

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

KIA CORP.,
TOYOTA MOTOR CORP.,
Petitioners,

v.

EMERGING AUTOMOTIVE LLC,
Patent Owner.

Case No. IPR2024-00981

U.S. Patent No. 9,365,188

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 9,365,188**

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION	1
II. STANDING.....	2
III. GROUNDS.....	2
IV. POSITA.....	2
V. BACKGROUND	3
A. '188 patent.....	3
1. Prosecution History.....	3
2. Priority Date	3
(a) Legal requirement.....	4
(b) The pre-October 2013 applications do not disclose “electronic key[s]”	5
VI. CLAIM CONSTRUCTION	8
VII. GROUNDS.....	8
A. Ground 1: Kleve	8
1. Claim 1	8
(a) 1[pre], 1[a].....	8
(b) 1[b].....	16
(c) 1[c]	16
(d) 1[d].....	17
(e) 1[e]	17
(f) 1[f].....	18
(g) 1[g].....	19
2. Claim 2	21
3. Claim 3	21
4. Claim 4	22
5. Claim 5	22
6. Claim 6	23

7.	Claim 7	23
8.	Claim 8	23
9.	Claim 9	23
10.	Claim 11	24
	(a) 11[a]	24
	(b) 11[b]	24
11.	Claim 12	25
12.	Claim 13	27
	(a) 13[a]	27
	(b) 13[b]	28
	(c) 13[c]	29
13.	Claim 14	29
14.	Claim 15	30
15.	Claim 16	30
	(a) 16[g]	30
16.	Claim 17	31
17.	Claim 18	32
	(a) 18[a]	32
	(b) 18[b]	32
18.	Claim 19	33
	(a) 19[g]	33
19.	Claim 20	34
	(a) 20[a]	34
	(b) 20[b]	35
B.	Ground 2: Klevé and Sekiyama.....	35
1.	Motivation to Combine	35
2.	1[b]	36
3.	1[g]	37

C.	Ground 3: Kleve (optionally with Sekiyama) and Mottla (Claim 10)	37
D.	Ground 4: Zaid and Harris	39
1.	Motivation to Combine	39
2.	Claim 1	41
	(a) 1[pre], 1[a]	41
	(b) 1[b]	47
	(c) 1[c]	48
	(d) 1[d]	48
	(e) 1[e]	50
	(f) 1[f]	51
	(g) 1[g]	52
3.	Claim 3	53
4.	Claim 5	53
5.	Claim 6	54
6.	Claim 7	54
7.	Claim 9	54
8.	Claim 11	54
	(a) 11[a]	54
	(b) 11[b]	55
9.	Claim 12	55
10.	Claim 13	56
	(a) 13[a], 13[b]	56
	(b) 13[c]	57
11.	Claim 14	57
12.	Claim 15	58
13.	Claim 16	58
	(a) 16[g]	59
14.	Claim 18	59

(a)	18[a]	59
(b)	18[b]	59
15.	Claim 19	59
(a)	19[g]	60
16.	Claim 20	61
(a)	20[a]	61
(b)	20[b]	61
E.	Ground 5: Zaid, Harris and Mottla	61
1.	Motivation to Combine	61
2.	Claims 2, 4, 8	63
3.	Claim 10	64
F.	Ground 6: Zaid, Harris and Patenaude	64
1.	Motivation to Combine	65
2.	Claim 17	66
G.	Ground 7: Kleve and Patenaude	67
VIII.	<i>FINTIV</i>	67
IX.	§325(D)	68
X.	MANDATORY NOTICES AND FEES	68
A.	Real Party-In-Interest	68
B.	Related Matters	68
C.	Counsel and Service Information	72
D.	Payment of Fees	75

EXHIBIT LIST

Ex.	Description
1001	U.S. Patent No. 9,365,188 (“’188 patent”)
1002	Prosecution History for U.S. Patent No. 9,365,188
1003	Declaration of Dr. Almeroth
1004	U.S. Pat. Pub. No. 2014/0129053 (“Kleve”) (prior art under at least §§ 102(a)(2) or pre-AIA § 102(e))
1005	Certified translation of JP2010126949A (“Sekiyama”) (prior art under at least Section §§ 102(a)(1), (2) or pre-AIA § 102(a), (e))
1006	JP 2010126949
1007	Declaration of Herman Kahn
1008	U.S. Pat. Pub. No. 2011/0112969A1 (“Zaid”) (prior art under at least §§ 102(a)(1), (2) or pre-AIA §§ 102(a), 102(b), 102(e))
1009	U.S. Pat. Pub. No. 2011/0312273A1 (“Harris”) (prior art under at least §§ 102(a)(1), (2))
1010	U.S. Pat. Pub. No. 2011/0060480A1 (“Mottla”) (prior art under at least §§ 102(a)(1), (2) or pre-AIA § 102(a), (b), (e))
1011	U.S. Pat. Pub. No. 2006/0136106 (“Patenaude”) (prior art under at least §§ 102(a)(1), (2) or pre-AIA § 102(a), (b),(e))
1012	U.S. Pat. App. No. 61/478,436
1013	U.S. Pat. App. No. 61/745,729
1014	U.S. Pat. App. No. 13/452,882
1015	U.S. Pat. App. No. 13/842,158
1016	U.S. Pat. App. No. 14/063,638

Petition for *Inter Partes* Review
U.S. Patent No. 9,365,188

1017	Order Granting Request For Ex Parte Reexamination, Reexamination Control No. 90/019,456, Patent No. 11,738,659 (April 15, 2024)
1018	Text Comparison of U.S. Pat. App. No. 13/842,158 to U.S. Pat. App. No. 14/063,638
1019	<i>Curriculum Vitae</i> of Dr. Almeroth

LIST OF CHALLENGED CLAIMS

Claim	Limitation
1[pre]	A method, comprising,
1[a]	receiving, by a server, a request from a user via a user account that has a vehicle associated therewith to generate an electronic key (e-key) for an identified recipient to use the vehicle, the request includes identifying information for enabling sending of the e-key to the recipient via an electronic transmission, the request includes a condition of use of the vehicle as set by the user via the user account;
1[b]	generating, by the server, the e-key, the e-key being assigned with the condition of use of the vehicle;
1[c]	transmitting, by the server, the e-key to the recipient using the identifying information so that a device of the recipient is implemented to use the e-key;
1[d]	transmitting, by the server, data to the vehicle to enable use of the vehicle via the e-key; and
1[e]	receiving, by the server, use data regarding use of the vehicle for when the vehicle is used via the e-key;
1[f]	wherein the use data identifies information regarding the use of the vehicle, and the information identifies a violation of the condition of use;
1[g]	wherein the server processes logic for generating the e-key and processes logic for analyzing the data regarding use of the vehicle when the e-key is used for the vehicle, the server or other servers connected to the server being accessible over the Internet, the vehicle having wireless communication systems for communicating with the server or other servers and for communicating with devices local to the vehicle.

Claim	Limitation
2	The method of claim 1, further comprising, sending a warning notification to the device of the recipient, or the vehicle, or both the device of the recipient, the warning notification identifying the violation of the condition of use.
3	The method of claim 1, wherein the request to generate the e-key is received from the user account that is one of an administrator of the vehicle, or an owner of the vehicle, or a rental car operator of the vehicle, or a fleet operator for the vehicle, or a user account holder that has the vehicle associated thereto, or a user authorized to request e-keys for the vehicle.
4	The method of claim 1, further comprising, sending data to one or both of the vehicle and the device of the recipient to notify that the e-key will become disabled due to the violation of the condition.
5	The method of claim 1, wherein the condition of use is one of a geographic restriction for where the vehicle is allowed to be used, or a speed restriction, or an occupancy restrictions, or a time frame of use, or a time expiration of use, or combinations thereof.
6	The method of claim 1, wherein the identifying information includes one or more of an email address, a phone number, a text, a message address, a notification, a link, a web address, a social network address, or combinations thereof.
7	The method of claim 1, wherein receiving use data for use of the vehicle for when the vehicle is used via the e-key includes one or

Claim	Limitation
	more of a history of where the vehicle has been, or speeds of the vehicle, or events of the vehicle, or multiple violations of the condition of use, or combinations thereof.
8	The method of claim 1, further comprising, sending messages to one or both of the vehicle and the device of the recipient regarding warnings of when the use of the vehicle may exceed, has exceeded, or is about to exceed the condition of use.
9	The method of claim 1, wherein the e-key provides access to at least one of operating functions of the vehicle, or opening the vehicle, or starting the vehicle, or using user interfaces of the vehicle, or turning-off the vehicle, or combinations thereof.
10	The method of claim 1, wherein the e-key enables graphical icons on a screen of the device to be active for enabling use of the vehicle, at least one of the graphical icons on the screen enabling unlocking of the vehicle, or turning on of the vehicle, or locking the vehicle.
11[a]	The method of claim 1, wherein the device is one of a smartphone, or a smartwatch, or smart glasses, or a portable device, or a computer, or a digital assistant, or a key fob, and
11[b]	wherein the e-key, once used via the device of the recipient, the e-key cannot be used via another device or sent to another device to enable use of the e-key without receiving new data from the server to reactivate the e-key.

Claim	Limitation
12	The method of claim 1, further comprising, receiving a plurality of requests to generate e-keys for the vehicle from time to time to the recipient or other recipients, such that a plurality of e-keys can be generated for the vehicle and the e-keys that are generated are associated with the user account, and any one of the generated e-keys are removable from being active via the user account, the user account being used for making the requests to generate the e-key or e-keys.
13[a]	The method of claim 1, further comprising, receiving data indicative that the device having the e-key remains within a communication distance of the vehicle during use of the e-key; and
13[b]	sending data to disable the e-key and prevent use of the vehicle after a period of time when the data indicates that the device is not within the communication distance of the vehicle for which the e-key is to be used or is used; and
13[c]	sending a notification or a report, or a log to an administrator of the vehicle to report activity of use of the vehicle in association with use of the e-key.
14	The method of claim 1, wherein the request to generate the e key for the identified recipient is made using a template having a set of privileges, wherein the template is selectable instead of selecting individual privileges to be associated with the e-key.
15	The method of claim 14, wherein the template is one of a child template, or a teen template, or a spouse template, or a mechanic template, or a valet attendant template, or a friend template, or a quest template, or a custom template.

Claim	Limitation
16[pre]	A method, comprising,
16[a]	receiving, by a server, a request from a user via a user account that has a vehicle associated therewith to generate an electronic key (e-key) for an identified recipient to use the vehicle, the request includes identifying information for enabling sending of the e-key to the recipient via an electronic transmission, the request includes a condition of use of the vehicle as set by the user via the user account;
16[b]	generating, by the server, the e-key, the e-key being associated with the condition of use of the vehicle;
16[c]	transmitting, by the server, the e-key to the recipient using the identifying information so that a device of the recipient is implemented to use the e-key;
16[d]	transmitting, by the server, data to the vehicle to enable use of the vehicle via the e-key; and
16[e]	receiving, by the server, use data regarding use of the vehicle for when the vehicle is used via the e-key;
16[f]	wherein the use data identifies information regarding the use of the vehicle, and the information identifies a violation of the condition of use;
16[g]	wherein the transmitted e-key is encrypted and configured for decryption to enable use of the vehicle using the e-key;
16[h]	wherein the e-key provides access to at least one of operating functions of the vehicle, or opening the vehicle, or starting the vehicle, or using user interfaces of the vehicle, or driving the vehicle, or turning-off the vehicle, or combinations of two or more thereof.

Claim	Limitation
17[a]	The method of claim 16, further comprising, receiving, by the server, data from the vehicle being indicative of interface inputs or settings made during use with the e-key, the inputs or settings being examined to identify patterns; and
17[b]	learning the patterns, by a process executed by the server, to provide recommendations to the recipient or to an account of the recipient, for settings that should or may be made to the vehicle when using the e-key.
18[a]	The method of claim 1, wherein the condition of use defines one or more privileges associated to use of the e-key, and further comprising,
18[b]	receiving a request from the device of the recipient to expand use, or remove a privilege, or add a privilege of the condition of use.
19[pre]	A method, comprising,
19[a]	receiving, by a server, a request from a user via a user account that has a vehicle associated therewith to generate an electronic key (e-key) for an identified recipient to use the vehicle, the request includes identifying information for enabling sending of the e-key to the recipient via an electronic transmission, the request includes a condition of use of the vehicle as set by the user via the user account;
19[b]	generating, by the server, the e-key, the e-key being assigned with the condition of use of the vehicle;
19[c]	transmitting, by the server, the e-key to the recipient using the identifying information so that a device of the recipient is implemented to use the e-key;

Claim	Limitation
19[d]	transmitting, by the server, data to the vehicle to enable use of the vehicle via the e-key; and
19[e]	receiving, by the server, use data regarding use of the vehicle for when the vehicle is used via the e-key;
19[f]	wherein the use data identifies information regarding the use of the vehicle, and the information identifies a violation of the condition of use;
19[g]	wherein the e-key received at the device of the recipient includes data to inform the recipient of a level of monitoring that is to occur of the vehicle when the e-key is used for the vehicle, wherein a log is made to save the use of vehicle to a cloud storage, or storage of the vehicle or both, the log including one or more of driving data that took place, or where the vehicle was driven, or speeds of the vehicle, or damage of the vehicle, or radio stations listened to, or conversations had, or images of drivers during specific times, or combinations to two or more thereof;
19[h]	wherein the e-key provides access to at least one of operating functions of the vehicle, or opening the vehicle, or starting the vehicle, or using user interfaces of the vehicle, or driving the vehicle, or turning-off the vehicle, or combinations of two or more thereof.
20[a]	The method of claim 19, wherein a plurality of e-keys for the vehicle are producible, the plurality of e-keys can co-exist, and wherein,
20[b]	only one e-key is associated with active use of the vehicle at one time; or a particular e-key in use with the vehicle can be swapped for another e-key having access to the vehicle, such that each e-key has the same or different privileges or conditions of use; or a priority order of e-keys is defined, such that higher level priority e-keys are placed in use over lower priority e-keys.

