 1. Almeroth, ¶[0096].

**1[c]: “a subsystem of the vehicle for enabling starting
of the vehicle for use of the vehicle; and”**

Zaid’s vehicle includes a vehicle access control component 206 connected to the bus 306, ECU 308 and actuators 310 for enabling starting the vehicle for use.

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., . . . *start engine*).” *Zaid*, ¶[0091], Fig.2. Vehicle actuators include “engine starter.” *Id.*, ¶[0123].

Accordingly, *Zaid* discloses this limitation of claim 1. Almeroth, ¶[0098].

1[d]: “communications circuitry of the vehicle interfaced with electronics of the vehicle, the communications circuitry being programmable to communicate with the server of the cloud system and communicate with a mobile device;”

Zaid discloses communications circuitry including a wireless device communication interface 202 in the vehicle access kit which is interfaced with the microprocessor 224 and memory 226.

Zaid discloses that the “microprocessor 224 unit (MPU) [is] connected to [interfaced with] the vehicle bus adapter and the short-range wireless link [the communications interface 202].” *Zaid*, ¶[0100].

The communication interface 202 is programmable to (1) communicate with the server of the cloud system and (2) communicate with a mobile device. The communication interface 202 communicates with the “central server [] sitting on [the] data network” (the server of the cloud system) and a “wireless communication device” (a mobile device). *Zaid*, ¶¶[0076], [0099], [0125]-[0126], [0130]. The communications interface 202 receives a vehicle reservation from a

central server. *Id.*, ¶¶[0126]-[0128] (“a central 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.”). The communications interface 202 also “includes a short-range wireless interface (e.g., Bluetooth and/or WiFi) for two-way communication” with the wireless communication device. *Id.*, ¶[0087]. The communications interface 202 is programmed with the pairing or network details to connect, illustrating that it is *programmable*. Almeroth, ¶[0101].

Zaid’s central server communicates the reservation over a “network” illustrated as a cloud system in Fig.1. *Id.*, ¶[0126]. Further, *Zaid* explains that the invention can be implemented as a “computer program product embodied on a computer readable storage medium.” *Id.*, ¶[0013]. Therefore, communication interface 202 contains communications circuitry programmable to communicate with the server of a cloud system (e.g., the “network”) and communicate with a mobile device (e.g., wireless communication device 106). Almeroth, ¶[0102].

As additional examples of communication between vehicle and mobile device, the communication device 202 receives commands communicated from mobile device to vehicle (*Id.*, ¶[0124]) and sends symmetric keys from vehicle to mobile device (*Id.*, ¶[0129]).

Although not required, the communication interface 202 also can communicate *directly* between vehicle and cloud server, without a mobile device. *See, e.g., id.*, ¶[0106] (“the vehicle access kit additionally includes a long-range mobile communication radio . . . for wireless communication to a vehicle reservation or sharing system [the server].”). A POSITA would have understood that the vehicle access kit’s long-range cellular radio can enable communications with the server for communicating vehicle reservations, vehicle usage data, or security keys through server updates. Almeroth, ¶[0104] (citing *Zaid*, ¶¶[0081] (“new private key” via server update), [0095], [0099] (“vehicle usage data” sent to central server), [0130] (“access control information” sent to and from server), claim 20). As Dr. Almeroth explains, “[i]ncorporating cellular radios into vehicles for communication with cloud services was well known in the art by at least October 2002, as evidenced by Ex. 1018. A [POSITA] would have interpreted *Zaid*’s disclosures of an in-vehicle cellular radio and server-vehicle communication in view of this knowledge.” Almeroth, ¶[0104] (citing Ex. 1018).

To the extent Patent Owner argues the claim requires direct communication between vehicle and server² and/or that *Zaid*’s disclosures of vehicle-mobile device and vehicle-server communications are provided in different embodiments (which

² Such a limitation is not required by the plain language of the claim.

Petitioner disputes), it would have been obvious to a POSITA to combine these embodiments to provide direct communication. Almeroth, ¶[0105] (citing Ex. 1018, 11 discussing vehicles equipped with “both WAN and WLAN technologies”). Specifically, it would have been obvious to a POSITA in 2013 to combine *Zaid*’s method of communicating the reservation to the vehicle via the wireless communication device with *Zaid*’s method of updating the private key at the vehicle via an update transmitted from the server *directly* to the vehicle. In this arrangement, the short-range wireless link and the long-range mobile communication radio together constitute the claimed communications circuitry. This provides multiple pathways for vehicle communication, resulting in added reliability and redundancy, improving user experience. Reliability is improved since direct-to-server communication does not require the user’s mobile device, avoiding power or service interruptions from the mobile device. Reliability and redundancy were important design considerations for a vehicle-based system since vehicles access different connectivity levels based on their location. Also, as *Zaid* notes, “cellular and satellite communication service fees can be expensive,” *Zaid*, ¶[0016], so by including both direct-to-server communications alongside communications via the user’s separately-paid-for mobile device, the vehicle designer optimizes connectivity while minimizing cost. A POSITA would have had a reasonable expectation of success in the combination given that, as the ’026

patent acknowledges, communications between a vehicle and a server, whether or not using an intervening mobile device were well established and common place by 2013. *See* '026 Patent, 2:2-4, *Zaid* ¶[0106], Almeroth, ¶[0106]. As Dr.

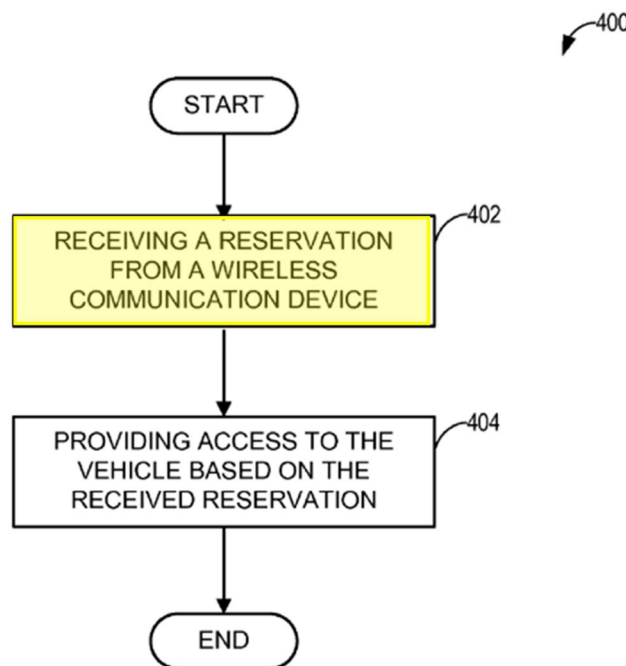
Almeroth explains, “a [POSITA] at the relevant time would have easily combined *Zaid*’s server update method with *Zaid*’s method of conveying a reservation to the vehicle via the wireless communication device.” Almeroth, ¶ [0105] (citing *Zaid*, ¶[0130]). In such a combination, the server would maintain control over the reservation authentication process and has added flexibility to use the wireless communication device to route data to the vehicle. Almeroth, ¶ [0106].

“Accordingly, a [POSITA] at the relevant time would have been motivated to make this combination to improve communication reliability with the vehicle rental system.” *Id.* *Zaid* is also analogous art to the '026 patent at least it is from the same field of endeavor, e.g., providing an electronic key system. *Compare Zaid* [Title] (“Vehicle Access Control Services and Platform”), ¶ [0090] *with* '026 Patent, Abstract (“A vehicle configured to communicate with a server of a cloud system to enable access to use the vehicle via one or more electronic keys is provided.”).

Accordingly, *Zaid* discloses or renders obvious this limitation of claim 1. Almeroth, ¶[0107].

1[e]: “wherein the communications circuitry of the vehicle is configured to receive a request from the mobile device for unlocking of the vehicle,

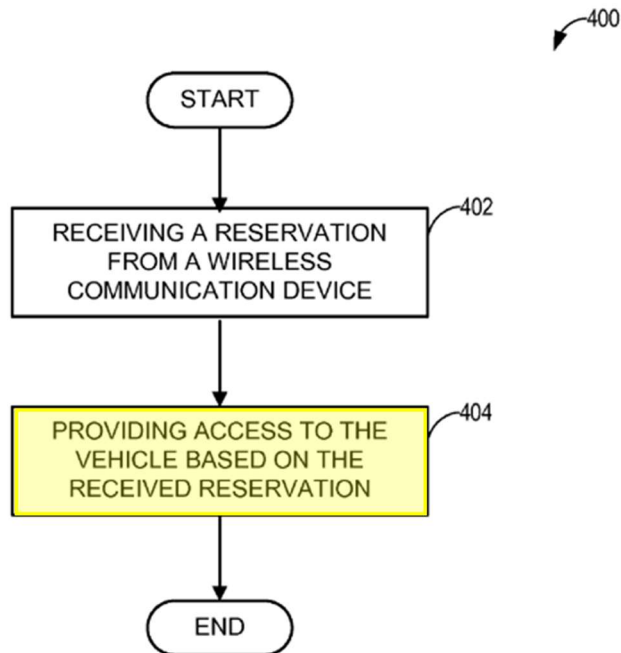
Zaid’s vehicle access kit via its wireless device communication interface 202 receives unlocking requests. These requests are referred to as “vehicle reservations,” which are sent from the user’s “wireless communication device,” the claimed “mobile device,” and provide vehicle access. *Zaid*, ¶¶[0067] (“access to the vehicle is provided when a vehicle reservation is received from the wireless communication device”), [0124], Fig.4 (reproduced below), Fig.6.



