

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.

Post Grant Review No. 2026-00008

U.S. Patent No. 12,337,715

PETITION FOR POST GRANT REVIEW

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION	1
II. MANDATORY NOTICES AND FEES	3
A. Real Party-In-Interest	3
B. Related Litigation	3
C. Counsel and Service Information	7
D. Payment of Fees	9
E. Requirements for Post Grant Review	10
III. GROUNDS	10
IV. POSITA	10
V. BACKGROUND	11
A. '715 patent	11
1. Prosecution History	11
2. Priority Date	14
(a) Legal requirement	16
(b) The pre-October 2013 applications do not disclose “electronic key[s]”	16
VI. CLAIM CONSTRUCTION	20
VII. GROUNDS	20
A. Ground 1: Kleve, Sekiyama, Hatton, and Xiao	20
1. Kleve (U.S. Patent Pub. No. 2014/0129053)	20
2. Sekiyama (Japanese Laid Open Patent Application Publication No. 2010-126949)	20
3. Hatton (U.S. Patent No. 9,002,536)	23
4. Xiao (U.S. Patent No. 8,737,913)	24
5. Motivation to Combine	25
(a) Centralized issuance and restriction enforcement (Kleve + Sekiyama)	26

(b)	Secure mobile-to-vehicle system via manufacturer app (Kleve + Hatton)	30
(c)	Account-backed, manufacturer-associated backend and telemetry (Kleve + Xiao)	33
(d)	Technical compatibility and routine implementation	36
(e)	Reasonable expectation of success	36
6.	Claim 1	38
(a)	1[pre] – “A method for sharing electronic keys (e-keys)”	38
(b)	1[a] – “processing a request to share an electronic key (e-key) of a vehicle with a recipient device, the request to share the e-key being received responsive to a message being sent to the recipient device from a sharing device;”	39
(c)	1[b] – “determining that the request to share the e-key was associated with a registered owner e-key;”	44
(d)	1[c] – “processing instructions to enable the e-key to be securely generated for use by the recipient device; and”	45
(e)	1[d] – “saving information regarding the e-key with a server associated with a manufacturer of the vehicle;”	48
(f)	1[e] – “wherein the e-key is enabled for said use on the vehicle by the recipient device.”	53
7.	Claim 2 – The method of claim 1, wherein the request to share the e-key includes a setting to assign a privilege level for use of the vehicle when used via the e-key, the privilege level provides one or more conditions of use of the vehicle.	53
8.	Claim 3 – The method of claim 2, wherein the one or more conditions of use defined via the privilege level is one of a geographic restriction for where the vehicle is allowed to be used, or a speed restriction, or an occupancy restriction, or a time frame of use, or an expiration-time of	

use, or unlocking of the vehicle, or driving of the vehicle,
or combinations of two or more thereof.54

9. Claim 4 – The method of claim 1, wherein the request is
enabled via an application executed via the sharing device,
the application provided by said manufacturer of the
vehicle to enable initiation of sharing of the e-key, the
application is associated with an owner account for the
vehicle.55

10. Claim 5 – The method of claim 1, wherein responsive to
said request, the e-key is generated, the generation of the
e-key includes one or more processes executed by the
server associated with the manufacturer of the vehicle, one
or more processes executed by one or more additional
server, one or more processes executed by the recipient
device, one or more processes executed by a computer, or
a combination of two or more thereof.57

11. Claim 6 – The method of claim 1, further comprising,
encrypting the e-key, the e-key being encrypted using
public/private key pairs that are generated and used for
security in communication.58

12. Claim 7 – The method of claim 1, further comprising,
receiving a deactivation request, the deactivation request
is used to disable the e-key for use by the recipient device
on the vehicle.59

13. Claim 8 – The method of claim 1, wherein the message to
share and enable the e-key for the recipient device is
communicated over a network, the communication
enables processing by one or more servers or devices, and
said one or more servers or devices include a server
associated with the sharing device or the recipient device,
and the server associated with the manufacturer of the
vehicle.60

14. Claim 9 – The method of claim 1, wherein the recipient
device is identified by one or more of an email address, a
phone number, a text message, a message address, a
notification, a link, a web address, a social network
address, or combination of two or more thereof.62

15. Claim 10 – The method of claim 1, wherein an application provided by a manufacturer of the vehicle includes a graphical user interface for registering the registered owner e-key for the vehicle and sharing of the e-key with one or more recipient devices.63
16. Claim 11 – The method of claim 1, wherein the e-key enabled for use on the vehicle using the recipient device enables unlocking and starting the vehicle when the recipient device uses the e-key with the vehicle, and the e-key is associated with at least one privilege associated with a type of operation use of the vehicle.64
17. Claim 1265
 - (a) 12[pre] – A system for enabling use and sharing of an electronic key (e-key) for a vehicle, comprising:65
 - (b) 12[a] – a server associated with a manufacturer of the vehicle, the server is configured to interface with an application provided by the manufacturer of the vehicle, the application provides access to data and logic for enabling sending a request to share the e-key for the vehicle with a recipient device;.....65
 - (c) 12[b] – the request to share is configured to be initiated by a message originating from the recipient device, and responsive to the request, processing the request to securely generate the e-key;.....66
 - (d) 12[c] – the server associated with the manufacturer of the vehicle assisting in enabling the e-key for use on the vehicle by the recipient device.66
18. Claim 13 – The system of claim 12, wherein the request to share the e-key includes enabling a setting to apply a privilege level for use of the vehicle via the e-key, the privilege level provides one or more conditions of use of the vehicle via the e-key.67
19. Claim 14 – The system of claim 12, wherein the e-key is encrypted, and wherein encryption uses a public/private process for security.67

- 20. Claim 15 – The system of claim 12, wherein the application includes a selectable option for disabling the e-key from use by the recipient device on the vehicle.....67
- 21. Claim 16 – The system of claim 12, wherein the e-key enabled for use on the vehicle using the recipient device enables unlocking and starting the vehicle when the recipient device uses the e-key with the vehicle, and the e-key is associated with at least one privilege associated with a type of operational use of the vehicle.67
- 22. Claim 1767
 - (a) 17[pre] – A method for providing access to a vehicle, comprising:.....67
 - (b) 17[a] – receiving confirmation of a sharing request being sent for an electronic key (e-key) for use of the vehicle by a recipient device, the sharing request originates responsive to a message transferred by an owner device to the recipient device;68
 - (c) 17[b] – receiving confirmation of the sharing request from the recipient device;68
 - (d) 17[c] – processing data related to the message by a server associated with a manufacturer of the vehicle, said processing data is performed to enable the e-key for use by the recipient device on the vehicle; and.....69
 - (e) 17[d] – enabling the e-key for use by the recipient device on the vehicle.70
- 23. Claim 18 – The method of claim 17, wherein the e-key is associated with at least one privilege associated with use of the vehicle, the at least one privilege is defined based on a setting associated with the sharing request, and wherein the recipient device is one of a smartphone, or a smartwatch, or smart glasses, or a computer, or a digital assistant, or a key fob, and wherein the e-key is unique for said sharing request and said use by said recipient device.70
- 24. Claim 19 – The method of claim 17, wherein the e-key is caused to be generated by either one of said owner device,

the server, the recipient device, a computer, the vehicle, or a combination of two or more thereof.71

25. Claim 20 – The method of claim 17, wherein the e-key is securely generated for the recipient device, and wherein the owner device has an owner e-key that was initially generated for the owner device to enable said sharing request, and the e-key is encrypted, and wherein encryption uses a public/private process for security.71

26. Claim 21 – The method of claim 17, wherein the e-key, once enabled, provides access to information via the recipient device regarding a level of charge of a battery of the vehicle for when the vehicle is an electric vehicle (EV).72

27. Claim 22 – The method of claim 17, wherein the e-key enabled for use on the vehicle using the recipient device enables unlocking and starting the vehicle when the recipient device uses the e-key with the vehicle, and the e-key is associated with at least one privilege associated with a type of operational use of the vehicle.73

28. Claim 2373

(a) 23[pre] – A system for enabling use and sharing of an electronic key (e-key) for a vehicle, comprising:73

(b) 23[a] – an onboard computer of the vehicle;73

(c) 23[b] – a communications system of the vehicle interfaced with the on-board computer, the on-board computer of the vehicle having program instructions for communication with a server associated with a manufacturer of the vehicle, the server is configured to interface with an application provided by the manufacturer of the vehicle, the application provides a user interface for initiating a request to share the e-key for the vehicle with a recipient device, the request to share is configured to be initiated using a message communicated to the recipient device, and responsive to the request, processing the request to enable generation of the e-key for use on the vehicle by the recipient device.74

29.	Claim 24 – The system of claim 23, wherein the e-key enabled for use on the vehicle using the recipient device enables unlocking and starting the vehicle when the recipient device uses the e-key with the vehicle, and the e-key is associated with at least one privilege associated with a type of operational use of the vehicle.	75
B.	Ground 2: Claims 1-11, 17-24 lack written description and enablement support.....	75
1.	What the '715 specification discloses (request to cloud/server; server-to-recipient delivery; optional notification).....	76
2.	No support for “message-caused” initiation of the sharing request (claims 1 and 23 (and their dependents))	77
C.	No support for “confirmation” events (independent claim 17 and dependents).....	78

EXHIBIT LIST

Ex.	Description
1001	U.S. Patent No. 12,337,715 (“the ’715 patent”)
1002	Prosecution History for U.S. Patent No. 12,337,715
1003	Declaration of Dr. Kevin Almeroth
1004	U.S. Pat. Pub. No. 2014/0129053 to Kleve et al.
1005	Certified Translation of JP2010-126949A to Sekiyama et al.
1006	JP 2010-126949
1007	Declaration of Herman Kahn
1008	U.S. Patent No. 9,002,536 to Hatton
1009	U.S. Pat. Pub. No. 2011/0312273 to Harris
1010	U.S. Pat. No. 8,737,913 to Xiao et al.
1011	U.S. Pat. No. 8,977,408 to Cazanans et al.
1012	U.S. Pat. App. No. 61/478,436
1013	U.S. Pat. App. No. 61/745,729
1014	U.S. Pat. App. No. 13/452,882
1015	U.S. Pat. App. No. 13/842,158
1016	U.S. Pat. App. No. 14/063,638
1017	Order Granting Request For Ex Parte Reexamination, 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

Petition for Post Grant Review
U.S. Patent No. 12,337,715

1019	<i>Curriculum Vitae</i> of Dr. Kevin Almeroth
1020	U.S. Patent No. 7,868,736 to Fukushima et al.
1021	U.S. Pat. App. No. 14/303,442
1022	U.S. Pat. App. No. 15/180,306
1023	U.S. Pat. App. No. 15/344,566
1024	U.S. Pat. App. No. 15/607,418
1025	U.S. Pat. App. No. 15/854,241
1026	U.S. Pat. App. No. 16/653,958
1027	U.S. Pat. App. No. 17/461,959
1028	U.S. Pat. App. No. 18/125,448
1029	BLUETOOTH Core Specification v.4.0
1030	Ex Parte Reexamination Control Number 90/019,456, Final Rejection

LIST OF CHALLENGED CLAIMS

Claim	Limitation
1[pre]	A method for sharing electronic keys (e-keys), comprising:
1[a]	processing a request to share an electronic key (e-key) of a vehicle with a recipient device, the request to share the e-key being received responsive to a message being sent to the recipient device from a sharing device;
1[b]	determining that the request to share the e-key was associated with a registered owner e-key;
1[c]	processing instructions to enable the e-key to be securely generated for use by the recipient device; and
1[d]	saving information regarding the e-key with a server associated with a manufacturer of the vehicle;
1[e]	wherein the e-key is enabled for said use on the vehicle by the recipient device.
2	The method of claim 1 , wherein the request to share the e-key includes a setting to assign a privilege level for use of the vehicle when used via the e-key, the privilege level provides one or more conditions of use of the vehicle.
3	The method of claim 2 , wherein the one or more conditions of use defined via the privilege level is one of a geographic restriction for where the vehicle is allowed to be used, or a speed restriction, or an occupancy restriction, or a time frame of use, or an expiration-time of use, or unlocking of the vehicle, or driving of the vehicle, or combinations of two or more thereof.

Claim	Limitation
4	The method of claim 1, wherein the request is enabled via an application executed via the sharing device, the application provided by said manufacturer of the vehicle to enable initiation of sharing of the e-key, the application is associated with an owner account for the vehicle.
5	The method of claim 1, wherein responsive to said request, the e-key is generated, the generation of the e-key includes one or more processes executed by the server associated with the manufacturer of the vehicle, one or more processes executed by one or more additional server, one or more processes executed by the recipient device, one or more processes executed by a computer, or a combination of two or more thereof.
6	The method of claim 1, further comprising, encrypting the e-key, the e-key being encrypted using public/private key pairs that are generated and used for security in communication.
7	The method of claim 1, further comprising, receiving a deactivation request, the deactivation request is used to disable the e-key for use by the recipient device on the vehicle.
8	The method of claim 1, wherein the message to share and enable the e-key for the recipient device is communicated over a network, the communication enables processing by one or more servers or devices, and said one or more servers or devices include a server associated with the sharing device or the recipient device, and the server associated with the manufacturer of the vehicle.

Claim	Limitation
9	The method of claim 1, wherein the recipient device is identified by one or more of an email address, a phone number, a text message, a message address, a notification, a link, a web address, a social network address, or combination of two or more thereof.
10	The method of claim 1, wherein an application provided by a manufacturer of the vehicle includes a graphical user interface for registering the registered owner e-key for the vehicle and sharing of the e-key with one or more recipient devices.
11	The method of claim 1, wherein the e-key enabled for use on the vehicle using the recipient device enables unlocking and starting the vehicle when the recipient device uses the e-key with the vehicle, and the e-key is associated with at least one privilege associated with a type of operation use of the vehicle.
12[pre]	A system for enabling use and sharing of an electronic key (e-key) for a vehicle, comprising:
12[a]	a server associated with a manufacturer of the vehicle, the server is configured to interface with an application provided by the manufacturer of the vehicle, the application provides access to data and logic for enabling sending a request to share the e-key for the vehicle with a recipient device;
12[b]	the request to share is configured to be initiated by a message originating from the recipient device, and responsive to the request, processing the request to securely generate the e-key;
12[c]	the server associated with the manufacturer of the vehicle assisting in enabling the e-key for use on the vehicle by the recipient device.

