Trials@uspto.gov
571-272-7822

Paper 37
Date: January 26, 2026

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

KIA CORP. and TOYOTA MOTOR CORP.,
Petitioners,

v.

EMERGING AUTOMOTIVE LLC,
Patent Owner.

IPR2024-01167
Patent 11,738,659 B1

Before THU A. DANG, GEORGIANNA W. BRADEN, and DANIEL J. GALLIGAN, *Administrative Patent Judges.*

BRADEN, *Administrative Patent Judge.*

JUDGMENT
Final Written Decision
Determining Some Challenged Claims Unpatentable
35 U.S.C. § 318(a)

I. INTRODUCTION

In this *inter partes* review, Kia Corp. and Toyota Motor Corp. (collectively "Petitioner") challenge the patentability of claims 1–21 of U.S. Patent No. 11,738,659 B1 (Ex. 1001, "the '659 patent"), which is assigned to Emerging Automotive LLC ("Patent Owner").

We have jurisdiction under 35 U.S.C. § 6. This Final Written Decision, issued pursuant to 35 U.S.C. § 318(a), addresses issues and arguments raised during the trial in this *inter partes* review. For the reasons discussed below, we determine Petitioner has proven by a preponderance of the evidence that claims 1–5 and 7–21 of the '659 patent are unpatentable in view of the challenges based on Kleve alone or in combination with Hatton, but has failed to prove that claim 6 is unpatentable in view of Kleve and Hatton. *See* 35 U.S.C. § 316(e) (2018) ("In an inter partes review instituted under this chapter, the petitioner shall have the burden of proving a proposition of unpatentability by a preponderance of the evidence."). We also determine Petitioner has failed to prove by a preponderance of the evidence that claims 1–21 of the '659 patent are unpatentable in view of the challenges based on Mikan alone or in combination with Xiao and/or Sekiyama. *Id.*

A. Procedural History

Petitioner filed the original Petition (Paper 3, "Pet.") challenging claims 1–21 of the '659 patent on the following basis:

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1, 3–21	103	Kleve[1], Hatton[2]
2	103	Kleve, Hatton, Sekiyama[3]
1–3, 5, 8–10	102	Mikan[4],
1–3, 5, 8–10	103	Mikan,
4, 11–18, 20, 21	103	Mikan, Xiao[5]
6, 7	103	Mikan, Sekiyama
19	103	Mikan, Xiao, Sekiyama

Pet. 2. Patent Owner filed a Preliminary Response (Paper 7, "Prelim. Resp."). Petitioner filed an authorized Reply to Patent Owner's Preliminary Response (Paper 8, "Prelim. Reply"), and Patent Owner filed an authorized Sur-reply to Petitioner's Reply (Paper 9, "Prelim. Sur-reply"). Trial was instituted on the asserted grounds of unpatentability. Paper 14 ("Inst. Dec."), 49.

During the trial, Patent Owner filed a Response (Paper 17, "PO Resp."), Petitioner filed a Reply (Paper 23, "Pet. Reply"), and Patent Owner filed a Sur-reply (Paper 26, "PO Sur-reply"). An oral hearing was held on October 27, 2025, a transcript of which appears in the record. Paper 35 ("Tr.").

Petitioner relies on testimony from Kevin C. Almeroth, Ph.D. ("Dr. Almeroth"). Ex. 1004. Patent Owner relies on testimony from Sam

[1] U.S. Patent Application Publication No. 2014/0129053 A1, published May 8, 2014 (Ex. 1005) ("Kleve").
[2] U.S. Patent No. 9,002,536 B2, issued April 7, 2015 (Ex. 1008) ("Hatton").
[3] JP Patent Application No. 2008-301427, published June 10, 2010, filed Nov. 26, 2008 (Ex. 1006) ("Sekiyama").
[4] U.S. Patent Application Publication No. 2008/0150683 A1, published June 26, 2008 (Ex. 1007) ("Mikan").
[5] U.S. Patent No. 8,737,913 B2, issued May 27, 2014 (Ex. 1010) ("Xiao").

Malek, Ph.D. ("Dr. Malek"). Ex. 2021; *see also* Ex. 2001 (declaration of Dr. Malek provided with Preliminary Response). The parties have entered into the record deposition transcripts of these declarants. Ex. 1048 (Malek Deposition); Ex. 2022 (Almeroth Deposition).

B. Real Parties in Interest

Petitioner identifies Toyota Motor Corp., Toyota Motor North America, Inc., and Toyota Motor Sales, U.S.A., Inc., Kia Corp., and Kia America Inc., as the real parties-in-interest. Pet. 71. Patent Owner identifies itself as the real party-in-interest. Paper 5 (Patent Owner's Mandatory Disclosures), 2.

C. Related Matters

The parties indicate that the '659 patent has been asserted in the following district court litigations: (1) *Emerging Automotive LLC v. Toyota Motor North America, et al.*, 2:23-cv-00434 (E.D. Tex.); and (2) *Emerging Automotive LLC v. Kia Corp., et al.*, 2:23-cv-00437 (E.D. Tex.). Pet. 71; Paper 5, 2. Petitioner further indicates that the cases have been consolidated for pretrial issues with the lead case being *Emerging Automotive LLC v. Kia Corp.*, No. 2:23-cv-00437-JRG (E.D. Tex.). Pet. 71.

D. The '659 patent

The '659 patent is titled "Vehicles and Cloud Systems for Sharing E-Keys to Access and Use Vehicles" and it issued on August 29, 2023. Ex. 1001, codes (45), (54). It is a continuation of a U.S. patent application and claims priority to several other continuation and continuation-in-part applications, as well as two provisional applications, the earliest of which was filed on April 22, 2011. *Id.* at codes (60), (63).

1. Written Description

The ’659 patent relates to systems and methods for generating and sharing electronic keys (e-Keys) with users and cloud-based processing systems. Ex. 1001, 1:66–2:2. In some embodiments, the ’659 patent discloses providing vehicle access to individuals, including an owner or “guest driver,” e.g., a friend, service person, or valet. *Id.* at 5:58–62, 10:30–34. According to the ’659 patent, this access can be provided by an electronic key, or e-key, which allows the holder of the e-key to use the vehicle. *Id.* at 6:1–3. The ’659 patent discloses that an e-key may be sent from a vehicle owner to another person, such as a guest. *Id.* at 10:40–51. The e-key allows use of the vehicle, and can further include privileges for the user, including speed limits, geographic restrictions, amount of time, etc. *Id.*

The ’659 patent describes creating profiles for users that have privileges set by an administrator. *Id.* at 16:46–52. For example, accounts for a driver may be created with “defined roles,” which can “include a set of privileges,” such as speed limit or geographic privileges. *Id.* at 17:27–48. In this way, according to the ’659 patent, logins of user profiles can be dynamically controlled. For example, “[a]dministrators can decide which settings are locked for specific logins or roles, which are open for the login user to toggle and which settings are to be enforced.” *Id.* at 17:19–26. “[U]se of the vehicle can be restricted to predefined rules,” including those based on the user profile. *Id.* at 22:24–25.

One embodiment of the ’659 patent is illustrated in Figure 29, which is reproduced below:

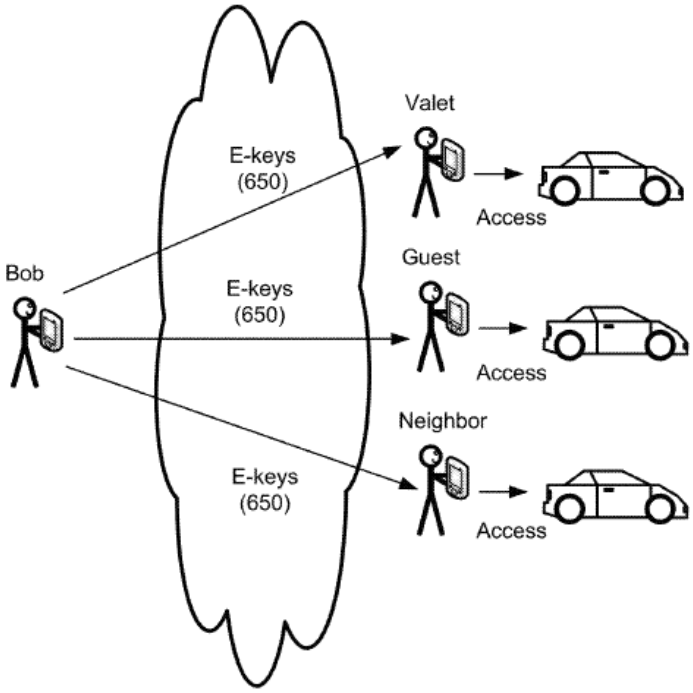

FIG. 29

Figure 29 of the ’659 patent, above, is an illustration showing the assignment of “e-keys for enabling access of a vehicle to a remote user.” *Id.* at 10:1–2. In Figure 29, vehicle owner Bob shares electronic keys 650 with users “valet,” “guest,” and “neighbor,” each having “various privilege settings.” *Id.* at 43:37–51.