Zaid, Fig.4 (annotated).

Zaid’s vehicle reservation includes a time period when a user is authorized to unlock a vehicle. During this time period, the user is granted access to the vehicle by unlocking. *See id.*, ¶[0069] (“the vehicle reservation includes a

reservation for a specified time period.”); *see also id.*, ¶¶[0124], [0129] (“granting access includes opening the vehicle door”), *see also id.*, [0090] (“a vehicle access control component 206 [] provides access to the vehicle by for example unlocking the vehicle door”), Fig.4 (reproduced below), Fig.6.



Zaid, Fig.4 (annotated).

Therefore, *Zaid*’s communications circuitry receives requests from the mobile device for unlocking of the vehicle.

Accordingly, *Zaid* discloses this limitation of claim 1. Almeroth, ¶[0111].

1[f]: the request from the mobile device including a unique access code obtained by the mobile device from the server to enable sending the request to the vehicle,”

Zaid's "vehicle reservation" is a request from the mobile device. *Id.* The vehicle reservation can include "a unique increment." *Zaid*, ¶¶[0081], [0130], claims 21-22. Like the "unique access code" in the '026 patent, disclosed in one embodiment as including an "incremental number" generated by a "incremental number generator" at the server, '026 Patent, 45:53-54, the unique increment in *Zaid* is a unique access code obtained by the mobile device from the server to enable sending the request to the vehicle. *Id.*, Almeroth, ¶[0112].

As described in limitations 1[d] and 1[e] above, the vehicle reservation and its associated unique increment is sent from the server to the wireless communication device and onwards to the vehicle. *Zaid*, ¶¶[0080] ("The vehicle reservation is booked at the server[.]"), [0126] ("a central server . . . communicates the vehicle reservation to a wireless communication device"), [0128] ("the reservation is forwarded from the wireless communication device to the vehicle access kit"). Upon receipt and decryption, vehicle access is granted. *See id.*, ¶[0129]. Thus, the request from the mobile device includes a unique access code obtained from the server to enable sending the access request to the vehicle.

Zaid's encrypted vehicle reservation also meets this limitation. Specifically, *Zaid* discloses an encrypted vehicle reservation having a unique increment, which is sent to the wireless communication device to enable access to the vehicle. *Zaid*, ¶¶[0125] ("the vehicle reservation is encrypted."), [0126] ("the vehicle reservation

is communicated to a wireless communication device of the user.”), [0130] (“each message for exchanging information such as a vehicle reservation and updates includes a unique increment.”). A POSITA at the relevant time would have recognized that *encryption* of the vehicle reservation would result in the creation of a unique code representing the vehicle reservation data. Almeroth, ¶[0116] (citing *Zaid*, ¶¶[0065-66]). As Dr. Almeroth explains, “[i]t would have been well known to a [POSITA] that commonplace encryption methods involve converting a plain message, via a cypher or encryption algorithm, into a ‘secret code’ that can be decrypted and read by a recipient. *See* Ex. 1019 (pincites omitted). A POSITA would understand that the “secret code” is “unique” to the reservation request because the corresponding decryption algorithm must be able to decrypt the secret code to its original form. *Id.* With this understanding, a [POSITA] would have viewed encryption as a process for generating a unique access code.” Almeroth, ¶¶[0115]-[0116] (citing Ex. 1019). *Zaid*’s encrypted vehicle reservation provides vehicle access. *Zaid*, ¶[0129] (“At 602, vehicle reservation is received from a wireless communication device. In various embodiments, the 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 squarely within the ’026 Patent’s description. *See* ’026 Patent, 45:51-55 (“The unique access code can be

generated by . . . any other generation device that can generate codes that are unique or substantially unique.”), 45:56 (“the access code is encrypted”), 46:26-29 (“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 this limitation of claim 1. Almeroth, ¶[0118].

1[g]: “wherein the unique access code is associated with privileges for use of the vehicle, the privileges are defined for the unique access code,”

Zaid’s unique access code is associated with privileges to (1) access the vehicle for a period of time (unlock the vehicle doors) and (2) use the vehicle for a period of time (start the vehicle). *Zaid*, ¶¶[0069] (“the vehicle reservation ***includes a reservation for a specified time period.***”), [0131] (“the vehicle reservation becomes invalid at the end of the vehicle reservation period”), Fig.6, claims 2, 3, 18, 42. *Zaid* explains that vehicle access and use may be provided for the time period by allowing for “unlocking [of] the vehicle door and/or allowing for starting of the vehicle engine.” *Id.*, ¶[0090]. Reserving a different vehicle for a different time would cause a vehicle reservation with a different unique access code, corresponding to different privileges for (1) vehicle access for a period of time and (2) use for a period of time, to be transmitted to the vehicle. *Id.*, ¶[0069] (“In various embodiments, ***the vehicle reservation includes a reservation time slot and vehicle identifier*** identifying the vehicle.”); *see also id.*, ¶[0130] (emphasizing the

importance of “the **uniqueness** of [each vehicle reservation] message to avoid a repeat message attack”). Each encrypted vehicle reservation in *Zaid* has a unique access code associated with it, defining privileges to (1) access the vehicle for a specified time period and (2) use the vehicle for a specified time period. *Id.* (“each message for exchanging information **such as vehicle reservation** [comprising time-limited access and use privileges] and updates **include a unique increment** for each message to avoid repeat message attack. . . . the unique increment may . . . **indicate the uniqueness of the message**”); *see also* limitation 1[g] (encrypted vehicle reservation as unique access code). Therefore, the unique access code is associated with privileges of use for the vehicle, and the privileges are defined for the unique access code.

Zaid’s privileges of (1) “access” (unlocking doors) during the time period and (2) “use” (starting) during the time period align with the “privileges” described in the ’026 Patent. Specifically, the ’026 Patent explicitly states that “the privilege settings defin[e] **types of functional access** of the vehicle, **expiration data** for the access code” (’026 Patent, 7:15-17) and “the privilege settings include a time code **defining a length of during which the e-keys will remain active**” (’026 Patent, 7:32-34). *See also* 5:56-67 (“privileges (e.g., what type of access . . . amount of time the e-keys will be valid (or else expire)”), 10:31-33, 36:49-50, 48:37-40, claim 7.

Accordingly, *Zaid* discloses this limitation of claim 1. Almeroth, ¶[0121].

**1[h]: the vehicle is configured to receive information
from the server to authenticate the request by the
mobile device,**

Zaid's vehicle receives encryption/decryption information, namely a security key, from the server to authenticate requests from the mobile device. Specifically, the vehicle access kit receives a private key from the server, which is used by the vehicle access kit to decrypt and thereby authenticate the vehicle reservation. *Zaid*, ¶[0081] (“the vehicle access control system (e.g., vehicle access control component) is configured to receive a server update . . . [which] includes a new private key to the vehicle access control system.”). *Zaid* utilizes these private keys from the server explicitly to “authenticate” the reservation. *Id.*, ¶[0126] (“decryption is used to ensure and *authenticate* that the intended wireless communication device is receiving the vehicle reservation rather than one that intercepts the vehicle reservation”). Therefore, *Zaid* receives information from the server, an updated private key, to authenticate requests from a mobile device.

To the extent Patent Owner argues that the information must be received *directly* from the server, and not via an intervening wireless communication device (which Petitioner disputes), such a limitation is not required by the plain language of the claim. Moreover, even if *direct* receipt were required, it would have been obvious to a POSITA to modify *Zaid* such that the private key is transmitted

directly from server to vehicle. Almeroth, ¶[0123]. *Zaid* already discloses that “as a backup” the vehicle may “additionally include[] a long-range mobile communication radio/interface, such as GSM radio, for communication to a vehicle reservation or sharing system.” *Id.*, ¶[0106]. A POSITA would recognize that “wireless communication” would include transmitting the private key used for authentication directly from the server when data tethering was unavailable. Utilizing the mobile communication radio for direct receipt of authentication information would have had improved security by, for example, eliminating the risk of decryption key theft from the intervening wireless communication device. Almeroth, ¶[0124]. A POSITA would understand that the number of devices with access to a symmetric or private decryption key should be kept to a minimum. *Id.* To the extent this is considered an alternative embodiment, a POSITA would have had a reasonable expectation of success in utilizing the mobile communication radio for direct receipt of authentication information from the server, since the vehicle already could include a long-range communication device providing all necessary hardware to for direct server communication—and as explained above in limitation 1[d], it does in fact communicate directly with the server. *Zaid*, [0106]. Additional programming is all that would have been required to directly receive the communications. As Dr. Almeroth explains, “a [POSITA] at the relevant time would have easily configured *Zaid*’s server update to communicate directly with

the vehicle.” Almeroth, ¶[0127] (citing *Zaid*, ¶[0130]). This combination would allow the server to routinely update the vehicle’s private key and prevent bad actors from exploiting a key routed through mobile device. *Id.* Accordingly, a POSITA at the relevant time would have been motivated to make this combination to improve security of the vehicle rental system. Almeroth, ¶[0127] (citing *Zaid*, ¶[0130]).