I. INTRODUCTION

The '188 patent relates to electronic keys on mobile devices to unlock vehicles. But by 2013, the priority date of the '188 patent, keyless entry systems via mobile devices were prolific. Indeed, the grounds presented in this petition rely on Kleve and Sekiyama, patents that resulted from Ford and Toyota's work in this area.

Ford's Kleve reference discloses a system where owners and renters create website accounts for short-term vehicle rentals with restrictions on vehicle usage, such as rental period and location—disclosing the purported innovation of the '188 patent. Upon the owner's request, the server transmits a “virtual key” to the renter's device for vehicle access. Kleve alone thus renders the claims obvious.

Like Kleve, Toyota's Sekiyama reference also discloses a server that generates an electronic key in response to a request. Both Kleve and Sekiyama are directed to electronic key systems. A POSITA would have found it obvious to combine Kleve's system with Sekiyama's teachings.

The Kleve-based grounds rely on the fact that the '188 patent is, at best, only entitled to claim priority to an October 2013 application. Even if entitled to the earliest filing date (which the claims are not), the '188 claims are unpatentable over Zaid, also directed to a keyless entry system for rental vehicles. Like Kleve, Zaid discloses a user reserving a rental vehicle, which results in a server generating an electronic key to be sent to the user's mobile device to allow the user to enter and

operate the vehicle. Thus, Zaid provides an alternative basis for invalidating the challenged claims.

II. STANDING

Petitioners certify the '188 patent is available for IPR and they are not estopped.

III. GROUNDS

Petitioners present the below grounds.

Ground	Basis	Reference(s)	Claims
1	§103	Kleve	1-9,11-20
2	§103	Kleve, Sekiyama	1-9,11-20
3	§103	Kleve, Mottla	10
4	§103	Zaid, Harris	1,3,5-7,9,11-16,18-20
5	§103	Zaid, Harris, Mottla	2,4,8,10
6	§103	Zaid, Harris, Patenaude	17
7	§103	Kleve, Patenaude	17

IV. POSITA

A POSITA had at least a four-year undergraduate degree in electrical engineering, automotive engineering, or closely related field and least two years of experience in the field of access control systems, vehicle electronics, and/or cryptography. Ex. 1003, ¶¶79-82. More education can supplement practical experience and vice versa. *Id.* Petitioners' expert exceeded this by the priority date. *Id.*

V. BACKGROUND

A. '188 patent

The '188 patent describes a vehicle owner assigning an e-key to a user. Ex. 1001, 40:64-41:1. In Figure 29, owner “Bob” shares e-keys 650 with three temporary users. *Id.*, 40:64-66, 41:12-13. This allows different users to have different keys with different conditions. *Id.*, 41:20-24; Ex. 1003, ¶¶54-59.

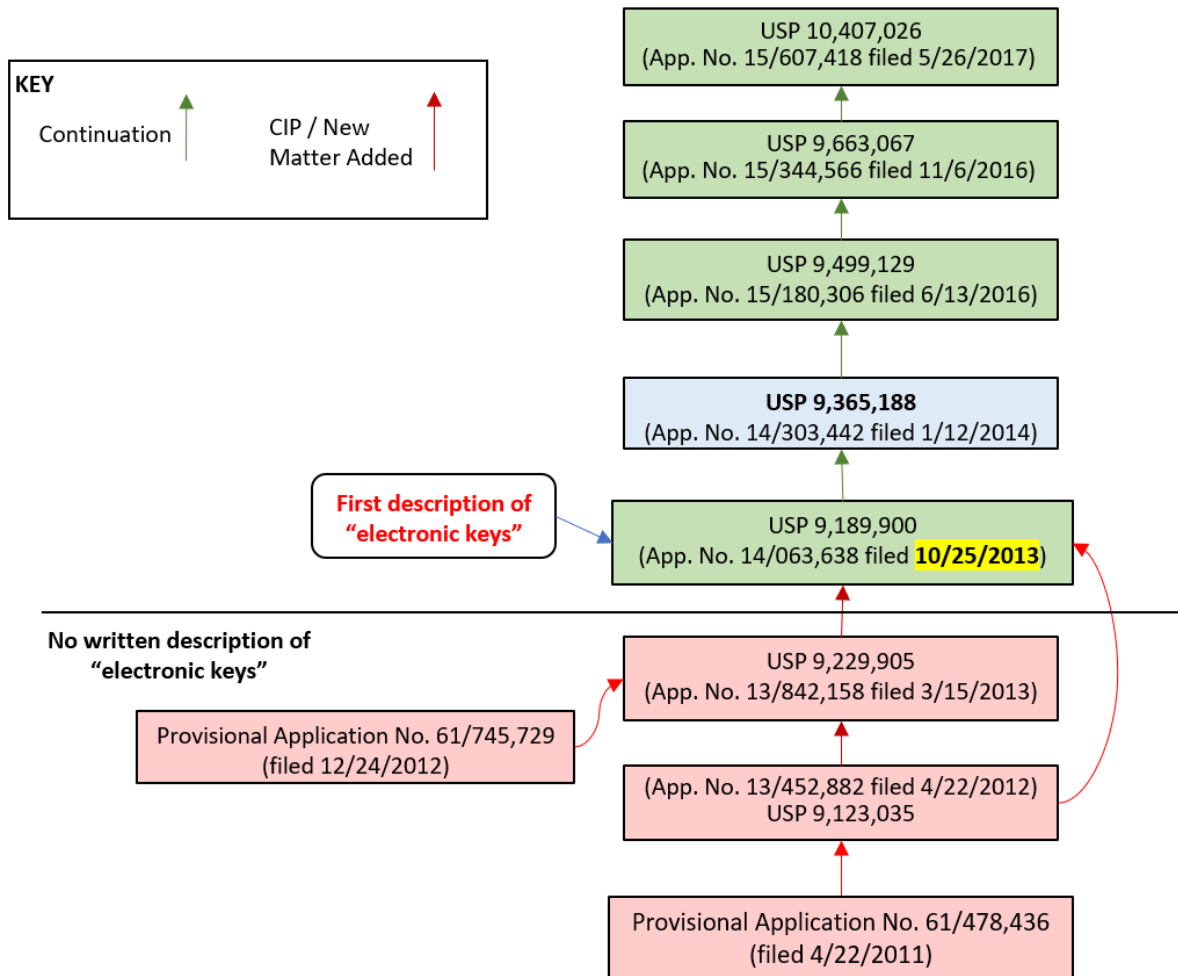
1. Prosecution History

The examiner issued no rejections, stating in the notice of allowance that the cited prior art does not disclose transmitting the e-key to the recipient. Ex. 1002; Ex. 1003, ¶60.

2. Priority Date

The '188 patent claims priority to various applications as shown below:

Petition for *Inter Partes* Review
U.S. Patent No. 9,365,188



The '188 patent is not entitled to a filing date before October 25, 2013, when the '638 Application introduced descriptions for "e-keys."

(a) Legal requirement

An earlier-filed U.S. application must "reasonably convey[s] to those skilled in the art that the inventor had possession of" the claimed subject matter. *Ariad Pharms., Inc. v. Eli Lilly & Co.*, 598 F.3d 1336, 1351 (Fed. Cir. 2010). Written description evaluates "the specification from the perspective of a [POSITA]." *Id.* A description cannot "merely render[] the invention obvious." *Id.*, 1352.

**(b) The pre-October 2013 applications do not disclose
“electronic key[s]”**

The claims are methods for requesting, generating, transmitting and using *electronic keys* (“e-keys”) for vehicle access. However, none of the earlier applications disclose “e-keys” or anything similar to an e-key.

The ’638 Application, filed October 25, 2013, introduced a significant amount of new material directed to e-keys. Ex. 1018; Ex. 1003, ¶¶61-70. For example, as Dr. Almeroth explains in detail, Figures 17-35 and their descriptions discuss the requesting, generating, transmission, and use of e-keys. *Id.*, 105, 122-28; Ex. 1003, ¶65.

Figure 35, introduced in the ’638 Application, depicts requesting, generating, and transmitting an e-key to Bob.

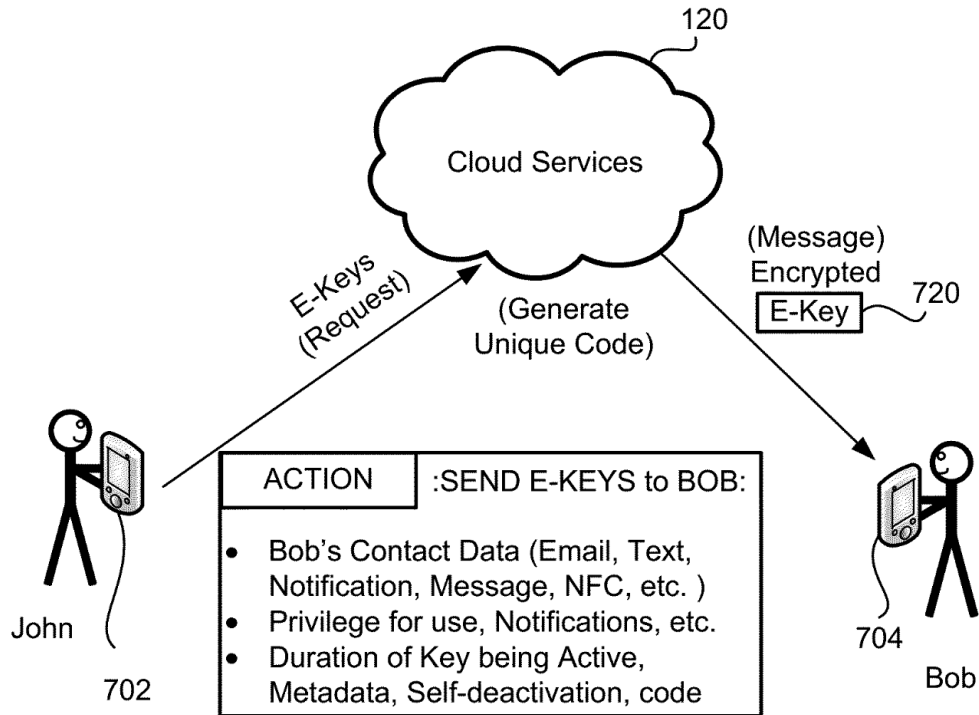


FIG. 35

Figure 33 shows Bob using an e-key to unlock and start John's vehicle.

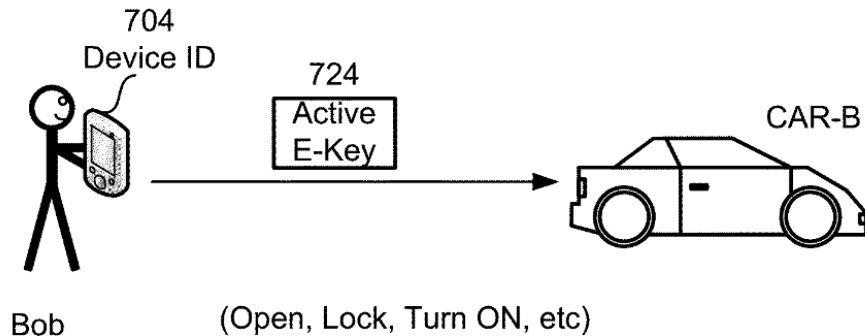


FIG. 33

By contrast, the earlier applications contain no disclosures relating to e-keys. The '158 Application is directed to sending vehicle user profiles from a server to a

mobile device that define settings for a vehicle, such as radio or comfort settings. Ex. 1015, Abstract. The '882 Application and provisionals are directed to electric vehicle charging. Ex. 1014, Abstract; Exs. 1012-13. Thus, a POSITA would not have considered the applicant to be in possession of the claimed subject matter. This is supported by Dr. Almeroth's testimony. Ex. 1003, ¶73.

PO may argue the e-keys are disclosed through the earlier applications' description of a server that communicates with a vehicle's lock or engine-starting mechanisms by request of a mobile device. Ex. 1015, 28, 42, 60-61. But e-keys are not disclosed in connection with such functionality, and the use of keyless remote control was well-known in the art at that time. Ex. 1010. A POSITA in 2013 would understand that to the extent the earlier applications described such a keyless control system, it was accomplished without the use of e-keys. Ex. 1003, ¶¶71-75. Alternatively, to the extent that PO argues that the mere disclosure of remote control access would indicate to a POSITA that the applicant had possession of the requesting, generating, and use of e-keys, then such claims would not be valid as remote access and control of a vehicle had long been known. *Id.*

Finally, in the USPTO's grant of *ex parte* reexamination of related patent US11,738,659 that similarly recites e-keys, they noted that the '436 Provisional "appears to lack support for several limitations claimed... includ[ing] for example, an 'eKey'." Ex. 1017, 4 n.1. Petitioners agree.

VI. CLAIM CONSTRUCTION

The claim terms should be given their plain and ordinary meaning under *Phillips*. Ex. 1003, ¶¶83-84.