Another embodiment of the ’659 patent is illustrated in Figure 31A, which is reproduced below:

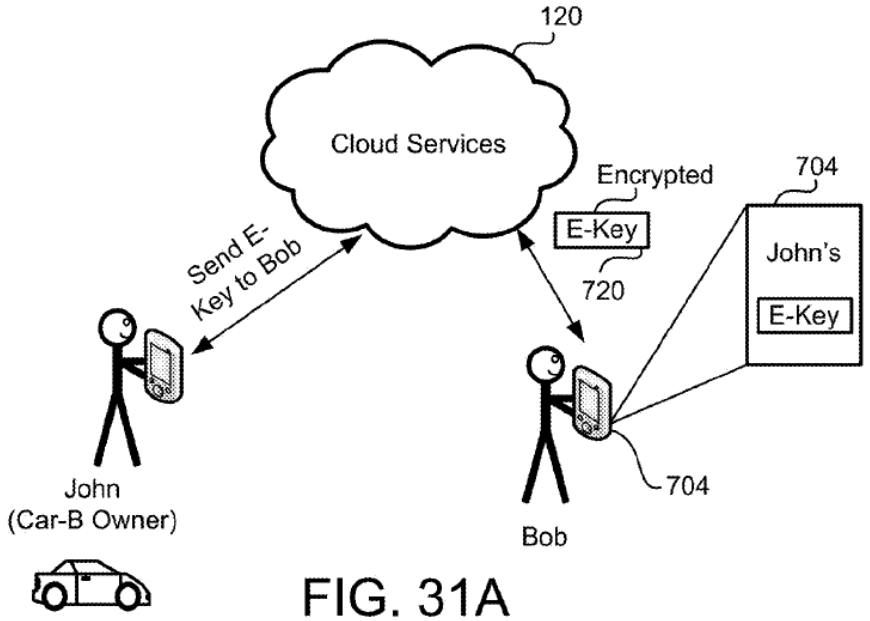

FIG. 31A

Figure 31A of the '659 patent, above, is an illustration showing a user (John) sending e-keys to another user (Bob) via mobile devices 702 (not labeled) and 704. *Id.* at 44:49–51. Per the '659 patent, the sending of the e-keys includes sending a request to a service, which may be operated by cloud services 120. *Id.* at 44:51–53. The '659 patent discloses that "[a]t the server, the server will generate an access code for the vehicle (carB)" and the "access code will then be encrypted by the server and then sent as encrypted e-keys 722 to Bob's device 704." *Id.* at 44:53–57. According to the '659 patent, Bob's device 704 may be a mobile device, such as a smart phone. *Id.* at 44:57–58.

The '659 patent explains that "[e]ach e-key, in one embodiment, will include a unique access code or substantially unique access code." *Id.* at 43:12–13. "The unique access code can be generated by a server, such as cloud services 120." *Id.* at 43:52–53. "The unique generation of access codes enables each electronic keyed [sic] to be different for each user and each e-key can expire at any time set by a requesting user." *Id.* at 43:60–64;

see also id. at 46:18–20 ("Each unique code can then be used to associate those e-keys with the same vehicle, but assigned to different devices/people with different privileges."). The unique access code "can be generated by a number generator, and [sic] alphanumeric random generator, in [sic] incremental number generator, or any other generation device that can generate codes that are unique or substantially unique." *Id.* at 45:66–46:2.

Another embodiment of the '659 patent is illustrated in Figure 33, which is reproduced below:

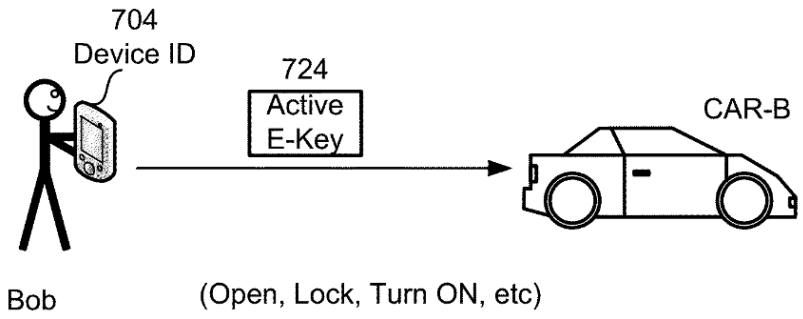

FIG. 33

Figure 33 shows Bob using an e-key to unlock and start John's vehicle (Car-B). *Id.* at 45:30–32. The '659 patent discloses that "access by Bob is facilitated by the activated e-keys 724, which are used via device 704 having the device ID that is paired or associated with the access code associated with the activated e-keys 724." *Id.* at 45:32–35.

2. Illustrative Claim

As noted previously, Petitioner challenges claims 1–21. Pet. 2. Claims 1, 11, and 18 are independent claims. Claim 1 is illustrative of the challenged subject matter and is reproduced below with Petitioner's

identifiers in brackets, which do not impact our analysis (*see* Pet. 2, List of Challenged Claims):

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

Ex. 1001, 52:11–39.

II. PRELIMINARY MATTERS

A. Claim Construction

A claim "shall be construed using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. [§] 282(b)." 37 C.F.R. § 42.100(b). Under that standard, the "words of a claim 'are generally given their ordinary and customary meaning.'" *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc).

Petitioner contends express claim construction is unnecessary and states that all terms should be given their plain and ordinary meaning. Pet. 9. Patent Owner does not address claim construction directly in its Response. *See* PO Resp.

Construction is needed only for those terms "that are in controversy, and only to the extent necessary to resolve the controversy." *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)). There are no claim terms in controversy that need be construed for our analysis.

B. Principles of Law Regarding Obviousness

A claim is unpatentable "if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains." 35 U.S.C. § 103; *see KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the

prior art; (3) the level of skill in the art; and (4) where in evidence, objective evidence of non-obviousness.[6] *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). When evaluating a combination of teachings, we must also "determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue." *KSR*, 550 U.S. at 418 (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)). Whether a combination of prior art elements would have produced a predictable result is an issue we weigh in the ultimate determination of obviousness. *Id.* at 416–17.

In an *inter partes* review, the petitioner must show with particularity why each challenged claim is unpatentable. *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016); 37 C.F.R. § 42.104(b). The burden of persuasion never shifts to the patent owner. *Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015).

We analyze the challenges presented in the Petition in accordance with the above-stated principles.

C. Level of Ordinary Skill in the Art

In determining the level of ordinary skill in the art, various factors may be considered, including the "type of problems encountered in the art; prior art solutions to those problems; rapidity with which innovations are made; sophistication of the technology; and educational level of active workers in the field." *In re GPAC, Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995) (quoting *Custom Accessories, Inc. v. Jeffrey-Allan Indus., Inc.,* 807 F.2d 955, 962, (Fed. Cir. 1986)). Furthermore, the prior art itself can reflect the

[6] Patent Owner has not presented objective evidence of non-obviousness.

appropriate level of ordinary skill in the art. *Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001).

Here, Petitioner asserts a person of ordinary skill in the art would have "had at least a four-year undergraduate degree in electrical engineering, automotive engineering, or a closely related field and at least two years of experience in the field of access control systems, vehicle electronics, and/or cryptography." Pet. 8–9 (citing Ex. 1004 ¶ 85). Dr. Almeroth supports Petitioner's position and further testifies that "[a]dditional education could substitute for professional experience and vice versa." Ex. 1004 ¶ 85.

Patent Owner does not assert a different level of skill in the art at the time of the alleged invention and appears to apply Petitioner's proposed level of skill. *See* PO Resp. Patent Owner's declarant, Dr. Malek, explicitly adopts Dr. Almeroth's level of skill in the art but states that his opinions would be applicable under any reasonable definition for an ordinarily skilled artisan at the critical time. *See* Ex. 2021 ¶ 38.

For the purposes of this Decision, we too adopt Petitioner's level of ordinary skill in the art because it appears consistent with the problems addressed in the '659 patent and the prior art of record.