Accordingly, *Zaid* discloses or renders obvious this limitation of claim 1. Almeroth, ¶[0128].

1[i]: and if the request is authentic, and³ the mobile device is provided with data to enable an electronic key to use the vehicle and the electronics of the vehicle instructs the subsystem of the vehicle to enable unlocking of the vehicle and enable starting of the vehicle for use of the vehicle via the electronic key consistent with the privileges of the unique access code.”

Zaid discloses that, if the vehicle reservation is authentic, the wireless communication device is provided with a symmetric key for unlocking and starting the vehicle, consistent with the time period of the reservation.

³ Applicant amended this claim limitation on July 19, 2019, by removing the “and” immediately preceding “the mobile device.” This amendment is not reflected in the issued claims, however. Regardless, *Zaid* discloses this limitation with or without the “and”.

First, *Zaid* discloses that the authenticity of the request is confirmed by decrypting using the private key of the vehicle, as described in limitation 1[h]. *Zaid*, ¶¶[0065-66], [0070], [0099], [0125-26], [0128], [0133], Fig.5, claims 10-13.

Second, if the request is authentic, the mobile device receives a symmetric key. *Id.*, ¶[0129] (“the vehicle access control system grants vehicle access by sending a symmetric key back to the wireless communication device”). The symmetric key is data provided to the mobile device to enable the mobile device with the vehicle reservation (an electronic key) to use the vehicle. *Id.* (“granting access includes opening the vehicle door, and/or allowing engine to be turned on by user”).

Third, use of the vehicle includes the microprocessor instructing the locking component of the ECU to enable unlocking, via the unlocking actuator, and instructing the engine starting component, via the starting actuator, of the vehicle access kit 200 to enable starting of the vehicle. *Id.*, ¶[0100] (“If authenticated, [the microprocessor 224] accepts commands (e.g., unlock doors, start engine, and/or other commands) from wireless communication device . . . and instructs the vehicle bus to actuate the corresponding car function.”). These commands from the mobile device illustrate unlocking and starting the vehicle via the enabled electronic key.

And fourth, use of the electronic key in *Zaid* is limited by the time period of the unique access code. When the time period expires, the privileges for access to and use of the vehicle are withdrawn and “the vehicle reservation becomes invalid.” *See Zaid*, ¶[0131]. Thus, use of the vehicle via the electronic key is consistent with the privileges of the unique access code.

Accordingly, *Zaid* discloses this limitation of claim 1. Almeroth, ¶[0134].

2. Claim 2

2[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,”

Zaid discloses that the communications interface 202 in the vehicle may receive additional vehicle reservations from other wireless communication devices. Almeroth, ¶[0135]. Specifically, *Zaid* discloses a vehicle *sharing* service where anyone can send requests from their mobile device to reserve a vehicle. *See, e.g., Zaid*, ¶¶[0077] (system permits “retrieving a list of nearby vehicles available for sharing”), [0016], [0095] (vehicle monitored “during *one or more reservations*”), [0134] (“*all the drivers* of a particular vehicle”), claim 34 (“one *or more* vehicle users”).

In this context, a POSITA would have understood that one or more users of the car sharing service would, using their respective wireless communication devices, book one or more vehicle reservations at the central server, which would

be transmitted to the communication interface 202 as discussed above in limitation 1[e]. Almeroth, ¶[0136].

Accordingly, *Zaid* discloses this additional limitation of claim 2. Almeroth, ¶[0137].

2[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 an administrator of the vehicle that enables assigning of electronic keys to use the vehicle.”

As discussed above for limitations 1[f] and 1[g], each vehicle reservation in *Zaid* is associated with a unique access code generated by the server and in turn is associated with privileges for vehicle access and use during a specific time period.

Zaid also discloses that each vehicle reservation is associated with a user account, which can have privileges assigned to it by a vehicle administrator to enable assigning electronic keys to the vehicle. Specifically, *Zaid* teaches that reservations can be “booked through one or more social networking websites, such as FourSquare® and Facebook®.” *Zaid*, ¶[0072]. On the social media sites, the user “*must first log into the social networking website*,” which connects the user to a user account and then requests a vehicle reservation. *Id.* *Zaid* tracks the “driving history” and “reputation” of the user, illustrating that the vehicle reservation and unique access code are associated with a user account. *Id.* The user tracking allows for 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 tracking of renter usage via the vehicle reservation, the vehicle reservation must be associated with the renter’s account. Almeroth, ¶[0139]. By providing a method for making reservations through a social media account, *Zaid* discloses a simple technique for associating the vehicle reservation and unique access code (whether unique increment or encrypted vehicle reservation) with a renter account. *Id.*

Finally, *Zaid* teaches that the vehicle owner or administrator assigns the privileges by defining the times that the system can assign electronic keys for the vehicle. *Zaid*, ¶[0077] (owner can “advertise or announce when the vehicle will be available for sharing. . .”). *Zaid*’s reservation system also “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 request sent by the owner would enable the requested duration for vehicle access and use. Almeroth, ¶[0140].

Accordingly, *Zaid* discloses this additional limitation of claim 2. Almeroth, ¶[0141].

3. Claim 3

“The vehicle of claim 2, wherein said vehicle is a shared vehicle.”

Zaid discloses that the vehicle can be a shared vehicle. *See, e.g., Zaid*,

¶[0016] (“Therefore, an improved way for providing *car sharing services* is needed.”), [0095] (“one *or more* reservations”), claim 34 (“one *or more* vehicle users”), [0069] (“the vehicle reservation includes a vehicle rental reservation.”), [0077] (“the vehicle will be available for sharing”).

Accordingly, *Zaid* discloses the additional limitations of claim 3. Almeroth, ¶[0143].

4. Claim 4

“The vehicle of claim 1, wherein said vehicle is identified as available for sharing and said vehicle is capable of being located based on a geographic location of the vehicle.”

Zaid’s vehicle can be advertised as available for sharing and is capable of being located based on its geographic location. Specifically, *Zaid* discloses an application on a mobile device for viewing which vehicles are available and where they are located. *Zaid*, ¶[0077] (“[T]he wireless communication device includes a vehicle reservation application or other software function (e.g., an iPhone or Droid 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*, . . . (c) *advertise or announce when the vehicle will be available for sharing*, . . . and/or (d) retrieving a list of nearby vehicles *available for sharing* . . .” As such, *Zaid* discloses that a user may

“retriev[e] a list of nearby vehicles available for sharing,” including the location of the vehicle. *Id.*

Accordingly, *Zaid* discloses the additional limitations of claim 4. Almeroth, ¶[0145].

5. Claim 5

“The vehicle of claim 1, wherein an application accessed by said mobile device is configured to enable finding a geo-location of said vehicle and enables requesting use of said vehicle.”

Zaid discloses a vehicle reservation application on the mobile device can be used to locate and request use of a shared vehicle.

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

Second, the user can request use of the vehicle via 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. . . . In various

embodiments, the computing device is *the same wireless communication device the reservation is sent to.*”).

It would have been obvious to a POSITA at the relevant time to implement *Zaid*’s vehicle reservation application in a manner that enables both geolocation (*Id.*, ¶[0077]) and requesting use of the vehicle (*Id.*, ¶[0125]) such that users only need to install one application. Almeroth, ¶[0149], [0150] (citing Ex. 1025, 2). This would have been nothing more than an obvious design choice that simplifies the user experience and would have been desirable to minimize user downloads and user confusion and maximize ease of use by providing the ability to locate and reserve a vehicle in a single application. A POSITA would have had a reasonable expectation of success in doing so since the ability to locate and the ability to reserve are already provided for in *Zaid* as functionalities available via the mobile device; combining such functionalities into one application would not have changed how they are programmed or operated. Almeroth, ¶[0151]. As Dr. Almeroth explains, “a [POSITA] at the relevant time would have easily implemented *Zaid*’s application for ‘advertis[ing] or announc[ing] the location of the vehicle’ such that the prospective renter may ‘retriev[e] a list of nearby vehicles available for sharing’ with the functionality of *Zaid*’s application for requesting use of a vehicle.” *Id.* A POSITA at the relevant time would have been

motivated to make this combination to simplify access to the shared vehicles.

Almeroth, ¶[0149] (citing *Zaid*, ¶¶[0077], [0125]).

Accordingly, *Zaid* discloses or renders obvious the additional limitations of claim 5. Almeroth, ¶[0152].