VII. GROUNDS

A. Ground 1: Kleve

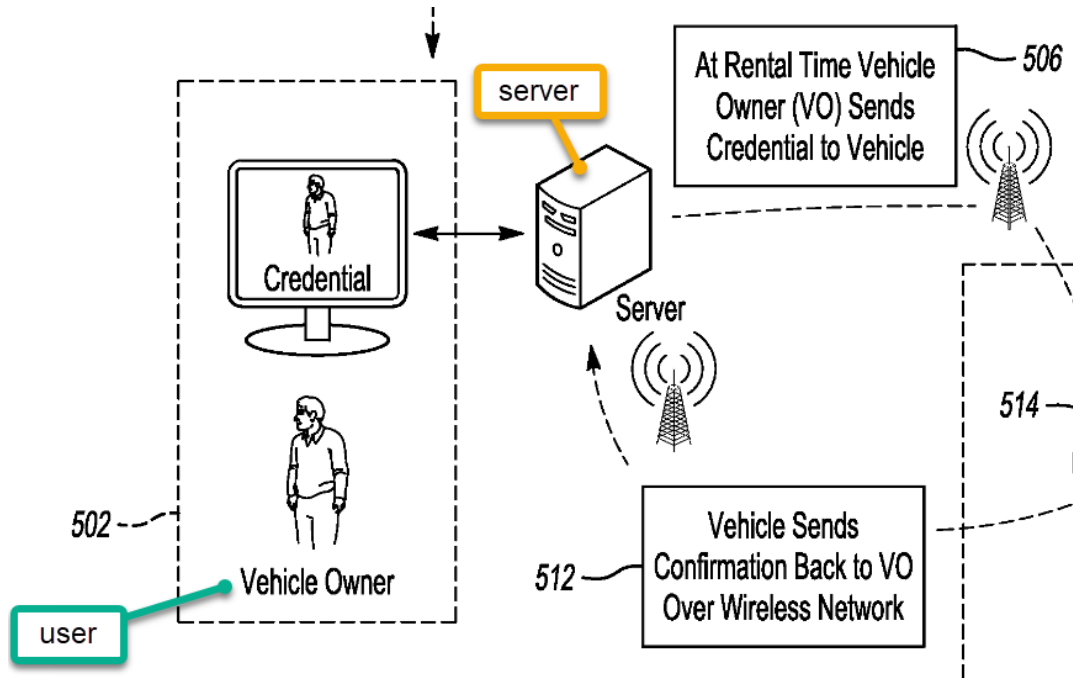
Ford's Kleve system allows vehicle rentals between Vehicle Owners and Temporary Users. Through website accounts, they negotiate a rental agreement, including conditions of use. Upon agreement, the Temporary User provides identifying information to the Vehicle Owner who submits it to the server to generate a time-limited virtual key. The virtual key is sent to the Temporary User's device to allow vehicle access. (Ex. 1003, ¶¶86-91, 99)

1. Claim 1

(a) 1[pre], 1[a]

“receiving, by a server, a request from a user via a user account that has a vehicle associated therewith to generate an electronic key (e-key) for an identified recipient to use the vehicle”: Kleve discloses that a server receives a request from Vehicle Owner (the claimed ***user***) via their user profile (***user account***) associated with a vehicle. This request results in the server generating a virtual key (***e-key***) for an identified Temporary User (***identified recipient***) to use the owner's vehicle. Ex. 1003, ¶¶100-15.

“*server*”: Kleve discloses “a vehicle rental micro-business” which comprises a *server*. Ex. 1004, ¶35 (“[T]he exemplary processes may be executed by a... remote computing system (e.g.,... *a server*).”); ¶36 (“The vehicle rental micro-business 200 may include a website.”); ¶69 (“server 634.”).



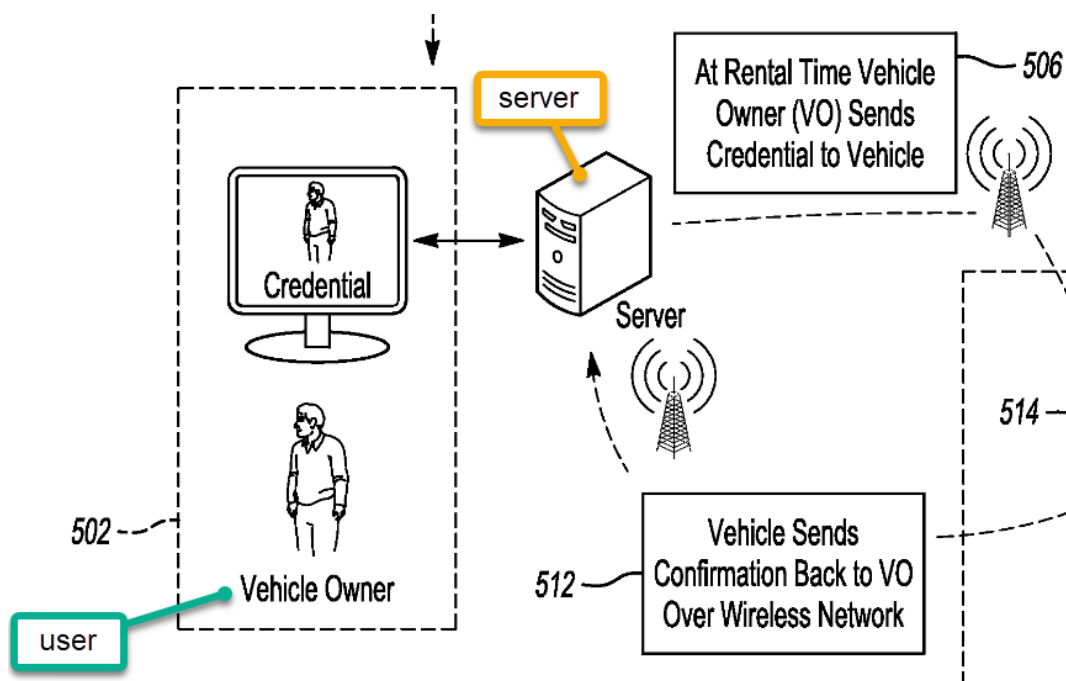
“*user account that has a vehicle associated therewith*”: Next, Kleve discloses that a Vehicle Owner may create a user profile (*user account*) on the server, and *associate a vehicle* with the profile. A Vehicle Owner “may set up a user profile using a website... that is stored in a database,” which includes “the make, model and year of the vehicle available for rent.” Ex. 1004, ¶37. A POSITA would understand that the website and database are part of a server system, because websites were hosted on servers and interacted with database servers. Ex. 1003, ¶104.

“identified recipient”: Kleve discloses that a Temporary User, an **identified recipient**, identifies himself to create a user profile for renting a car. For the Temporary User account, the website collects **“identification** and payment from [the] Temporary User,” including “photo of forms of ID, [and] unique Temporary User **identification** to validate and pay for the rental service.” Ex. 1004, ¶¶36-37.

The “Temporary User” uses his user profile to browse available cars on the server. Ex. 1004, ¶47. When the Temporary User selects a vehicle, “the Temporary User and vehicle Owner agree to terms 316,” and then the agreement “can be signed and payment made through the website.” *Id.* Thus, Kleve discloses that a Vehicle Owner’s **user account** is used to host vehicle information and allow the Vehicle Owner to come to an agreement with a Temporary User for vehicle rental. Ex. 1003, ¶¶105-06.

“receiving, by a server, a request from a user via a user account... to generate an electronic key”: After agreement, the Vehicle Owner (**user**) sends a request to the server via their user profile (**user account**) to generate a virtual key, **an e-key**. Specifically, “the vehicle Owner may enter in vehicle authorization credentials based on information received by the Temporary User **to set up a virtual key**.” Ex. 1004, ¶62. Kleve further states that such a request is “entered into the server.” *Id.*, ¶63. The entering of this information is a **request sent by the user** to generate an e-

key. As in Figure 5 (annotated below), credentials are sent to the server via a user's computer (such as via a website).



Kleve states that the virtual key is only generated after the Vehicle Owner has “already setup a user profile,” **a user account**. Ex. 1004, ¶62. In the following sentence, Kleve states that the Vehicle Owner “may enter in vehicle authorization credentials [i.e., make a request]... to set up a virtual key[.]” *Id.* Thus, the request is made **via a user account**. Ex. 1003, ¶¶107-08.

Alternatively, it would have been obvious to have the request made via a user account. A POSITA would have been motivated to have the server receive the request from Vehicle Owner's profile to know which vehicle and which Temporary User the virtual key is intended for, since the Vehicle Owner profile has the vehicle and rental agreement information. Ex. 1003, ¶109. As Dr. Almeroth explains, this

“provides the well-known benefits of increasing security, reliability and user satisfaction, because requests made from the Vehicle Owner’s user profile can be relied on as having been authorized by the actual Vehicle Owner.” *Id.* POSITA implementing requests from users via their accounts in this way would have had a reasonable expectation of success, since such a configuration was the default method for users to interact with server-based reservation systems. *Id.*

A POSITA would further understand that Kleve’s server generates the virtual key (***e-key***). Ex. 1003, ¶110. Temporary User identification is first “entered into the server and [then] ***used as a virtual key***, or in addition to the virtual key,” which means the server receives the identification to generate and accompany the virtual key. Ex. 1004, ¶63. Kleve further states that the “virtual key may be sent... to the VCS, Temporary User’s nomadic device, and/or vehicle Owner[’]s nomadic device,” indicating the server generates the virtual key and sends it to those various destinations. *Id.* It would not be necessary for the key to be sent to the Vehicle Owner’s device if it was the one that generated it.¹

¹ Kleve’s disclosure in ¶69 that the “[V]ehicle Owner may then generate a virtual key” is optional and, in any case, a POSITA would understand that the Vehicle Owner “generates” a virtual key by requesting one from the server as discussed. Ex. 1003, ¶111.

Alternatively, a POSITA would have found it obvious to generate the virtual key at the server (rather than the Vehicle Owner's device). Generating the key requires that the Vehicle Owner enter "authorization credentials" from the Temporary User into the server, and the server stores the Temporary User's user profile that contains recorded copies of those credentials (such as "photos of credit cards, photo of forms of ID," etc.) to confirm the Temporary User's identity. Ex. 1004, ¶¶62, 37. Thus, as Dr. Almeroth explains, a POSITA "would be motivated to have the server generate the key since the server (1) maintains the identity of the Vehicle Owner (by the request being sent via a user account), (2) maintains the identity of the Temporary User (via the authorization credentials), and (3) confirms that they have entered into a rental agreement for a specific vehicle." Ex. 1003, ¶112. A POSITA would have known that generating the key at the server "increases security, reliability and user satisfaction since the server can confirm all the necessary information needed before providing the virtual key," as Dr. Almeroth explains in detail. Ex. 1003, ¶113. It also does not rely on the availability of the Vehicle Owner's personal device. *Id.* A POSITA would have reasonably expected success because authenticating and generating keys at a server was well-known and could have been accomplished using numerous existing approaches. *Id.*, ¶114.

"electronic key (e-key) for an identified recipient to use the vehicle": Kleve discloses that the virtual key (**e-key**) allows the Temporary User to **use the vehicle**.

Kleve discloses that “the Temporary User may use their virtual key credential to **access the vehicle.**” Ex. 1004, ¶67. Kleve further states generally that the virtual key is “used to enter and enable the vehicle **drive away event.**” *Id.*, ¶44.

“the request includes identifying information for enabling sending of the e-key to the recipient via an electronic transmission”: Kleve discloses that the Vehicle Owner includes the Temporary User’s identifying information in the request to the server to enable sending of the virtual key (**e-key**) to the Temporary User. Ex. 1004, ¶¶62-63; Ex. 1003, ¶¶116-17. Specifically, the request sent to the server includes “vehicle authorization credentials based on information received by the Temporary User [**identifying information**]” which is used “to setup a virtual key,” thus **enabling the sending of that key.** *Id.*, ¶¶62-63 (“photo of forms of ID”). Kleve also discloses that the virtual key may be sent to the Temporary User “through an email,” thus indicating that the request includes an email address as **identifying information.** *Id.*, ¶39.

Kleve further discloses that the virtual key is sent to the Temporary User **via an electronic transmission.** Kleve states that the virtual key “may be sent in an encrypted message to the... Temporary User’s **nomadic device,**” which is a wireless electronic device such as a “cell phone, smart phone, PDA, or any other device having **wireless remote network connectivity.**” *Id.*, ¶¶63, 25.

“the request includes a condition of use of the vehicle as set by the user via the user account”: Kleve discloses that a Vehicle Owner’s request may set ***conditions of use of the vehicle*** via the owner’s user profile. Ex. 1003, ¶¶118-123. Specifically, Kleve discloses that a Vehicle Owner and Temporary User can, via their website user profiles (***user accounts***), negotiate a rental agreement including restrictions (***conditions of use of the vehicle***). Ex. 1004, ¶38 (“The Owner and Temporary User may agree to terms and conditions for the rental period ***using the website.***”); ¶47.

The restrictions include “rental period” (¶38), “speed, global position coordinates, or load weight restrictions” (¶40), “destination location” (¶51), “prohibited areas where the owner does not want their vehicle to be used” (¶73), and “top vehicle speed, limiting the cargo load, and alerting the vehicle owner if the driver enters an area deemed to be prohibited by the owner” (¶75).

Kleve discloses that the agreed conditions are sent with the request to generate a virtual key. Ex. 1003, ¶120. The virtual key “enable[s] the keyless drive system for the appropriate Temporary User ***during a given rental period,***” indicating the request included the restrictions so that the virtual key could be associated with said time limited-use conditions. Ex. 1004, ¶39; ¶68 (“Once the rental period has expired the virtual key may be reset and cleared from the VCS.”).

Alternatively, as Dr. Almeroth explains in detail, a POSITA would understand that it would have been a desirable modification to include the reservation conditions in the request, so that the generated virtual key is associated with such restrictions, allowing the restrictions to be monitored and enforced. Ex. 1003, ¶¶121-23. Kleve already discloses that monitoring and enforcing are important aspects of its system, providing a strong motivation to permit such monitoring by conveying the conditions to the server in the request where they could be incorporated into the virtual key. *Id.*; Ex. 1004, ¶¶40-43 (describing monitoring and enforcing restrictions). Monitoring and enforcement increases reliability and efficiency of the rental system. A POSITA would have had a reasonable expectation of success in including the reservation condition with the request by using well-known network APIs and/or data structures to include multiple data in a single transmission. Ex. 1003, ¶123.

(b) 1[b]

As discussed above, Kleve discloses or renders obvious a server that generates a virtual key (*e-key*) and assigns to it the rental agreement restrictions (*condition of use of the vehicle*), including the rental period. Ex. 1003, ¶124.

(c) 1[c]

As discussed above for the limitation “the request includes identifying information for enabling sending of the e-key to the recipient,” Kleve discloses

transmitting, by the server, the e-key to the recipient using the identifying information, and specifically to the Temporary User’s nomadic device (*device of the recipient*). See, e.g., Ex. 1004, ¶¶62-63.