III. ANALYSIS

A. Summary of References

1. Kleve (Ex. 1004)

Kleve is a U.S. patent application publication titled "Credential Check and Authorization Solution for Personal Vehicle Rental." Ex. 1004, code (54). Kleve discloses a vehicle computing system ("VCS") that includes the ability to use a vehicle rental micro-business that is integrated into the VCS. *Id.* ¶ 36.

One embodiment of Kleve is shown in Figure 2, reproduced below.

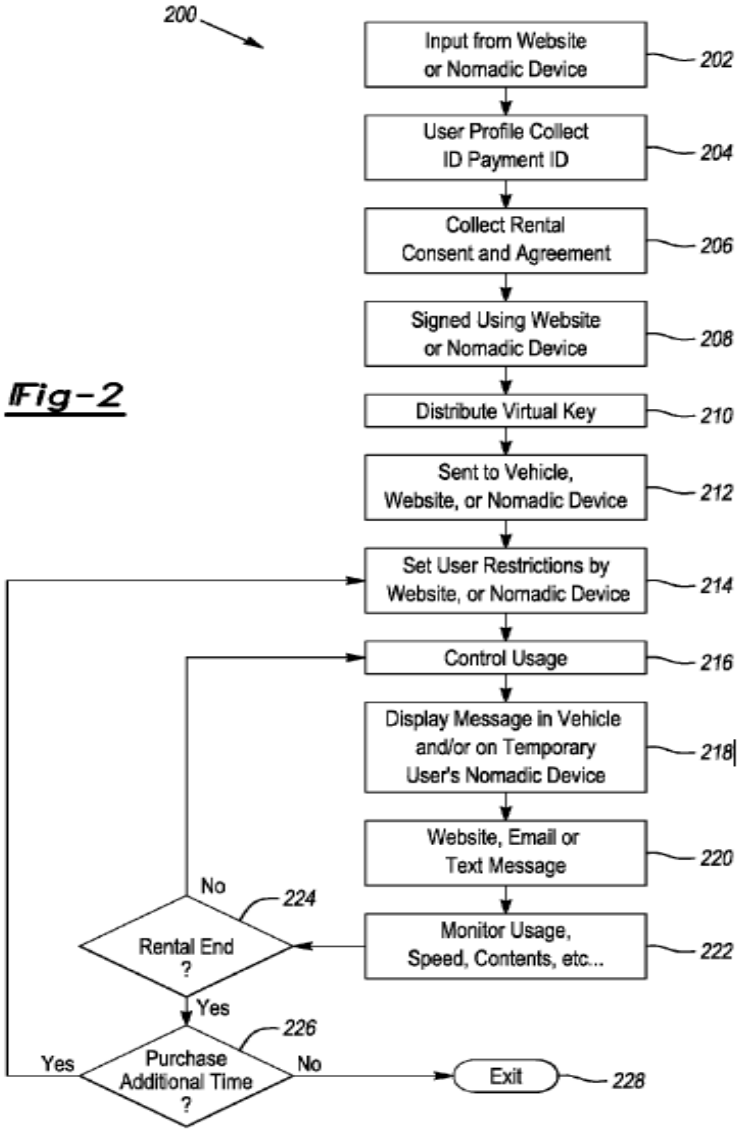

Figure 2, above, is a flow chart illustrating the steps of a vehicle rental micro-business as taught by Kleve. *Id.* ¶ 11. As part of Kleve's system, an Owner and Temporary User "may set up a user profile using a website or a nomadic device communicating" with a site that is stored in a database. *Id.* ¶ 37, Fig. 2 at step 202. According to Kleve, a "Temporary User may also fill out a user profile using the website or nomadic device to include, but not limited to, photos of credit cards, photo of forms of ID, facial recognition, voice print recognition, matrix barcode (ex. two-dimensional code), code word or phrase for speech recognition, temporary mobile web login IDs and

password, or other types of unique Temporary User identification to validate and pay for the rental service at step 204." *Id.* ¶ 37, Fig. 2 at step 204. Using this system, an Owner can rent out their vehicle and the Temporary User may agree to terms to rent a vehicle. *Id.* ¶ 38.

Per Kleve, the Owner and Temporary User "may agree to terms and conditions for the rental period using the website or nomadic device" as shown at step 206 in Figure 2. *Id.* ¶ 38. Kleve discloses the use of an identifier from a vehicle rental administrative system that is configured to activate a vehicle during a prescribed rental period. *Id.* ¶¶ 7, 39. Kleve specifically discloses that in Figure 2 at step 210, the system generates a virtual key to distribute to the Temporary User and VCS (located within the vehicle itself). *Id.* ¶¶ 35, 39. Kleve then discloses that at step 214 of Figure 2, the Owner may have access to control use of the vehicle being rented by the Temporary User. *Id.* ¶ 40. According to Kleve, these restrictions "may be based on, but not limited to, the owner's selection of parameters including, but not limited to, speed, global position coordinates, or load weight restrictions." *Id.*

Kleve additionally explains that "during the rental term the VCS may monitor the Temporary User's utilization of the vehicle including, but not limited to, renter verification, driving behavior, vehicle location, speed, fuel level, and other vehicle information requested by the vehicle owner." *Id.* ¶ 73. "The continuous monitoring of the Temporary User's behavior during the rental period may be transmitted to the server . . . ." *Id.* ¶ 76.

Kleve explains that Temporary User's use of the shared vehicle may be subject to "restriction limits [privileges] initially set by the Owner at the beginning of the rental term." *Id.* ¶ 43. According to Kleve, "[t]he restrictions may be based on, but not limited to, the [O]wner's selection of

parameters including, but not limited to, speed, global position coordinates, or load weight restrictions." *Id.* ¶ 40. Kleve specifies that during the rental term, the "control parameters" of the shared vehicle are "monitor[ed]" to determine whether a "restriction" has been exceeded. *Id.* ¶¶ 40, 53. When a restriction is exceeded, Kleve teaches that "the Temporary User and Owner may be notified." *Id.* ¶ 40. Kleve discloses that "an in-vehicle display message may be sent [from the server] to notify the Temporary User if a restriction limit has been exceeded." *Id.* ¶¶ 40, 53. Kleve states that "[t]he display message to alert the Temporary User of a restriction violation may be sent to the vehicle display information console." *Id.* ¶ 53.

2. Hatton (Ex. 1008)

Hatton is a U.S. Patent titled "Key FOB Security Copy to a Mobile Phone." Ex. 1008, code (54). Hatton explains that a mobile device can enable one or more processors to receive vehicle key security codes from a vehicle key, where the mobile device receives a signal from a transmitter associated with a vehicle key, the signal being indicative of one or more security codes associated with the vehicle key. *Id.* at code (57). According to Hatton, the mobile device may store the one or more security codes in memory and configure a mobile device application to implement one or more vehicle control functions using the security codes. *Id.*

Hatton teaches that "mobile device 124 may be configured using a software application to communicate with the VCS," using encrypted data to control the vehicle. *Id.* at 7:11–45. Hatton also teaches that the encrypted data may be used to securely generate an electronic key on the mobile device, such as by a user "typing a pin number on the [software] application [on the mobile device]," and associating the pin number "as the primary or secondary key." *Id.* at 15:37–41. Hatton explains that the virtual key and

encrypted data can be communicated between the mobile device and the VCS using "wireless communication technologies." *Id.* at 7:56–60.

3. Sekiyama (Ex. 1006)

Sekiyama is a Japanese patent application publication titled "Electronic Key System." Ex. 1006, code (54). Sekiyama provides an electronic key system that allows restrictions on functions that can be executed with a duplicate electronic key to be imposed when a duplicate electronic key is generated. *Id.* at code (57). Sekiyama discloses a server that generates an e-key. *Id.* ¶ 26 ("[A]n electronic key [is] outputted from the center server 20."). This key performs "door lock locking / unlocking" and "the permission for engine start." *Id.* ¶ 18.

4. Mikan (Ex. 1007)

Mikan is a U.S. patent application publication titled "Wireless Device as Programmable Vehicle Key." Ex. 1007, code (54). Mikan is directed to the use of "wireless devices for providing secure operation of a vehicle." *Id.* at code (57). One embodiment of Mikan is shown in Figure 2, a block diagram, reproduced below. *Id.* ¶ 5.