6. Claim 6

6[a]: “The vehicle of claim 1, wherein an application accessed by said mobile device is configured to enable sending instructions to said server to share the vehicle with a user to enable use of the electronic key on said vehicle,”

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. Specifically, 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 of the vehicle via an electronic key. *Id.*, ¶[0080].

Accordingly, *Zaid* discloses this limitation of claim 6. Almeroth, ¶[0154].

6[b]: “wherein the electronic key has functions enabled via graphical user interfaces of the application of the mobile device.”

Zaid's vehicle reservation application includes "user interfaces" for booking a vehicle reservation. *Zaid*, ¶¶[0072], [0080], [0125]. *Zaid* discloses that the reservation is booked "at the server 110 via a user interface 116 displayed on a computing device 118," and *Zaid* also discloses that "[i]n various embodiments, the computing device 118 is the same wireless computing device 108 used by a user to access the vehicle [the user's mobile device]." *Id.*, ¶[0080]. *Zaid* discloses that mobile device generally includes "a rich visual interface" ¶[0026], which provides the graphical user interfaces for booking vehicle reservations via "social networking websites, such as FourSquare® and Facebook®" ¶[0072], each a graphical user interface. Thus, *Zaid* discloses user interfaces on the mobile device that enable the electronic key functionality.

Zaid further discloses that the electronic key can unlock the vehicle via commands sent from the mobile device. *Id.*, ¶[0124] ("[O]nce vehicle access is provided, the user can send commands from the wireless communication device to . . . open the vehicle door, turn on the engine, and/or otherwise allow the user to use the vehicle."). A POSITA would have understood that, by providing the user with the ability to reserve the vehicle with an app and send commands from the wireless communication device, *Zaid* teaches enabling functionality in the vehicle reservation application to use the ekey once vehicle access is granted. Almeroth,

¶[0156]. Therefore, *Zaid* discloses that graphical user interfaces of an application on the mobile device are used to enable functions of the electronic key.

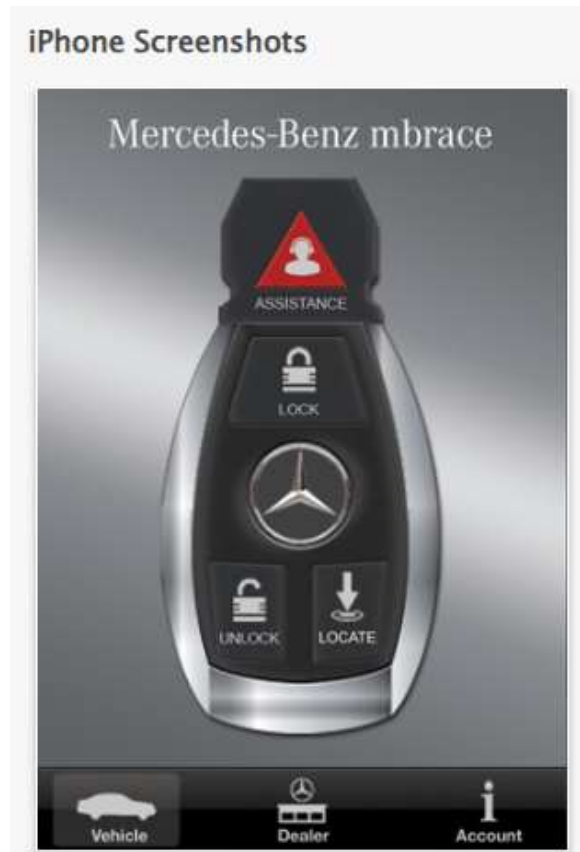
To the extent Patent Owner argues that *Zaid* does not explicitly disclose that user interfaces displayed on the user's mobile device via the vehicle reservation application are "graphical" (which Petitioner disputes), it would have been obvious to a POSITA at the relevant time to implement *Zaid*'s user interfaces graphically.

Almeroth, ¶[0158]. A POSITA would have had a reasonable expectation of success in doing so since mobile device applications with graphical user interfaces and keyless entry systems were well known by 2013. *See Zaid*, ¶¶[0026], [0051].

Providing access to the electronic key via a *graphical* user interface, as opposed to any other interface, would require no more than a typical smart phone application coupled to existing keyless entry technologies. Almeroth, ¶[0157]. As Dr.

Almeroth explains, "a [POSITA] at the relevant time would have interpreted *Zaid*'s vehicle reservation application such that the application incorporates graphical windows for controlling functions of the vehicle, rather than using a command line interface or otherwise." *Id.* A POSITA in 2013 would have been well aware of graphical mobile application design and development propagated by Apple and Google as early as 2007. *Id.* Indeed, some of the earliest mobile device applications concerned graphical user interfaces for making reservations, as evidenced by Ex. 1020. Further, applications for graphically enabling electronic

key functions on mobile devices were well established, such as the Mercedes mbrace app, as evidenced by Ex. 1026, which shows a graphical user interface on an iPhone for unlocking a vehicle via an electronic key.



Ex. 1026 at 2.

Accordingly, *Zaid* discloses or renders obvious this additional limitation of claim 6. Almeroth, ¶[0159].

7. Claim 7

“The vehicle of claim 1, wherein said privileges associated with the unique access code define a period of time for use of said vehicle.”

Zaid discloses privileges to (1) access the vehicle during a “specified time period” and (2) use the vehicle during a “specified time period.” These privileges are defined by the vehicle reservation and thus associated with *Zaid*’s unique increment in the encrypted vehicle reservation. *Zaid*, ¶¶[0069] (“the vehicle reservation includes *a reservation for a specified time period. . .*”), ¶[0129], ¶[0131], Fig.6, claims 2, 3, 18, 42.

Accordingly, *Zaid* discloses the additional limitations of claim 7. Almeroth, ¶[0161].

8. Claim 11

“The vehicle of claim 1, wherein said privileges associated with the unique access code define constraints for use of the vehicle, and said constraints include one or more of geographic restrictions, age restrictions, time of day restrictions, speed restrictions, or combinations thereof.”

Zaid discloses privileges to (1) access the vehicle during a specified time period and (2) use the vehicle during a specified time period. These privileges define constraints for use of the vehicle in the form of the “specified time period” of *Zaid*’s vehicle reservation, which is associated with the unique increment in the encrypted vehicle reservation. *Zaid*, ¶[0069].

To the extent it is argued that the specified time period is not a time of day restriction, it would have been obvious to a POSITA at the relevant time to configure *Zaid*’s vehicle reservation time period such that the privileges to access

and use the vehicle during a specified time period are only available during daylight hours, a “time of day,” or to only particular ages of drivers. Almeroth, ¶[0163]. A POSITA at the relevant time could have easily implemented *Zaid*’s vehicle reservation system such that a user may reserve the vehicle for not only a limited amount of time, but also only from, for example, sunrise to sunset, a “time of day restriction.” Alternatively or additionally, it would have been a simple modification for *Zaid*’s application to include age restrictions so only drivers over the age of, for example, 21 or 25 may reserve vehicles. These are common rental car requirements and would have been obvious to anyone implementing a vehicle reservation system and any implementer would have had a reasonable expectation of success in their implementation. *See* Ex. 1035. A POSITA at the relevant time would have been motivated to implement these limitations given that they are typical rental restrictions. Almeroth, ¶¶[0169] (citing Exs. 1015-17), [0170].

Accordingly, *Zaid* discloses or renders obvious the additional limitations of claim 11. Almeroth, ¶[0166].

9. Claim 12

“The vehicle of claim 1, wherein an application of the mobile device provides graphical user interfaces for use of the electronic key, and the application includes a reservation function for said vehicle.”

Claim 12 is very similar to claim 6, but further requires the application to include a reservation function. *Zaid*’s vehicle reservation application includes a

reservation function. *Zaid*, ¶¶[0077] (“the wireless communication device includes ***a vehicle reservation application***”), [0125].

As described for limitation 6b, the user may also send commands with the electronic key (to “unlock doors, start engine”) via the wireless communication device and its reservation application. *Id.*, ¶¶[0100], [0124], [0129].

To the extent that Patent Owner argues that *Zaid* does not explicitly disclose that the method for sending commands for use of the electronic key is implemented using “graphical user interfaces” (which Petitioner disputes), it would have been obvious to a POSITA at the relevant time to implement graphical user interfaces for the reasons discussed above in limitation 6[b].

Accordingly, *Zaid* discloses or renders obvious the additional limitations of claim 12. Almeroth, ¶[0170].

10. Claim 14

“The vehicle of claim 1, wherein the electronics include decryption logic for decrypting data associated with the unique access code.”

Zaid’s microprocessor decrypts the received vehicle reservation “to verify [its] authenticity.” *Zaid*, ¶[0128]. *Zaid* discloses that the microprocessor “includes proprietary firmware code [logic] that enables the system to authenticate nearby mobile handsets. . . [and i]f authenticated, it accepts commands, (e.g., unlock doors, start engine and/or other commands)[.]” *Id.*, ¶[0100]. Memory 226 stores

“various instructions, codes, and data information” including “a locally stored private key” which is used in decryption. *Id.*, ¶[0101]. The proprietary firmware code stored in memory 226 that enables authentication is the decryption logic for decrypting data associated with the unique access code such as commands to unlock or start the vehicle in the limited time period. The electronics may also be considered to include the reservation authentication unit 216 which is also provided with the vehicle access kit 200 and may provide cryptography functionality. *See Zaid*, Fig.2, ¶[0096].