Claim	Limitation
13	The system of claim 12, wherein the request to share the e-key includes enabling a setting to apply a privilege level for use of the vehicle via the e-key, the privilege level provides one or more conditions of use of the vehicle via the e-key.
14	The system of claim 12, wherein the e-key is encrypted, and wherein encryption uses a public/private process for security.
15	The system of claim 12, wherein the application includes a selectable option for disabling the e-key from use by the recipient device on the vehicle.
16	The system of claim 12, wherein the e-key enabled for use on the vehicle using the recipient device enables unlocking and starting the vehicle when the recipient device uses the e-key with the vehicle, and the e-key is associated with at least one privilege associated with a type of operational use of the vehicle.
17[pre]	A method for providing access to a vehicle, comprising:
17[a]	receiving confirmation of a sharing request being sent for an electronic key (e-key) for use of the vehicle by a recipient device, the sharing request originates responsive to a message transferred by an owner device to the recipient device;
17[b]	receiving confirmation of the sharing request from the recipient device;
17[c]	processing data related to the message by a server associated with a manufacturer of the vehicle, said processing data is

Claim	Limitation
	performed to enable the e-key for use by the recipient device on the vehicle; and
17[d]	enabling the e-key for use by the recipient device on the vehicle.
18	The method of claim 17, wherein the e-key is associated with at least one privilege associated with use of the vehicle, the at least one privilege is defined based on a setting associated with the sharing request, and wherein the recipient device is one of a smartphone, or a smartwatch, or smart glasses, or a computer, or a digital assistant, or a key fob, and wherein the e-key is unique for said sharing request and said use by said recipient device.
19	The method of claim 17, wherein the e-key is caused to be generated by either one of said owner device, the server, the recipient device, a computer, the vehicle, or a combination of two or more thereof.
20	The method of claim 17, wherein the e-key is securely generated for the recipient device, and wherein the owner device has an owner e-key that was initially generated for the owner device to enable said sharing request, and the e-key is encrypted, and wherein encryption uses a public/private process for security.
21	The method of claim 17, wherein the e-key, once enabled, provides access to information via the recipient device regarding a level of charge of a battery of the vehicle for when the vehicle is an electric vehicle (EV).

Claim	Limitation
22	The method of claim 17 , wherein the e-key enabled for use on the vehicle using the recipient device enables unlocking and starting the vehicle when the recipient device uses the e-key with the vehicle, and the e-key is associated with at least one privilege associated with a type of operational use of the vehicle.
23[pre]	A system for enabling use and sharing of an electronic key (e-key) for a vehicle, comprising:
23[a]	an onboard computer of the vehicle;
23[b]	a communications system of the vehicle interfaced with the on-board computer, the on-board computer of the vehicle having program instructions for communication with a server associated with a manufacturer of the vehicle, the server is configured to interface with an application provided by the manufacturer of the vehicle, the application provides a user interface for initiating a request to share the e-key for the vehicle with a recipient device, the request to share is configured to be initiated using a message communicated to the recipient device, and responsive to the request, processing the request to enable generation of the e-key for use on the vehicle by the recipient device.
24	The system of claim 23 , wherein the e-key enabled for use on the vehicle using the recipient device enables unlocking and starting the vehicle when the recipient device uses the e-key with the vehicle, and the e-key is associated with at least one privilege associated with a type of operational use of the vehicle.

I. INTRODUCTION

U.S. Patent No. 12,337,715 (“the ’715 patent”) claims the use and sharing of electronic vehicle keys (“e-keys”) via a mobile application and backend servers. By the October 2013 priority date, this architecture was already well known: onboard vehicle controllers communicating with cloud services and user smartphones to provision time and function-restricted access with encrypted exchanges and account-based management.

Ground 1 (Obviousness). Petitioners rely principally on **Sekiyama**, developed by Toyota, which discloses a server-mediated electronic-key system issuing restricted duplicate keys in response to an owner request, with the keys used by a recipient device to lock/unlock and start the vehicle. We combine Sekiyama with: **Kleve**, developed by Ford, which teaches owner–recipient term setting and direct, encrypted delivery of a “virtual key” to the recipient device; **Hatton**, also developed by Ford, which teaches a (manufacturer-provided) mobile app that performs encrypted, app-mediated key handling and device recognition to enable unlock/start through the in-vehicle computing system; and **Xiao**, developed by Verizon, which teaches account-centric, automobile-company-associated servers and mobile/server/PAN communications (including delivering status such as battery charge level to the phone). A person of ordinary skill in the art (“POSITA”) would have been motivated to integrate these familiar, interoperable elements to improve

security, manageability, and user experience, with a reasonable expectation of success and predictable results. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 416–22 (2007).

Ground 2 (§112(a)). Independent claims 1 and 23 (and their dependents) add a message-caused initiation requirement—*i.e.*, the share request is initiated responsive to a message sent to the recipient device—that the specification does not describe. Independent claim 17 (and dependents) further add confirmation requirements—receipt of a confirmation that a share request was sent and receipt of a confirmation from the recipient device—that likewise are not disclosed. The specification depicts an owner-to-server request, server-to-recipient delivery, and optional notification/activation guidance, not the claimed causal couplings or confirmations. As such, claims 1–11 and 17–24 lack written description and enablement support under 35 U.S.C. §112(a).

Because the claims are obvious over Sekiyama in view of Kleve, Hatton, and Xiao—and several also fail §112—Petitioners respectfully request institution and cancellation of claims 1–24.

II. 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., Toyota Motor Sales, U.S.A., Inc., and Toyota Connected North America, Inc.

B. Related Litigation

Patent Owner is currently asserting the '715 patent against Petitioners in the following litigations:

Name	Number	Court	Filed
<i>Emerging Automotive LLC v. Toyota Motor North America Inc. et al.</i>	2:25-cv-00782	EDTX	Aug. 12, 2025
<i>Emerging Automotive LLC v. Kia Corp. et al.</i>	2:25-cv-00799	EDTX	Aug. 15, 2025

To the best of Petitioners' knowledge, the '715 patent is related to the following U.S. applications, including those that had been pending as of the issuance of the '715 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

Petition for Post Grant Review
U.S. Patent No. 12,337,715

13/842,158	9,229,905	3/15/2013
13/906,335	9,104,537	5/30/2013
13/911,072	9,809,196	6/5/2013
13/934,215	9,581,997	7/2/2013
13/937,202	9,346,365	7/8/2013
14/050,314	9,171,268	10/9/2013
61/896,007		10/25/2013
14/063,638	9,189,900	10/25/2013
14/063,837	9,139,091	10/25/2013
14/145,693	9,372,607	12/31/2013
14/173,818	9,697,733	2/6/2014
14/176,138	9,697,503	2/9/2014
14/222,670	9,348,492	3/23/2014
14/246,145	9,229,623	4/7/2014
14/251,537	9,230,440	4/11/2014
14/275,569	9,467,515	5/12/2014
14/281,892	9,545,853	5/20/2014
14/288,356		5/27/2014
14/303,442	9,365,188	6/12/2014
14/316,559	9,371,007	6/26/2014
14/338,636	9,648,107	7/23/2014
14/499,039	9,536,197	9/26/2014
14/595,186	9,177,305	1/12/2015
14/599,541	9,177,306	1/18/2015
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

Petition for Post Grant Review
U.S. Patent No. 12,337,715

15/071,120	9,426,225	3/15/2016
15/085,094	10,286,842	3/30/2016
15/161,373	9,434,270	5/23/2016
15/180,306	9,499,129	6/13/2016
15/188,971	9,815,382	6/21/2016
15/191,506	9,597,973	6/23/2016
15/243,933	10,286,798	8/22/2016
15/243,948	10,225,350	8/22/2016
15/257,016	9,718,370	9/6/2016
15/290,430	10,223,134	10/11/2016
15/344,566	9,663,067	11/6/2016
15/351,422	9,672,823	11/14/2016
15/384,314	10,411,487	12/19/2016
15/387,651	10,181,099	12/22/2016
15/404,574	10,274,948	1/12/2017
15/420,098	10,424,296	1/31/2017
15/444,892	10,396,576	2/28/2017
15/444,328	10,308,244	2/28/2017
15/463,287	9,738,168	3/20/2017
15/469,517	9,855,947	3/25/2017
15/469,520	9,963,145	3/25/2017
15/470,881	10,535,341	3/27/2017
15/607,418	10,407,026	5/26/2017
15/615,812	9,818,088	6/6/2017
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

Petition for Post Grant Review
U.S. Patent No. 12,337,715

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	5/12/2019
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
16/653,958	11,104,245	10/15/2019
16/785,621	10,926,762	2/9/2020
16/785,629	11,294,551	2/9/2020
16/785,640		2/9/2020
16/788,253	11,396,244	2/11/2020
16/929,083	11,427,101	7/14/2020
16/987,919	11,305,666	8/7/2020
16/733,233	11,602,994	1/2/2020
17/088,349	11,889,394	11/3/2020
17/088,535	11,472,310	11/3/2020
17/094,804	11,396,240	11/10/2020
17/182,892	11,731,618	2/23/2021
17/329,935	11,935,013	5/25/2021
17/461,959	11,738,659	8/30/2021
17/713,216	12,197,710	4/4/2022
17/873,096	12,337,716	7/25/2022
17/873,119	11,772,502	7/25/2022
17/968,475	11,975,631	10/18/2022
18/076,278		12/6/2022
18/125,448	11,794,601	3/23/2023
18/236,677	12,330,637	8/22/2023
18/376,409	12,257,914	10/3/2023
18/530,125		12/5/2023
18/427,686		1/30/2024
90/019,456		3/25/2024
18/977,798		12/11/2024

Petition for Post Grant Review
U.S. Patent No. 12,337,715

19/012,653		1/7/2025
19/026,361		1/17/2025
19/248,175		6/24/2025
19/248,414		6/24/2025

C. Counsel and Service Information

Petitioners provide the following counsel and service information. Petitioners consent 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.

<u>Lead Counsel</u>	<u>Back-Up Counsel</u>
<p>For Kia:</p> <p>James M. Glass (Reg. No. 46,729) jimglass@quinnemanuel.com</p> <p>QUINN EMANUEL URQUHART & SULLIVAN, LLP 295 5th Avenue New York, NY 10014 Tel: (212) 849-7000 Fax: (212) 849-7100</p>	<p>For Kia:</p> <p>Quincy Lu (Reg. No. 76,954) quincylu@quinnemanuel.com</p> <p>QUINN EMANUEL URQUHART & SULLIVAN, LLP 1109 First Avenue, Suite 210 Seattle, WA 98101 Tel: (206) 905-7000 Fax: (206) 905-7100</p>
<p>For Toyota:</p> <p>Joshua L. Goldberg (Reg. No. 59,369) joshua.goldberg@finnegan.com</p> <p>FINNEGAN HENDERSON FARABOW GARRETT & DUNNER, LLP 901 New York Avenue, NW Washington, DC 20001 Tel: (202) 408-4000 Fax: (202) 408-4400</p>	<p>Jeffrey S. Gerchick (<i>pro hac vice</i> forthcoming) jeffgerchick@quinnemanuel.com</p> <p>QUINN EMANUEL URQUHART & SULLIVAN, LLP 1300 I Street, NW Washington, DC 20005 Tel: (202) 538-8000 Fax: (202) 538-8100</p> <p>Brett Watkins (Reg. No. 60,458) brettwatkins@quinnemanuel.com</p>
	<p>QUINN EMANUEL URQUHART & SULLIVAN, LLP 700 Louisiana Street, Suite 3900 Houston, TX 77002 Tel: (713) 221-7000 Fax: (713) 221-7100</p> <p>For Toyota:</p> <p>James R. Barney (Reg. No. 46,539) james.barney@finnegan.com</p>

	<p>Aidan Skoyles (Reg. No. 61,119) aidan.skoyles@finnegan.com</p> <p>Nicholas Eitsert (Reg. No. 78,843) nicholas.eitsert@finnegan.com</p> <p>FINNEGAN HENDERSON FARABOW GARRETT & DUNNER, LLP 901 New York Avenue, NW Washington, DC 20001 Tel: (202) 408-4000 Fax: (202) 408-4400</p> <p>Robert D. McCutcheon (Reg. No. 38,717) rmccutcheon@munckwilson.com</p> <p>Jared M. Hoggan (<i>pro hac vice</i> forthcoming) jhoggan@munckwilson.com</p> <p>MUNCK WILSON MANDALA, LLP 1900 Texas Capital Center 2000 McKinney Avenue Dallas, TX 75201 Tel: (972) 628-3600 Fax: (972) 628-3616</p>
--	--

D. Payment of Fees

The undersigned authorizes the Office to charge the fee required for this Petition (and any additional fees) to Deposit Account No. 50-5708.

E. Requirements for Post Grant Review

Petitioners certify the '715 patent is available for PGR, and Petitioners are not barred or estopped from requesting this proceeding.

The earliest possible effective filing date for the claims of the '715 patent is October 25, 2013, the filing date of the continuation-in-part application adding the disclosure related to electronic keys.

The '715 patent issued on June 24, 2025, and the instant Petition was timely filed within nine months of issuance.

III. GROUNDS

Petitioners present the below grounds.

Ground	Basis	Reference(s)	Claims
1	§103	Sekiyama, Kleve, Hatton, and Xiao	1-5, 7-19, 21-24
2	§112	N/A	1-11, 17-24

IV. POSITA

A POSITA had at least a four-year undergraduate degree in electrical engineering, automotive engineering, or a closely related field and at least two years of experience in the field of access control systems, vehicle electronics, and/or cryptography. EX1003, ¶¶84-85. More education can supplement practical experience and vice versa. *Id.* Petitioners' expert exceeded this by the priority date. *Id.*

V. BACKGROUND

A. '715 patent

The '715 patent describes a vehicle owner assigning an e-key to a user. EX1001, Abstract; 42:35–61. In Figure 29, owner “Bob” shares e-keys 650 with three temporary users. *Id.* This allows different users to have different keys with different conditions. *Id.*; EX1003, ¶¶54-59.

1. Prosecution History

On October 11, 2023, Applicant filed a continuation application claiming priority to a string of nine continuations, two continuations-in-part, and two provisional applications. EX1002, Filing Receipt, at 1. On August 5, 2024, the examiner rejected the claims based on double-patenting over related U.S. Patent Nos. 11,738,659 and 11,794,601. EX1002, Non-Final Rejection, at 4. On February 5, 2025, Applicant filed terminal disclaimers to overcome the rejection. *See* EX1002, Amendment, at 8.

In its remarks, Applicant included a “Disclosure of Related Proceedings,” noting “three [of its] related applications ... are currently involved in litigation and proceedings before the Paten Trail (sic) and Appeal Board (PTAB).” *Id.* Applicant noted that IPR2024-00981 was filed for U.S. Pat. No. 9,365,188 and is pending; that IPR2024-00785 was filed for U.S. Pat. No. 10,407,026 and institution was denied; that IPR2024-01167 was filed for U.S. Pat. No. 11,738,659 and is pending; and that EPR 90/019,456 was filed for U.S. Pat. No. 11,738,659 and is pending. *Id.* at 9.

Applicant filed an information disclosure statement with nearly 400 references, including the art raised in the *inter partes* review (“IPR”) and *ex parte* reexamination (“EPR”) proceedings, but failed to disclose the Board’s institution decisions in IPR2024-00981 (entered December 18, 2024) and IPR2024-01167 (entered January 27, 2025) and the USPTO’s Final Rejection decision in EPR 90/019,456 (mailed February 11, 2025).