Kleve further discloses that Temporary User’s device receives the virtual key for vehicle access, *i.e.*, the device ***is implemented to use the e-key***. Ex. 1003, ¶¶125-26. For example, Kleve discloses that the “virtual key may be sent in an encrypted message to the... Temporary User’s nomadic device” and that “the Temporary User may use their virtual key credential to access the vehicle.” Ex. 1004, ¶¶63, 67.

(d) 1[d]

Kleve discloses that the server transmits a copy of the virtual key ***to the vehicle to allow use of the vehicle via the virtual key*** when presented by the Temporary User. Ex. 1003, ¶127. Kleve discloses that the “virtual key may be sent to the vehicle allowing Temporary User access to the Owner’s vehicle.” Ex. 1004, ¶¶62, 59, 66-69. As discussed for limitation “electronic key (e-key) for an identified recipient to use the vehicle,” Kleve discloses the virtual key allows vehicle access and use.

(e) 1[e]

Kleve discloses that the vehicle monitors the Temporary User’s usage of the vehicle with the e-key and transmits the monitoring data to the server. Ex. 1003, ¶128. For example, Kleve discloses “continuous ***monitoring*** of the Temporary

User's behavior during the rental period [*i.e.*, ***when the vehicle is used via the e-key***] may be ***transmitted to the server***" including transmitting "GPS data . . . to the server." Ex. 1004, ¶76. Kleve discloses monitoring and transmitting to the server the "vehicle speed, acceleration force, wheel speed, breaking, steering, vehicle weight, throttle and pedal position" to determine whether "the Temporary User is using the vehicle under extreme circumstances or if they are driving responsibly." *Id.*, ¶78.

(f) 1[f]

Kleve discloses that monitoring data regarding vehicle use is used to identify violations of the restrictions (***condition of use***). Ex. 1003, ¶¶129-30. Kleve discloses that the monitoring data includes ***information regarding use of the vehicle and identifies a violation*** such as "***unauthorized*** objects or cargo, ***unauthorized*** driving behavior, ***unauthorized*** driver, and/or an ***unauthorized*** trailer tow." Ex. 1004, ¶76; ¶40 ("[T]he control parameters use restrictions may be monitored and if a restriction exceeds a limit the Temporary User and Owner may be notified."). The monitoring data described above indicates whether "the Temporary User is using the vehicle under extreme circumstances or if they are driving responsibly." *Id.*, ¶78.

Kleve explains that, "if a restriction exceeds a limit the Temporary User and Owner may be notified" (*id.*, ¶40), which "allow[s] the Owner continued control of the vehicle with the use of vehicle ***restriction limits*** initially set by the Owner at the

beginning of the rental term” (*id.*, ¶43). *Id.*, ¶53. Kleve’s “restriction limits” may be based on, e.g., “speed, global position coordinates, or load weight restrictions.” For example, “[i]f the Temporary User enters a restricted area, he may be notified by the system and the vehicle may enter a remedial actions limiting vehicle speed.” *Id.*, ¶41. As a separate example, Kleve also uses the monitoring data to enforce the “end time restriction” by determining if the vehicle is still in use as the end of the rental period. *Id.*, ¶43; Ex. 1003, ¶129.

(g) 1[g]

“wherein the server processes logic for generating the e-key and processes logic for analyzing the data regarding use of the vehicle when the e-key is used for the vehicle”: As discussed above, Kleve discloses or renders obvious that the server generates the e-key (1[b]) and analyzes vehicle use data (1[f]). This limitation further requires ***logic processing*** that performs those functions. Kleve discloses “a computer readable storage medium for storing instructions that, when executed by a processor is configured to enable a vehicle rental transaction.” Ex. 1004, ¶9. A POSITA would have understood and considered it obvious that, the “instructions” refer to ***logic*** processed in the server for generating an ekey and analyzing data regarding vehicle use. Ex. 1003, ¶¶131-34. Kleve discloses that the server is a “remote computing system,” which a POSITA would understand to include CPU and memory, and performs functions by ***logic processing***, that is, executing CPU

instructions. *Id.* A POSITA would also consider it obvious that a “server” or “remote computing system” performs its disclosed functions using ***logic processing*** because that was the well-known and conventional means for a computer to perform functions. *Id.*, ¶135. A POSITA would find it beneficial and have had a reasonable expectation of success in using a general-purpose computer (with CPU to execute instructions) for a server because of the commodification of computer hardware and software, making such systems significantly cheaper and easy to access. *Id.*

“the server or other servers connected to the server being accessible over the Internet”: Kleve discloses that the server system (including the website and database) are accessible over the Internet. For example, Kleve discloses that data to a server is “sent over the internet.” Ex. 1004, ¶58. Kleve also discloses that the server and the owner or Temporary User’s devices (cell phones) can communicate via a “website,” *i.e.*, the Internet. *Id.*, ¶¶36, 30, 56; Ex. 1003, ¶136.

“the vehicle having wireless communication systems for communicating with the server or other servers and for communicating with devices local to the vehicle”: Kleve discloses that a Vehicle Owner’s vehicle wirelessly communicates with a server and a Temporary User’s device (***devices local to the vehicle***). *Id.*, ¶137. For example, with respect to the server, Kleve discloses that the “vehicle computing system located in a vehicle” communicates with “a remote computing system (e.g., and without limitation, a ***server***) connected through [a] ***wireless***

device.” Ex. 1004, ¶¶35, 28 (“onboard modem 63”). With respect to **devices local to the vehicle**, Kleve discloses that the vehicle has a “BLUETOOTH transceiver” which “allow[s] communication with the nomadic device” such as “the Temporary User’s nomadic device... using a wireless connection.” *Id.*, ¶61. Kleve also discloses that “the Temporary User’s nomadic device may be paired with the VCS.” *Id.*, ¶72.

2. Claim 2

Kleve discloses that when a Temporary User violates a rental agreement restriction (**condition of use**), the system will provide a warning notification to the Temporary User or vehicle. Ex. 1003, ¶138. Specifically, Kleve discloses that “the control parameters use restrictions may be monitored and if a restriction exceeds a limit **the Temporary User** and Owner may be notified,” such as “[e]mail notification, text messages or **an in-vehicle display message.**” Ex. 1004, ¶40. For example, Kleve discloses that, if “the rental period is soon to expire,” the system may notify the Temporary User and Vehicle Owner. *Id.*, ¶54.

3. Claim 3

As discussed above in 1[a], Kleve discloses the limitation “receiving, by a server, a request from a user via a user account... to generate an electronic key,” and further discloses that the request is made via the Vehicle Owner’s user profile (**user account of an owner of the vehicle**). Ex. 1004, ¶62; Ex. 1003, ¶139.

4. Claim 4

Kleve discloses that the Temporary User (**recipient**) is notified of the rental period expiration (**violation of the condition**), which disables the e-key. Ex. 1003, ¶¶140-41. Specifically, “if a restriction exceeds a limit the Temporary User and Owner may be notified.” Ex. 1004, ¶40. These notifications may be sent “through the website, with an email notification, or on the Owner's nomadic device at step 220.” *Id.* Further, warning notifications are sent to the user and owner. *Id.*, ¶53. Kleve further discloses terminating the virtual key if the vehicle detects usage after the rental period expires, and also providing notification thereof. *Id.*, ¶¶54-55.

Kleve also discloses that the system may “warn and induce remedial actions” in response to a violation. *Id.*, ¶54. Remedial actions include “preventing the vehicle from being started [i.e., **disabling the ekey**].” *Id.*, ¶53, 41-42.

A POSITA would have understood ” Kleve’s “preventing the vehicle from being started” to be implemented by **disabling the e-key**, since that is the mechanism for starting the vehicle is enabled. Further, a POSITA would have understood that it is preferable to allow the Owner to start the vehicle while preventing the Temporary User. Ex. 1003, ¶143 (citing Ex. 1004, ¶45).

5. Claim 5

As discussed above for the limitation “condition of use of the vehicle as set by the user via the user account,” the Vehicle Owner and Temporary User may

negotiate a “rental period” (*time frame of use / time expiration of use*), “speed” (*speed restriction*), and “global position coordinates” or “prohibited areas” (*geographic restriction*). Ex. 1004, ¶¶38, 40, 51, 73; Ex. 1003, ¶144.

6. Claim 6

As discussed above for the limitation “the request includes identifying information,” Kleve discloses that the request includes *identifying information* such as *an email address*. Ex. 1004, ¶39; Ex. 1003, ¶145.

7. Claim 7

As discussed above for limitations 1[e] and 1[f], the received use data includes “GPS data” (*history of where the vehicle has been*), “vehicle speed” (*speeds of the vehicle*), or various “unauthorized” behaviors (*multiple violations of the condition of use*). Ex. 1004, ¶¶76, 78; Ex. 1003, ¶146.

8. Claim 8

As discussed above for claim 2, Kleve discloses that the system will send a warning to the vehicle or device of the recipient when use of the vehicle has violated a restriction (*exceed the condition of use*). Ex. 1004, ¶40 (“the control parameters use restrictions may be monitored and if a restriction exceeds a limit *the Temporary User* and Owner may be notified,” such as “[e]mail notification, text messages or *an in-vehicle display message*”); Ex. 1003, ¶147.

9. Claim 9

As discussed above for the limitation “electronic key (e-key) for an identified recipient to use the vehicle,” Kleve discloses that the virtual key (***e-key***) allows the Temporary User to “access the vehicle” (***opening the vehicle***) and “enable the vehicle drive away event” (***starting the vehicle***). Ex. 1004, ¶¶67, 44; Ex. 1003, ¶148.

10. Claim 11

(a) 11[a]

Kleve’s Temporary User’s device is a “***cell phone, smart phone, PDA.***” Ex. 1004, ¶¶63, 25; Ex. 1003, ¶149.

(b) 11[b]

Kleve discloses that once the Temporary User’s device uses the virtual key, the “virtual key may terminate,” *i.e.*, the key is deactivated and ***cannot be used via another device or sent to another device.*** Ex. 1004, ¶49; Ex. 1003, ¶150-52.

The virtual key is unique to the Temporary User’s device. Ex. 1004, ¶62. Kleve creates the virtual key after agreement between Vehicle Owner and Temporary User and sends it “to the vehicle allowing Temporary User access to the Owner’s vehicle.” *Id.*, ¶63. Thus, because Kleve grants the *Temporary User* access (and no one else) the virtual key is tied to the agreement and the Temporary User’s identification, and cannot be used by another device. Because the virtual key is verified by the vehicle by confirming the Temporary User’s credentials, the virtual key cannot be used ***without receiving new data from the server to reactive the e-***

key, specifically, updated credentials reflecting the new device. *Id.*, ¶¶67-68; Ex. 1003, ¶152.

Alternatively, a POSITA would have found it obvious to restrict the virtual key to a specific device upon first use of the virtual key. Ex. 1003, ¶¶153-54. A POSITA would be motivated to do this because by not restricting the key until first use, a Temporary User may choose which device will operate the e-key, improving flexibility and user experience. *Id.* Restricting the key to the specific device after first use increases security, as it prevents the e-key from being stolen. *Id.* A POSITA would also consider it obvious to allow for a Temporary User to transfer the e-key to a different device, after which it must be reactivated (such as by resending the Temporary User's credentials to authorize the Temporary User). *Id.* This provides the benefit of flexibility and better user experience without decreasing security. *Id.*

A POSITA would have reasonably expected such a modification to succeed because it was well within the skill of an ordinary artisan to restrict a virtual key to a specific device such as by associating the virtual key with the unique identifier or properties of the specific device and disallowing any usage of the virtual key by any device that does not match the unique identifier or properties. *Id.*

11. Claim 12

As discussed above in claim 1, Kleve discloses ***requests to generate e-keys for the vehicle*** where the ***e-keys that are generated are associated with the user***

account, with the Vehicle Owner's user profile (*user account*) **being used for making the requests to generate the e-key or e-keys**. Ex. 1003, ¶¶155-56.

Kleve discloses that **a plurality** of e-keys may be requested. Ex. 1003, ¶157. Kleve discloses that “generat[ing] and deliver[ing] **virtual keys** to the Temporary User.” Ex. 1004, ¶48. Since e-keys are specific to a Temporary User, the Vehicle Owner's user profile must request multiple e-keys for multiple Temporary Users, since the users are **Temporary** Users that use the vehicle for a **rental period**, *i.e.*, multiple Temporary Users can rent the vehicle for different rental periods. *Id.*, ¶74 (“once the schedule rental is complete the virtual key may be terminated, allowing the vehicle to be secured for... the **next temporary user scheduled to use the vehicle**.”). The virtual key is generated after the Temporary User and Vehicle Owner sign a rental agreement (*id.*, ¶39), and thus a Vehicle Owner with multiple agreements results in multiple virtual keys. Kleve discloses a process where “the Owner and Temporary User may rate their experience on the website to notify others of their satisfaction each person had during the transaction at step 360,” indicating that the vehicle will to be rented to different Temporary Users, requiring multiple requests for virtual keys. *Id.*, ¶55.

Kleve further discloses that **any one of the generated e-keys are removable from being active via the user account**, specifically that “once the Temporary User has completed the rental period and returned the vehicle to the appropriate drop off,

the virtual key may terminate allowing the system to reset any private information stored on the vehicle-based computing system.” *Id.*, ¶49. The virtual key is terminated, *i.e.*, *removed from being active, via the user account* because the Vehicle Owner’s user profile defines the rental period through the rental agreement and to which the virtual key is associated, and thus upon expiration of the rental period, the virtual key’s termination requires deactivation via the user account. Ex. 1003, ¶158.