The vehicle reservation is decrypted with the data such as the vehicle identifier, time of use, and mobile device identification that is associated with the unique access code. *Id.*, ¶[0069].

Accordingly, *Zaid* discloses the additional limitations of claim 14. Almeroth, ¶[0173].

11. Claim 18

“The vehicle of claim 1, wherein the mobile device is one of a smartphone, or a smartwatch, or smart glasses, or a computer, or a digital assistant.”

Zaid discloses that the wireless communication device can be “any suitable wireless communication device that supports long-range wireless connectivity. . . . Examples of which include a *smart phone*[.]” *Zaid*, ¶[0073].

Accordingly, *Zaid* discloses this additional limitation of claim 18. Almeroth, ¶[0175].

12. Claim 19

“The vehicle of claim 1, wherein the access code for use of the vehicle is generated in response to a request to generate the electronic key for the mobile device, the mobile device being identified using information that includes one or more of an email address, a phone number, a text number, a message address, a notification, a link, a web address, a social network address, or a combination of two or more thereof.”

Zaid discloses that the access code for using the vehicle is generated in response to a request to generate the electronic key for the mobile device. Specifically, *Zaid*’s user utilizes the vehicle reservation application to request issuance of an encrypted vehicle reservation and associated unique increment, which are provided to the mobile device to enable the ability to access and use the vehicle. *Zaid*, ¶¶[0077], ¶[0081].

Zaid also discloses users logging in to social networking websites before making a reservation, and using this log in as a tracking mechanism to determine which users are using the shared vehicle. *Zaid*, ¶[0072]. As such, the mobile device making the request is identified to the server using the user’s social network address or an email address. As Dr. Almeroth explains, “a [POSITA] at the relevant time would have been familiar with Facebook Login. It was well known that Facebook Login provides connected applications with identification of the

Facebook user, including the user ID (i.e., a social network address) and, in some cases, the user's email address." Almeroth, ¶[0177] (citing Exs. 1022, 1023, 1024).

As another example, *Zaid* discloses that the "identity of the wireless communication device is used to identify the driver . . ." *Zaid*, ¶[0134]. A POSITA would have appreciated that the identity of the wireless communication device would include information such as a phone number or email address. Almeroth, ¶[0178] (citing *id.*, ¶[0026]).

Accordingly, *Zaid* discloses the additional limitations of claim 19. Almeroth, ¶[0179].

13. Claim 20

"The vehicle of claim 1, wherein the privileges defines one of a geographic restriction for where the vehicle is allowed to be used, or a speed restriction, or an occupancy restriction, or a time frame of use restriction, or a time of day use restriction, or a time expiration of use restriction, or a combination of two or more thereof."

Zaid discloses privileges to (1) access and (2) use the vehicle during a time period. *Zaid*, ¶[0069]. These are "time frame of use" and "time expiration of use" restrictions.

Accordingly, *Zaid* discloses the additional limitations of claim 20. Almeroth, ¶[0181].

B. Ground 2: Zaid in view of Patenaude renders obvious claim 10

The obvious combination of *Zaid* and *Patenaude* teaches all limitations of claim 10, rendering the claim obvious.

Patenaude discloses monitoring entertainment selections at a telematics unit, determining a user entertainment selection profile based on monitoring, and automatically activating entertainment units based on monitoring. Ex. 1007 (*Patenaude*), Abstract. *Patenaude* endeavors to “determine and predict entertainment selections,” in particular, by learning a user’s preferences and developing an “entertainment selection profile” for that user which can be stored remotely via a vehicle telematics unit. *Id.*, ¶¶[0001], [0024].

Patenaude is analogous art to the ’026 because its disclosures are pertinent to the particular problem faced by the ’026 patent inventor (utilizing remote connectivity to provide added functionality and improve user experience). Almeroth, ¶¶[0186]-[0189]. For example, *Patenaude* describes efforts to overcome limitations in prior systems that could not utilize telematics to provide enhanced experiences via predicted entertainment selections. *Patenaude*, ¶¶ [0002]-[0005]. Similar efforts are described throughout the ’026 Patent. *See, e.g.*, 2:2-5, 5:56-67, 9:56-60. Further, the ’026 patent describes sharing access to a vehicle via remote communication and managing profiles of information related to users. *See, e.g.*, ’026 Patent 16:57-17:2. *Patenaude* describes utilizing the same remote

communication functionality and user profiles for providing entertainment recommendations. *Patenaude*, ¶¶[0005]-[0006].

It would have been obvious to combine *Zaid* with *Patenaude*, disclosing claim 10.

1. Claim 10

10[preamble]: “The vehicle of claim 1, further comprising,”

10[a]: “the electronics receiving interface input data during use of the vehicle by a user via the electronic key,”

Zaid discloses that the microprocessor and memory receive data from vehicle sensors during the vehicle use. *Zaid*, ¶¶[0101] (memory for storing “data information”), ¶[0123] (vehicle access kit, including processor and memory, receives vehicle sensor data from ECU and actuators). A POSITA at the relevant time would have understood that microprocessor and memory (the “electronics”) receive data whenever the vehicle is operating, including during use by a user via electronic key, as in Ground 1. *Almeroth*, ¶[0185]. *See also* Ground 1, Claim 1.

Patenaude describes a “telematics unit 120” that communicates with “entertainment units 135, 136 and 137” such that “data is transmitted . . . to the telematics unit 120” “upon power-up of the entertainment units 135, 136 and 137.” *Patenaude*, ¶¶[0038], [0042]-[0043]. *Patenaude*’s “data” includes “an entertainment unit factor” which is *interface* input data. *Id.* Specifically, the “entertainment unit

factor” includes radio inputs. *Id.*, ¶[0052]. *Patenaude* discloses a processor 122 and memory 128 in telematics unit 120, analogous to *Zaid*’s microprocessor 224 and memory 226 electronics within access kit 200. Memory 128 receives “entertainment unit factors and selection time factors[.]” *Id.*, ¶[0055].

It would have been obvious to a POSITA at the relevant time to combine the receipt of interface input data, as in *Patenaude*, with *Zaid*’s vehicle, such that *Zaid*’s electronics receive “entertainment unit factor[s]” (interface input data) from entertainment units 135, 136 and 137. A POSITA at the relevant time would have been motivated to make this combination to provide additional functionality to *Zaid*’s vehicle sharing service.

Accordingly, *Zaid* and *Patenaude* render obvious claim 10. Almeroth, ¶[0191].

10[b]: “the interface input data being examined to determine learned patterns, the learned patterns used to identify recommendations for settings of the vehicle during the use or future uses of the vehicle or other vehicles.”

Patenaude discloses examining user entertainment inputs (interface input data) and identifying patterns based on use history. *Patenaude* discloses generating recommendations for settings during vehicle use. Almeroth, ¶[0192].

Based on “entertainment unit factors” and “selection time factors,” *Patenaude*’s telematics unit “determines patterns in the entertainment selections”.

Patenaude, ¶[0055]. “After a minimum number of entertainment unit factors and selection time factors are stored in the in-vehicle memory 128, the processor 122 applies an algorithm on the stored entertainment unit factors and selection time factors.” *Id.* This algorithm automatically configures desired entertainment settings. *Id.*, ¶[0073]. Specifically, “the telematics unit 120 powers-up at least one entertainment unit 135, 136, or 137 based on the retrieved user-specific entertainment selection profile.” *Id.*, ¶[0074].

It would have been obvious to a POSITA at the relevant time to combine *Patenaude* with *Zaid*’s vehicle, such that *Zaid*’s electronics and communications circuitry perform *Patenaude*’s pattern learning and setting recommendations. Specifically, *Patenaude*’s telematics unit functions could easily be performed with *Zaid*’s electronics and communications circuitry. Incorporating pattern learning system to make recommendations based on inputs would have been an obvious functionality to incorporate into a system for sharing vehicles since users may not know how to utilize a new vehicle interface and/or their favorites may not be stored. A system that learns preferred settings such as *Patenaude* recommends those settings automatically to *Zaid*’s shared vehicle users. Almeroth, ¶[0194]. As Dr. Almeroth explains, “[t]he functions of *Patenaude*’s telematics unit could easily be performed on *Zaid*’s electronics and communications circuitry. The only

modification would need to be done in software such that *Zaid*'s a user is provided suggestions based on past vehicle use stored in their profile.” Almeroth, ¶[0196].