On March 12, 2025, the examiner issued a Notice of Allowance, including as reason for allowance that the “closest prior art by Suyama ([U.S.] Pat. No.: 7,375,440[]) does not teach or suggest ... ***a server associated with the manufacturer*** of the vehicle configured to enable sharing of e-key with a recipient device.” EX1002, Notice of Allowability, at 2 (emphasis added).

But, as discussed below, the phrase “associated with a manufacturer of the vehicle” is nonfunctional descriptive material, and therefore is not entitled to patentable weight under the printed matter doctrine because “it claims the content of information” (*i.e.*, who operates the server) and lacks any “functional relationship” to the server. *Praxair Distribution, Inc. v. Mallinckrodt Hosp. Prods. IP Ltd.*, 890 F.3d 1024, 1031–32 (Fed. Cir. 2018); *see also Catalina Mktg. Int’l v. Coolsavings.com, Inc.*, 289 F.3d 801, 809 (Fed. Cir. 2002). Who owns/operates or is “associated with” the server does not alter the server’s structure or the method’s operation. EX1003, ¶61.

Furthermore, as detailed in Ground 1 below, a POSITA would have understood that Sekiyama's (JP 2010-126949 A, not Suyama) server is *associated with a manufacturer of the vehicle*. EX1003, ¶62. Sekiyama is a Japanese patent application invented by employees of Toyota Motor Corp. and assigned to Toyota Motor Corp. EX1005. Accordingly, a POSITA would have recognized that the “center server” described in Sekiyama was a server associated with the manufacturer of the vehicle, as the “electronic key system” described in Sekiyama would have been understood to have been developed for use by Toyota and its vehicles. EX1003, ¶62.

It further would have been an obvious option to host Sekiyama's server functions on a server operated by (or on behalf of) the vehicle manufacturer. *Id.*, ¶63. Multiple contemporaneous references teach manufacturer-associated servers for e-key services. For example, Xiao explains that its wireless automobile key service servers “may be associated with an automobile company.” EX1010, 3:12–21; *see also id.*, 3:46–54, 4:46–56, 12:8–13, 16:48–54.¹ Thus, a POSITA would have found

¹ In the relevant period, OEM-hosted cloud servers and account-based provisioning for mobile/vehicle services were conventional. *See, e.g.*, EX1009 (Harris), ¶[0038] (OEM server provisioning/authentication); EX1011 (Cazanas), 6:27–34, 12:13–30, 15:4–32 (cloud accounts storing user/vehicle identifiers and

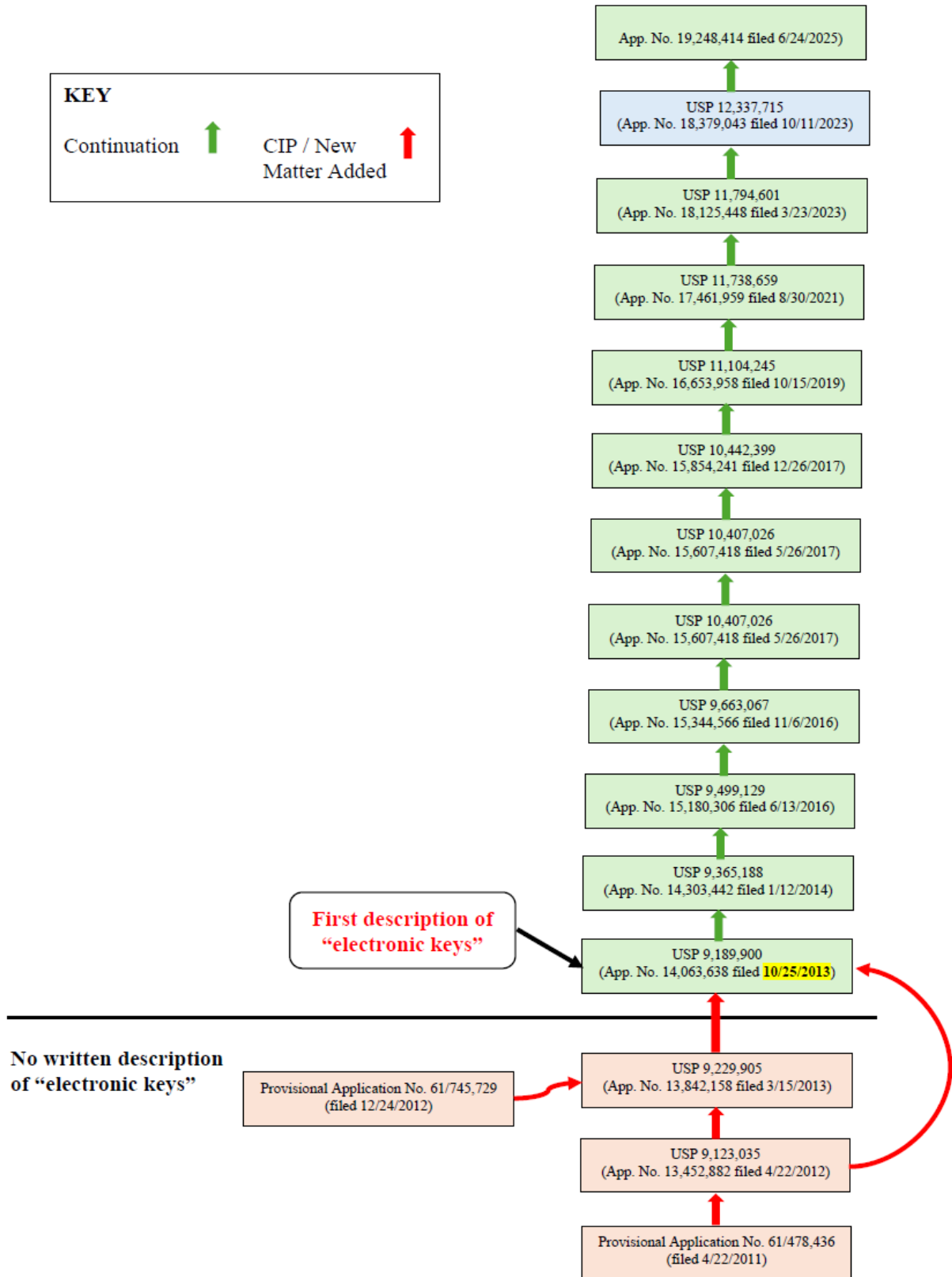
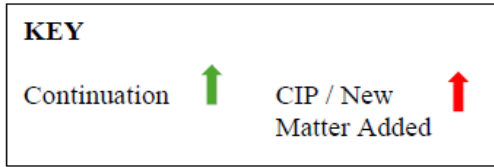
it obvious to implement Sekiyama's saving of e-key information on a manufacturer-associated server as one of a finite, predictable set of options for the owner/operator of the server (*e.g.*, vehicle manufacturer, telematics provider, carrier, third-party) with no change to functionality and with a reasonable expectation of success. EX1003, ¶63.

2. Priority Date

The '715 patent claims priority to various applications as shown below:

policies). These references are cited as background corroboration of industry practice; to the extent the manufacturer-associated-server limitation is accorded patentable weight, it is satisfied by Xiao. EX1003, ¶63, n.2.

Petition for Post Grant Review
U.S. Patent No. 12,337,715



The '715 patent is not entitled to a filing date before October 25, 2013, when U.S. Pat. App. No. 14/063,638 (“the '638 Application”) introduced descriptions for “e-keys.”

(a) Legal requirement

An earlier-filed U.S. application must “reasonably convey[] to those skilled in the art that the inventor had possession of the claimed subject matter.” *Ariad Pharms., Inc. v. Eli Lilly & Co.*, 598 F.3d 1336, 1351 (Fed. Cir. 2010). Written description evaluates “the specification from the perspective of a [POSITA].” *Id.* A description cannot “merely render[] the invention obvious.” *Id.* at 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. EX1018; EX1003, ¶¶65–74. For example, as Dr. Kevin Almeroth explains in detail, Figures 17–35 and their descriptions discuss the requesting, generating, transmission, and use of e-keys. EX1018, 105, 122–28; EX1003, ¶69.

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

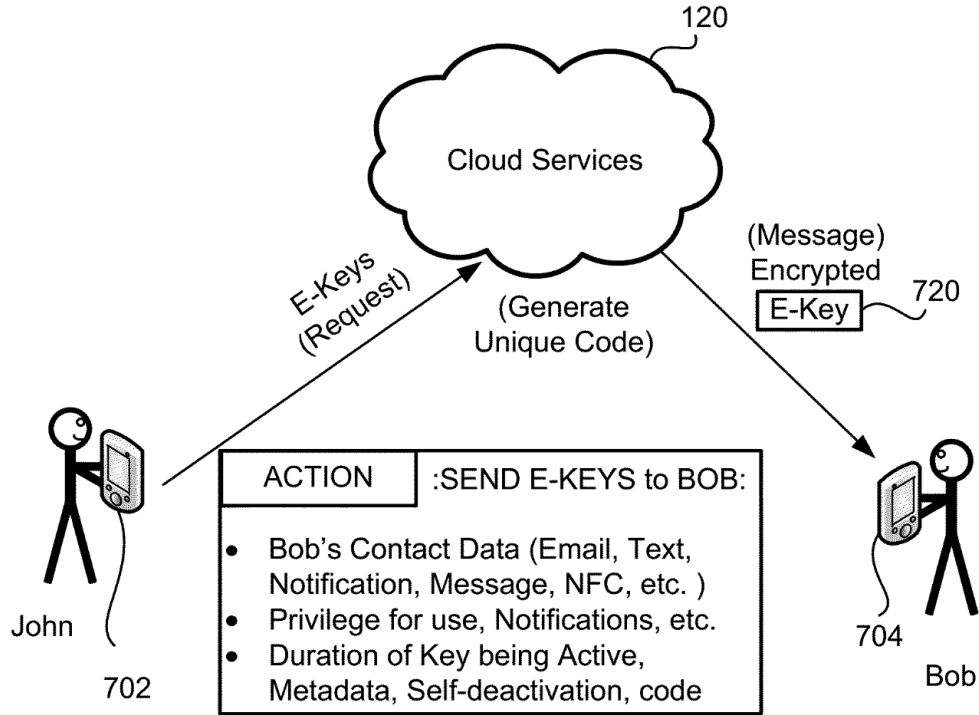


FIG. 35

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

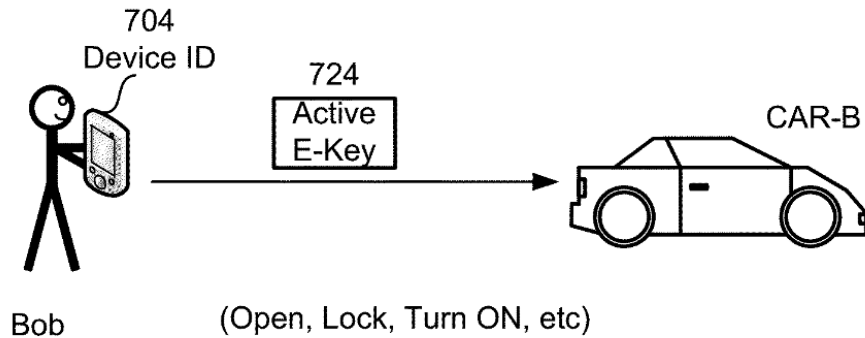


FIG. 33

By contrast, the earlier applications contain *no disclosures* relating to e-keys.

U.S. Pat. App. No. 13/842,158 ("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. EX1015, Abstract. U.S. Pat. App. No. 13/452,882 (“the ’882 Application”) and provisionals are directed to electric vehicle charging. EX1014, Abstract; EX1012; EX1013. 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. EX1003, ¶¶77; *see also id.*, ¶¶65-80.

Patent Owner (“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. EX1015, 28, 42, 60–61. ***But e-keys are not disclosed in connection with such functionality, and keyless remote control was already well-known in the art. See, e.g., EX1010 (Xiao), 1:5–39.*** 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. EX1003, ¶¶75-80. 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.*

In related IPR2024-00981 and IPR2024-01167, PO did not claim a priority date earlier than Oct. 25, 2013. In its Institution Decisions, the Board noted:

“Patent Owner agrees that the [related patents directed to e-keys are] entitled to a priority date of at least Oct. 25, 2013” and “does not assert that any of petitioner’s references fail to qualify as prior art” based on an earlier priority date. IPR2024-00981, Paper 10, at 33–34; IPR2024-01167, Paper 14, at 30–31.

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

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

Subject matter first appearing in the ’638 application includes FIGs 17-35 and their accompanying descriptions. “E-keys” consistent with the claims are not depicted or described prior to the ’638 application but they are depicted in newly-presented FIGs 29-35. In contrast, the term/stem “key” appears in the earlier ’158 application as filed only three times: p. 18 (historical use of a vehicle’s keys), p. 27 (communication pairing using pairing keys) and p. 27 (vehicle settings synced to a key fob).

EX1030, Application/Control Number: 90/019,456, Final Rejection, at 2–3. The PTO further noted that the Patent Owner “does not seek to traverse any prior art currently of record based on priority.” *Id.*

VI. CLAIM CONSTRUCTION

The claim terms should be given their plain and ordinary meaning under *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005). EX1003, ¶¶88-89.

VII. GROUNDS

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

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

Sekiyama was filed on November 26, 2008, and published on June 10, 2010. It is thus prior art under at least §102(a)(1), or pre-AIA §§102(a)-(b). EX1003, ¶91.

Sekiyama is a Toyota patent application publication that describes an “electronic key system that allows restrictions on functions that can be executed with a duplicate electronic key.” EX1005, Abstract. Sekiyama teaches restricting a “duplicate electronic key” so that it “allows execution of only a subset of functions out of a plurality of functions.” *Id.*, ¶[0007]. The subset of functions may include “locking/unlocking a door lock of a vehicle, ... starting a drive source of the vehicle ... [or] unlocking the trunk.” *Id.*, ¶[0008] (internal quotation marks omitted). EX1003, ¶92.

Sekiyama further discloses a server-mediated e-key issuance flow in which a first mobile device (portable telephone A) sets restriction items and transmits a restricted duplicate e-key issuance request to a center server; the server issues the

restricted duplicate e-key and returns it to portable telephone A, which then transmits the received e-key to a second mobile device (portable telephone B). The recipient device (portable telephone B) stores and uses the e-key with the vehicle's electronic-key ECU (*e.g.*, ECU 41) to control locking/unlocking and engine start. EX1005, ¶¶[0032]–[0040], [0018]; EX1003, ¶93.

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

Kleve was filed November 7, 2012, and published May 8, 2014. It is thus prior art under at least §102(a)(2), or pre-AIA §102(e). EX1003, ¶94.