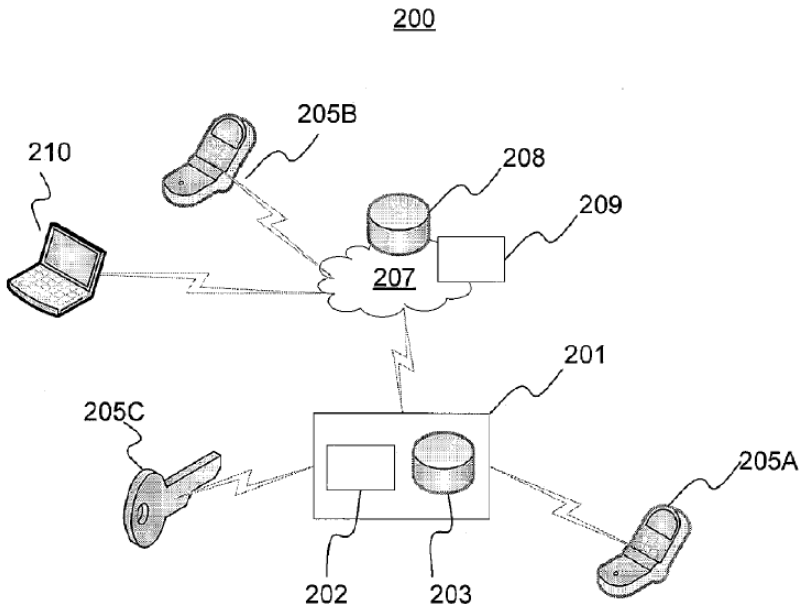

FIG. 2

Figure 2, above, is a block diagram illustrating an embodiment of wireless vehicle security system 200. *Id.* ¶ 11. According to this embodiment, the system may include multiple keys, which may be "electronic keys" that are "embedded in a wireless device such as a cellular telephone or Personal Digital Assistant." *Id.* ¶ 50. Mikan explains that a "vehicle operation policy" may assign specific "vehicle operation features" (*e.g.*, "unlocking a door," "opening a trunk," or "engaging an ignition") that are accessible to different electronic keys. *Id.* ¶¶ 49, 51.

Mikan discloses that system 200 includes a "control unit 202" that is "in communication with wireless network 207" using well known wireless communication techniques, such as WiFi. *Id.* ¶ 52. According to Mikan, control unit 202 may also "interface with vehicle 201" to "control vehicle functions and … sense operation of vehicle 201." *Id.* ¶ 53. For example, the control unit may "lock and unlock the vehicle doors" or "sense vehicle speed

and the status of the ignition." *Id.* Mikan's system also includes local and master databases that maintain information about vehicles, keys, and operation policies associated with different vehicles and keys. *Id.* ¶¶ 51, 54. Mikan then disclose that control unit 202 may employ the vehicle operation policies to "block and/or limit operation of vehicle 201 . . . when an access request does not conform with vehicle operation policy." *Id.* ¶ 77.

5. Xiao (Ex. 1010)

Xiao is a U.S. patent application publication titled "Methods and Systems for Providing a Wireless Automobile Key Service." Ex. 1010, code (54). Xiao discloses a system that uses a mobile device to "command[] an automobile." *Id.* at 2:29–30. Xiao's 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.* at 4:33–36, 4:46–56. According to Xiao, 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.* at 12:8–13.

B. Claims 1 and 3–21 Allegedly Rendered Obvious by Kleve Alone or in Combination with Hatton

Petitioner contends that Kleve in combination with Hatton teaches every limitation of claims 1 and 3–21. Pet. 9–36. Patent Owner disagrees. PO Resp. 5–53. Patent Owner specifically challenges whether Petitioner has shown that the combination of Kleve with Hatton teaches or suggests "coded data" that "includes privilege settings," as required by the challenged

independent claims. *Id.* Patent Owner further challenges whether Petitioner has demonstrated a reason to combine Kleve with Hatton. *Id.* at 54–57.

1. Analysis of Independent Claim 1

a) Limitation [1a]

Claim 1 recites

> [1a] memory associated with the on-board computer of the vehicle having program instructions for instructing unlocking and starting of the vehicle;

Ex. 1001, 52:16–18.

For this limitation, Petitioner contends that "Kleve discloses memory associated with the VCS processor." Pet. 16 (citing Ex. 1005, Fig. 1). According to Petitioner, Kleve's memory includes random access memory (RAM) and a hard disk drive (HDD) or flash memory. *Id.* (citing Ex. 1005 ¶ 22). Petitioner asserts that this memory is used to store data. *Id.* (citing Ex. 1005 ¶ 31). According to Petitioner, "Kleve's processor executes instructions stored at a 'storage medium [*i.e.*, memory]' that 'enable a vehicle rental transaction' by 'activat[ing] [*i.e.*, starting] the vehicle during a prescribed rental period' and, 'enabl[ing] a keyless driveaway.'" *Id.* (citing Ex. 1005 ¶¶ 9, 71).

Patent Owner has not provided separate arguments regarding Kleve alone or in combination with Hatton in regards to these challenged claims. *See* PO Resp. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

We have reviewed the Petition's analysis and find it persuasive. Specifically, we find that a person of ordinary skill in the art would have understood that Kleve's memory (including random access memory (RAM) and a hard disk drive (HDD) or flash memory) would have included

program instructions for instructing unlocking and starting of a vehicle. Kleve discloses that one of its embodiments includes a computer readable storage medium for storing instructions that, when executed by a processor is configured to enable a vehicle rental transaction. *See* Ex. 1005 ¶ 9. Then Kleve states that after e-key comparison and authorization, "the vehicle may enable driveaway access to that Temporary User for the scheduled time period of the rental agreement" and for "the duration of the rental term, the Temporary User may again input the same identifying credentials to unlock and drive." *Id.* ¶ 71. Additionally, we credit the testimony of Dr. Almeroth, whose testimony is consistent with Kleve's disclosure. *See* Ex. 1004 ¶¶ 120–123.

Accordingly, based on our review of the entire trial record, including sufficient explanation and cited credible supporting evidence regarding limitation [1a], we find that Petitioner has shown sufficiently that Kleve in view of Hatton teaches or suggests limitation [1a].

b) Limitations [1b] – [1c]

Claim 1 recites the following limitations:

> [1b] communications circuitry of the vehicle interfaced with the onboard computer of the vehicle and the sub-system, the communications circuitry is configured to process program instructions to enable communication with a server,
>
> [1c] the communications circuitry includes wireless communication circuitry for enabling local connection with a mobile device, the mobile device is configured to use the eKey for said unlocking and said starting the vehicle;

Ex. 1001, 52:19–33.

For these limitations, Petitioner contends that Kleve discloses multiple communications circuits interfaced with its on-board computer and sub-

systems for communicating with a server located on a cloud network. Pet. 17 (citing Ex. 1004 ¶¶ 124–129). Petitioner notes that Kleve's VCS may use a "BLUETOOTH transceiver 15 to communicate 17 with a user's nomadic device 53 (*e.g.*, cell phone, smart phone…)," which in turn communicates "with a network 61 outside the vehicle 31." *Id.* (citing Ex. 1005 ¶¶ 25, 29–30, Fig. 1).

Petitioner further contends that Kleve's communications circuitry includes wireless communication circuitry (*e.g.*, modem 63, Bluetooth transceiver 15, and wireless router 73), which enables local connection to a mobile device. Pet. 19 (citing Ex. 1005 ¶ 25; Ex.1004 ¶ 129). Petition argues that Kleve's mobile device is configured to use a virtual key (eKey) to "unlock and drive" (which entails starting) the vehicle. *Id.* (citing Ex. 1005 ¶¶ 9, 71; Ex. 1004 ¶ 130).

Patent Owner does not address these claim limitations. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

We have reviewed the Petition's analysis and evidence, and we agree with Petitioner that Kleve in view of Hatton teaches or suggests these limitations.

c) Limitations [1d] – [1f]

Claim 1 further recites the following limitations:

> [1d] wherein the wireless communications circuitry of the vehicle is configured to receive coded data from the mobile device when using the eKey, the coded data enables functions of said eKey for said unlocking and use of the vehicle, the coded data is associated to the eKey for use by the mobile device,

> [1e] the coded data includes privilege settings associated with the eKey for limiting types of use of the vehicle when using the eKey with the vehicle;
>
> [1f] wherein use of the vehicle using the eKey is tracked to identify and log actions taken using the vehicle while the eKey is used.