A POSITA at the relevant time would have been motivated to make this combination to provide additional functionality to *Zaid*'s vehicle. Almeroth, ¶[0195] (citing Ex. 1018, 13). For example, *Zaid* recognizes “allow[ing] media providers to stream music to the car via the vehicle access kit.” *Zaid*, ¶[0118]. Implementing *Patenaude*'s learning and suggesting entertainment selections with *Zaid*'s vehicle would be a natural design choice since *Zaid*'s shared vehicle users may be unfamiliar with the interface and/or not have their favorites stored and could benefit from automatic suggestions. A POSITA would have had a reasonable expectation of success in the combination since *Zaid*'s shared vehicle already includes necessary hardware for *Patenaude*'s entertainment suggestion system, e.g., wireless communication, processor and memory, centralized server, music streaming functionality, and vehicle audio components. Almeroth, ¶[0196] (citing *Zaid*, ¶[0085]).

Accordingly, *Zaid* and *Patenaude* render obvious this additional limitation of claim 10. Almeroth, ¶[0197].

C. Ground 3: *Zaid* in view of Gilbertson renders obvious claim 13

Zaid discloses sending data to a server during use of a vehicle including, for example, acceleration data, as described below regarding limitation 13[a]. *Zaid*

also discloses time-limited reservations expiring. As described below regarding limitation 13[b], the obvious combination of *Zaid* with *Gilbertson* (Ex. 1008) provides a system for receiving requests from a server to *cancel* the electronic key, teaching all the limitations of claim 13 and rendering the claim obvious.

Gilbertson discloses “electronically controlling access” to a locked receptacle using an “electronic key” comprising an “internal code needed to open the lock.” *Gilbertson*, claim 1. Relevant to element 13[b], *Gilbertson* explains that “administrators designated by the supplier can add and **deactivate** keys from the software of the invention.” *Id.*, ¶[0064]. *Zaid* and *Gilbertson* are both analogous art to the ’026 patent at least because each is from the same field of endeavor, namely, electronic key systems. Almeroth, ¶[0207]. *Gilbertson* also discloses time-limited electronic keys for access control which are functionally similar to the electronic key disclosed in *Zaid*, at least to the extent there would have been a need to deactivate access remotely. *Gilbertson*, ¶[0033]; *Zaid*, ¶[0131].

As described below, it would have been obvious to combine *Zaid* with *Gilbertson*, which discloses the limitations of claim 13.

1. Claim 13

13[a]: “The vehicle of claim 1, wherein the vehicle sends data to the server during the use of the electronic key on the vehicle, the data including at least use metrics of the vehicle, the use metrics being stored by the server as history of use for the electronic key;”

Zaid discloses that the “vehicle access kit” sends “usage data” to the “central server” during the “vehicle reservation.” *Zaid*, ¶¶[0099] (“the vehicle access kit includes *vehicle usage data reporting unit* 222 configured *to report and communicate back to a central server. . . .*”); [0095] (“the vehicle access kit 200 further includes an accelerometer 214 *for monitoring acceleration of the vehicle during one or more reservations to provide vehicle usage data.*”).

Zaid further discloses that the “usage data” is stored to establish “member driving history and reputation” to allow the vehicle owner to “have better control over the type of user the owner is lending/sharing/renting vehicle to.” *Id.*, ¶[0072]. A POSITA would have understood that *Zaid*’s “member driving history” is compiled at the server by storing “use metrics” (e.g., acceleration data) during specific “reservations” (uses of the claimed “electronic key”). Almeroth, ¶[0202] (citing *Zaid*, ¶[0099]).

Accordingly, *Zaid* discloses this additional limitation of claim 13. Almeroth, ¶[0203].

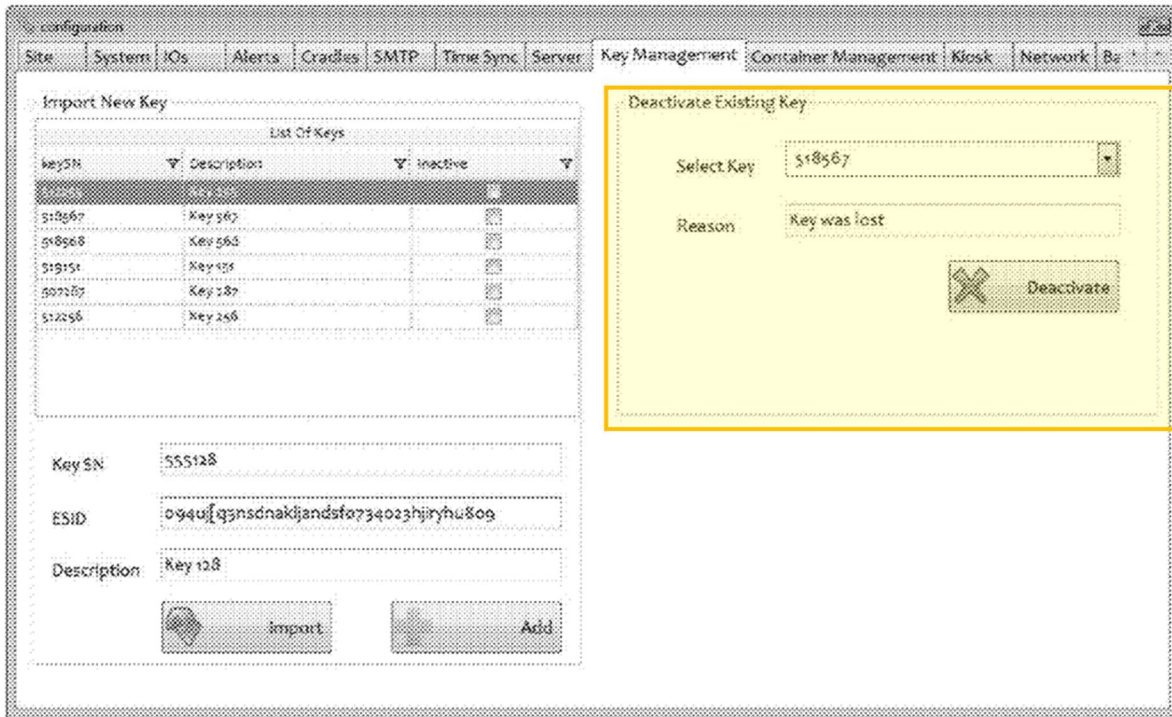
13[b]: “wherein vehicle, after receiving from the server a request to cancel the electronic key, the vehicle receives deactivation instructions to one or both of the mobile device and the vehicle.”

Zaid discloses that vehicle reservations expire after the period of time, at which point a reservation “becomes invalid” and access is “withdrawn.” *Zaid*, ¶[0131], Fig.6.

A POSITA at the relevant time would have understood that requests from a server to cancel the electronic key would be a trivial addition to the system disclosed in *Zaid*. A cancel request would cause the central server to send deactivate instructions to the wireless communication device and the reserved vehicle to invalidate the reservation. Almeroth, ¶[0206].

By 2013, systems for *deactivation* of electronic keys were well known and found naturally alongside systems for remote *activation* of electronic keys. *Gilbertson* teaches “electronically controlling access” to a locked receptacle using an “electronic key” comprising an “internal code needed to open the lock.” *Gilbertson*, claim 1. *Gilbertson* explains that “administrators designated by the supplier can add and ***deactivate*** keys from the software of the invention.” *Id.*, ¶[0064].

Deactivation of *Gilbertson*’s “electronic keys” is accomplished via a deactivation request at a user interface on a computing device. *See id.*, Figs. ScreenShot AD, AE (below).



Gilbertson, ScreenShot AE (annotated).

It would have been obvious to combine *Gilbertson*'s deactivation function with *Zaid*'s application such that the owner/administrator of the vehicle is provided the ability to deactivate e-keys. Almeroth, ¶[0210] (citing *Zaid*, [0077]). Such a deactivation function would operate in the same manner as *Zaid*'s vehicle reservation function: “[t]he [*deactivation request*] is booked at the server 110 via a user interface 116 displayed on a computing device 118. The server may be configured to interact with a plurality of vehicle access control systems for [*deactivating*] access control to a plurality of vehicles.” *Zaid*, ¶[0080]. Using the deactivation request received at the vehicle via *Zaid*'s “tethering” or “GSM radio,” the vehicle would invalidate the vehicle reservation. *Id.*, ¶[0106]. In such a

configuration, “[a]t 506, the [*deactivation request*] is communicated to a wireless communication device of the user.” *Id.*, ¶[0126]. Using the deactivation request received at the wireless communication device, the wireless communication device would also invalidate the vehicle reservation. Almeroth, ¶[0210].

A POSITA at the relevant time would have been motivated to make this combination to provide the vehicle owner with additional control over the vehicle. As *Zaid* explains, the vehicle owner should be provided with “an increased level of vehicle security.” *Zaid*, ¶[0114]. A POSITA would naturally have looked to other references in the field of access control for methods to improve on *Zaid*’s security. *Gilbertson* explains that electronic keys can be deactivated, for example, if the “[k]ey was lost.” *Gilbertson*, Screen Shot AE. A POSITA would have understood that lost electronic keys (that is, lost devices comprising eKeys), provide an opportunity for malicious actors to access the vehicle without authorization by passing the electronic key off as their own. Deactivating lost keys, however, prevents such unauthorized access. Accordingly, a POSITA would have recognized that *Gilbertson*’s deactivating keys increases vehicle security, which *Zaid* notes is preferred. Almeroth, ¶[0211] (citing *Zaid*, ¶[0114]).