Kleve is a Ford patent application publication directed to an owner-to-temporary-user “rental micro-business” implemented via a smartphone application and a website. EX1004, Abstract, ¶¶[0036], [0056]. Once rental terms are agreed to, the Owner “enter[s] . . . authorization credentials . . . to set up a virtual key,” and the system “may generate a virtual key to distribute to the Temporary User and VCS [vehicle computing system],” which it then sends “in an encrypted message” to the Temporary User's nomadic device (*e.g.*, smartphone); the virtual key is “used to enter and enable the vehicle drive away event.” *Id.*, ¶¶[0039], [0044], [0062]–[0063], Fig. 3B; EX1003, ¶95.

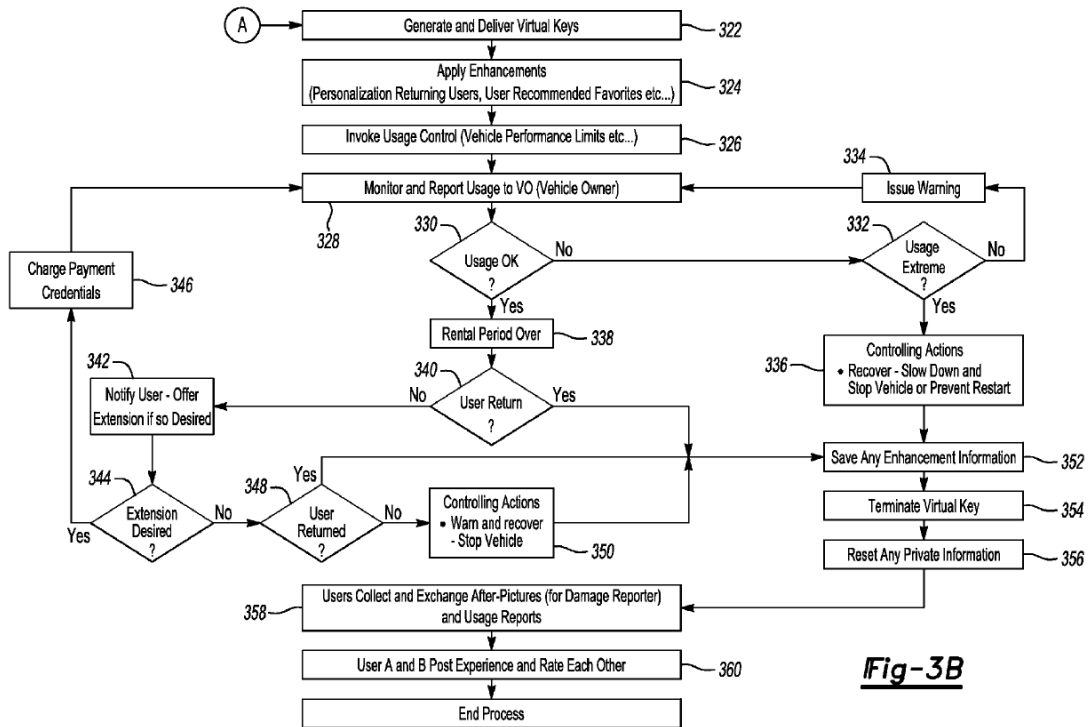
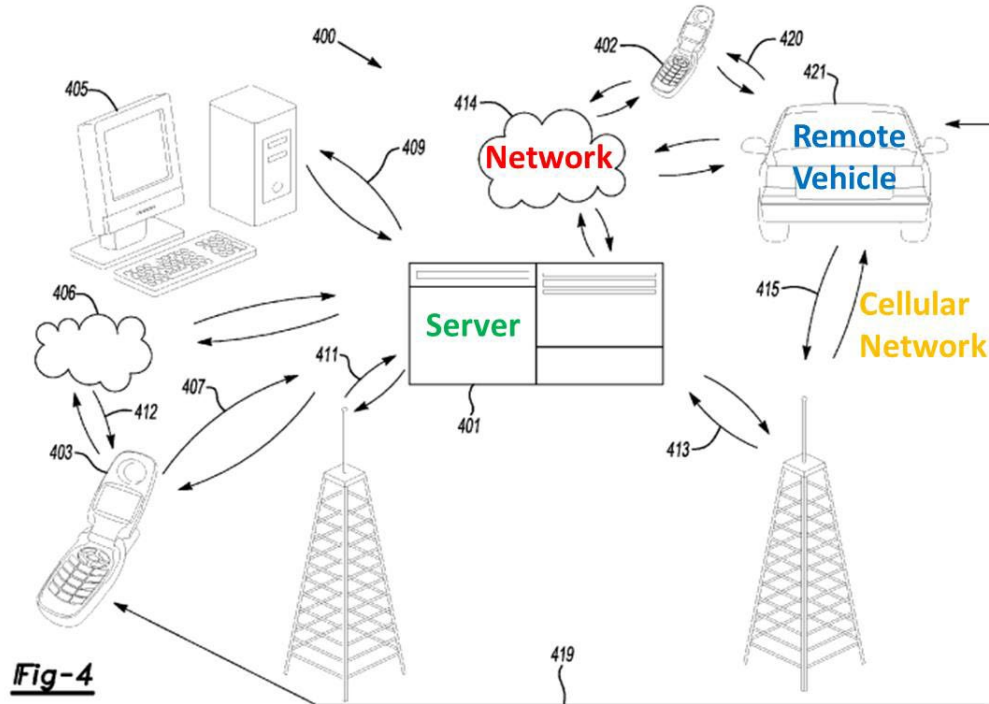


Fig-3B

Kleve’s vehicle includes a VCS that communicates wirelessly with a server system (depicted as “server(s) 401”), either directly or via a user’s mobile device (e.g., over Bluetooth or cellular), and the server “may route an incoming signal from a nomadic device ... to the appropriate remote vehicle.” EX1004, ¶¶[0035], [0057], [0060], Fig. 4; EX1003, ¶96.



The vehicle owner may impose time-bounded (*i.e.*, rental period), speed, and geographic restrictions on usage, and the system monitors and enforces them—issuing warnings, preventing start and restart or slowing and stopping the vehicle upon violations, and terminating and clearing the virtual key at the end of the rental. EX1004, ¶¶[0040]–[0043], [0051]–[0055], [0068]; EX1003, ¶97.

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

Hatton was filed March 14, 2013, and issued April 7, 2015. It is thus prior art under at least §102(a)(2), or pre-AIA §102(e). EX1003, ¶98.

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

Compare EX1004 (Kleve), Fig. 1, *with* EX1008 (Hatton), Fig. 1; EX1003, ¶99. Hatton teaches that a “mobile device 124 may be configured using a software application to communicate with the VCS,” with encrypted data used for device recognition and to unlock and start the vehicle. EX1008, 7:21–23; *see also id.*, 7:11–45, 7:49–56. The application “may be ... developed and/or associated with the vehicle manufacturer.” EX1008, 12:46–51; EX1003, ¶99.

Hatton further teaches secure, app-mediated key data on the device—for example, a user “typ[es] a pin number on the [software] application,” which is “associated as the primary or secondary key.” EX1008, 15:37–41. Once recognized, the mobile device can “start[] the vehicle” and “unlock[]/lock[] doors,” with wireless communication technologies used for mobile-VCS exchanges. *Id.*, 13:24–27; *see also id.*, 7:56–60; EX1003, ¶100.

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

Xiao was filed on December 22, 2010, published on June 28, 2012, and issued May 27, 2014. It is thus prior art under at least §102(a)(1), or pre-AIA §§102(a)-(b). EX1003, ¶101.

Xiao generally describes “providing a wireless automobile key service.” EX1010, Abstract; EX1003, ¶102. Xiao’s system uses a mobile device to “command[] an automobile.” EX1010, 2:29–30. The mobile device includes a “wireless automobile key service application” through which the operator of the

vehicle “register[s] for the disclosed wireless automobile key service ... and create[s] an account for one or more mobile devices 110, automobile operators, and/or automobiles 112.” *Id.*, 4:33–36, 4:46–56. A user’s account may include information about the user’s “mobile ID 610, operator authentication information 612, operator profile information 614, automobile permissions information 616, and a default automobile ID 617.” *Id.*, 12:8–13. Xiao further teaches that the server infrastructure “may be associated with an automobile company,” and mobile–server communication over cellular and PAN (*e.g.*, Bluetooth) links. *Id.*, 3:18–19, 3:46–54, 4:46–56, Fig. 4. In operation, the mobile device can request automobile health and status information—including “battery charge level”—and receive/display a report on the device. *Id.*, 6:49–63, 7:35–55; EX1003, ¶102.

5. Motivation to Combine

A POSITA would have been motivated to combine Sekiyama’s system of sharing of e-keys with (i) Kleve’s website for owner and recipient to agree to terms, (ii) Hatton’s manufacturer-provided mobile application and encrypted device with VCS key handling, and (iii) Xiao’s automobile company-associated server and account framework, with a reasonable expectation of success and predictable results. EX1003, ¶103, *see also id.*, ¶¶104–128. *See KSR*, 550 U.S. at 416–22 (underscoring that it is obvious to combine familiar elements according to known methods to yield

predictable results, that market forces and design incentives can supply motivation, and that common sense applies).

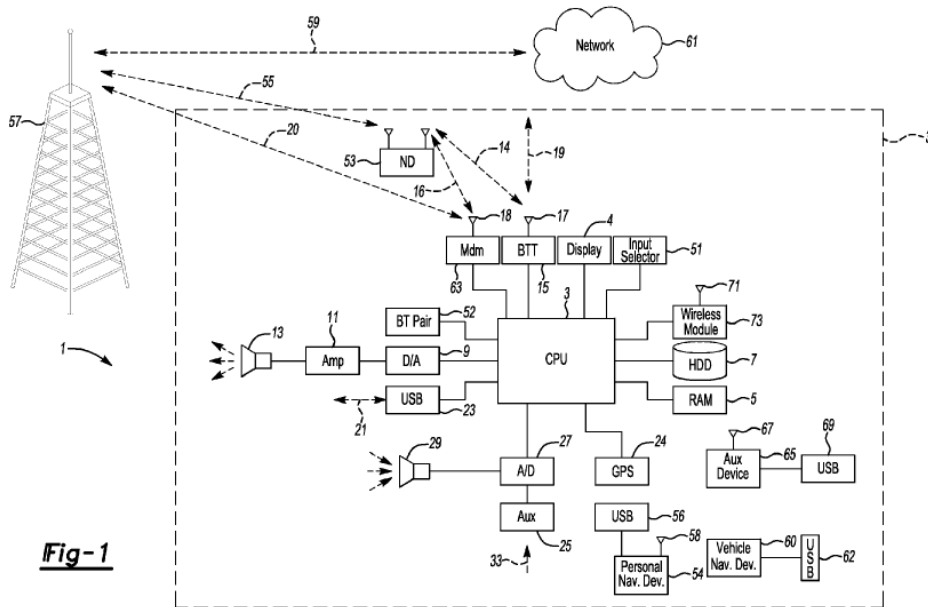
(a) **Pre-agreement of restrictions and distribution of e-key (Sekiyama + Kleve)**

Sekiyama teaches an e-key sharing system designed to enable owners to “lend” their vehicles to others (*e.g.*, valets or other “borrowers”), with restrictions on usage time, vehicle access, and functions. *See, e.g.*, EX1005, Abstract; ¶[0038] (“This eliminates the need to *lend* a physical key.”) (emphasis added); ¶[0047] (“[T]he restricted duplicate electronic key has been transmitted *from owner A to borrower B.*”) (emphasis added); ¶[0048] (“[I]t becomes possible to *lend a duplicate electronic key to another person* while resolving the security problems involved Moreover, by lending a restricted duplicate electronic key with a *set expiration time*, the need for the *borrower* to perform the action of returning the duplicate key is eliminated.”) (emphasis added). In such lending scenarios, a POSITA would have recognized the practical need to capture agreed terms before issuance (*e.g.*, identity, duration, permitted functions) to ensure controlled access and auditability. EX1003, ¶104.

A POSITA would have found it obvious to agree to the terms of the restricted usage, such as the expiration period, prior to generating the restricted e-key. EX1003, ¶105. Further, a POSITA would have understood that Sekiyama’s restricted e-key could be monetized in a rental or car-sharing business context and

would have been motivated to look to contemporaneous rental/car-sharing art for known mechanisms to capture agreed terms before issuance. *Id.* Kleve is one such example, teaching a website/app workflow where the parties agree to terms that the server then uses to issue a virtual key. *See* EX1004, ¶¶[0036]–[0039], [0062]–[0063]; EX1003, ¶105.

Both Sekiyama and Kleve depict the same client-server/VCS pattern (owner device ↔ server ↔ VCS/vehicle controller, with PAN/cellular links), so Kleve’s Fig. 1 serves as a representative diagram of this Sekiyama/Kleve architecture. *See* EX1004, ¶¶[0021]–[0036], Fig. 1; EX1005, ¶¶[0014]–[0016], [0021], [0031], [0034]–[0039]; EX1003, ¶106.



In the combined system, a POSITA would use Kleve's server-hosted owner profile/account (with owner credentials and vehicle data, EX1004, ¶[0036]) to authenticate the owner and bind sharing requests and restriction settings to the owner's registered e-key (master key) within the Sekiyama/Kleve architecture by using the logged-in owner profile to look up and apply the restriction items associated with the master e-key during issuance (EX1005, ¶¶[0012], [0036]), with ECU authentication against stored encrypted data (*Id.*, ¶[0015]). EX1003, ¶107. This is a routine server-side association of account → key → restrictions familiar to a POSITA. EX1003, ¶107. Using Kleve's term-capture/UI flow to populate Sekiyama's server-side restriction fields is a routine integration of complementary components in a shared client-server/VCS architecture, with predictable results and a reasonable expectation of success. In short, the combination yields a flexible platform that supports different sharing scenarios. *Id. See KSR*, 550 U.S. at 417–22.

Moreover, a POSITA would also be motivated because an executed agreement between the parties would allow the owner legal recourse via contract law. EX1003, ¶108. It would also clearly set out the applicable restrictions for the recipient—reducing inadvertent violations. *Id.* For example, knowing the usage period in advance helps ensure the vehicle is returned to the proper location before expiration. *Id.* As Dr. Almeroth explains, rental and car-sharing arrangements routinely employ written agreements that specify who may use the vehicle, for how

long, and under what conditions; these agreements are pervasive in vehicle-sharing contexts. Integrating that contract workflow (including the agreed restrictions) into the e-key issuance process is a straightforward application of common industry practice, ensuring the server captures the parameters before issuance, enabling automated enforcement, and improving auditability—a routine design choice with predictable results and a reasonable expectation of success. *See id.*, ¶108; *KSR*, 550 U.S. at 417–22.