(i) Petitioner's Contentions

Petitioner contends Kleve discloses that a virtual key is wirelessly communicated to the vehicle using encrypted data, which Petitioner argues renders it obvious to include privilege settings in the "coded data." Pet. 19 (citing Ex. 1004 ¶¶ 131–137); Pet. Reply 16 (citing Ex. 1004 ¶¶ 110–113). Petition asserts Kleve teaches that a virtual key may be sent "in an encrypted message" to "the VCS," and is associated with the virtual key, thereby meeting this claim limitation. *Id.* (citing Ex. 1005 ¶ 63); Tr. 9:24–11:12, 18:19–19:3, 21:20–22:7. According to Petitioner, Kleve independently discloses this limitation, because Kleve discloses using a "matrix barcode (ex. two-dimensional code) [*i.e.*, coded data] . . . as the virtual key," which can be communicated using an optical scanner on a smart phone to allow a user "enter and enable the vehicle drive away event." *Id.* at 20 (citing Ex. 1005, ¶¶ 44, 45, 71; Ex. 1004 ¶¶ 132–133); Pet. Reply 18; Tr. 36:15–16.

Petitioner argues that Kleve's wireless communication circuity could be used in combination with Hatton's teachings to receive encrypted wireless communications associated with an electronic key for enabling virtual key unlock and drive functionality. Pet. 19–20 (citing Ex. 1004 ¶ 134). According to Petitioner, this would simplify activation and use of the virtual key while preventing unauthorized access to the vehicle. *Id.* at 20. Petitioner concludes that an ordinarily skilled artisan would have

applied "Kleve's existing encryption techniques to wireless communication protocols as disclosed by Hatton to facilitate secure transmission via a temporary user's mobile device." Pet. Reply 18 (citing Ex. 1004 ¶¶ 111–112).

Petitioner next contends that, in Kleve, "the virtual key, represented as encrypted data, includes privilege settings that limit types of use of the vehicle." Pet. 20 (citing Ex. 1004 ¶¶ 138–140). Petitioner provides the example of where Kleve's "vehicle's 'Owner' 'may set user restrictions . . . based on . . . parameters including, but not limited to, speed, global position coordinates, or load weight restrictions.'" *Id.* at 20–21 (citing Ex. 1005 ¶ 40). According to Petitioner, such restrictions can "be set in accordance with the types of use intended by the owner and temporary user." *Id.* at 21 (citing Ex. 1005 ¶¶ 76, 83). Therefore, Petitioner concludes that a person of ordinary skill of art at the critical time would have found it obvious to include the use restrictions within the encrypted data associated with the virtual key in order to prevent tampering by a temporary user. *Id.*

Petitioner further contends that another restriction set in Kleve is the rental period, which is set as part of the virtual key when the virtual key is generated. Pet. Reply 1 (citing Pet. 15–16, 20); *see* Ex. 1005 ¶¶ 38 ("The Owner and Temporary User may agree to terms and conditions for the rental period using the website . . . ."), 39, 47, 68 ("Once the rental period has expired the virtual key may be reset and cleared from the VCS.")); *see also* Tr. 31:25 ("[t]he virtual key is tied to the rental period").

Petitioner additionally argues that enforcing a rental period before a rental period begins is both common sense and clear from Kleve's disclosure. Pet. Reply 3. Petitioner cites to Kleve's Figure 6 to demonstrate that the parties agree to the restrictions (i.e., the rental period including both

the start and end time for the rental period), after which the vehicle owner's device sends a request to simultaneously "Generate Virtual Key and Vehicle Restrictions." *Id*. at 3 (citing Ex. 1005, Fig. 6). Then the Temporary User can use the vehicle "within the scheduled rental time," which "Appl[ies] Restrictions." *Id*. at 3 (alteration in original; citing Ex. 1005 ¶ 70, Fig. 6). Petitioner argues that Kleve makes clear that the virtual key is assigned and transmitted prior to the start of the rental period. *Id*. at 4 (citing Ex. 1005 ¶ 54, 62, 63, 75, Fig. 7).

Relying on Figure 7, Petitioner notes that in Figure 7 the VCS "may begin monitoring and report usage" at step 702 and then "wait for the rental period to start at step 704." Pet. Reply 4 (citing Ex. 1005 ¶ 75), 14. Thus, according to Petitioner, "enforcement of the rental period begins before step 704." *Id.* at 4. Petitioner argues that Patent Owner's view of "Kleve ignores such teachings," and instead elevates "a single, admittedly optional, step from Figure 2 to argue that Kleve's restrictions can *only* be set after the rental period starts." *Id.* at 5 (emphasis in original). Petitioner asserts, however, that "Kleve's system is not so limited." *Id.*

Petitioner further cites Patent Owner's argument, which relies on Figure 2 (at step 214), that Kleve "provides a separate, *optional* operation to allow only the Owner to 'set user restrictions.'" Pet. Reply 7 (quoting PO Resp. 13 (citing Ex. 1005 ¶ 40, Fig. 2)) (emphasis in original). Petitioner contends that this shows that step 214 is optional by Patent Owner's admission, while enforcement of the rental period is not optional. *Id.* (citing Ex. 1005 ¶¶ 8, 39, 51, 54). Therefore, Petitioner concludes that an ordinarily skilled artisan would have understood there is a mechanism to enforce the rental period that does not require the use of step 214. *Id.* This further

explains why Kleve does not include the start of the rental period[7] in the exemplary list of restrictions that can be set at step 214. *Id.* (citing Ex. 1005 ¶ 40; Ex. 1048, 13:18–14:4).

Petitioner then argues that association of the rental period with the E-key is critical to the security in Kleve because if the rental period were not associated with the E-key then an unscrupulous renter could just go to the car and, at the very least, gain access to that car. Tr. 13:7–17. Petitioner thus concludes that it would be advantageous and obvious to associate the virtual key with the restrictions to limit a vehicle's use to the agreed upon rental period and that Kleve teaches to do so. Pet. Reply 16–17.

Lastly, Petitioner provides arguments and evidence that Kleve discloses tracking the use of a rental vehicle to identify and record (or log) actions taken by a temporary user using a virtual key. Pet. 21–22 (citing Ex. 1004 ¶¶ 141–142, 160–165). Petitioner specifically argues that Kleve discloses "restrictions" that "may be monitored and if a restriction exceeds a limit the Temporary User and Owner may be notified." *Id.* at 21 (citing Ex. 1005 ¶ 40; Fig. 3B).

(ii) Patent Owner's Contentions

Patent Owner disagrees with Petitioner's reading of Kleve and contends there is no teaching of a vehicle circuitry "that is configured to 'receive coded data from a mobile device . . . the coded data includes privilege settings.'" PO Resp. 1–2, 4–60; PO Sur-Reply 4–7. Patent Owner contends that Kleve discloses distinct operations for (1) forming a rental

[7] Petitioner argues that, per Kleve's disclosure, step 214 can be for extending the "rental period end time." Pet. 9 (citing Ex. 1005 ¶ 43), 12–13 (citing Ex. 1005 ¶ 51, Fig. 3 (step 326 implements restrictions, steps 346 to 328 extend the end time)).

agreement, (2) setting up and distributing a virtual key, and (3) setting user restrictions. PO Resp. 5. Therefore, Patent Owner specifically contends that: (1) a rental period is not a user restriction and is not part of the e-key; (2) neither the "set up" of a virtual key nor the distribution of a virtual key includes the rental agreement terms or any other restrictions; (3) to monitor and control vehicle usage, a Vehicle Owner may "set user restrictions," but that is done after creating the e-key; and (4) Kleve's virtual key credential is operable independent of the agreed-upon rental period. PO Resp. 6–26.

Patent Owner argues that Kleve's system checks credentials that are used as a "virtual key" for use of a "personal vehicle rental." PO Resp. 5. (citing Ex. 1005, face page, ¶ 36). Relying on Figure 2 of Kleve, Patent Owner further argues that Kleve's system includes a restriction setting that is available to only a Vehicle Owner and only at the beginning of the rental term, after a virtual key has been sent to the vehicle and that a rental agreement term (agreed to by both parties) does not set a user restriction. *Id.* (citing Ex. 1005 ¶¶ 51, 40). According to Patent Owner, all user restrictions are set up at step 214 of Figure 2 and are monitored and controlled by a vehicle's "VCS" or vehicle computing system. *Id.* at 5–6 (citing Ex. 1005 ¶¶ 41, 43, 51; Ex. 2021 ¶¶ 49–52). Therefore, Patent Owner concludes that the vehicle rental period term is independent of any "virtual key" and is distinct from a "user restriction." *Id.* at 6 (citing Ex. 1005 ¶¶ 40, 51, Fig. 2; Ex. 2021 ¶¶ 47–52).