Since *Zaid* activates the electronic key, no additional hardware would have been required to implement deactivating the same. Accordingly, it would have

been obvious to modify *Zaid* to accommodate a request to cancel the electronic key, as in *Gilbertson*. Almeroth, ¶[0213].

A POSITA would have had a reasonable expectation of success in combining the deactivation feature of *Gilbertson* with the shared vehicle of *Zaid* since the feature is a minor addition, provided in software, to the hardware already provided in *Zaid*. Almeroth, ¶[0214]. A deactivation request would be analogous to a reservation request, except it would indicate that the privileges provided in the unique access code of the reservation should be terminated (e.g., by adjusting the specified time period of the reservation to none). To account for safety concerns, a POSITA would have understood that when combining *Gilbertson*'s deactivation feature of with *Zaid*'s vehicle, such deactivation should not occur while the vehicle is in motion or without appropriate warning to vehicle occupants. Almeroth, ¶[0212]. However, cancellation of the privileges would be a desirable and obvious feature to include, for example, to immobilize a vehicle that had been stolen or was being used in an impermissible or illegal manner. *Id.*

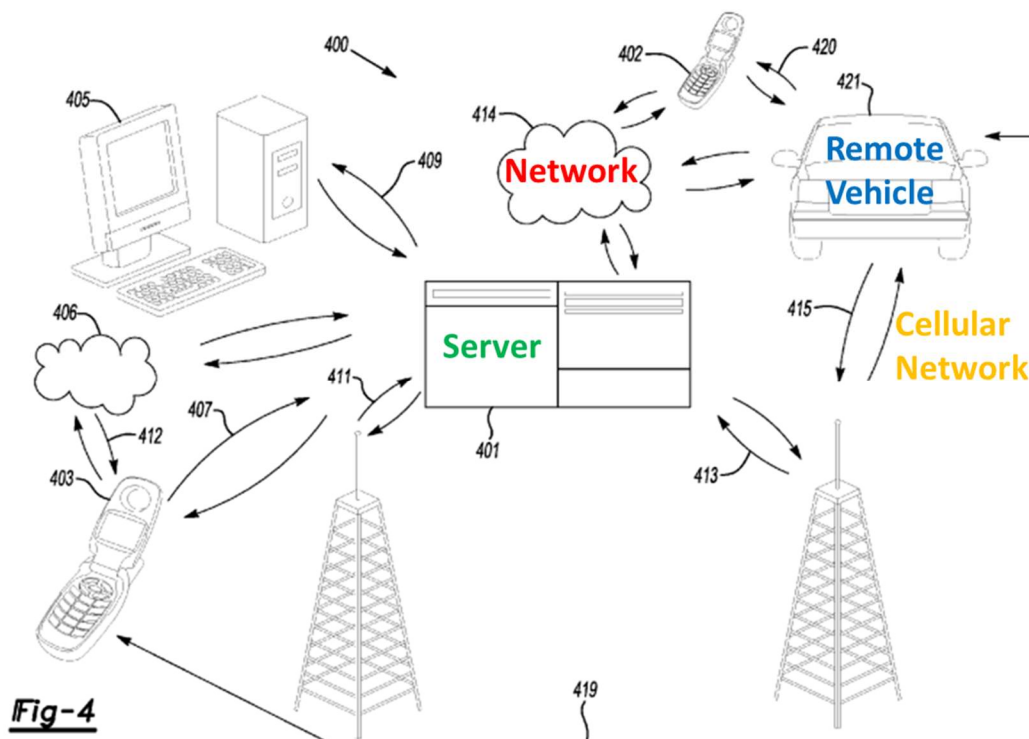
Accordingly, *Zaid* and *Gilbertson* render obvious this additional limitation of claim 13. Almeroth, ¶[0215].

D. Ground 4: *Zaid* in view of *Kleve* renders obvious claim 15

The obvious combination of *Zaid* and *Kleve* teaches all limitations of claim 15, rendering the claim obvious.

The use of in-vehicle displays for notifying a vehicle user to vehicle status and condition was well known in the art, as evidenced by, *e.g.*, *Kleve*. Indeed, *Kleve* discloses a vehicle comprising a “touchscreen visual display 4” which may display messages to “notify the Temporary User if a restriction limit has been exceeded.” *Kleve*, ¶¶[0023]-[0024], [0040], [0043], [0047], [0049], [0053].

Like *Zaid*, *Kleve* (Ex. 1006) also discloses in-vehicle wireless communication circuitry for bidirectional communications with a server. As illustrated in Figure 4, annotated below, *Kleve* discloses a “remote vehicle 421” in communication with a “server(s) 401” via “network 414” or “cellular network 415.” *Kleve*, ¶¶[0057], [0060].



Kleve, Fig.4 (annotated).

Kleve describes an “authorization solution for personal vehicle rental.” *Id.*, title; *compare Zaid*, title. Like *Zaid*, *Kleve* teaches that the communications illustrated above enable a rental system for “keyless drive-away” of a rented vehicle via a “virtual key.” *Kleve*, ¶¶[0036], [0039], [0064], [0065].

Zaid and *Kleve* are both analogous art to the claimed invention of the ’026 patent because the references are from the same field of endeavor as the claimed invention (electronic key systems); and/or (2) the references are reasonably pertinent to the problem faced by the inventor (utilizing remote connectivity to provide added functionality and improve user experience). *In re Bigio*, 381 F.3d 1320, 1325 (Fed. Cir. 2004). For example, *Zaid* describes “an improved way for providing car sharing services” utilizing a “wireless communication device” as an e-key for accessing a shared vehicle during a reservation period. *Zaid*, ¶¶[0016], [0067]. *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]. Both *Zaid* and *Kleve* recognize the benefit of implementing an e-key via a mobile device for conveying vehicle access to shared and rented vehicles. As described below, it would have been obvious to combine *Zaid* with *Kleve*, which discloses the limitations of claim 15.

1. Claim 15

“The vehicle of claim 1, wherein the vehicle sends data regarding use of the vehicle to the server, and the

vehicle receives instructions from the server regarding a violation of the privileges associated with the electronic key, the vehicle is configured to receive at least one notification for displaying or outputting an indication regarding the violation.”

As described in limitation 13[a], above, *Zaid* discloses sending data to a server during use of a vehicle including, for example, GPS and acceleration data. *See, e.g., Zaid*, ¶¶[0098], [0099], [0133]. *Zaid* explains that “vehicle usage data reporting unit 222 [is] configured to report and communicate back [usage data] to a central server” (*id.*, ¶[0099]) for “analy[sis] to generate driver driving profile and/or car driving profile” (*id.*, ¶[0134]).

Like *Zaid*, *Kleve* also discloses sending usage data to a server during use of a vehicle. Specifically, *Kleve* explains that “during the rental term the [vehicle computing system] may **monitor** the Temporary User's utilization of the vehicle including, but not limited to, renter verification, **driving behavior, vehicle location, speed, fuel level**, and other vehicle information requested by the vehicle owner.” *Kleve*, ¶[0073]. “The continuous monitoring of the Temporary Users behavior during the rental period may be **transmitted to the server**.” *Id.*, ¶[0076]; *see also id.* (“The GPS data may be transmitted to the server and monitored using the vehicle owner's nomadic device.”). *Kleve* further discloses privileges of vehicle speed, location, and weight. *See, e.g., id.*, ¶[0040]. *Kleve* teaches that the usage data is “monitor[ed]” to identify potential “violation[s]” of these privileges. *Id.*,

¶[0053]. Specifically, *Kleve* describes generating and distributing “virtual keys” for accessing a shared vehicle, wherein the “virtual keys” enable the shared vehicle to differentiate between drivers (“Owner” or “Temporary User”). *Id.*, ¶[0045]. *Kleve* explains that “Temporary Users” use of the shared vehicle may be subject to “restriction limits [privileges] initially set by the Owner at the beginning of the rental term.” *Id.*, ¶[0043]; *see also id.*, ¶[0040] (“The restrictions may be based on, but not limited to, the owner's selection of parameters including, but not limited to, ***speed, global position coordinates***, or load weight restrictions.”). During the rental term, the “control parameters” of the shared vehicle are “monitor[ed]” to determine whether a “restriction” has been exceeded. *Id.*, ¶¶[0040], [0053]. *Kleve* discloses that a server may perform this determination. *Id.*, [0035] (“the exemplary processes may be executed by a computing system in communication with a vehicle computing system. . . (e.g., and without limitation, *a server*)”). Almeroth, ¶[0223].

When a restriction is exceeded, *Kleve* teaches that “the Temporary User and Owner may be notified.” *Id.*, ¶[0040]. Specifically, “an in-vehicle display message may be sent [from the server] to notify the Temporary User if a restriction limit has been exceeded.” *Id.*; *see also id.*, ¶[0053] (“The display message to alert the Temporary User of a restriction violation may be sent to the vehicle display information console.”).