A POSITA would have also considered it obvious that *any one of the generated virtual keys are removable via the user account* in order to facilitate, for example, cancellations by the Vehicle Owner. Ex. 1003, ¶159. A POSITA would be motivated by the well-known benefit of allowing flexibility for Vehicle Owners to cancel rentals if appropriate. *Id.* For example, if the vehicle is damaged and needs to be repaired, it would be desirable to allow the Vehicle Owner to cancel any rental agreements (and therefore associated virtual keys) until the vehicle can be repaired or a replacement obtained. *Id.* A POSITA would have reasonably expected such a modification to succeed because it would simply involve providing a mechanism for cancellation of rentals, such as a button within an app that sent a request to the server for cancellation—a simple change well-within the abilities of a POSITA. *Id.*

12. Claim 13

(a) 13[a]

Kleve discloses that the vehicle has a “BLUETOOTH transceiver” to communicate with “the Temporary User’s nomadic device” during use of the virtual key. Ex. 1004, ¶61. A POSITA would understand that the Bluetooth connection requires that the device be within communication distance of the vehicle. *See* Ex. 1004, Abstract (“A vehicle computing system includes a processor programmed and configured to establish communication with a wireless device **brought into proximity of a vehicle.**”). Thus, the vehicle is always receiving data indicative of the Temporary User’s device being within communication distance of the vehicle. Ex. 1003, ¶160.

(b) 13[b]

Kleve discloses that the virtual key is terminated after the Temporary User has “returned the vehicle to the appropriate drop off.” Ex. 1004, ¶55. A POSITA would understand that detecting that the Temporary User has performed the drop off ideally requires determining that the Temporary User is no longer in proximity to the vehicle—walking away indicates the Temporary User has given up possession of the vehicle (*e.g.* no longer present in the vehicle or unloading the vehicle), and can now be safely locked. Ex. 1003, ¶161. A POSITA would thus consider it obvious to perform proximity detection by sending data indicating that the device is not within, for example, Bluetooth communication distance of the vehicle. *Id.* This could be easily achieved by sending to the server an indication that the Temporary

User's device is no longer connected to Bluetooth, after which the server can terminate the virtual key per the drop off procedure. *Id.* Alternatively, it also would have been obvious to track the Temporary User's device location to determine proximity to the vehicle. *Id.* A POSITA would be motivated to perform proximity detection to allow for easy drop off procedures that does not require the Temporary User to do anything beyond park the vehicle and walk away. *Id.* This would improve the user experience.

(c) 13[c]

As discussed above for limitation 1[e], Kleve discloses that the Temporary User's use of the vehicle with the virtual key is monitored to ensure compliance with the restrictions in the rental agreement. Ex. 1003, ¶162.

13. Claim 14

As discussed above for limitation 1[a], Kleve discloses a request to generate a virtual key is made using a rental agreement. Ex. 1004, ¶47. Kleve further discloses that the rental agreement can be made ***using a selectable template having a set of privileges associated with the virtual key.*** Ex. 1003, ¶163. For example, Kleve discloses selecting a “standard rental agreement form” or “a custom form based on the type of use the Temporary User is requesting to use the vehicle for.” Ex. 1004, ¶38. A POSITA would understand that a these forms are a ***template having a set of privileges***, such as maximum vehicle speed, restricted vehicle

location, use for a specified time period or other standard usage for a vehicle. Kleve discloses that “[t]he Owner may create a standard rental agreement” with preset privileges or “develop a custom form based on the type of use the Temporary User is requesting to use the vehicle for,” such as “mov[ing] furniture.” *Id.*

14. Claim 15

As discussed above for claim 14, Kleve discloses “a **custom form** based on the type of use the Temporary User is requesting to use the vehicle for.” Ex. 1004, ¶38. A POSITA would understand that the custom form is a **custom template** based on various types of usage. Ex. 1003, ¶164.

15. Claim 16

Limitations 16[pre]-16[f] are identical to limitations 1[pre]-1[f], respectively. Limitation 16[h] is identical to claim 9. Thus, Kleve discloses or renders obvious those limitations for the same reasons as set forth above. Ex. 1003, ¶165.

(a) 16[g]

Kleve discloses that the virtual key (**e-key**) “may be sent in an **encrypted message**.” Ex. 1004, ¶63. An encrypted message is **configured for decryption** because the message could not be readable without decryption. For example, Kleve discloses that the virtual key could be a “matrix barcode (ex. two-dimensional code)” to be scanned by the vehicle. Ex. 1004, ¶44. A POSITA would understand an encrypted matrix barcode is unusable until it is decrypted. Ex. 1003, ¶166. A POSITA would have also considered it obvious to decrypt the encrypted message

since encryption-decryption mechanisms were well-known and implementation of such was within the skill of a POSITA. *Id.*

As discussed in limitation 1[a], the virtual key (*e-key*) enables use of the vehicle.

16. Claim 17

“receiving, by the server, data from the vehicle being indicative of interface inputs or settings made during use with the e-key”: Klevé discloses that the vehicle “monitor[s] the... vehicle location.” Ex. 1004, ¶73. Location data is “transmitted to the server.” *Id.*, ¶76.

Klevé discloses that “frequent destinations” are a vehicle “setting[.]” *Id.*, ¶50. Thus, a location (which is transmitted to the server) in the form of frequent destinations is ***indicative of settings made during use with the e-key***. Ex. 1003, ¶¶168-70.

“the inputs or settings being examined to identify patterns; and learning the patterns, by a process executed by the server”: Klevé discloses that the server provides “stored frequent destinations sent to the [vehicle].” Ex. 1004, ¶50. A POSITA would have considered “frequent destinations” to be a ***learned, identified pattern***. Ex. 1003, ¶171. A POSITA would have also considered it obvious for the server to identify patterns in the vehicle location data to learn frequent destinations. *Id.* A POSITA would have been motivated to provide renters the convenience of

having favorite destinations for car rental. *Id.* A POSITA would have reasonably expected such a modification to succeed because it merely uses GPS locations to determine visited locations, well-within a POSITA's skill. *Id.*

“to provide recommendations to the recipient or to an account of the recipient, for settings that should or may be made to the vehicle when using the e-key”: Kleve discloses that a Temporary User may have “vehicle preset settings applied when renting a vehicle” such as “stored frequent destinations.” Ex. 1004, ¶50. A POSITA would understand that “frequent destinations” are a ***recommendation to the recipient*** for destinations the recipient may want to visit again. Ex. 1003, ¶172.

17. Claim 18

(a) 18[a]

As discussed above for the limitation “the request includes a condition of use of the vehicle,” Kleve discloses privileges associated with the virtual key (***e-key***), such as vehicle access and use for a period of time. Ex. 1004, ¶38-42; Ex. 1003, ¶173.

(b) 18[b]

Kleve discloses that the Temporary User (***recipient***) may request extending the rental period through the user's device. For example, Kleve discloses that if the “rental period may expire soon,... the system may allow the Temporary User to

purchase additional rental time... with the use of... a nomadic device [***device of the recipient***].” *Id.*, ¶43; Ex. 1003, ¶174.

18. Claim 19

Limitations 19[pre]-19[f] are identical to limitations 1[pre]-1[f], respectively. Limitation 19[h] is identical to claim 9. Thus, Kleve discloses or renders obvious those limitations for the same reasons as set forth above. Ex. 1003, ¶175.

(a) 19[g]

“wherein the e-key received at the device of the recipient includes data to inform the recipient of a level of monitoring that is to occur of the vehicle when the e-key is used for the vehicle”: As discussed above in limitation 1[e], Kleve discloses monitoring various uses of the vehicle. A POSITA would have considered it obvious to include with the virtual key (***e-key***) a notification to the Temporary User (***recipient***) about the ***level of monitoring*** that will occur. Ex. 1003, ¶177. Indeed, a POSITA would understand that such level of monitoring will be disclosed in the rental agreement between the Vehicle Owner and Temporary User, not least because local privacy laws may require such monitoring to be disclosed in advance. *Id.* In any case, a POSITA would have considered it obvious to inform the Temporary User of such monitoring, because it will encourage the Temporary User to use the vehicle within the agreed-upon restrictions, and would have expected to

succeed in doing so since, as discussed above, providing notifications could be easily accomplished using conventional, well-known third-party systems. *Id.*

“wherein a log is made to save the use of vehicle to a cloud storage, or storage of the vehicle or both, the log including one or more of driving data that took place, or where the vehicle was driven, or speeds of the vehicle, or damage of the vehicle, or radio stations listened to, or conversations had, or images of drivers during specific times, or combinations to two or more thereof”: As discussed above for limitations 1[e] and 1[f], Kleve discloses monitoring and uploading data that includes ***where the vehicle was driven*** and ***speeds of the vehicle***. Ex. 1004, ¶¶76, 78, 80. Kleve further discloses that such data is ***saved to a cloud storage or the vehicle***. For example, the data is “transmitted to either the server... or saved on a storage device for later download.” *Id.*, ¶78. In addition, because the “Vehicle Owner may review monitored data at a given time throughout the rental period,” a POSITA would understand that the data is saved on the server (***cloud storage***) for review by the Vehicle Owner. *Id.*; Ex. 1003, ¶178.

19. Claim 20

(a) 20[a]

As discussed for claim 12, Kleve discloses or renders obvious generating a plurality of virtual keys (***e-keys***) that co-exist, such as generating virtual keys for

different Temporary Users for different rental periods. Ex. 1003, ¶179; Ex. 1004, ¶¶44, 69.

(b) 20[b]

Kleve discloses that a virtual key is only active for the specified rental period. Kleve discloses one key per user and one user per rental period. Ex. 1004, ¶39 (“The virtual key may also be sent to the vehicle configuring the VCS to enable the keyless drive system for the appropriate Temporary User *during a given rental period.*”); ¶49 (“Once the Temporary User has *completed the rental period* and returned the vehicle to the appropriate drop off, *the virtual key may terminate* allowing the system to reset any private information stored on the vehicle-based computing system.”). Thus, when there are multiple virtual keys for different users and rental periods, only one virtual key is active at one time. Ex. 1003, ¶180.

B. Ground 2: Kleve and Sekiyama

To the extent that PO argues Kleve’s server does not generate e-keys, a POSITA would have considered that obvious in view of Sekiyama. Ex. 1003, ¶¶181-82.

1. Motivation to Combine

A POSITA would have been motivated to combine Kleve’s system with Sekiyama’s teaching of a server that generates an e-key to unlock and start a vehicle. See Ex. 1005, ¶¶18, 26.

There were well-known benefits of centralizing e-key generation, including better security and reliability. Ex. 1003, ¶183. In Kleve, generating the key requires that the Vehicle Owner enter “authorization credentials” from the Temporary User, and the server stores the Temporary User’s user profile containing those credentials (e.g. “photo of forms of ID,” etc.) to confirm the Temporary User’s identity. Ex. 1004, ¶¶62, 37. As Dr. Almeroth explains in detail, POSITA would be motivated to have the server generate the key since it can confirm Vehicle Owner’s account sent the request, confirm the identity of the Temporary User, and confirm a rental agreement between them. Ex. 1003, ¶183. Having the server centrally confirm all necessary information before issuing a key increases security and reliability. *Id.*

A POSITA would have a reasonable expectation of success. *Id.*, ¶184. Having Kleve’s server generate a key would have been well-within the capabilities of a POSITA. *Id.* Since Kleve already discloses a mechanism for generating a key and discloses that the server transmits the key to the Temporary User and vehicle, there would be a reasonable expectation of success for having the server perform that mechanism. *Id.*

Kleve, Sekiyama and the ’188 patent are all directed to the same field of electronic key systems. See Ex. 1001, Abstract; Ex. 1004, ¶48; Ex. 1005, ¶26; Ex. 1003, ¶185.

2. 1[b]

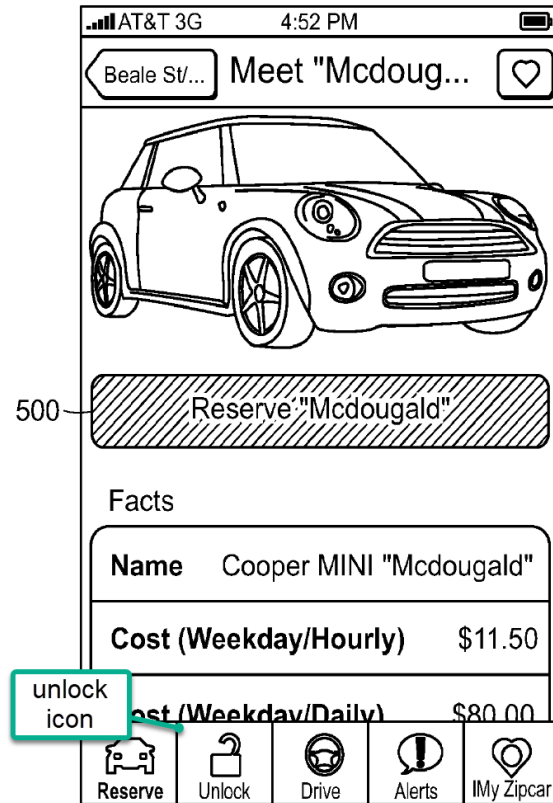
Sekiyama discloses a server that generates an e-key. Ex. 1005, ¶25 (“an electronic key [is] output from the center server 20.” This key performs “door lock locking / unlocking” and “engine start permission.” *Id.*, ¶18. It would have been obvious to modify Kleve such that the server generates the e-key, to the extent it does not already do so. Ex. 1003, ¶¶186-87.

3. 1[g]

Sekiyama discloses the server processes logic for analyzing the data regarding use of the vehicle when the e-key is used for the vehicle. *Id.*, ¶¶21-23 (“[Server’s] vehicle status monitoring unit 22 acquires information related to the vehicle status of the vehicle 40 based on signals outputted from the vehicle 40.”). It was obvious to include a monitoring unit in Kleve to perform logic processing. Ex. 1003, ¶¶188-189.

C. Ground 3: Kleve (optionally with Sekiyama) and Mottla (Claim 10)

Mottla discloses a GUI with “an unlock icon” for remotely “unlock[ing] the vehicle doors,” thereby disclosing claim 10. Ex. 1010, ¶33; Fig. 5.