Once terms are finalized and a key must be delivered, there are a finite number of well-known delivery models in secure access systems—*e.g.*, server-to-recipient-device issuance (as in *Kleve*, EX1004), owner-device relay to the recipient device (*e.g.*, Bluetooth or e-mail, as in *Sekiyama*, EX1005, ¶[0031]), or physical handover. EX1003, ¶109. A POSITA would understand the scenario-dependent tradeoffs: server issuance provides remote immediacy, centralized logging, and automation, but depends on network availability; short-range relay (*e.g.*, Bluetooth) is simple and offline-capable, but requires proximity and compatible devices; e-mail relay enables remote delivery without proximity, but introduces manual steps and third-party client handling; physical handover offers direct control, but requires in-person exchange and lacks automation. EX1003, ¶109. Given these known options, a POSITA would view *Kleve*'s server-to-device issuance as an obvious choice to try within *Sekiyama*'s restricted e-key framework, particularly where convenience,

auditability, and remote access are desired—fitting naturally into the shared client-server/VCS architecture and yielding predictable results with a reasonable expectation of success. *See id.*; *KSR*, 550 U.S. at 421–22.

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

With any e-key system, a POSITA would have been motivated to enhance security, including securing exchanges among the server, mobile devices, and the vehicle using well-known encryption and authentication methods. EX1003, ¶110.

For example, Sekiyama explains that conventional e-key systems “perform authentication” between an e-key and a vehicle using wireless communication (*e.g.*, transmitting “ID codes” or “key codes” with expirations), and that security can be improved by “imposing restrictions on the number of activations” and/or by “generating signature data based on random numbers during communication between an electronic key and a vehicle.” EX1005, ¶¶[0002]–[0003]. In Sekiyama’s e-key system, the vehicle ECU “performs *authentication* of the electronic key” before enabling “locking/unlocking of the door lock” and “permission to start the engine,” based on recognized key information; the ECU’s “electronic key recognition unit 42” compares “the *encrypted* data stored in the storage unit with the key information read from the portable telephone 10, 30.” *Id.*, ¶¶[0015], [0040] (emphasis added); EX1003, ¶111.

Kleve likewise employs a smartphone app/website within a VCS ecosystem and sends a virtual key to the recipient device “in an *encrypted* message.” EX1004, ¶¶[0036]–[0039], [0063]; EX1003, ¶112. Kleve further teaches secure BLUETOOTH communications between a renter’s smartphone and the vehicle’s VCS (*e.g.*, Ford SYNC). EX1004, Abstract, ¶¶[0008]–[0009], [0021]; *see also* ¶[0031] (“[I]ncoming data can be passed through the nomadic [smartphone] device ... through the onboard BLUETOOTH transceiver and into the vehicle’s internal processor 3.”); EX1003, ¶112.

A POSITA would recognize that when control of—or access to—an asset occurs electronically, significant security protections are needed, and would continually look to strengthen those protections to increase owner trust, even for short term scenarios (*e.g.*, valet). EX1003, ¶113. Within that effort, a domain-aligned reference like Hatton would be a natural source of additional, well-understood security mechanisms for app-mediated VCS exchanges. *Id.*

Hatton discloses a mobile application (optionally manufacturer-provided) that communicates with the vehicle computing system (“VCS”) using encrypted data, supports device recognition, and enables a user to enter a PIN associated “as the primary or secondary key.” EX1008, 7:11–56, 12:46–51, 13:24–27, 15:37–41; EX1003, ¶114.

Having captured terms per Kleve, a POSITA would next secure the mobile-to-VCS exchanges (*e.g.*, activation and command flows) to protect contract-bounded access and key material in the Sekiyama + Kleve rental context—where restricted e-keys are issued, a virtual key is generated and delivered to the recipient, and restrictions (functions/time) are enforced. EX1005, ¶¶[0007]–[0008], [0017], [0034]; EX1004, ¶¶[0036]–[0039], [0062]–[0063]; EX1003, ¶115. Among the finite, well-known methods in VCS ecosystems are app-mediated encrypted communications with device recognition, and PIN gating—precisely the pattern Hatton supplies in the same Ford VCS-style architecture. EX1003, ¶115. Under *KSR*, selecting a known security pattern (Hatton) to harden a known issuance/use flow (Sekiyama + Kleve) is “combin[ing] ... familiar elements according to known methods ... [with] predictable results.” *KSR*, 550 U.S. at 416; EX1003, ¶115.

Each reference depicts an in-vehicle computing node with processor/memory, user I/O (*e.g.*, display, microphone), wireless transceivers (*e.g.*, Bluetooth and cellular modems) for pairing with a nomadic device and server communications, and a vehicle network interface (*e.g.*, CAN) to body/engine control modules (locks, start/ignition). *See* EX1004, ¶¶[0021]–[0036], Fig. 1; EX1008, 2:54–5:53, Fig. 1; EX1005, ¶¶[0014]–[0016], [0039]–[0040]; EX1003, ¶116. This shared topology confirms drop-in interoperability and supports a reasonable expectation of success (*see* §5(e)); EX1003, ¶116.

A POSITA would further be motivated to select Hatton’s manufacturer-associated app implementation (EX1008, 12:46–51) to align the mobile application with OEM VCS services and security (PIN control, device recognition, encrypted exchanges), a routine fit in the same client–server/VCS architecture. EX1003, ¶117. And because Kleve ties the app to an owner account (user profile) for initiating key sharing (EX1004, ¶¶[0036]–[0037], [0047]), integrating Hatton’s app preserves that owner-account association while adding the OEM app’s security/usability features—yielding predictable results with a reasonable expectation of success (*see* §5(e)). *See* EX1003, ¶117; *KSR*, 550 U.S. at 417–22.

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

Sekiyama, developed by Toyota, and Kleve/Hatton by Ford, are e-key systems operating in an OEM vehicle-computing context (cloud-connected servers, mobile devices and onboard vehicle computing systems). EX1003, ¶118. Starting from that combined baseline, a POSITA would first inventory the backend’s expected duties—hosting owner/recipient accounts and permissions (per Kleve), enforcing restriction/expiration (per Sekiyama), and supporting secure app↔VCS exchanges (per Hatton)—and then look to contemporaneous automotive backend art implementing those duties in practice (often on OEM-associated cloud servers) and exposing device-visible status/telemetry. *Id.*

Kleve already teaches user accounts and a mobile/website flow that captures terms and delivers a virtual key. EX1004, ¶¶[0036]–[0039], [0062]–[0063]. Sekiyama provides server-side issuance and restriction enforcement. EX1005, ¶¶[0007]–[0008], [0017], [0034]. Hatton supplies secure, app-mediated exchanges with the VCS (encrypted communications, device recognition, PIN gating). EX1008, 7:11–56, 13:24–27, 15:37–41. Together these references play complementary roles: Sekiyama supplies restricted e-key issuance/enforcement; Kleve supplies the account/app term-capture and delivery workflow; Hatton supplies app-layer security (encrypted exchanges, device recognition, PIN gating); and Xiao adds OEM-associated hosting and device-visible telemetry—yielding predictable benefits in security, manufacturer integration, and status visibility. EX1003, ¶119.

Xiao contributes two conventional backend elements that complement this base: (i) servers “associated with an automobile company” communicating with the mobile app over cellular and PAN (*e.g.*, Bluetooth), and (ii) device-visible vehicle status/telemetry, including battery charge level requested from the vehicle and displayed on the device. EX1010, 3:12–20, 3:46–54, 4:33–36, 4:46–56, 6:49–63, 7:35–55, 12:8–13; EX1003, ¶120.

A POSITA would have been motivated to add Xiao because the base system (restricted e-keys in a contractual setting with secure app↔VCS exchanges) benefits from a manufacturer-associated backend for service integration and policy

propagation, and from surfacing status to the device after issuance. The references are architecture-compatible: Kleve's account/app flow remains the account mechanism; Sekiyama's server enforces restrictions; Hatton secures the app↔VCS path; and Xiao adds manufacturer association and telemetry reporting within the same client-server/VCS pattern. EX1003, ¶121. Implementing Xiao's manufacturer-associated server simply hosts the existing account/permission records (as taught by Kleve) and exposes status calls to the app (as taught by Xiao), without redesign. *See* EX1004, Fig. 1; EX1008, Fig. 1; EX1010, 4:46–56; EX1003, ¶121. Xiao's OEM hosting and telemetry operate as drop-in backend services within the same client–server/VCS pattern (cellular/PAN links, authenticated exchanges), requiring no architectural redesign. EX1003, ¶121.

With Xiao, the combined system (i) uses servers associated with the vehicle manufacturer; (ii) communicates over cellular/PAN; and (iii) allows the recipient device to access vehicle status such as battery charge level—while Sekiyama enforces function/time limits and Kleve/Hatton provide term capture and secure app/VCS operation. *See* EX1010, 6:49–63, 7:35–55; EX1005, ¶¶[0007]–[0008], [0034]; EX1004, ¶¶[0036]–[0039], [0062]–[0063]; EX1008, 7:11–56, 13:24–27; EX1003, ¶122. This is a routine, predictable integration of well-understood backend elements, with a reasonable expectation of success. *See* EX1003 ¶122; *KSR*, 550 U.S. at 417–22.

(d) Technical compatibility and routine implementation

All four references operate in the same field—vehicle e-key services built around a mobile app, a backend server, and a VCS/onboard controller. EX1004 (Kleve), ¶¶[0021]–[0036], [0039], [0048]–[0049]; EX1005 (Sekiyama), ¶¶[0007]–[0008], [0034]–[0040]; EX1008 (Hatton), 1:6–8; EX1010 (Xiao), Abstract; EX1003, ¶123.

They use standard communication links (cellular, Bluetooth/PAN) and conventional data flows (app ↔ server; app ↔ VCS). EX1004, ¶¶[0035], [0057], [0060], [0063]; EX1008, 7:11–60; EX1010, 3:46–54, Fig. 4; EX1003, ¶124.

The combinations require straightforward software integration (UI elements, API calls, and encryption that the art already uses) and predictably improve security, manageability, and user experience—consistent with *KSR*'s “predictable results” rationale. *See KSR*, 550 U.S. at 417–22; *see also* EX1003 ¶125.

(e) Reasonable expectation of success

A POSITA would have had a reasonable expectation of success integrating these references because each teaches known elements performing their conventional roles within a shared client-server/VCS ecosystem, with minimal redesign or incompatibility (EX1003, ¶126):

- **Server/device workflow and routing:** Sekiyama contemplates issuance by a center server and device-side use of a restricted/duplicate key, with the owner

terminal sending the issuance request and the server returning the key for use on the recipient device—*i.e.*, split processing across phone and server with server-routed communications. EX1005, ¶¶[0032]–[0040].

- **Agreement capture and delivery flow:** Kleve provides the app/website workflow to establish terms (user profiles, term exchange) and then deliver the virtual key to the recipient device, fitting the same phone ↔ server ↔ VCS pattern. EX1004, ¶¶[0036]–[0039], [0048]–[0049], [0062]–[0063].
- **Secure mobile ↔ VCS exchanges:** Hatton supplies app-mediated encrypted communications, device recognition, and PIN-gated key use in a Ford VCS topology indistinguishable from Kleve’s, confirming drop-in compatibility of secure exchanges. EX1008, 7:11–56, 13:24–27, 15:37–41; *compare* EX1008, Fig. 1, *with* EX1004, Fig. 1. A POSITA would therefore expect success whether secure key material is generated server-side (as in Sekiyama’s issuance of key information used for ECU authentication, EX1005, ¶¶[0015], [0036]) or device-side (as in Hatton’s PIN-associated mobile key, EX1008, 7:11–56, 15:37–41), because both rely on standard encryption and credential verification at the vehicle ECU. EX1003, ¶126.
- **Account/telemetry backend:** Xiao teaches account-centric backends that “may be associated with an automobile company,” with mobile ↔ server and PAN/cellular links, and status/health reporting to the device (*e.g.*, battery

charge level), which align with the same communication layers used in the above references. EX1010, 3:12–20, 3:46–54, 4:33–36, 4:46–56, 6:49–63, 7:35–55, 12:8–13.

As Dr. Almeroth explains, implementing the combination uses standard interfaces (e.g., app UI to capture terms; API calls for issuance and acknowledgments; existing encrypted mobile ↔ VCS channels; account tables for identities/permissions; telematics/status endpoints), all within conventional VCS and server architectures—*a routine engineering task yielding predictable results* under *KSR*. See EX1003 ¶127; *KSR*, 550 U.S. at 417–22.

Taken together, these references teach interoperable, conventional components such that a POSITA would have a reasonable expectation of success implementing either server-side or device-side secure key generation within the combined system. See EX1003, ¶128; see also EX1005, ¶¶[0015], [0036]; EX1008, 7:11–56, 15:37–41.

6. Claim 1

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

To the extent the preamble is limiting, the Sekiyama + Kleve + Hatton + Xiao combination (hereafter “the combined system”) discloses *a method for sharing electronic keys (e-keys)*. EX1003, ¶129. Sekiyama teaches an “electronic key system” in which the “server 20 of the management center” performs “issuance of

electronic keys.” EX1005, ¶[0021]. The electronic key system can issue a “master key,” which “allows all functions of the vehicle 40 to be executed without restrictions,” as well as “restricted *duplicate* electronic keys,” which “allows only a subset of the plurality of functions.” *Id.*, ¶[0012] (emphasis added). The restricted duplicate keys are “lent out ... to others,” indicating that they are *shared* keys. *Id.*, ¶[0051], [0048] (“[I]t becomes possible to lend a duplicate electronic key to another person while resolving the security problems involved.”). In the combined system, Sekiyama and Kleve supply the familiar owner–recipient transaction flow and delivery mechanics for sharing, Hatton supplies the app-mediated secure handling used when the recipient device presents/uses the shared key with the VCS, and Xiao supplies the account/server context typical of manufacturer-associated backends. *See* EX1004, ¶[0036]–[0039], [0062]–[0063]; EX1005, ¶[0025]–[0027], [0031]–[0040]; EX1008, 7:11–56, 15:37–41; EX1010, 3:12–20, 4:33–36, 12:8–13; EX1003, ¶129.

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

In the combined system, Sekiyama teaches “*processing a request to share an electronic key (e-key) of a vehicle with a recipient device*” where an owner’s device requests the issuance of a restricted key for use by a recipient device. EX1003, ¶130.

Specifically, Sekiyama teaches that “portable telephone A 10” (*i.e.*, a **sharing device**) issues “a restricted duplicate electronic key issuance **request**” to the “management center.” EX1005, ¶[0035] (emphasis added). In response, the restricted key is sent for use by “portable telephone B 30” (*i.e.*, a **recipient device**) to allow access to a vehicle. *Id.*, ¶¶[0038]–[0039].