Patent Owner cites to Kleve's Figures 2 and 5 to support its position that the vehicle owner does not "have access to control usage of the vehicle being rented by the Temporary User" until step 214 (in Figure 2) and step 506 (in Figure 5), after a virtual key is distributed. PO Resp. 7–12 (citing Ex. 1005, Figs. 2, 5, ¶¶ 38, 40–41, 43, 51, 84, 86, 89). According to

Patent Owner, the parties agree to specific conditions for a vehicle when they are negotiating terms for a contract. *Id*. at 8 (citing Ex. 1005 ¶¶ 46, 84–85, 89–90, 38, Figs. 8–9). When the parties agree to final terms, a website can generate a rental agreement and collect payment and signatures. *Id*. (citing Ex. 1004 ¶¶ 38, 47, 85, 90, Fig. 3A). But Patent Owner argues that Kleve fails to teach a way for the parties' agreed-upon conditions to be included in the set up or distribution of an e-key. *Id*. at 8–9.

Patent Owner contends that, in Kleve, the vehicle owner can set user restrictions at the beginning of the rental term (as shown in step 214 of Figure 2), which is after the distribution of the virtual key (in step 210), wherein those restrictions will be monitored and controlled by the vehicle's VCS (at step 222). PO Resp. 13–14 (citing Ex. 1005, Fig. 2, ¶¶ 40–41, 43, 51, 75; Ex. 2021 ¶¶ 47–50). Patent Owner argues that using these distinct methods, the vehicle owner can then enforce compliance with the restriction "by inputting, for example, load weight restrictions, as well as set additional user restrictions that are not necessarily agreed or contemplated in the rental agreement." *Id*. at 14–15 (citing Ex. 2029 ¶ 46, 49–50), 16–20 (citing Ex. 1005, Figs. 3B, 7B, ¶¶ 43, 53, 54, 75, 84–85, 89–90; Ex. 2021 ¶¶ 51–53.).

Patent Owner asserts that setting the restrictions and monitoring such restrictions are distinct operations from making the rental agreement and sending out the e-key. PO Resp. 14–15. Patent Owner then goes further and argues that

> [b]ecause the Owner does not have the option to set rental restrictions until the beginning of the rental term at step 214—when those restrictions are "initially set"—neither the rental agreement terms themselves, nor the generation of a virtual key (each of which precedes the distribution of the virtual key, at

> step 210) could possibly qualify as *Kleve*'s Owner-set restrictions.

Id. (citing Ex. 1005 ¶¶ 40–41, 43, Fig. 2; Ex. 2021 ¶¶ 46, 49–50.).

Patent Owner further argues that, in Kleve, a rental period cannot be a condition that is part of an e-key because the rental end period can be extended and the same e-key will continue to work for remote access of a rented vehicle. PO Resp. 18–19 (citing Ex. 1004 ¶ 43). Patent Owner notes that "[a]t step 226, if the Temporary User decides that he may need to purchase additional rental time, the system may update the new rental period end time restriction and continue to monitor usage of the vehicle." *Id*. at 18 (quoting Ex. 1004 ¶ 43) (citing Ex. 1004, Fig. 2, ¶ 54). Patent Owner argues that Kleve also provides examples where the virtual key remains operable after the rental term has ended and will not be terminated until the vehicle rental exit process, at step 228, after the rental period is over. *Id*. at 23–24 (citing Ex. 2021 ¶ 59). According to Patent Owner, there is no way to "update" or change the rental period at steps 206, 208, or 210 of Figure 2, which is when the rental agreement is negotiated or the e-key is created and distributed. *Id*. at 20; *see* PO Sur-Reply 18–17 (arguing that neither Figures 3 nor 7 provide a mechanism for extending the rental term).

Next, citing to Figure 5 of Kleve, Patent Owner contends that the vehicle owner can enter in "vehicle authorization credentials based on information *received by the Temporary User* to set up a virtual key." PO Resp. 9 (citing Ex. 1005, Fig. 5, ¶ 62). According to Patent Owner, this unique "Temporary User identification or 'credential' is ultimately to be 'used as a virtual key'" and it does not include any information about the rental period in it. *Id*. at 10–11 (citing Ex. 1004 ¶¶ 44, 62–64, 67; Ex. 2021 ¶ 46). Patent Owner argues that the vehicle owner sends those credentials

directly to the vehicle so that it can compare them to those entered by an authorized temporary "at rental time" and that means it is not necessary for the e-key to have the rental period associated with it. *Id*. at 12 (citing Ex. 1005, Fig. 5, ¶ 66; Ex. 2021 ¶ 62).

Patent Owner further contends that Dr. Almeroth's testimony in support of Petitioner's positions is incorrect and contrary to the express disclosures of Kleve. PO Resp. 27–28. Patent Owner argues that Dr. Almeroth's proposed modification to Kleve "disregards and contradicts the very purpose and design of Kleve's solution," which is to allow the Vehicle Owner alone the ability to control usage of their own vehicle. *Id.* at 28. Then, Patent Owner asserts that during his deposition "Dr. Almeroth admitted his testimony was wrong." PO Sur-Reply 7 (citing PO Resp. 47–48 (citing Ex. 2022, 27:5–10, 27:21–28:1; Ex. 2021 ¶ 96)). Thus, Patent Owner concludes that Kleve's virtual key credential is operable independent of the agreed-upon rental period and cannot include any rental agreement terms in an "already-generated, already-distributed, and already-used virtual key." PO Resp. 44–45.

Lastly, Patent Owner further contends that the "coded data" sent in "encrypted messages" is sent via Kleve's server "to the VCS, Temporary User's nomadic device, and/or vehicle Owner[']s nomadic device." PO Sur-Reply 2–3, 6–8 (citing Ex. 1005 ¶ 63), 12 ("*Kleve* never disclose[s] including any 'privilege setting' in any coded data sent from a mobile device to a vehicle . . . ."), 14 ("There remains no evidence, nor reason for the Board to conclude that *Kleve*'s vehicle would *also receive* any restriction from the Temporary User's mobile device."), 20–22; Tr. 34:17–19, 40:11–16, 42:21–24, 53:5–7, 55:11–15. Patent Owner argues that Petitioner's cite to Kleve's matrix barcode is insufficient because the barcode does not

include the rental agreement or any of its alleged conditions. PO Sur-Reply 9. Thus, according to Patent Owner, this "encrypted message" is not "from the mobile device," as required by the claims. *Id.* at 9. Patent Owner, therefore, argues that whether combined with Hatton or not, the challenges based on Kleve fail to meet all the claim limitations. *Id.*

(iii) Analysis

First, we are persuaded that Kleve's "virtual key" is coded data because it is wirelessly communicated from a server to a Temporary User's nomadic device in an encrypted format. *See* Ex. 1005 ¶¶ 38, 63. Additionally, we find that the vehicle's wireless communications circuitry receives the coded data from the Temporary User's nomadic device (i.e., "from the mobile device"), when the eKey is used on the vehicle. *See* Ex. 1005 ¶¶ 7–9, 31, 38, 44, 45, 71; Tr: 36:15–16, 59:1–8.

Second, we are persuaded that Petitioner shows Kleve teaches, or at least suggests, that the "coded data includes privilege settings associated with the eKey for limiting the types of use of the vehicle," because we find that Kleve's virtual e-key includes a rental period, specifically the start of the rental period, which we find to constitute a privilege setting that limits the type of use of a rental vehicle. We do not agree with Patent Owner that Kleve's e-key does not provide a rental period restriction because Kleve expressly discloses that the "terms and conditions for the rental period" are agreed to before the virtual key is generated. Ex. 1005 ¶ 38. Rather, we agree with Petitioner that Kleve describes an e-key that is only operable during a rental period because Kleve transmits the e-key before the start of the rental period and discloses "[t]he virtual key may also be sent to the vehicle configuring the VCS to enable the keyless drive system for the

appropriate Temporary User during a given rental period." Ex. 1005 ¶¶ 39, 51, 54, 62, 69–70, 75, Figs. 3–7; *see* Pet. Reply 2–3.

We note Patent Owner's citations to Kleve's Figures 2 and 5 to indicate control restrictions are added after the distribution of a virtual key. PO Resp. 13–14. We agree with Patent Owner that the vehicle owner in Kleve can set user restrictions at the beginning of the rental term (as shown in step 214 of Figure 2), which is after the distribution of the virtual key (in step 210). And we understand Patent Owner's position that Kleve's setting the restrictions and monitoring such restrictions are distinct operations from making the rental agreement and sending out the e-key. *Id.* Although they may be distinct operations, we are unpersuaded that Kleve's vehicle owner cannot set any restriction prior to step 214 in Kleve's Figure 2 or that such restrictions cannot be associated with the e-key.