Incorporating this icon into Kleve (with or without Sekiyama) enabled by the e-key was obvious. Ex. 1003, ¶¶190-92. As Dr. Almeroth explains in detail, a POSITA would be motivated by the benefits of a user-friendly GUI, as on-demand unlocking via icon gives the user better control over vehicle access, and using an unlock icon (instead of text) is more user-friendly. *Id.* A POSITA would have also been motivated to allow the Temporary User on-demand control of locking/unlocking instead of unlocking the vehicle upon scanning of the virtual key—that would allow a Temporary User to use the unlock icon after the virtual key has been scanned and authorized, providing a better user experience while maintaining security. *Id.*, ¶191. A POSITA would have a reasonable expectation of

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

Kleve, Mottla, and the '188 patent are all directed electronic key systems. Ex. 1010, Abstract; Ex. 1001, Abstract; Ex. 1004, ¶48; Ex. 1003, ¶193.

D. Ground 4: Zaid and Harris

Zaid discloses a system where vehicle owners list vehicles for renters via social media accounts. When the owner accepts a renter's request, the server encrypts the reservation (an e-key) and sends it to the user's device for vehicle access and control. (Ex. 1003, ¶¶92-97, 194)

To the extent PO argues that Zaid fails to disclose that the e-key request contains the renter's identifying information, or that the encrypted vehicle reservation is not an e-key, such limitations were taught in Harris. Ex. 1003, ¶195.

1. Motivation to Combine

A POSITA would have been motivated to modify Zaid with Harris's generating e-keys following authentication of a user. Ex. 1003, ¶¶196-202.

Harris teaches a server distributing e-keys for cars. Ex. 1009, ¶¶38-41. A temporary user "identifies themselves to a server," "[t]he server recognizes the credentials," and grants "a new key" used to "start the vehicle." *Id.*, ¶40. The key is a "unique" "code" such as "a 2048 byte number." *Id.*, ¶¶33, 37-38.

Incorporating these teachings into Zaid had the well-known benefits of better security and user experience, as Dr. Almeroth explains in detail. Ex. 1003, ¶198. Requiring a user to authenticate themselves ensures the user’s identity, increasing security. A POSITA would understand the importance of ensuring any recipient of a key (for a high-value asset like a vehicle) is properly authenticated as someone with permission. This provides a better user experience for the vehicle owner, including peace of mind.

A POSITA would have also known the benefits of a code-based key. Ex. 1003, ¶199. Harris explains a code-based key is used to “match[] to one or many codes within the automobile” only after which a car “can be accessed; and the engine can be started.” Ex. 1009, ¶33. A POSITA would have known that code matching requires less time and processing power than decryption of a vehicle reservation as taught in Zaid. This increases efficiency and allows for quicker access to a vehicle.

In view of the above, a POSITA would have—based on Harris’s teachings and the POSITA’s knowledge—modified Zaid to include a renter’s identifying information with an e-key request for the server to authenticate the renter, and then generate a key code accompanied with the encrypted reservation sent to the renter’s device. Ex. 1003, ¶200. Zaid’s server also provides the code to the rental vehicle. Thus, matching the key code grants vehicle access, while the reservation is decrypted to determine the conditions of use. Alternatively, as taught in Harris, the key code

itself can embed the conditions of use, such as a key being “limited in time and usable for only 3 to 15 minutes” or “one ride.” Ex. 1009, ¶¶39-40. This is suitable for Zaid, since Zaid similarly discloses “a specified time period” as a condition of use. Ex. 1008, ¶69.

A POSITA would have had a reasonable expectation of success. Providing identifying information for authentication, and the use of key codes, had long been in use and implementation was within the capabilities of a POSITA. Ex. 1003, ¶201.

Zaid, Harris, and the ’188 patent are all directed to the same field of electronic key systems. See Ex. 1001; Ex. 1008, Abstract; Ex. 1009, ¶33; Ex. 1003, ¶202.

2. Claim 1

(a) 1[pre], 1[a]

“receiving, by a server, a request from a user via a user account that has a vehicle associated therewith to generate an electronic key (e-key) for an identified recipient to use the vehicle”: Zaid discloses or renders obvious a vehicle owner (**user**) that can use a **user account** (such as through Facebook) to facilitate a vehicle rental reservation that causes the server to generate an encrypted reservation (**e-key**) to allow an identified user (**identified recipient**) to use the owner’s vehicle. Ex. 1003, ¶¶203-14.

“server”: Zaid discloses that “the received vehicle reservation is booked at a central **server** via a user interface displayed on a computing device.” Ex. 1008, ¶72.

It is through this central server that the rental user's device will receive an encrypted reservation (*e-key*). *See, e.g., id.*, ¶125.

“user account that has a vehicle associated therewith”: Zaid discloses that a vehicle owner can list a vehicle for rental on the vehicle reservation application. Ex. 1008, ¶77 (“[A] vehicle reservation application... enables a vehicle... owner... to... advertise... the vehicle will be available for sharing.”). A POSITA would understand that the listing of the vehicle is associated with a user account belonging to the vehicle owner. Ex. 1003, ¶206. Zaid already discloses that the vehicle reservation application can be accessed “through... social networking websites, such as... Facebook®,” that the user logs into. Ex. 1008, ¶72. A POSITA would understand that the vehicle owner accesses the reservation application via such an account so the application can associate a vehicle with the correct person in order to, for example, allow the owner to “update the server(s) (e.g., online vehicle reservation system) of various vehicle related information such as vehicle availability and vehicle location.” *Id.*, ¶79; Ex. 1003, ¶206. A POSITA would further understand that an account is required to facilitate rental payments or confirm insurance. *Id.*

A POSITA would alternatively consider it obvious for an owner to access the rental application through a user account to associate their vehicle with the account, providing the known benefit of increasing security and improving the vehicle owner

experience. *Id.*, ¶207. For example, allowing a vehicle owner to create an account would provide a mechanism for the application to confirm the identity of the vehicle owner, confirm ownership status, and the presence of insurance. *Id.* It would also improve the owner’s user experience, allowing him to, *e.g.*, receive payment for the rental and have centralized vehicle information and history. *Id.* In addition, a POSITA would have a reasonable expectation of success because Zaid’s system already supports social media accounts and implementation would simply be a matter of requiring a vehicle owner to use a user account before offering vehicles for rental. *Id.*

“*identified recipient*”: Zaid discloses that the rental user is an ***identified recipient*** by identifying him or herself when accessing the “central server” “through one or more social networking websites, such as FourSquare® and Facebook®,” where the “user must first log into the social networking website before he/she can view the advertisement and make reservation.” Ex. 1008, ¶72. A POSITA would understand that by logging in through a social networking website, the user has identified him or herself and is therefore an ***identified recipient***. Ex. 1003, ¶208.

In addition, Harris teaches that “the [renter] identifies themselves to a server” which “recognizes the credentials... and allows the user to get a new key.” Ex. 1009, ¶40. As discussed above, a POSITA would have been motivated to incorporate this teaching into Zaid. Ex. 1003, ¶209.

“receiving, by a server, a request from a user via a user account... to generate an electronic key”: Zaid discloses that the server receives a vehicle reservation (**request**) which results in generating an encrypted reservation (**e-key**). Specifically, Zaid states that a “vehicle reservation is booked by a user at a **central server**,” after which “the central server encrypts the message containing the vehicle reservation.” Ex. 1008, ¶125. A POSITA would understand that the vehicle reservation request is sent to the server from the owner’s user account, because the owner advertises when the vehicle is available for reservation, and the owner has “control over the type of user the owner is lending/sharing/renting vehicle to.” Ex. 1008, ¶¶72, 77, 79; Ex. 1003, ¶210. Thus, Zaid discloses the owner decides whether a reservation will proceed—a POSITA would therefore understand that the reservation request to the server comes from the owner through the owner’s account. *Id.*

In the alternative, a POSITA would have found it obvious that the reservation request is sent by the owner through the owner’s account. Ex. 1003, ¶¶211-12. Since both the renter and the owner accounts are involved in making the reservation, whether the reservation request is sent by the renter or the owner is a mere design choice—the system can handle the request regardless of the source. *Id.* Moreover, a POSITA would have been aware of the known benefits of having the owner account send the request, because that allows the owner greater control over which renters are allowed to reserve the vehicle, especially in view of Zaid’s teachings that

“a tracking mechanism can be established to track group member driving history and reputation and allow the vehicle owner to have better control over the type of user the owner is lending/sharing/renting vehicle to.” Ex. 1008, ¶172. Since the owner is also the one bearing the risk of vehicle loss, it would be advantageous to have the owner send the request to ensure that the owner has truly consented to the reservation. Ex. 1003, ¶212. A POSITA would have a reasonable expectation of success in having the owner’s account send the request, because that is a mere design choice using conventional networking APIs and coding practices well within the capabilities of a POSITA. *Id.*

“*electronic key (e-key) for an identified recipient to use the vehicle*”: Zaid discloses that the encrypted reservation is an **e-key** that is sent to the recipient to allow **use of the vehicle**. Ex. 1003, ¶213. Specifically, Zaid teaches that “the central server encrypts the message containing the vehicle reservation” and then “communicated to a wireless communication device of the user [*i.e.*, **identified recipient**].” Ex. 1008, ¶¶125-26. The reservation is used to grant “vehicle access” to the recipient, which includes “opening the vehicle door, and/or allowing engine to be turned on by the user,” *i.e.*, **use of the vehicle**. *Id.*, ¶129.

In addition, Harris teaches the generating of a “key” in the form of a “code” such as “a 2048 byte number,” where “[i]f the code on the key matches to one or many codes within the automobile, then the car systems can be accessed; and the

engine can be started.” Ex. 1009, ¶33. This key is generated by a server after a user authenticates themselves. *Id.*, ¶40. As discussed above, a POSITA would have been motivated to combine this teaching with Zaid by generating a code in addition to encrypting the reservation, both of which are sent to the renter’s device for gaining access to the vehicle. Ex. 1003, ¶214.

“the request includes identifying information for enabling sending of the e-key to the recipient via an electronic transmission”: Zaid discloses that the reservation request includes ***identifying information about the recipient***, such as information about their social networking account in order to allow the vehicle owner to track the user’s “driving history and reputation.” Ex. 1008, ¶72. Such information enables sending of the e-key to the recipient because it “allow[s] the vehicle owner to have better control over the type of user the owner is lending/sharing/renting vehicle to.” *Id.*; Ex. 1003, ¶215.

In addition, the reservation request contains a reservation which a POSITA would understand to have ***identifying information about the recipient*** because the reservation originates with the recipient’s account, and the resulting encrypted vehicle reservation is sent to the recipient following the owner’s request. Ex. 1008, ¶72 (“[T]he received vehicle reservation is booked... through one or more social networking websites.”). This allows the encrypted reservation to be routed to the renter’s device. Ex. 1003, ¶216.

In addition, Harris teaches that a user sends to a server identifying credentials, *i.e.*, “the user identifies themselves to a server” and “[t]he server recognizes the credentials.” Ex. 1009, ¶40. As discussed above, a POSITA would have been motivated to combine these teachings with Zaid such that a renter provides identifying credentials to the owner when originating the reservation, and that the owner includes the credentials when requesting the key so that the server can send the vehicle reservation to the renter. Ex. 1003, ¶217.

Zaid teaches that the encrypted reservation is sent as an ***electronic transmission***. Zaid teaches that “the central server encrypts the message containing the vehicle reservation” and then “communicated to a wireless communication device of the user [*i.e.*, ***identified recipient***].” Ex. 1008, ¶¶125-26. Since the communication is encrypted and sent over a wireless network, a POSITA would understand that it is an ***electronic transmission***. Ex. 1003, ¶218.

“the request includes a condition of use of the vehicle as set by the user via the user account”: Zaid states that the reservation request “includes a reservation for a specified time period,” which is ***a condition of use of the vehicle***. Ex. 1008, ¶69. This condition is ***set by the user via the user account*** such as when the owner “announces ***when the vehicle is available for sharing***,” which sets limits on the specific time period for reserving the vehicle. *Id.*, ¶77; Ex. 1003, ¶219.

(b) 1[b]

As discussed above, Zaid discloses or renders obvious that the server generates an encrypted reservation (***e-key***) and assigns it to a rental period restriction (***condition of use of the vehicle***). Ex. 1008, ¶69. In addition, Harris discloses generating a key in the form of a code, including embedding a condition of use such as a period of time. Ex. 1009, ¶¶33, 39 (“one ride”), 40 (“The new key may be limited in time.”). As discussed above, it would have been obvious to incorporate this teaching into Zaid by including the key code with the encrypted reservation. Ex. 1003, ¶220.

(c) 1[c]

As discussed above for the limitation “the request includes identifying information for enabling sending of the e-key to the recipient,” Zaid in view of Harris renders obvious ***transmitting, by the server, the e-key to the recipient using the identifying information***, and specifically to the renter’s device (***device of the recipient***).

As also discussed above, Zaid further discloses that when the renter’s device receives the encrypted reservation (***e-key***), it can be used to access the vehicle, *i.e.*, the device ***is implemented to use the e-key***. Ex. 1008, ¶129. And it would have been obvious to also include Harris’s key code with the encrypted reservation, as discussed in Section VII.D.1. Ex. 1003, ¶¶221-22.

(d) 1[d]

Zaid discloses that the server transmits a decryption key to the vehicle to decrypt the encrypted reservation (**e-key**) which **enables use of the vehicle via the e-key**. *Id.*, ¶223. Specifically, Zaid discloses that “the vehicle access control system... is configured to receive a **server update**” which “includes a new **private key**.” Ex. 1008, ¶81. This private key is used to decrypt the encrypted reservation, which “verif[ies] the authenticity of the wireless communication device is the intended device,” thereby enabling use of the vehicle. *Id.*, ¶128. Harris further discloses transmitting a key code to the vehicle such that it can be matched with the key code of the user’s device. Ex. 1009, ¶33.