Further, as expressly taught by Kleve, it would have been obvious in the combined system for the server to send the key to the recipient device (EX1004, ¶¶[0062]–[0063] (describing the owner entering information into a server to “set up a virtual key,” which is “sent in an encrypted message ... to the Temporary User’s nomadic device,” *i.e.*, a **recipient device**)). EX1003, ¶131. As discussed in §5(a), a POSITA would have implemented server-to-recipient issuance as part of the combined system as a routine client-server integration yielding predictable results. *See* EX1004, ¶¶[0062]–[0063]; EX1005, ¶¶[0035], [0038]–[0039]; EX1003, ¶131.

“the request to share the e-key being received responsive to a message being sent to the recipient device from a sharing device”:

As explained in Ground 2 (§112), *the ’715 patent’s specification does not explain how the e-key request is responsive to a message sent from the sharing device to the recipient device.* EX1003, ¶132. And while PO may argue that the overall flow “implies” such coupling or that a POSITA would infer missing app internals, the specification itself never links a recipient-bound message to the

server's receipt/processing of the request. *Id.* The specification describes that "the app on the user's mobile device can request that a message be sent to the recipient, so that the recipient can receive the e-keys and be granted access to the vehicle," and particularly that the recipient receives "instructions for obtaining/validating/using the e-keys." EX1001, 5:11–19. *That is, the '715 patent describes a way for the owner to message a recipient that the e-key is available. However, the '715 patent generally describes that the owner requests the issuance of the e-key without any reference to such a message. Id.*, 42:10–11 ("Bob [the owner] can request that keys be sent to the valet"), 42:35–37 ("FIG. 29 illustrates an example where an owner of the vehicle Bob, is able to assign electronic keys (e-keys) 650 to any number of users."), 43:37–46 ("[T]he user-owner of the vehicle can assign a valet with access to the vehicle by going on an application (App or website) ... and requesting that the e-keys be sent to the recipient."), 43:47–51 ("[A] user, John ... is able to communicate and send e-keys to another user (Bob). In this example, the sending of e-keys will include the sending of the request to a server"), 44:51–54 ("[T]he request is associated with the user account making the request. The user account will be John's account, which will have predefined information associated with the vehicles that John is able to

assign e-keys for.”), 45:37–43 (“[A] request is sent by John ... to send e-keys to Bob.”)²; EX1003, ¶132.

Thus, while the ’715 patent describes the owner providing a message to the recipient, it does not disclose a causal relationship between that message and the sending of a request by the owner (or the recipient) or the processing thereof. EX1003, ¶133. To the extent PO asserts that this claim limitation “responsive to” requires a direct causal connection between a message being sent to a recipient and the issuance/processing of a request (i.e., the server receives/processes the request because of the recipient-bound message), the claim fails written description and enablement support and is invalid under 35 U.S.C. §112(a) (see Ground 2 (§112); EX1003, ¶133).

Regardless of PO’s §112 position, and even under a non-causal reading, the combined system renders this limitation obvious. EX1003, ¶134. Kleve describes that, prior to the request for an e-key, the owner and recipient “have already ... both agreed to the rental agreement.” EX1004, ¶[0062]. Kleve explains that the

² The ’715 patent provides an example where “the recipient may directly request e-keys,” but does not provide any disclosure in that example of the recipient’s request being responsive to receiving a message from an owner’s device. EX1001, 48:57–59.

agreement of terms involves the owner and recipient messaging each other. For example, Kleve describes that the owner can deliver to the recipient a “standard rental agreement form” or a “custom form based on the type of use the Temporary user [recipient] is requesting to use the vehicle for.” EX1004, ¶[0038]. In Kleve, the recipient’s acceptance/return of the terms precedes the owner’s submission of those agreed terms to the server, which then sets up the key—so the recipient-facing message(s) function as the trigger for the owner/server request flow. EX1004, ¶¶[0038], [0062]. Once that owner request exists, Sekiyama supplies the downstream mechanics: the center server generates key information according to owner-set restriction items and issues a restricted duplicate key for the recipient device; the vehicle ECU authenticates and controls use based on that key information. EX1005, ¶¶[0034]–[0036], [0038]–[0040], [0015]. A POSITA would, from this end-to-end flow in the combined system—owner↔recipient messaging (Kleve) followed by server-side processing and issuance (Sekiyama)—understand that the processing is “responsive to” the message in ordinary client-server e-key workflows. See EX1004, ¶¶[0038], [0062]; EX1005, ¶¶[0034]–[0039]; EX1003, ¶134.

As discussed in §5(a) above, a POSITA would have found it obvious to incorporate these teachings into the combined system. EX1003, ¶135.

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

In the combined system, Sekiyama teaches that the server determines that the request to share originates from, and therefore is associated with, the owner’s device, *i.e.*, **a registered owner e-key**. EX1003, ¶136. Specifically, Sekiyama teaches that “portable telephone A 10,” the owner’s device, “functions as a master key that allows all functions of the vehicle 40 to be executed without restrictions.” EX1005, ¶[0012].

Sekiyama further teaches that “portable telephone A 10 performs a restricted duplicate electronic key issuance request” that is sent to the server. *Id.*, ¶[0035]. In response to that request, the server “issues an electronic key that functions as a restricted duplicate electronic key,” with restrictions set “according to the restriction items that were set on the portable telephone A 10,” *i.e.*, **a registered owner e-key**. *Id.*, ¶[0036]. In other words, because the server issues a specific restricted key in accordance with the specific restrictions set by the **registered owner e-key**, the server has determined the request is associated with that registered owner e-key. EX1003, ¶137.

Kleve discloses that the owner “may set up a user profile” on the server (e.g., via website/nomadic device) including vehicle-identifying information (make/model/year). EX1004, ¶[0037]. A POSITA would understand that this profile creation is the server-side **registration** step—*i.e.*, creation of an authenticated owner

account linked to the vehicle(s)—because subsequent actions (including sharing) are performed while logged in under the owner’s credentials. EX1003, ¶138. Accordingly, when the owner submits the sharing request while authenticated, the server determines that the request is associated with the owner’s registered credentials/e-key. *Id.* This is consistent with Sekiyama’s server issuing a restricted key “according to” restriction items set from the owner’s master key (EX1005, ¶[0036]) and with Xiao’s account/credential model (mobile ID, authentication data, permissions) that ties requests to a registered account/e-key. EX1010, 4:33–36; 12:8–12. Motivation to incorporate Kleve’s server-hosted owner profile/account—and Xiao’s account/credential framework for binding sharing requests to a registered owner e-key—is discussed in §5 (Motivation to Combine); EX1003, ¶138.

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

“processing instructions”: In the combined system, Sekiyama discloses a “center server” which performs various operations, including through the use of an “electronic key issuance unit 21.” *See, e.g.,* EX1005, ¶[0021]. A POSITA would understand that a server performs operations by processing instructions, specifically, server program code and firmware that comprises of instructions that are executed by a processor. EX1003, ¶139. Sekiyama expressly identifies server 20’s “electronic

key issuance unit 21” as the module that processes the owner’s request and performs issuance. EX1005, ¶¶[0021], [0035]–[0036].

“enable the e-key to be securely generated”: Sekiyama teaches that the recipient’s e-key is *securely generated*. EX1003, ¶140. In particular, when the restricted key is generated, the server generates “key information ... according to the restriction items that were set” by the owner. EX1005, ¶[0036]. Such “key information” is used by the vehicle to “authenticate[] the electronic key by comparing the encrypted data stored in the [vehicle’s] storage unit with the key information read from the portable telephone 10, 30.” *Id.*, ¶[0015]. Specifically, the “key information” allows the system to “determine[] whether the electronic key is a key that allows execution of functions of the vehicle 40.” *Id.* In other words, Sekiyama describes that e-keys are generated with “key information” that matches encrypted information stored on the vehicle to authenticate the key—thereby ensuring that the key was securely generated. EX1003, ¶140. A POSITA would recognize this as the standard encryption/authentication model in vehicle ECUs (key information generated per owner-set restrictions and later verified against encrypted vehicle data), consistent with §5(e). EX1005, ¶¶[0015], [0036]; EX1003, ¶140. Likewise, as discussed above, Kleve teaches user accounts and a mobile/website flow that captures terms and delivers a virtual key. Kleve describes its communications, in one embodiment, as employing Bluetooth. The Bluetooth

standard as it existed prior to the priority date included BR/EDR secure simple pairing, a secure communication. (EX1029 (Bluetooth Core Specification v4.0) at page 85; see also pages 85-92).³ Indeed, Bluetooth states that the goal of secure simple pairing is to “protect[] against passive eavesdropping and protect against man-in-the middle (MITM) attacks (active eavesdropping).” *Id.* A person of ordinary skill in the art would thus understand that Kleve’s discussion of Bluetooth

³ As Dr. Almeroth testifies, the Bluetooth standard, and the Bluetooth specification, are both very well known in the industry. EX1003, ¶140, n.4. Bluetooth.com is the well-known repository for versions of the Bluetooth standard *Id.* The Bluetooth standard (Bluetooth Core Specification v4.0) attached at EX1029 was downloaded from the Bluetooth.com archive at <https://www.bluetooth.com/specifications/archived-specifications/> and <https://www.bluetooth.com/specifications/specs/core-specification-4-0/>. EX1003, ¶140, n.4. A POSITA familiar with the standard would understand that the date printed on the front of the standard, June 30, 2010, is reliable and indicates the document was publicly available at least on that date, and a POSITA, having deep understanding of the Bluetooth standard, would have been readily able to locate and search the standard. *Id.*

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

Additionally, Hatton also teaches secure on-device generation and use of an electronic key by a mobile app—the user enters a PIN and the system associates that PIN as a primary/secondary key, with encrypted data used for device recognition and start/unlock—which a POSITA would have combined with Sekiyama to meet this limitation. EX1008, 7:11–56, 13:24–27, 15:37–41; EX1003, ¶141. A POSITA would have had a reasonable expectation of success implementing either server-side (Sekiyama) or device-side (Hatton) secure key generation for the reasons explained in §5(e). EX1003, ¶141.

“e-key ... for use by the recipient device”: Sekiyama teaches that the “restricted duplicate electronic key” is delivered to “portable telephone B 30” (*i.e.* ***recipient device***). EX1005, ¶[0038]. The key is “use[d][by] ... the duplicate key user B [by] ... transmit[ting] the key information to ... [a vehicle’s] electronic key ECU 41,” which controls the vehicle, such as “locking/unlocking” and “start[ing] the engine ... based on the recognized key information.” *Id.*, ¶[0039]–[0040]; EX1003, ¶142.

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

“saving information regarding the e-key with a server”: In the combined system, Sekiyama teaches that the server receives, maintains, and saves “key

information” regarding the restricted key, such as “the functions that will be usable with the restricted duplicate electronic key” and “the expiration” of the key. EX1005, ¶¶[0034], [0036], [0025] (“Information related to the subset of functions that was set is outputted to the center server 20.”).⁴ A POSITA would understand that issuing and enforcing a restricted, expiring e-key requires the server to persist that key information at least through the access period so it can be used for authentication and expiration checks. EX1003, ¶143.

In addition, during operation of the restricted key, the server “periodically” requests and the vehicle “transmits a vehicle status related signal to the center server.” EX1005, ¶¶[0041]–[0042]. Such information can be “check[ed]” by the owner’s device “at any time” via request. *Id.*, ¶¶[0043]–[0044]. Thus, Sekiyama’s disclosure of periodic uploads and on-demand owner queries indicates that the server stores status/usage information related to the active e-key, *i.e.*, “saving information regarding the e-key.” EX1003, ¶144. A POSITA would recognize this as routine server-side management of e-key records (e.g., key parameters and active-use status) to support validation, expiration, and owner visibility; the claim does not require any

⁴ A POSITA would understand that “outputted to the center server 20” means the server stores the e-key information (*i.e.*, persists the key information for later authentication and expiration checks). (EX1003, ¶143, n.4)

particular schema, and implementing such storage would have been conventional.

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

“server associated with a manufacturer of the vehicle”: As an initial matter, the phrase “associated with a manufacturer of the vehicle” is nonfunctional descriptive material and therefore is not entitled to patentable weight under the printed matter doctrine, because “it claims the content of information” (*i.e.*, who operates the server) and lacks any “functional relationship” to the server. *Praxair*, 890 F.3d at 1031–32; *see also Catalina*, 289 F.3d at 809.⁵ Who owns/operates the server does not alter the server’s structure or the method’s operation. EX1003, ¶145. Nor does characterizing manufacturer operation as “improving reliability/security” supply the missing functional tie—those are at most asserted advantages of *who* hosts the same server functions, not a change to *how* the claimed saving/processing occurs. *See Praxair*, 890 F.3d at 1032 (informational content lacking functional relation is not given patentable weight). Even if this phrase is accorded patentable

⁵ To the extent the Examiner relied on this phrase in allowing the claims, the Examiner erred in according the phrase patentable weight.

weight, the limitation is also met—or obvious—on the merits, as set out below.
EX1003, ¶145.

A POSITA would have understood that Sekiyama’s server is *associated with a manufacturer of the vehicle*. EX1003, ¶146. Sekiyama is a Japanese patent application invented by employees of Toyota Motor Corp. and assigned to Toyota Motor Corp. EX1005. Accordingly, a POSITA would have recognized that the “center server” described in Sekiyama was a server associated with the manufacturer of the vehicle, as the “electronic key system” described in Sekiyama would have been understood to have been developed for use by Toyota and its vehicles. EX1003, ¶146. And even if PO argues Sekiyama lacks an explicit statement of OEM hosting, that only underscores why the claim, if given weight, remains obvious: choosing an OEM-operated server is one of a finite set of routine hosting options (OEM, telematics provider, carrier, third-party) with predictable, generic benefits and no change to the underlying key-saving functionality.

It further would have been an obvious option to host Sekiyama’s server functions on a server operated by (or on behalf of) the vehicle manufacturer. EX1003, ¶147. Multiple contemporaneous references teach manufacturer-associated servers for e-key services. Xiao explains that its wireless automobile key service servers “may be associated with an automobile company.” EX1010, 3:12–20; *see*

also id., 3:46–54, 4:46–56, 12:8–12, 16:48–54.⁶ Thus, a POSITA would have found it obvious to implement Sekiyama’s saving of e-key information on a manufacturer-associated server as one of a finite, predictable set of options for the owner/operator of the server (*e.g.*, vehicle manufacturer, telematics provider, carrier, third-party) with no change to functionality and with a reasonable expectation of success. EX1003, ¶147. A POSITA would have been motivated to select the OEM-associated option taught by Xiao because it centralizes account/permission management, integrates with OEM telematics/ECU support workflows, and improves auditability and lifecycle controls (*e.g.*, credential resets, expiration enforcement)—all without altering Sekiyama’s key-saving/processing operations (EX1010, 3:12–21; 3:46–54; 12:8–13); EX1003, ¶147. This is a routine hosting choice in the same client–server/VCS architecture, yielding predictable results with a reasonable expectation of success (see §5(e)); EX1003, ¶147.