It would have been obvious to a POSITA at the relevant time to implement *Kleve*'s privileges and violation notification method with *Zaid*'s existing usage data monitoring system such that if a user exceeds the time period for access, including unlocking and starting the vehicle, the vehicle receives a notification regarding the violation. Almeroth, ¶[0225]. As Dr. Almeroth explains, "a [POSITA] at the relevant time could have easily implemented *Kleve*'s privileges and violation notification method within *Zaid*'s existing usage data monitoring system such that *Zaid*'s server sends a notification to the vehicle for display when the privileges for use of the vehicle have been exceeded, e.g., the time period for use has elapsed." Almeroth, ¶[0227].

A POSITA at the relevant time would have been motivated to make this combination to encourage the user of *Zaid*'s shared vehicle to promptly return or check-in the vehicle if the period for use has expired. Almeroth, ¶[0226].

A POSITA would have had a reasonable expectation of success in the combination since all necessary hardware for providing in-vehicle notifications regarding violations was already present in *Zaid*'s shared vehicle. The only modification would need to be done in software such that the notification was sent to the vehicle upon observing the violation. Almeroth, ¶[0227].

Accordingly, *Zaid* and *Kleve* render obvious claim 15. Almeroth, ¶[0228].

VII. Grounds for Standing

Petitioner certifies that the '026 patent is available for IPR and that Petitioner is not barred or estopped from requesting IPR challenging the patent claims on the grounds herein.

VIII. The Board Should Not Exercise Discretion to Deny Institution

A. The *Fintiv* Factors Do Not Warrant Denial

EA asserts the '026 patent against Petitioners in the Eastern District of Texas. *See* Section X.B. The *Fintiv* factors demonstrate that the Board should not deny institution under *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020) (precedential) (“*Fintiv*”).

Regarding Factor 1, a stay has been neither requested nor granted. Thus, Factor 1 is neutral.

Regarding Factor 2, trial is set for July 21, 2025, before the Board’s anticipated FWD. In light of the Board’s holistic analysis, however, the trial date is not determinative. *See e.g., NetNut Ltd. v. Bright Data Ltd.*, IPR2021-01492, Paper 12 at 9-16 (PTAB Mar. 21, 2022) (instituting review with trial date six months before FWD deadline; no stipulation regarding district court arguments made). Thus, in view of the other factors, Factor 2 does not warrant denial.

Under Factor 3, the Board considers Petitioner’s timing. *Fintiv* at 11. Petitioner moved with speed and diligence in bringing this challenge—within three months after EA served infringement contentions—mitigating against the parties’

investment. *CoolIT Sys., Inc. v. Asetek Danmark A/S*, IPR2021-01195, Paper 10 at 11-14 (PTAB Dec. 28, 2021) (finding petitioner acted diligently where it filed the petition five months after patent owner identified asserted claims); *Fintiv* at 11.

The Board also considers “the amount and type of work already completed in the parallel litigation[.]” *Fintiv* at 9. Here, by institution, the district court’s investment will be nominal. The Markman hearing is expected after institution, as is completion of discovery and dispositive motions. Ex. 1036, 2. *Protect Animals with Satellites LLC, v. OnPoint Sys., LLC*, IPR2021-01483, Paper 11 at 14-15 (PTAB Mar. 4, 2022); *Fintiv* at 9-10; *NetNut*, Paper 12 at 11-12. Thus, Factor 3 favors institution.

Regarding Factor 4, this factor does not warrant denial. *See e.g., NetNut Ltd.*, Paper 12 at 9-16 (instituting review with no stipulation regarding district court arguments made). This Petition challenges four additional claims not asserted in the litigation (Ex. 1037, 3), creating additional nonoverlapping issues. *3Shape A/S v. Align Tech., Inc.*, IPR2020-00223, Paper 12 at 34 (PTAB May 26, 2020) (nonoverlap of six claims supports institution); *Apple Inc. v. Neodron, Ltd.*, IPR2020-00778, Paper 10 at 19 (PTAB Sept. 14, 2020) (same; two claims). Thus, Factor 4 favors institution.

Regarding Factor 5, although Petitioner is a defendant in the litigation, this does not warrant denial. *See, e.g., 3Shape*, Paper 12 at 32-34 (institution despite Petitioner being defendant in district court); *Apple*, Paper 10 at 19-20 (same).

Factor 6 favors institution because the merits of this Petition are strong. The Petition relies upon materially different and non-cumulative primary references not applied during prosecution. *See* Section VII.A, *infra*.

Accordingly, the *Fintiv* factors favor institution.

B. The *Becton, Dickinson* Factors Do Not Warrant Denial

The factors in *Becton, Dickinson & Co. v. B. Braun Melsungen AG*, IPR2017-01586, Paper 8 at 17-18 (PTAB Dec. 15, 2017) do not favor denial. *See also Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH*, IPR2019-01469, Paper 6 (PTAB Feb. 13, 2020) (precedential).

Zaid was submitted during prosecution in an IDS containing 357 other references. Ex. 1002, 138. However, there is no evidence that the Examiner considered *Zaid*, and the arguments presented here are non-cumulative of those during prosecution. *See Nintendo Co., Ltd. et al. v. Gamevice, Inc.*, IPR2023-00643, Paper 11 at 18-19 (PTAB Nov. 6, 2023) (mere citation in IDS insufficient to trigger noninstitution under § 325(d)).

The reference that was substantively addressed by the Examiner during prosecution, *Ehrman*, disclosed an ID and password for accessing a vehicle. Ex.

1002, 173-74. *Ehrman* did not disclose an electronic key providing time-limited access as in *Zaid*. Accordingly, the asserted references are non-cumulative of references considered during prosecution. The *Becton* factors thus do not warrant denial.

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., Kia Corporation and Kia America Inc.

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

To the best of Petitioner's knowledge, the '026 patent is, or has been, involved in the following district court litigations and Board proceedings.

Name	Number	Court	Filed
<i>Emerging Automotive LLC v. Toyota Motor Corp. et al.</i>	2:23-cv-00434	EDTX	Sept. 20, 2023
<i>Emerging Automotive LLC v. Kia Corp. et al.</i>	2:23-cv-00437	EDTX	Sept. 22, 2023

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

To the best of Petitioners' knowledge, the '026 patent is related to the following U.S. applications that had been pending as of the issuance of the '026 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
61/745,729		12/24/2012
13/842,158	9,229,905	3/15/2013
14/063,638	9,189,900	10/25/2013
14/303,442	9,365,188	6/12/2014
15/180,306	9,499,129	6/13/2016
15/344,566	9,663,067	11/6/2016
15/696,618	9,928,488	9/6/2017
15/854,241	10,442,399	12/26/2017
15/928,054	10,282,708	3/21/2018
16/405,036	11,132,650	5/7/2019

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

Lead Counsel	Back-Up Counsel
<u>For Toyota</u> Joshua L. Goldberg (Reg. No. 59,369) joshua.goldberg@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 901 New York Ave NW Washington, DC 20001 Tel: 202-408-4000 Fax: 202-408-4400 <u>For Kia</u> James M. Glass (Reg. No. 46,729) jimglass@quinnemanuel.com QUINN EMANUEL URQUHART & SULLIVAN, LLP 51 Madison Avenue, 22nd Floor New York, NY 10010 Tel: (212) 849-7000 Fax: (212) 849-7100	<u>For Toyota</u> James R. Barney (Reg. No. 46,539) james.barney@finnegan.com Aidan Skoyles (Reg. No. 61,119) aidan.skoyles@finnegan.com Nicholas Eitsert (Reg. No. 78,843) nicholas.eitsert@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 901 New York Ave NW Washington, DC 20001 Tel: 202-408-4000 Fax: 202-408-4400 <u>For Kia</u> Quincy Lu (Reg. No. 76,954) quincylu@quinnemanuel.com

Lead Counsel	Back-Up Counsel
	QUINN EMANUEL URQUHART & SULLIVAN, LLP 1109 First Avenue, Suite 210 Seattle, WA 98101 Tel: (206) 905-7000 Fax: (206) 905-7100 Jeffrey S. Gerchick <i>Pro hac vice</i> forthcoming jeffgerchick@quinnemanuel.com QUINN EMANUEL URQUHART & SULLIVAN, LLP 1300 I Street NW Washington, DC 20005 Tel: (202) 538-8000 Fax: (202) 538-8100 Brett Watkins (Reg. No. 60,458) brettwatkins@quinnemanuel.com QUINN EMANUEL URQUHART & SULLIVAN, LLP 700 Louisiana St., Suite 3900 Houston, TX 77002 Tel: (713) 221-7000 Fax: (713) 221-7100

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: April 23, 2024

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 13,874 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: April 23, 2024

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 1001-1026, 1029-1039 were served on April 23, 2024, on counsel of record for the subject patent by FedEx Priority Overnight at the addresses below.

Correspondence Address of Record	Litigation Counsel
Albert Penilla 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

/Lisa C. Hines/
Lisa C. Hines
Case Manager
FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.