To the extent PO argues that the vehicle does not receive the update from the server but instead from the renter’s device, a POSITA would have found it obvious to have the server directly transmit the server update to the vehicle. Ex. 1003, ¶224. Indeed, Zaid expressly discloses an embodiment where “the vehicle access kit additionally includes a long-range mobile communication radio/interface, such as GSM radio, which can be used for **wireless communication to a vehicle reservation or sharing system**.” Ex. 1008, ¶106. Zaid discloses that such wireless communication replaces the communication via the user’s device. *Id.* A POSITA would have found it obvious to combine these embodiments in Zaid such that the “server update” is sent directly to the vehicle using this wireless connection. Ex. 1003, ¶224. A POSITA would be motivated to make this combination because it

would be advantageous to allow the vehicle to receive server updates without requiring proximity to a renter's device. *Id.* As Zaid notes, "cellular and satellite communication service fees can be expensive" (Ex. 1008, ¶16), so by including both direct-to-server communications alongside communications that rely on the user's separately-paid-for mobile device, the vehicle designer optimizes connectivity while minimizing cost. This would ensure that the vehicle is more likely to have the most recent server updates, as the timing of when a renter's device will be in proximity is unpredictable. Ex. 1003, ¶224. Reliability and redundancy would have been important considerations in the design of a vehicle-based system since vehicles have access to different levels of connectivity based on their changing location. *Id.* Reliability is improved since direct-to-server communication does not rely on the user's mobile device to connect, avoiding the possibility of power or service interruptions from the mobile device. *Id.*

The combination would also be an obvious design choice, and would have a reasonable expectation success. *Id.*, ¶225. As the '188 patent acknowledges, communications between vehicle and server, whether or not via a mobile device, were common by 2013. Ex. 1001, 1:47-49; Ex. 1008, ¶106. A POSITA would have easily combined Zaid's server update method with Zaid's transmission of a reservation to the vehicle.

(e) 1[e]

Zaid discloses that, when the renter is operating the vehicle, the server receives “control information” such as “location information” and “vehicle usage information” including “e.g., speed/acceleration, pedal position, air intake, altitude, temperature.” Ex. 1008, ¶¶130, 98; *see also* ¶¶95 (“monitoring acceleration of the vehicle during one or more reservations to provide vehicle usage data”), 99 (“the vehicle usage data and other information are communicated back to the central server.”). Such information is *use data regarding use of the vehicle*. Ex. 1003, ¶226.

(f) 1[f]

Zaid discloses that the received “control information” *identifies information regarding the use of the vehicle*, such as “location information” and “vehicle usage information.” Ex. 1008, ¶130. Zaid further discloses that “vehicle access is withdrawn when the vehicle reservation becomes invalid.” *Id.*, ¶131. Because, as a POSITA would have understood, vehicle use and access must not be revoked while the vehicle is in use (e.g., to prevent collision), Kleve discloses that “a time-out period elapses before vehicle access is withdrawn.” *Id.* Additionally, it would have been obvious to a POSITA to extend this teaching to preventing withdraw of vehicle access or use whenever the vehicle is in use, even if the Temporary User has violated the time period condition of use. This would prevent the vehicle from being deactivated while, *e.g.*, the Temporary User is travelling on the highway, which

could otherwise cause an accident. As described above, Zaid’s system already receives and monitors use data indicative of whether the vehicle is currently traveling (*e.g.*, speed/acceleration). Adding such a safety check to identify whether the Temporary User is still operating the vehicle after the rental period (*i.e.*, a violation of the condition of use) thus would have been a clear and straightforward design choice. Ex. 1003, ¶227.

(g) 1[g]

“wherein the server processes logic for generating the e-key and processes logic for analyzing the data regarding use of the vehicle when the e-key is used for the vehicle”: As discussed above, Zaid discloses or renders obvious that the server generates the e-key and analyzes vehicle use data. A POSITA would have understood that, to perform these functions, the server ***processes logic*** related to those functions, such as execution of CPU instructions. Ex. 1003, ¶¶228-29. Zaid discloses that its teachings “can be implemented in numerous ways, including ***as a process...*** such as a ***processor configured to execute instructions.***” Ex. 1008, ¶13. A POSITA would have understood the “instructions” refer to ***logic processed*** in the server for generating an e-key and analyzing data regarding vehicle use. Ex. 1003, ¶229.

“the server or other servers connected to the server being accessible over the Internet”: Zaid discloses that the server communicates over “the Internet and/or a wireless network, such as cellular network.” Ex. 1008, ¶126; Ex. 1003, ¶230.

“the vehicle having wireless communication systems for communicating with the server or other servers and for communicating with devices local to the vehicle”: Zaid discloses that “the vehicle access kit additionally includes a long-range mobile communication radio/interface, such as GSM radio, which can be used for wireless communication to a vehicle reservation or sharing system (e.g., as another and/or backup network communication channel),” *i.e.*, ***a server***. Ex. 1008, ¶106. As discussed above, a POSITA would have found it obvious to combine this embodiment with the other embodiments taught in Zaid. Ex. 1003, ¶231. Zaid further teaches that the vehicle communicates with a renter’s device in proximity. *Id.*, ¶99 (“[N]earby wireless communication device that has established wireless connection via for example a short-range wireless link with the vehicle access kit.”).

3. Claim 3

As discussed above, Zaid discloses or renders obvious the limitation “receiving, by a server, a request from a user via a user account... to generate an electronic key,” and that the request is via the owner’s user profile (***user account of an owner of the vehicle***). *See, e.g.*, Ex. 1008, ¶77; Ex. 1003, ¶232.

4. Claim 5

As discussed above for the limitation “condition of use of the vehicle as set by the user via the user account,” Zaid discloses that the vehicle reservation can set a condition of use “for a specified time period” and “reservation time slot” (***time frame of use / time expiration of use***). Ex. 1008, ¶69; Ex. 1003, ¶233.

5. Claim 6

As discussed above for the limitation “the request includes identifying information,” Zaid discloses that the request includes ***identifying information*** such as a Facebook account, *i.e.*, ***a social network address***. Ex. 1008, ¶72; Ex. 1003, ¶234.

6. Claim 7

As discussed above for limitations 1[e] and 1[f], the received use data includes “location information” (***where the vehicle has been***), “accident information” (***events of the vehicle***), or “acceleration” (***speeds of the vehicle***). Ex. 1008, ¶¶130, 95; Ex. 1003, ¶¶235.

7. Claim 9

As discussed above for the limitation “electronic key (e-key) for an identified recipient to use the vehicle,” Zaid and Harris disclose that the e-key allows ***opening the vehicle*** and ***starting the vehicle***. Ex. 1003, ¶236.

8. Claim 11

(a) 11[a]

Zaid discloses the “wireless communication device” is a “smart phone.” Ex. 1008, ¶73; Ex. 1003, ¶237.

(b) 11[b]

Zaid discloses that the encrypted reservation (***e-key***) is “decrypted... using a private key of the wireless communication device.” Ex. 1008, ¶99. Only the renter’s device can decrypt the reservation and use the e-key. Ex. 1003, ¶238. Another device cannot decrypt/use the e-key unless it is first re-encrypted by that other device’s public key, *i.e., receiving new data from the server to reactivate the e-key*. *Id.*

9. Claim 12

As discussed above, Zaid discloses or renders obvious ***requests to generate e-keys for the vehicle*** where the ***e-keys that are generated are associated with the user account***, with the vehicle owner’s user profile (***user account***) ***being used for making the requests to generate the e-key or e-keys***.

Zaid discloses that a ***plurality*** of e-keys may be requested from ***time to time***. Zaid’s reservation includes “a specified time period” and “reservation time slot,” which a POSITA would understand to mean a *temporary* usage that can accommodate multiple renters. Ex. 1008, ¶69; Ex. 1003, ¶¶239-40. A POSITA would understand that an owner’s user profile requests multiple encrypted

reservations (e-keys) because multiple renters can rent the vehicle for different rental periods. *Id.*

Zaid further discloses that ***any one of the generated e-keys are removable from being active via the user account.*** Ex. 1008, ¶131 (“vehicle access is withdrawn when the vehicle reservation ***becomes invalid.***”). A POSITA would understand that deactivation is via the owner’s account, because as discussed above, the vehicle reservation (including time-out period) was sent to the server using the owner’s account, and so later deactivation occurs via the same user account transmission. Ex. 1003, ¶241. A POSITA would also consider it obvious to deactivate a user account by owner’s request to facilitate cancellation by the owner, for the same reasons discussed in Ground 1 (and by Dr. Almeroth), which apply to Zaid given its similarities with Kleve in disclosing a vehicle rental/sharing system. *Id.*

10. Claim 13

(a) 13[a], 13[b]

Zaid discloses that “the vehicle reservation becomes invalid [***disable the e-key and prevent use of the vehicle***] when the wireless communication device is removed from the communication range of the vehicle access control system,... removed from physical or wireless communication with the vehicle wireless communication device.” Ex. 1008, ¶131. “[T]he vehicle access control system

periodically communicates with the wireless communication device to verify that the authentic wireless communication device is in communication with the vehicle access control system by verifying the symmetric key of the wireless communication device,” *i.e.*, ***receiving data indicative that the device remains within a communication distance of the vehicle.*** *Id.*; Ex. 1003, ¶242.

(b) 13[c]

As discussed above for limitation 1[e], Zaid discloses that the renter’s use of the vehicle is monitored to ensure compliance with the conditions of the vehicle reservation. *Id.*, ¶243; Ex. 1006, ¶¶130 (“vehicle usage information”), 131 (monitoring “vehicle reservation period”).

11. Claim 14

Zaid discloses two ***selectable templates***: a “vehicle owner” template and a “user template”—each define vehicle access and use ***privileges***, *e.g.*, use for a period of time. Ex. 1008, ¶72. The vehicle owner template reserves “an unlimited time period,” whereas the user template reserves for a limited time period, after which they “become[] invalid.” *Id.*, ¶¶69, 131. Zaid’s time periods are consistent with the ’188 patent’s description of “templates.” Ex. 1001, 48:7-8; Ex. 1003, ¶¶244, 247.

A POSITA would have understood that Zaid’s “vehicle rental application” allows selecting between vehicle owner and temporary user reservation templates, for the purpose of generating a “reservation request” for the proper user, *e.g.* “for

the vehicle owner,” “the ***reservation includes*** an ***unlimited time period for access to the vehicle.***” *Id.*, ¶72; Ex. 1003, ¶245.

Further, it would have been obvious to incorporate templates defining the privileges for use of the vehicle into Zaid’s application. *Id.*. This would have been nothing more than an obvious design choice. As Dr. Almeroth explains, a POSITA “would have easily implemented Zaid’s time slot assignments as templates distinguishing vehicle owners from non-owner users, and be motivated to automate portions of the reservation requests process for improving ease of use.” Ex. 1003, ¶246 (citing Ex. 1008, ¶85).

12. Claim 15

As discussed above for claim 14, Zaid discloses or renders obvious renter and owner templates, which a POSITA would understand to be ***templates customized*** for a renter or owner. Ex. 1003, ¶248. In addition, Zaid discloses that reservations can be “shared among members of a... family,” *i.e.*, ***child or spouse templates*** as a POSITA would understand the reservation template to include information and privileges for sharing a reservation among a family, *e.g.* authenticating a child/spouse and verifying they can drive. Ex. 1008, ¶70; Ex. 1003, ¶248.

13. Claim 16

Claim limitations 16[pre] to 16[f] are identical to limitations 1[pre] to 1[f]. Limitation 16[h] is identical to claim 9. Zaid discloses or renders obvious those limitations for the same reasons as set forth above. Ex. 1003, ¶249.

(a) 16[g]

As discussed above, Zaid discloses an encrypted reservation as an *e-key*. Zaid further discloses that the e-key is decrypted by the vehicle to enable use of the vehicle. Ex. 1008, ¶128; Ex. 1003, ¶250.

14. Claim 18

(a) 18[a]

As discussed above for the limitation “the request includes a condition of use of the vehicle,” Zaid discloses conditions associated with the encrypted reservation (*e-key*), such as a time period for vehicle access/use and time slot. Ex. 1008, ¶69; Ex. 1003, ¶251.

(b) 18[b]

Zaid discloses that the renter’s device can *request removal of a privilege*, specifically “the vehicle reservation becomes invalid when the wireless communications device is removed from the communication range of the vehicle access control system.” Ex. 1008, ¶131; Ex. 1003, ¶252.

15. Claim 19

Claim limitations 19[pre] to 19[f] are identical to limitations 1[pre] to 1[f], respectively. Limitation 19[h] is identical to claim 9. Thus, Zaid discloses or renders obvious those limitations for the same reasons as set forth above. Ex. 1003, ¶253.

(a) 19[g]

“wherein the e-key received at the device of the recipient includes data to inform the recipient of a level of monitoring that is to occur of the vehicle when the e-key is used for the vehicle”: As discussed above, Zaid discloses monitoring various uses of the vehicle. A POSITA would have considered it obvious to include with the encrypted reservation (***e-key***) a notification to the renter (***recipient***) about the ***level of monitoring*** that will occur. Ex. 1003, ¶¶254-55. Indeed, a POSITA would understand that such level of monitoring will be disclosed in the reservation agreement between the owner and renter, not least because local privacy laws may require such monitoring to be disclosed in advance. *Id.* In any case, a POSITA would have considered it obvious to inform the renter of such monitoring because it would have encouraged the renter to use the vehicle within the agreed-upon restrictions, and notifications were reasonably expected to succeed given widespread use of app-based notifications by 2013. *Id.*

“wherein a log is made to save the use of vehicle to a cloud storage, or storage of the vehicle or both, the log including... where the vehicle was driven, or speeds of the vehicle,...”: As discussed for limitations 1[e] and 1[f], Zaid

discloses monitoring and uploading data that includes ***where the vehicle was driven*** and acceleration (***speeds of the vehicle***). Ex. 1008, ¶¶95, 130. Zaid further discloses that such data is ***saved to a cloud storage or the vehicle***, i.e., “sent to a central server.” *Id.*; Ex. 1003, ¶256.

16. Claim 20

(a) 20[a]

As discussed above for claim 12, Zaid discloses or renders obvious generating a plurality of virtual keys (***e-keys***) that can co-exist, such as generating virtual keys for different renters for different time periods and time slots. Ex. 1003, ¶257.

(b) 20[b]

Zaid discloses that a virtual key is only active for the specified time period. Ex. 1008, ¶131 (“[T]he vehicle reservation becomes invalid at the end of the vehicle reservation period.”). Thus, when there are multiple virtual keys for different rental periods, only one virtual key is active at one time. Ex. 1003, ¶258.