⁶ As noted above, in the relevant period, OEM-hosted cloud servers and account-based provisioning for mobile/vehicle services were conventional. *See, e.g.*, Harris (OEM server provisioning/authentication, EX1009, ¶[0038]) and Cazanias (cloud accounts storing user/vehicle identifiers and policies, EX1011, 6:27–34, 12:13–30, 15:4–33). These references are cited as background corroboration of industry practice; the limitations at issue are satisfied by Xiao. EX1003, ¶147, n.6.

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

In the combined system, Sekiyama teaches that the “restricted duplicate electronic key” is delivered to “portable telephone B 30” (*i.e.*, *recipient device*). EX1005, ¶[0038]; EX1003, ¶148. The key is “use[d] [by] ... the duplicate key user B [by] ... transmit[ting] the key information to ... [a vehicle’s] electronic key ECU 41,” which controls the vehicle, such as “locking/unlocking” and “start[ing] the engine ... based on the recognized key information.” EX1005, ¶¶[0039]–[0040]. A POSITA would recognize this enablement/use as the standard ECU authentication flow (comparing key information to encrypted vehicle data, *id.*, ¶[0015]), making implementation feasible and predictable in the combined system, as discussed in §5(e); EX1003, ¶148.

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

In the combined system, Sekiyama teaches that key request includes various “restriction items,” *i.e.*, *settings to assign a privilege level for use of the vehicle*. EX1003, ¶149. Specifically, Sekiyama teaches that the owner’s device “sets restriction items for the restricted duplicate electronic key,” which are then sent with the request. EX1005, ¶¶[0034]–[0036], Fig. 3 (indicating that the restrictions are set by the owner device).

The “restriction items” provide for *conditions of use of the vehicle*, specifically a “subset of functions[] of the vehicle 40 that can be utilized with the restricted duplicate electronic key.” *Id.*, ¶[0025]; EX1003, ¶150. Such functions include “locking and unlocking of the door lock, permission to start the engine, locking and unlocking of the trunk, locking and unlocking of the console compartment, permission to use the on-board unit functioning as a car navigation device, permission to use the on-board unit functioning as a communication device capable of sending and receiving email,” and “conditions for using those functions (for example, usage time).” EX1005, ¶[0016]–[0017] (internal quotation marks omitted).

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

As discussed above for claim 2, in the combined system, Sekiyama teaches *conditions of use* that include a “conditions for using those functions (for example, usage time)” (*i.e.*, *time frame of use, or an expiration-time of use*), “locking and unlocking of the door lock,” and “permission to start the engine.” *Id.*, ¶[0016]–[0017] (internal quotation marks omitted); EX1003, ¶151.

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

The plain meaning of “application” to a POSITA at the time of the patent is software instructions to perform a particular task. EX1003, ¶152. Accordingly, a POSITA would understand that, in the combined system, Sekiyama’s teachings of an owner’s device (*i.e.*, **sharing device**) issuing the sharing of an e-key is performed by an application on the device. *Id.*

In addition, Kleve discloses an application for requesting an e-key that is associated with an owner account. EX1003, ¶153. For example, Kleve discloses a “rental microbusiness” implemented as a “smart phone application” that an Owner uses to log into and manage a user profile (owner account) and to initiate sharing/distribution of virtual keys from the sharing device. EX1004, ¶¶[0036] (smartphone application is used to manage “assets and/or user profile”), [0037] (Owner “may set up a user profile ... that is stored in a database”), [0047]. In Kleve’s system, “an Owner and Temporary User may use [the smartphone application] to manage their assets and/or user profile,” including to “distribut[e] a virtual key to the Temporary User.” *Id.*, ¶[0036]. Kleve further explains that the Owner, through the application and/or website user interface tied to the owner profile, initiates sharing by entering the Temporary User’s credentials and causing the system to “set

up a virtual key,” which is then delivered to the recipient. *Id.*, ¶¶[0039], [0062]–[0063], [0047]–[0048], [0051], [0069] (generation/delivery flow). Thus, the “request is enabled via an application executed via the sharing device,” and the application is “associated with an owner account for the vehicle.” As discussed above, a POSITA would have found it obvious to incorporate these teachings into Sekiyama. EX1003, ¶153.

A POSITA would have understood—and it would have been obvious—that the software application may be developed by and/or associated with a vehicle manufacturer. EX1003, ¶154. Sekiyama is a patent invented by and assigned to Toyota Motor Corp. Accordingly, the recited software application functions of the owner’s device would have been developed by Toyota and therefore associated with a vehicle manufacturer. *Id.* Furthermore, Hatton expressly discloses a Ford VCS/SYNC architecture, explaining that a “software application 212 ... may be an application that was developed and/or associated with the vehicle manufacturer,” and that the app communicates with the VCS to perform key functions (recognition, start/unlock). EX1008, 12:46–51; *see also id.*, 7:11–45, 7:49–60, 13:24–27. A POSITA would have been motivated to incorporate Hatton’s manufacturer-associated app flows into the combined system to leverage existing VCS security/usability features (PIN-gated access, device recognition, encrypted exchanges) and to align the owner’s mobile app with OEM back-end services—an

ordinary fit in the same client-server/VCS architecture with predictable results (*see* §5(b); §5(e)); EX1003, ¶154.

Further, as with claim 1[d], the phrase “the application provided by said manufacturer of the vehicle” merely identifies the source of the software and is non-functional descriptive material. *See* claim 1[d]; *Praxair*, 890 F.3d at 1031–32; *Catalina*, 289 F.3d at 809. Who supplies the app does not alter the structure or operation of the claimed method. EX1003, ¶155.

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

As discussed above for claim 1, in the combined system, Sekiyama teaches that in response to the key request, a server *associated with the manufacturer of the vehicle* (to the extent that limitation has patentable weight) executes a process for generating an e-key. EX1005, ¶¶[0036]–[0037], Fig. 3. The generation of the e-key further includes delivery to the recipient device, which likewise involves a process executed by the recipient device, specifically its “electronic key reception unit.” *Id.*, ¶¶[0028], [0038]; EX1003, ¶156.

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

In the combined system, Sekiyama teaches that the e-key is authenticated by comparing it to “the encrypted data stored” on the vehicle. EX1005, ¶[0015]. A POSITA would have therefore understood that the e-key is likewise encrypted in order to match that information to the stored encrypted data. EX1003, ¶157.

This limitation also would have been obvious in view of Hatton, which teaches the use of encrypted communications in an e-key system to prevent unauthorized access to the vehicle and to recognize the authorized mobile device. EX1008, 9:50–63; *see also id.*, 7:33–45, 7:49–56; EX1003, ¶158.

It would have been obvious to a POSITA that the encryption operations may use public/private key pairs because public/private key pair encryption was a well-known and widely used encryption technique well before October 2013, and a POSITA would have been capable of implementing public/private key pair encryption in Sekiyama’s system. EX1003, ¶159. Contemporaneous references confirm that public/private key pair encryption was well-known years before the ’715 patent, including in electronic key systems for vehicles. *See, e.g.*, EX1020 (Fukushima), 15:34–51 (explaining public/private key–pair encryption for securing vehicle communications); EX1003, ¶159.

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

In the combined system, Sekiyama teaches that when the restricted key’s “usage period has ended,” the vehicle’s “electronic key ECU” disables the e-key—specifically, “settings are changed to disable use of the subset of functions that was usable with the restricted duplicate electronic key.” EX1005, ¶[0045]. A POSITA would have understood that the ECU sends a *deactivation request* to the vehicle systems to disable those functions. EX1003, ¶160. A POSITA would have understood that the disablement occurs in response to received control signal/request within the vehicle system when the expiration condition is met (*i.e.*, a deactivation request internal to the ECU/vehicle network that is used to disable the key). *Id.*

In addition, as part of the disabling of the e-key, the ECU “transmits a signal (usage end data) [to the server] notifying that the usage period of the restricted duplicate electronic key has ended,” and that message is used to complete the deactivation flow (*e.g.*, terminate active connections/permissions). EX1005, ¶[0045]. In the combined system, that “usage end” notification constitutes a deactivation request used to disable the e-key (server- and vehicle-side). EX1003, ¶161.

Further, even beyond expiration-driven disablement, it would have been obvious to include an explicit deactivation command (owner/server-initiated)

delivered via the app/UI: Hatton provides the manufacturer-associated mobile app and secure VCS command path (PIN/device recognition/encrypted exchanges), and Kleve provides the owner account/UI through which access is granted and can likewise be withdrawn. EX1003, ¶162. A POSITA would have implemented an app-triggered “disable/revoke” operation as a routine complement to the time-based disablement disclosed in Sekiyama, yielding predictable results. *See* §5(b); §5(e); EX1008, 7:11–56, 12:46–51, 13:24–27, 15:37–41; EX1004, ¶¶[0036]–[0039], [0047], [0062]–[0063]; EX1003, ¶162.

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

“wherein the message to share and enable the e-key for the recipient device is communicated over a network”: In the combined system, Sekiyama teaches that the server is “connected to a network” which is involved with the “issuance of electronic keys.” EX1005, ¶[0021]. The owner’s device likewise has “network connection functions.” *Id.*, ¶[0024]. A POSITA would therefore understand that the request for an e-key is communicated over a network. EX1003, ¶163. Similarly, the recipient device also has “network connection functions,” and a POSITA would have understood that the reception of the e-key is performed using those network

connections. EX1005, ¶¶[0028], [0031] (“Examples of the means of communication going from portable telephone A 10 to portable telephone B 30 include Bluetooth, ... email attachments, and the like.”); EX1003, ¶163.

In addition, as discussed above for limitation 1[a], it would have been obvious in view of Kleve for the owner and recipient device to message each other to enable the e-key. EX1003, ¶164. Kleve discloses that such communications are performed over a network. *Id.* Specifically, Kleve states that rental agreement terms are exchanged and agreed-to by the owner and recipient device via a “website using smart phones or a smart phone application.” EX1004, ¶[0047]. A POSITA would understand that access to a website involves network communications. *Id.* (“Acceptance may be sent back to the Owner over the wireless network.”); EX1003, ¶164.

“the communication enables processing by one or more servers or devices”:

See Claim 5; EX1003, ¶165.

“include a server associated with the sharing device or the recipient device”:

As discussed above for claim 1, the owner’s device (*i.e.*, ***sharing device***) connects to and sends a request to a server. The server is therefore ***associated*** with that device. EX1003, ¶166.

“the server associated with the manufacturer of the vehicle.” See limitation 1[d]. As noted with respect to claim 1[d], the phrase “associated with the

manufacturer of the vehicle” merely identifies the source of a server and is non-functional descriptive material not entitled to patentable weight under the printed-matter doctrine; who operates the server does not change the method’s structure or operation. *See Praxair*, 890 F.3d at 1031–32; *Catalina*, 289 F.3d at 809; EX1003, ¶167. In any event, a POSITA would have understood the server to be manufacturer-associated in typical deployments: Sekiyama is invented by/assigned to Toyota and describes OEM-integrated key/ECU functions (EX1005, ¶¶[0014]–[0015], [0039]–[0040]), and contemporaneous art expressly teaches manufacturer-associated servers (Xiao, EX1010, 3:12–20); EX1003, ¶167.

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

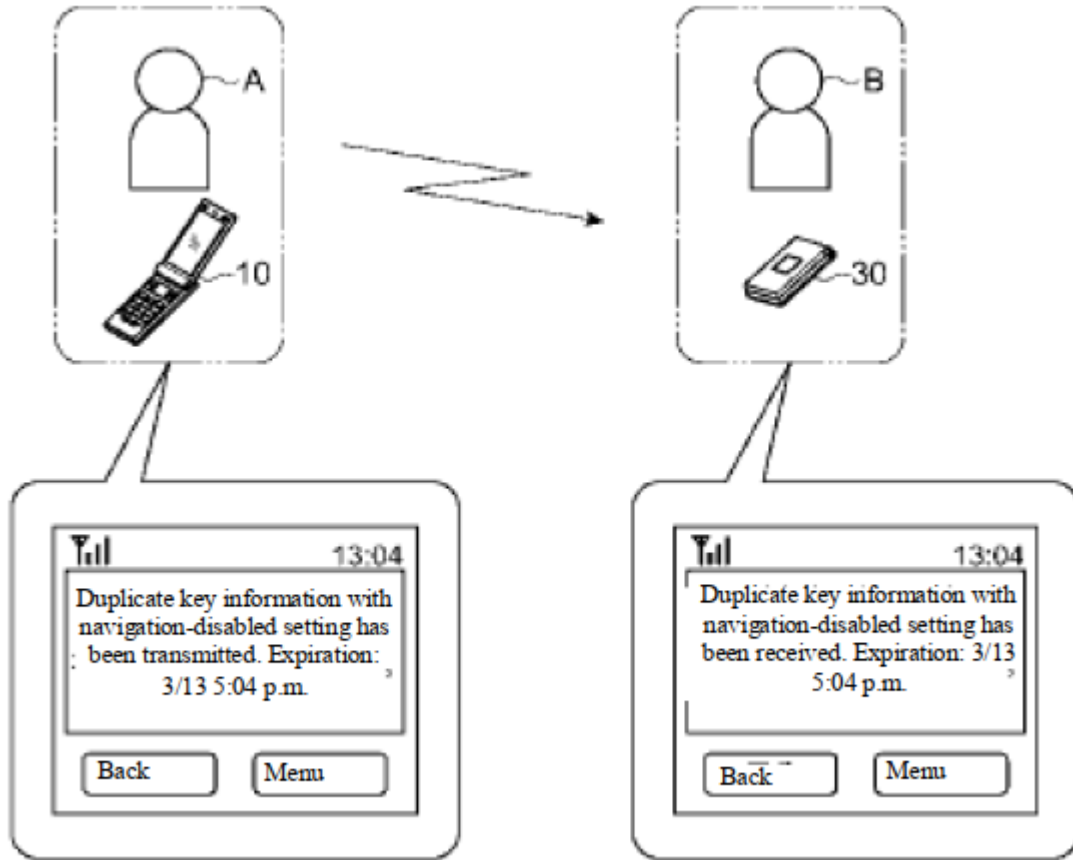
In the combined system, Sekiyama discloses that the *recipient device* is a “portable telephone” with “calling functions,” which a POSITA would understand is identified by a *phone number*. EX1005, ¶[0028]; EX1003, ¶168. In addition, the recipient device has “email sending and receiving functions” and is therefore identified by *an email address*. *Id.*

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

“application provided by a manufacturer of the vehicle”: See Claim 4; EX1003, ¶169.

“graphical user interface for registering the registered owner e-key for the vehicle”: See limitation 1[b]. Kleve’s “website” used to register the owner’s user profile is a *graphical user interface for registering the registered owner*. As discussed above, a POSITA would have found it obvious to combine Kleve’s user profile system with Sekiyama’s issuance of master keys to register the master key. EX1003, ¶170.