Contrary to Patent Owner's position, it appears that, in Kleve, a rental start period is included prior to step 210, whereas restrictions that can be monitored separately (such as vehicle weight, speed, or geographic area of use) are set at step 214. *See* Ex. 1005, Fig. 2; ¶¶ 40–41, 43. Based on Kleve's teaching of "monitor[ing] the vehicle for the *entire* rental period" (Ex. 1005 ¶ 54 (emphasis added)), we find that Kleve's rental period restriction may be assigned prior to the start of the rental period in order to monitor usage for the entire period. *See* Ex. 1005 ¶¶ 38–39.

We do not agree with Patent Owner's position that Kleve fails to teach a way for the parties' agreed-upon privileges or conditions to be included in the set up or distribution of an e-key. *See* PO Resp. 8–9. Kleve specifically teaches that "[t]he Owner and Temporary User may agree to terms and conditions for the rental period," after which its "system may generate a virtual key to distribute to the Temporary User and VCS" so as "to enable

the keyless drive system for the appropriate Temporary User during a given rental period." *See* Ex. 1005 ¶¶ 38–39. Although Kleve's system allows the Temporary User to purchase additional rental time and the system may update the new rental period end time restriction, such allowances does not negate the fact that Kleve teaches the rental start period is part of the e-key and allows a Temporary User to access the rental vehicle and remotely start the vehicle. *See id.* ¶¶ 39, 43.

Next, turning to Figure 5, we are unpersuaded by Patent Owner's contention that a "unique Temporary User identification or 'credential'" is "used as a virtual key" that does not include any information about the rental period in it. *See* PO Resp. 9–10 (citing Ex. 1005, Fig. 5, ¶ 62). This argument is unavailing because Kleve discloses that its virtual key does not have to be the same as a "credential." *See* Ex. 1005 ¶¶ 62–64. Kleve teaches that the virtual key is sent at step 502 in Figure 5 and provides access to the vehicle during the rental period, while a credential is sent at step 506 and allows a rental vehicle to authenticate a temporary user. *See id.* Additionally, not every embodiment of Kleve uses credentials but every relied-upon embodiment allows the use of a virtual key.

Additionally, we credit the testimony of Dr. Almeroth, who opines that Kleve discloses that certain restrictions are sent with the request to generate a virtual key. Ex. 1004 ¶¶ 118–123. Specifically, Dr. Almeroth testifies that Kleve discloses that the virtual key "enable[s] the keyless drive system for the appropriate Temporary User during a given rental period." *Id.* According to Dr. Almeroth, this "indicates that rental agreement restrictions were sent with the request so that the virtual key could be associated with said restrictions." *Id.* (citing Ex. 1005 ¶¶ 39, 68 ("Once the rental period has expired the virtual key may be reset and cleared from the

VCS.”)). Dr. Almeroth further testifies that the virtual key in Kleve is always generated after the rental agreement. *Id.* (citing Ex. 1005 ¶¶ 39 (“[O]nce the Temporary User selects the vehicle, pays the appropriate amount and signs a consent agreement, th[e]n the system may generate a virtual key to distribute to the Temporary User and VCS.”), 68).

We do not agree with Patent Owner’s argument that Dr. Almeroth’s declaration testimony contradicts Kleve. *See* PO Resp. 27–29. Rather, as discussed previously, we find that Kleve’s vehicle owner can set a restriction, such as the rental start period, prior to step 214 in Kleve’s Figure 2 and that such restrictions can be associated with the e-key. We also do not agree with Patent Owner’s argument that (1) Dr. Almeroth’s declaration testimony contradicts his deposition testimony or that (2) Dr. Almeroth “admitted his testimony was wrong.” *See* PO Sur-Reply 7 (citing PO Resp. 47–48 (citing Ex. 2022, 27:5–10, 27:21–28:1; Ex. 2021 ¶ 96)). In a particular embodiment to which Dr. Almeroth was citing, he noted that the e-key is always generated after the rental agreement. *See* Ex. 2022, 26:14–20. Then the following exchange occurs:

> Q. So you use typically and always. So always does not refer to all of the embodiments of Kleve, is that fair?
>
> A. I think a person of skill in the art could read Kleve and understand that there are probably multiple ways in which the flow of actions among the parties could occur. And I think thinking about a real world scenario, in most cases you have an agreement before you would generate an eKey, but maybe, maybe not. I don’t -- I don’t know that the real world is necessarily cut and dry.
> So reading -- a person reading Kleve would understand it’s describing embodiments where it’s

> always the case. That might be a pretty common scenario, but I don't know that it would necessarily be a hard and fast rule in every embodiment or in the understanding a person of skill in the art would have.

Id. at 28:3–20. There is nothing in the deposition testimony by Dr. Almeroth that appears inconsistent with his declaration testimony nor does there appear to be the kind of admission touted by Patent Owner. Instead, it is Dr. Malek who takes an overly narrow view of Kleve that appears inconsistent with Kleve's disclosure when read as a whole. *See, e.g.*, Ex. 2021 ¶¶ 82–88. Therefore, we do not credit or agree with Dr. Malek's testimony that Kleve fails to teach the concept of a virtual key created with the agreed-upon rental period as a restriction. *See id.* ¶ 57.

Thus, based on the entire trial record, we find that Petitioner has provided persuasive explanation and cited credible evidence that Kleve alone or in combination with Hatton teaches or suggests the challenged claim limitations.

d) Rationale to Combine

Petitioner contends a person of ordinary skill in the art at the critical time would have been motivated to combine Kleve's system with Hatton's teaching of an e-key system for vehicles. Pet. 12 (citing Ex. 1004 ¶¶ 109–115); Pet. Reply 17–18. According to Petitioner, "[t]here were well-known benefits of using encrypted data for wireless communications" including being able to ensure that only authorized receivers can view messages that are sent over radio waves. Pet. 12 (citing Ex. 1004 ¶ 110). Petitioner argues that "[f]or electronic key systems, encrypted communications would be particularly effective to prevent unauthorized access to the vehicle" while "[a]ssociating encrypted data with specific electronic keys would further

facilitate an owner's monitoring and control of vehicle use by individual users." *Id.* at 12–13. According to Petitioner, a person of ordinary skill in the art would have "been motivated to bind the virtual key to the receiving user's mobile device (*e.g.*, by associating the virtual key with an identifier unique to the mobile device) to prevent unauthorized distribution to third parties." *Id.* at 13 (citing Ex. 1004 ¶ 111).

Petitioner explains that a person of ordinary skill in the art would have been "particularly motivated to look to Hatton's teachings to improve Kleve because both Kleve and Hatton are Ford references directed to similar electronic key systems for use in a vehicle." *Id.* (citing Ex. 1004 ¶ 113). Petitioner cites as an example the fact that "both Kleve and Hatton describe an identical architecture for a computing system within a vehicle (the 'VCS' in both references) and a 'vehicle rental' business using that system." *Id.* at 13–14 (citing Ex. 1005 ¶¶ 21–36, Fig. 1; Ex. 1008, 2:54–5:53, Fig. 1).

Petitioner further argues that a person of ordinary skill in the art would have had a reasonable expectation of success in applying Hatton to Kleve because "Kleve already uses its wireless communications circuitry for encrypted communications (*e.g.*, with a server)" and "[c]onfiguring the wireless communications circuitry to additionally receive encrypted messages associated with a virtual key and including use restriction information directly from a mobile device would have been a straightforward and routine application of well-known techniques in wireless communications and encryption." *Id.* at 14 (citing Ex. 1004 ¶ 114; Ex. 1005 ¶ 63). Petition then concludes that "it would have been obvious to a POSITA to use one of several standard, well-known encryption techniques (such as public/private key encryption) to implement the encryption schemes

described by Kleve and Hatton, and a POSITA would have been capable of implementing such encryption techniques within those systems." *Id.*

Patent Owner disagrees with Petitioner because it contends that Hatton is directed to encryption for authentication and not encryption for confidentiality. PO Resp. 54–56 (citing Ex. 2021 ¶¶ 104–117). According to Patent Owner, these are distinct concepts so a person of ordinary skill in the art at the critical time would not have been motivated to modify Kleve in view of Hatton in order to add encryption for authentication purposes. *Id.*

Patent Owner then contends that Petitioner fails to explain how Kleve could be modified as proposed because "Hatton does not disclose generating any encrypted data at a mobile device." *Id.* at 56 (citing Ex. 2021 ¶ 115). Patent Owner explains that because Hatton's encrypted data is assigned to a vehicle at the manufacturing process, it would not have been obvious in view of Hatton to generate encrypted data to include restrictions for use in a rental vehicle because the encrypted data would have already been generated. *Id.* (citing Ex. 1008, 8:24–36, 14:7–18). Patent Owner argues that "[u]nder Petitioners' theory, encrypted data would need to be generated each time 'restrictions' were created or modified, but Hatton does not have a mechanism for doing this." *Id.* at 57.