E. Ground 5: Zaid, Harris and Mottla

Mottla describes a car rental app. The vehicle sends usage data to a server, which sends a notification to the renter’s device indicating rental agreement violations, including exceeding the rental period. It was obvious to combine Zaid with Mottla to provide notifications. Ex. 1003, ¶¶259-65.

1. Motivation to Combine

A POSITA would have been motivated to modify Zaid’s rental car system with Mottla’s teachings of notifications and a GUI.

Mottla teaches “push notification[s] sent by the reservation server” to a user’s “mobile device.” Ex. 1010, ¶37. Such messages “alert the member about reservation start and end times.” *Id.*, ¶38. Mottla also discloses an app GUI with unlock icons to unlock a vehicle. *Id.*, ¶33.

A POSITA would be motivated by the benefits of customer push notifications and a user-friendly GUI. Ex. 1003, ¶¶262-63. By the 2010s, smartphone apps were expected to have functional, user-friendly GUIs and receive notifications. Some benefits include informing a renter about the expiration of the rental period, which would remind them to not exceed the rental period, reducing the risk of vehicle unavailability and increasing user satisfaction. *Id.* A POSITA would have also known of the benefits of an unlock icon activated by an e-key—provide the user better control over vehicle access (such as unlocking on-demand instead of in proximity of the vehicle) while maintaining security, because it is the encrypted reservation that gives vehicle access to the renter. *Id.*

A POSITA would have a reasonable expectation of success. Ex. 1003, ¶264. Providing push notifications and GUI icons were industry standards and implementation was within the capabilities of a POSITA. *Id.*

Zaid, Mottla, and the '188 patent are all directed to mobile device-driven rental vehicle systems. Ex. 1001, 23:30; Ex. 1008, Abstract; Ex. 1010, Abstract; Ex. 1003, ¶265.

2. Claims 2, 4, 8

These claims recite sending a notification to the recipient's device "identifying the violation of the condition of use" (claim 2), "notify[ing] that the e-key will become disabled due to the violation of the condition" (claim 4), and "warnings of when the use of the vehicle may exceed, has exceeded, or is about to exceed the condition of use" (claim 8). As discussed above, Zaid describes a "reservation time period" as a condition of use for the vehicle. Mottla teaches "push notification[s] sent by the reservation server" to a user's "mobile device." Ex. 1010, ¶37. Such messages "alert the member about reservation start and end times." *Id.*, ¶38.

A POSITA would have considered it obvious to combine Zaid's vehicle rental system with Mottla's method of sending the notification after the end time in order to properly warn the renter to induce return of the car. Ex. 1003, ¶¶266-69. In this combined system, following identification of the violation of the time period condition of use, Zaid's server sends a push notification to the Temporary User and the vehicle instructing the Temporary User to terminate use and return the vehicle.

This would encourage prompt return of the vehicle and help prevent lengthy overstays.

In addition, because Zaid discloses that “the vehicle reservation [*e-key*] becomes invalid at the end of the vehicle reservation period” (Ex. 1008, ¶131), a warning about the expiration is also a warning that the reservation (e-key) is invalid (disabled). If PO argues that the notification must recite “invalid,” it would have been obvious to inform the renter of the consequence of violating the rental period, to encourage timely return of the vehicle. Ex. 1003, ¶269. There would be a reasonable expectation of success in providing such a notification due to conventional and well-known systems for providing push notifications, as discussed above. *Id.*

3. Claim 10

Mottla discloses an application GUI with “an unlock icon 1200” which “unlock[s] the vehicle doors.” Ex. 1010, ¶33. As discussed above, it would have been obvious to incorporate the disclosed in Mattla icon into Zaid, specifically on the renter’s device to allow for locking and unlocking capabilities via the device activated by the e-key. Ex. 1003, ¶¶270-73.

F. Ground 6: Zaid, Harris and Patenaude

Patenaude discloses a method for determining a user vehicle entertainment selection profile and automatically activating entertainment units based on

monitoring of a user's entertainment selections. It would have been obvious to incorporate these teachings into Zaid. Ex. 1003, ¶¶274-80.

1. Motivation to Combine

It was obvious to modify Zaid with Patenaude's teachings of a user entertainment selection profile.

Patenaude endeavors to "determine and predict entertainment selections" by learning a user's preferences and developing a user's "entertainment selection profile" stored in a vehicle. *Id.*, ¶¶1, 24.

A POSITA would have been motivated to make this combination to provide useful functionality. Ex. 1003, ¶277. For example, Zaid already recognizes the benefit of "allow[ing] media providers to stream music to the car via the vehicle access kit." Ex. 1008, ¶118. Patenaude's method for learning entertainment selections improves Zaid, as its users be unfamiliar with the interface of a shared vehicle and could benefit from automatic suggestions based on past vehicle use stored with their user profile. Ex. 1003, ¶278. A POSITA would have had a reasonable expectation of success in the combination since Zaid's shared vehicle already includes all necessary hardware for Patenaude's entertainment suggestion system. *Id.*, ¶279. The combination would involve Zaid's electronics receiving Patenaude's "entertainment unit factor" from entertainment units and then performing Patenaude's pattern learning and setting recommendations. *Id.*

Patenaude, Zaid, and the '188 patent are reasonably pertinent to the problem faced by the inventor (utilizing remote connectivity to provide added functionality and improve user experience).. Ex. 1001, 15:11-16; Ex. 1011, ¶¶5-6; Ex. 1003, ¶280.

2. Claim 17

Patenaude describes transmitting an “entertainment unit factor,” *i.e.*, **interface input data** that include radio inputs. Ex. 1011, ¶¶38, 42-43, 52; Ex. 1003, ¶¶281-83.

Based on the “entertainment unit factor” and “selection time factors,” Patenaude’s telematics unit “determines patterns in the entertainment selections” of a user. Ex. 1011, ¶55. The algorithm automatically configures the user’s desired entertainment settings for when they are using the vehicle. *Id.*, ¶73 Specifically, “during stage S612, 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.*, ¶75.

As described above, it would have been obvious to combine these teachings with Zaid’s system.

G. Ground 7: Kleve and Patenaude

As discussed above, Patenaude discloses claim 17. It would have been obvious to combine Kleve with Patenaude to render obvious claim 17. Ex. 1003, ¶¶284-87.

A POSITA would have been motivated to combine Patenaude with Kleve’s rental car system for the same reasons described in Ground 6, because Kleve and Zaid’s systems are similar and are similarly compatible with Patenaude. The benefits of Patenaude discussed in Ground 6 apply equally to Kleve—*e.g.*, learning preferences adds additional, desirable functionality. *Id.*

A POSITA would have had a reasonable expectation of success for similar reasons given in Ground 6 because, like Zaid, Kleve includes all necessary hardware to implement Patenaude’s system, including wireless communication, computing systems, and vehicle settings, and implementation would simply require adding software to receive Patenaude’s data and perform its algorithms. *Id.*

Finally, as discussed in Grounds 2 and 6, Kleve and Patenaude are analogous to the ’188 patent. *Id.*

VIII. *FINTIV*

Fintiv weighs against denial. A stay has not been requested, which is neutral. Trial is July 21, 2025, about four months before the FWD, but is weighed with other

relevant factors. IPR2021-01492, Paper 12, 9-16 (six months before FWD, no stipulation); IPR2021-01195, Paper 10 at 11, 14 (five months; *Sand* stipulation).

Petitioners filed this petition less than 8 months after the complaint. Fact discovery just began, and no depositions have occurred. Claim construction has not begun and the hearing will not occur until after institution.

Petitioners also challenge seven claims not asserted in the parallel litigations. Finally, the merits are strong.

IX. §325(D)

None of the above references were considered during prosecution. Zaid was submitted with an IDS containing 364 other references. Ex. 1002, 95-103. However, there is no evidence that the Examiner considered Zaid, and this Petition presents non-cumulative arguments. IPR2023-00643, Paper 11.

X. MANDATORY NOTICES AND FEES

A. Real Party-In-Interest

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

B. Related Matters

To the best of Petitioner's knowledge, the '188 patent is, or has been, involved in the following district court litigations and Board proceedings.

Petition for *Inter Partes* Review
U.S. Patent No. 9,365,188

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 Petitioner’s knowledge, the ’188 patent is related to the following U.S. applications that had been pending as of the issuance of the ’188 patent, and their corresponding issued patents (if applicable):

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

Petition for *Inter Partes* Review
U.S. Patent No. 9,365,188

14/176,138	9,697,503	2/9/2014
14/222,670	9,348,492	3/23/2014
14/246,145	9,229,623	4/7/2014
14/251,537	9,230,440	4/11/2014
14/275,569	9,467,515	5/12/2014
14/281,892	9,545,853	5/20/2014
14/288,356		5/27/2014
14/303,442	9,365,188	6/12/2014
14/316,559	9,371,007	6/26/2014
14/338,636	9,648,107	7/23/2014
14/499,039	9,536,197	9/26/2014
14/595,186	9,177,305	1/12/2015
14/599,541	9,177,306	1/18/2015
14/602,256	9,129,272	1/21/2015
14/640,004	9,423,937	3/5/2015
14/672,038	10,286,919	3/27/2015
14/677,341	9,778,831	4/2/2015
62/185,578		6/27/2015
14/790,409	9,215,274	7/2/2015
14/801,803	9,193,277	7/16/2015
14/872,404	9,335,179	10/1/2015
14/880,970	9,579,987	10/12/2015
62/254,858		11/13/2015
14/949,883	9,493,130	11/24/2015
14/952,911	9,288,270	11/25/2015
14/987,755	10,218,771	1/4/2016
14/989,100	10,839,451	1/6/2016
14/997,429		1/15/2016
15/071,120	9,426,225	3/15/2016
15/085,094	10,286,842	3/30/2016
15/161,373	9,434,270	5/23/2016
15/180,306	9,499,129	6/13/2016
15/188,971	9,815,382	6/21/2016
15/191,506	9,597,973	6/23/2016
15/243,933	10,286,798	8/22/2016
15/243,948	10,225,350	8/22/2016
15/257,016	9,718,370	9/6/2016
15/290,430	10,223,134	10/11/2016
15/344,566	9,663,067	11/6/2016

Petition for *Inter Partes* Review
U.S. Patent No. 9,365,188

15/351,422	9,672,823	11/14/2016
15/384,314	10,411,487	12/19/2016
15/387,651	10,181,099	12/22/2016
15/404,574	10,274,948	1/12/2017
15/420,098	10,424,296	1/31/2017
15/444,892	10,396,576	2/28/2017
15/444,328	10,308,244	2/28/2017
15/463,287	9,738,168	3/20/2017
15/469,517	9,855,947	3/25/2017
15/469,520	9,963,145	3/25/2017
15/470,881	10,535,341	3/27/2017
15/607,418	10,407,026	5/26/2017
15/615,812	9,818,088	6/6/2017
15/657,112	9,802,500	7/22/2017
15/683,286	9,925,882	8/22/2017
15/696,618	9,928,488	9/6/2017
15/714,113	10,821,845	9/25/2017
15/723,790	9,916,071	10/3/2017
15/786,578	10,210,487	10/17/2017
15/787,295	10,071,643	10/18/2017
15/787,414	10,286,875	10/18/2017
15/787,677	10,453,453	10/18/2017
15/787,691	10,821,850	10/18/2017
15/788,419	10,289,288	10/19/2017
15/841,721	10,714,955	12/14/2017
15/854,241	10,442,399	12/26/2017
15/859,730	10,829,111	1/1/2018
15/927,975	10,086,714	3/21/2018
15/928,054	10,282,708	3/21/2018
15/972,198	10,576,969	5/6/2018
16/150,252	10,245,964	10/2/2018
16/280,020	11,017,360	2/19/2019
16/285,706	10,652,312	2/26/2019
16/290,936	10,554,759	3/3/2019
16/293,617		3/5/2019
16/405,036	11,132,650	5/7/2019
16/409,819	11,203,355	5/11/2019
16/411,109	10,824,330	5/13/2019
16/411,525	10,572,123	5/14/2019

16/552,885	11,518,245	8/27/2019
16/566,872	11,370,313	9/10/2019

C. Counsel and Service Information

Petitioner provides the following counsel and service information.

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

LEAD COUNSEL	BACK-UP COUNSEL
---------------------	------------------------

For Kia: James M. Glass (Reg. No. 46729) 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 For Toyota: 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	For Kia: Quincy Lu (Reg. No. 76,954) quincylu@quinnemanuel.com 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 Quinn Emanuel Urquhart & Sullivan LLP 1300 I Street NW Washington, DC 20005 Tel: (202) 538-8000 Fax: (202) 538-8100 Email: jeffgerchick@quinnemanuel.com Brett Watkins Registration No. 60,458 Quinn Emanuel Urquhart & Sullivan LLP 700 Louisiana St., Suite 3900 Houston, TX 77002 Tel: (713) 221-7000 Fax: (713) 221-7100 Email: brettwatkins@quinnemanuel.com For Toyota: 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
--	---

D. Payment of Fees

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

Date: May 29, 2024

Respectfully submitted,

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

Counsel for Petitioner

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

1. This Petition complies with the type-volume limitation of 14,000 words, comprising 13,970 words, as counted using the Microsoft Word software that was used to prepare this paper, excluding the parts exempted by 37 C.F.R. § 42.24(a).

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

Date: May 29, 2024

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

Counsel for Petitioners

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on May 29, 2024, true and correct copies of the foregoing document and supporting materials were served in its entirety on the Patent Owner at the following address of record as listed on PAIR via Priority Mail Express® or Express Mail:

Penilla IP, APC-Patent Law
Re : US Pat. No. 9,365,188
5619 Scotts Valley Drive
Suite 280
Scotts Valley, CA 95066

Official Correspondence Address

Courtesy copies were also sent via electronic mail to Patent Owner's counsel of record in the related district court proceeding

mbelloli@bdiplaw.com

Date: May 29, 2024

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

Counsel for Petitioners