“graphical user interface for ... sharing of the e-key with one or more recipient devices”: Sekiyama teaches a graphical user interface for *sharing of the e-key with one or more recipient devices*. EX1003, ¶171. In particular, Sekiyama discloses, and depicts in Figure 2, a graphical user interface (“GUI”) “when the restricted duplicate electronic key has been transmitted from owner A to borrower B.” EX1005, ¶[0047].



Sekiyama also teaches that the e-key can be shared as an “email attachment,” which a POSITA would have understood involves graphical user interfaces. *See id.*, ¶[0031]; EX1003, ¶172.

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

See Claims 2 and 3; EX1005, ¶[0049] (“[T]he subset of functions that become usable with the restricted duplicate electronic key can be set to only the function of locking/unlocking the door lock of the vehicle and the function of starting the drive

source of the vehicle”). The restricted e-key can also be associated with a *at least one privilege associated with a type of operation use* such as “permission to use the on-board unit functioning as a communication device capable of sending and receiving email.” EX1005, ¶[0017] (internal quotation marks omitted). Using a vehicle to send/receive email is a privilege associated with a *type of operation use* where the vehicle operates as a communication device. EX1003, ¶173.

In addition, Kleve teaches that the owner and temporary user can agree to various *privileges associated with a type of operation use*, such as “speed, global position coordinates, or load weight restrictions.” EX1004, ¶[0040]. Kleve provides an example where the temporary user may wish to operate the vehicle to “move furniture,” and thus can agree with the owner on a privilege that defines “what can and cannot be transported.” *Id.*, ¶[0038]; EX1003, ¶174.

17. Claim 12

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

See limitation 1[pre]; EX1003, ¶175.

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

“a server associated with a manufacturer of the vehicle”: *See* limitation 1[d].

Further, “associated with/provided by the manufacturer” merely identifies source

and is non-functional descriptive material not entitled to patentable weight; who operates or supplies the server/app does not change the system's structure or operation. *See Praxair*, 890 F.3d at 1031–32; *Catalina*, 289 F.3d at 809; EX1003, ¶176.

“the server is configured to interface with an application provided by the manufacturer of the vehicle, the application provides access to data and logic for enabling sending a request to share the e-key for the vehicle with a recipient device”: *See* Claim 4; EX1003, ¶177.

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

See limitations 1[a] and 1[c]. As discussed above for limitation 1[a], in the combined system, Sekiyama in view of Kleve renders obvious an e-key request that is initiated by communications between the owner and recipient device involving agreement to rental terms. EX1003, ¶178.

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

“the server associated with the manufacturer of the vehicle”: *See* limitation 1[d]. Further, *“associated with the manufacturer”* merely identifies source and is non-functional descriptive material not entitled to patentable weight. *See Praxair*, 890 F.3d at 1031–32; *Catalina*, 289 F.3d at 809; EX1003, ¶179.

“assisting in enabling the e-key for use on the vehicle by the recipient

device”: see limitation 1[c]; EX1003, ¶180.

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

See Claim 2; EX1003, ¶181.

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

See Claim 6; EX1003, ¶182.

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

See Claim 7; EX1003, ¶183.

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

See Claim 11; EX1003, ¶184.

- 22. Claim 17**

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

See limitation 1[pre]. Sekiyama discloses that the restricted key *provides access to a vehicle*. EX1005, ¶[0040]; EX1003, ¶185.

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

See limitation 1[a]; EX1003, ¶186.

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

The '715 specification does not describe the system “receiving confirmation of the sharing request from the recipient device.” EX1003, ¶187. Accordingly, this limitation lacks written description and enablement support and renders claim 17 invalid under 35 U.S.C. §112(a) (*see* Ground 2). Even if PO argues that the specification need not recite hardware/protocol details, §112(a) still requires that the specification itself demonstrate possession/enablement of the claimed confirmation step; here, the specification nowhere discloses a recipient-originated confirmation returning to the system. EX1003, ¶187.

In any event, adding a recipient-side “accept/received” confirmation back to the backend/server is a routine client-server pattern that fits Sekiyama and Kleve’s architecture without changing it. EX1003, ¶188. Kleve already provides owner app/website interactions, permits portions of the process to execute on the phone and/or a remote server, and routes device signals via a server system. EX1004, ¶¶[0035] (processes may execute on a cellular telephone and/or a remote computing system), [0057] (server routing signals from a nomadic device), [0039], [0062]–

[0063] (key generation/delivery), [0068]–[0071] (time-bounded activation/usage enforcement), [0048]–[0049] (remote credential verification). Messaging acknowledgments over communication networks (*e.g.*, app-to-server “accept” or receipt acks) were widely used and would be applied here for reliability/audit, resend/cancel flows, and coordination with time-bounded activation. A POSITA would have included such a recipient confirmation (*e.g.*, “accept invite,” “key received”) with a reasonable expectation of success using well-understood app-to-server acknowledgments. EX1003, ¶188. *See KSR*, 550 U.S. at 416–22.

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

See limitations 1[c] and 1[d]. The e-key request includes *data related to the message* because, as taught by Sekiyama, the request includes vehicle use restrictions/privileges, and as taught by Kleve, such restrictions and privileges are agreed to by the owner and recipient. Thus, the request includes *data related to the message*. EX1003, ¶189.

As noted with respect to limitation 1[d], “*associated with the manufacturer*” merely identifies source and is non-functional descriptive material not entitled to patentable weight. *See Praxair*, 890 F.3d at 1031–32; *Catalina*, 289 F.3d at 809. In any event, manufacturer-associated servers for e-key services were conventional (*see* limitation 1[d]); EX1003, ¶190.

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

See limitation 1[e]; EX1003, ¶191.

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

“the e-key is associated with at least one privilege ... defined based on a setting associated with the sharing request.” See Claim 2; EX1003, ¶192.

“the recipient device is one of a smartphone ... or a digital assistant”: In the combined system, Sekiyama teaches that the recipient device is a “portable telephone” with “email sending and receiving functions,” which at the time of the patent would have been understood to be a *smartphone or digital assistant*. EX1005, ¶[0028]; EX1003, ¶193.

“the e-key is unique for said sharing request and said use by said recipient device.” In the combined system, Sekiyama teaches that the owner sets a unique set of restrictions that are sent with the request to generate a unique restricted key for the recipient device. EX1005, ¶[0034]–[0036]; EX1003, ¶194.

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

In the combined system, Sekiyama teaches that the e-key is generated by the server. EX1005, ¶[0036]. Sekiyama also teaches that the e-key is caused to be generated by the owner device sending a request. *Id.*, ¶[0035]; EX1003, ¶195.

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

In the combined system, Kleve—alone or in combination with Hatton and/or Sekiyama—discloses and/or renders this claim obvious. EX1003, ¶196.

“the e-key is securely generated for the recipient device” / “the e-key is encrypted, and wherein encryption uses a public/private process for security.” See limitation 1[c] and Claim 6; EX1003, ¶197.

“wherein the owner device has an owner e-key that was initially generated for the owner device to enable said sharing request.” In the combined system, Sekiyama teaches that the owner device “functions as a master key,” *i.e.*, **owner e-key**. EX1005, ¶[0024]. This master key is *initially generated* prior to any request for a “restricted duplicate electronic key.” *Id.*, ¶[0035]. The master key enables the sharing request, because Sekiyama teaches that it is only the owner’s device

operating as a master key which can request a “restricted duplicate electronic key.”

Id. Indeed, a POSITA would understand that the “restricted duplicate electronic key” is a **duplicate** of the master key (in that it allows access to the vehicle), but a restricted version of said key. EX1003, ¶198.

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

In the combined system, Sekiyama in view of Xiao renders this claim obvious. EX1003, ¶199. Sekiyama provides the enabled e-key sharing/use framework (*see, e.g.,* EX1005, ¶¶[0034]–[0040]). Xiao teaches that the mobile device (the recipient device) can request automobile health information including “battery charge level” from the vehicle and receive a report transmitted back to the mobile device displaying that charge level (*e.g.,* mobile device 110 requesting/receiving health data such as battery charge level). EX1010, 6:49–63, 7:35–55, 10:1–13, 14:3–11, 19:37–46. A POSITA would have been motivated to integrate Xiao’s telemetry/status reporting (including battery charge level) into Sekiyama’s e-key sharing framework to provide status visibility during temporary access (*e.g.,* monitoring range/charge to coordinate use/return), auditing, and remote diagnostics in the same phone ↔ server ↔ vehicle architecture—a routine combination yielding predictable results (*see* §5(c); EX1005, ¶¶[0034]–[0040]; EX1010, 6:49–63; EX1003, ¶199. Thus, “***the e-key, once enabled, provides access to information via the recipient device***

regarding a level of charge of a battery of the vehicle for when the vehicle is an electric vehicle (EV).”

To the extent PO argues that Xiao does not expressly disclose an EV, applying Xiao’s “battery charge level” reporting to an EV would have been an obvious, vehicle-agnostic application: in an EV, the reported battery charge level corresponds to the traction-battery state of charge, with no change to the underlying client-vehicle communication or UI logic. EX1003, ¶200; *see also KSR*, 550 U.S. at 416–22.

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

See Claims 2–3 and 11; EX1003, ¶201.

28. Claim 23

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

See limitations 1[pre] and 12[pre]; EX1003, ¶202.

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

In the combined system, Sekiyama teaches that the vehicle includes an “electronic key ECU 41” which “comprises a CPU that performs computation processing.” EX1005, ¶[0014]; EX1003, ¶203.

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

“a communications system of the vehicle interfaced with the on-board computer, the on-board computer ... having program instructions for communication with a server”: In the combined system, Sekiyama teaches that the ECU 41 “is configured to be capable of communicating with portable telephones 10, 30, as well as with a center server 20 of a management center that performs issuance of electronic keys.” EX1005, ¶[0014]; EX1003, ¶204.

“server associated with a manufacturer of the vehicle”: See limitation 1[d]; EX1003, ¶205. Furthermore, *associated with a manufacturer* is non-functional descriptive material not entitled to patentable weight. *Praxair*, 890 F.3d. at 1031-32; *Catalina*, 289 F.3d at 809. Even if this phrase is accorded patentable weight, the limitation is also met—or obvious—on the merits for the reasons set out in §6(e) (*see* 1[d]); EX1003, ¶205.

“the server is configured to interface with an application provided by the manufacturer of the vehicle.” See Claim 4; EX1003, ¶206. Further, “provided by the manufacturer” is non-functional descriptive material for printed-matter purposes.

“the application provides a user interface for initiating a request to share the e-key for the vehicle with a recipient device.” See Claims 4 and 10; EX1003, ¶207.

“the request to share is configured to be initiated using a message communicated to the recipient device.” See limitation 1[a]; EX1003, ¶208.

“and responsive to the request, processing the request to enable generation of the e-key for use on the vehicle by the recipient device.” See limitations 1[a], 1[e]; EX1003, ¶209.

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

See Claims 2–3 and 11; EX1003, ¶210.

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

To satisfy the written description requirement under 35 U.S.C. §112, the specification must fully support the claimed subject matter and must describe an invention so as to “reasonably convey[] to those skilled in the art that the inventor

had possession of the claimed subject matter as of the filing date.” *Ariad Pharm.*, 598 F.3d at 1351. The purpose of the written description requirement is to ensure that a patent's claims “do[] not overreach the scope of the inventor’s contribution to the field of art as described in the patent specification.” *Reiffin v. Microsoft Corp.*, 214 F.3d 1342, 1345 (Fed. Cir. 2000). The specification must describe the claimed features—not merely render them obvious. *See Lockwood v. Am. Airlines, Inc.*, 107 F.3d 1565, 1572 (Fed. Cir. 1997).

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

The specification describes a sharing flow in which a user (*e.g.*, the owner) sends a request to cloud/server infrastructure identifying the recipient and privileges; the server generates and encrypts the e-key and sends it to the recipient device; the recipient then uses the e-key with the vehicle. *See, e.g.*, EX1001, 5:11–19 (“[T]he app on the user’s mobile device can request that a message be sent to the recipient ... [with] instructions for obtaining/validating/using the e-keys.”), Figs. 26–35 (ops. 741–745) and accompanying text (cloud receives the request; generates a unique access code; encrypts with the vehicle’s public key; sends encrypted e-keys to the recipient device, which the recipient then uses with the vehicle). These passages describe an optional message/notification or link that provides instructions or launches an app/webpage to complete activation. EX1003, ¶212. They do not

describe (i) a message to the recipient that causes the server to receive or process a share request, nor (ii) the system receiving acknowledgment that a sharing request was sent or receiving acknowledgment from the recipient device. *Id.* To the extent the claims require such causation or acknowledgments, the specification is silent on any mechanism, protocol, or architecture to implement them. *Id.*

Against that backdrop, several claim limitations add procedural steps and causal couplings that the specification never describes. EX1003, ¶213. Those new requirements lack written description and enablement support under §112(a). *Id.* From an enablement perspective, the absence of any teaching on how to implement these causation/acknowledgment flows would require a POSITA to devise and integrate unclaimed messaging and backend protocols without guidance (*id.*), amounting to undue experimentation under the *Wands* factors. *See In re Wands*, 858 F.2d 731, 737 (Fed. Cir. 1988).

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

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

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

The specification never describes a message to the recipient that causes the server to receive/process the share request or that initiates the request. EX1003, ¶¶214-216. The only “message” described is a notification/instructional message to help the recipient obtain/activate an already-issued e-key. *See* EX1001, 5:11–19, Figs. 26–35 (ops. 741–745); EX1003, ¶216. There is no disclosure of any causal coupling between sending a message to the recipient and the server’s receipt/processing of a share request. EX1003, ¶216. Accordingly, independent claim 1 lacks written description and enablement, and its dependent claims 2–11 fall with it. *Id.* For the same reason, claim 23 (and dependent claim 24) lack §112(a) support to the extent they require initiation of the share request “using a message communicated to the recipient device.” *Id.*

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

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

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

The written description contains no disclosure of (i) the system receiving a confirmation that a sharing request was sent, or (ii) the system receiving a confirmation from the recipient device. EX1003, ¶¶217-219. The depicted flow simply assumes the server sends the e-key to the recipient, with no two-way

acknowledgment path and no recipient-originated confirmation back to the server. See EX1001, Figs. 26–35 (ops. 741–745) and accompanying text. EX1003, ¶219. Even if PO argues the specification need not recite hardware/protocol details or that known messaging systems make confirmations readily implementable by a POSITA, §112(a) still requires that the specification itself demonstrate possession/enablement of the claimed confirmation steps; here, it nowhere discloses a recipient-originated or “request-sent” confirmation returning to the system. *Id.* Accordingly, independent claim 17 lacks written description and enablement, and dependent claims 18–22 fall with it. *Id.*

Date: October 21, 2025

Respectfully submitted,

By: /s/ James M. Glass

James M. Glass

Counsel for Petitioners

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

1. This Petition complies with the type-volume limitation of 18,700 words, comprising 14,441 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: October 21, 2025

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 October 21, 2025, 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: October 21, 2025

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