After review of the arguments and evidence, we agree with Petitioner's position. Specifically, we agree that (1) both Kleve and Hatton are directed to use of electronic key systems for vehicles (*see* Ex. 1005 ¶¶ 7–9, 39, 63; Ex. 1008, 1:48–52, 1:61–2:2, 5:25–34) and (2) encrypted communications would have been understood to be effective in preventing unauthorized access to the vehicle, something that is taught explicitly by Hatton (*see* Ex. 1008, 9:50–63). Given these disclosures by Kleve and Hatton, we find that a person of ordinary skill in the art would have had a

reasonable expectation of success in combining these teachings and arriving at the challenged claims. Accordingly, we find that a person of ordinary skill in the art at the critical time would have had a reason to combine the teachings of Kleve with that of Hatton.

e) Summary Regarding Challenge to Independent Claim 1 Based on Kleve Alone or in Combination with Hatton

Based on the entire trial record, Petitioner has demonstrated by a preponderance of the evidence that independent claim 1 would have been obvious to a person of ordinary skill in the art at the critical time in view of Kleve alone or in combination with Hatton.

2. Analysis of Independent Claims 11 and 18, and Dependent Claims 3–5, 7–10, 14–17, 19, and 21

Petitioner provides arguments and evidence regarding independent claims 11 and 18, as well as dependent claims 3–5, 7–10, 14–17, 19, and 21 in view of Kleve alone or in combination with Hatton. Pet. 22–36. Patent Owner has not provided separate arguments regarding Kleve alone or in combination with Hatton in regards to these challenged claims. *See* PO Resp. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

We have reviewed the Petition's analysis of the other claimed subject matter not discussed in the previous sections and we agree with the analysis. Based on our review of the arguments and evidence submitted for these challenged claims and the reasons discussed previously, we find that Petitioner has demonstrated by a preponderance of the evidence that Kleve alone or in combination with Hatton would have rendered independent claims 11 and 18, as well as dependent claims 3–5, 7–10, 14–17, 19, and 21 obvious to a person of ordinary skill in the art at the critical time.

3. *Analysis of Dependent Claim 6*

Dependent claim 6 recites: "The sub-system of the vehicle of claim 1, wherein an application associated with said mobile device is configured to enable sharing of said eKey with a recipient user having a recipient mobile device, the sharing is enabled via a message initiated from said mobile device."

Petitioner provides arguments and evidence that Kleve meets this claim because Kleve discloses a "rental microbusiness" implemented as a "smart phone application" that enables sharing virtual keys. Pet. 25 (citing Ex. 1005 ¶ 36). Petitioner argues that 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.* According to Petitioner, "[d]istribution is enabled by the owner using the smartphone application to send messages agreeing to rental terms and generating the virtual key." *Id.* (citing Ex. 1005 ¶¶ 39, 47–48, 51, 69; Ex. 1004 ¶¶ 154, 156). Petitioner asserts that it would have been obvious to an ordinarily skilled artisan that "the smartphone application may also be used to enable multiple authorized temporary users to share virtual keys with each other" and that a person of ordinary skill in the art "would have been motivated to allow such sharing to facilitate rentals to groups (*e.g.*, families, travel groups) where multiple members may use the vehicle." *Id.* (citing Ex. 1004 ¶ 155). Petitioner further asserts that an ordinarily skilled artisan "could implement such sharing using the same or similar software used to enable an owner to distribute virtual keys to temporary users." *Id.* at 25–26.

Patent Owner disputes Petitioner's position and argues that Kleve fails to meet the claim limitation. PO Resp. 79–80; PO Sur-Reply 29–30. Patent

Owner explains that in at least one embodiment, even after a virtual key is distributed to the Temporary User, Kleve requires that the Vehicle Owner sends the "credential" to the vehicle "at rental time," and, "at rental time," the Temporary User inputs their "credential" at the vehicle. PO Resp. 80 (citing Ex. 1005, Fig. 5, ¶ 66). That means, according to Patent Owner, the vehicle must compare and confirm a "match" between these two credentials before authorizing the Temporary User's drive. *Id.* Therefore, Patent Owner argues that Kleve discourages its Temporary User—whose own vehicle usage will be specifically monitored and controlled by the Vehicle Owner's actions—from sharing an eKey for the vehicle with some other user. *Id.* (citing Ex. 2021 ¶¶ 137–138). Patent Owner further argues that such sharing among Temporary Users "would render meaningless Kleve's disclosures that even for an already-authorized Temporary User, an additional credential match must occur before the drive is authorized." *Id.* (citing Ex. 2021¶ 139; Ex. 1005, Fig. 5).

We agree with Patent Owner. Petitioner's argument appears to be purely hindsight analysis based on the teachings of the '659 patent and the limitations of challenged claim 6 because there is insufficient evidence or teachings in the cited prior art to suggest the sharing of virtual keys. Petitioner's argument that having "rental microbusiness" implemented as a "smart phone application" that enables sharing virtual keys is insufficient to show obviousness, because, as noted by Patent Owner, certain embodiments in Kleve appear to discourage or even hinder the sharing of virtual keys. These embodiments require the use of credentials associated with the virtual key, where the credentials can be "facial recognition, voice print recognition, matrix barcode (ex. two-dimensional code), code word or phrase for speech recognition, temporary mobile web login IDs and password, or other types

of unique Temporary User identification to validate and pay for the rental service." *See* Ex. 1005 ¶ 37.

Dr. Almeroth testifies that multiple people could be authorized on the same vehicle if they collectively rent a vehicle and that a person of ordinary skill in the art would "have been motivated to enable each user to share the virtual key with other authorized users associated with the same rental request." Ex. 1004 ¶ 55. But given Kleve's disclosure that the system handles key generation and distribution (Ex. 1005 ¶ 39), the evidence does not show that a person of ordinary skill in the art would have wanted to give this control to each authorized user who has received an e-key. "It is impermissible to use the claimed invention as an instruction manual or 'template' to piece together the teachings of the prior art so that the claimed invention is rendered obvious." *Fritch*, 972 F.2d 1260, 1266 (Fed. Cir. 1992) (citing *In re Gorman*, 933 F.2d 982, 987 (Fed. Cir. 1991)).

Kleve's teachings undermine Petitioner's position, and do not support a finding of obviousness. Accordingly, we determine that Petitioner has not demonstrated by a preponderance of the evidence that Kleve alone or in combination with Hatton would have rendered dependent claim 6 obvious to a person of ordinary skill in the art at the critical time.

4. Analysis of Dependent Claims 12, 13, and 20

Claim 12 recites: "The system of a vehicle as recited in claim 11 wherein a server is configured for communication with the application executed by the mobile device, the server is one of a plurality of servers, and one of said servers is associated with a manufacturer of the vehicle."

Petitioner provides arguments and evidence that Kleve meets this claim because Kleve discloses an application on a mobile device that communicates with a server. Pet. 30 (citing Ex. 1004 ¶¶ 173–176).

Petitioner notes that Kleve's server may be one of a plurality of servers. *Id.* According to Petitioner, "Kleve's server system may include at least an 'automated call server and/or web host,' each of which may be operated as a separate server." *Id.* (citing Ex. 1005 ¶ 57; Ex. 1004 ¶ 174).

Claim 12 additionally requires that one of the servers "is associated with a manufacturer of the vehicle." Petitioner contends that this limitation is not entitled to any patentable weight under the printed matter doctrine because "it claims the content of information" (i.e., who operates the server) and lacks any "functional relationship" to the server. *Id.* at 30–31 (citing *Praxair Distribution, Inc. v. Mallinckrodt Hosp. Prods. IP Ltd.*, 890 F.3d 1024, 1031–32 (Fed. Cir. 2018)). Petitioner argues that the server's owner would not change the underlying functionality and implementation of the system. *Id.* at 31 (citing Ex. 1004 ¶ 175). Regardless, Petitioner asserts that a person of ordinary skill in the art would have understood, and it would have been obvious, that the server may be associated with a manufacturer of the vehicle because Kleve is a Ford patent, and thus the disclosed system would have been developed for use by Ford. *Id.* (citing Ex. 1004 ¶ 176). Petitioner further asserts that "[c]ontemporaneous references confirm that electronic key systems including servers operated by vehicle manufacturers were well known by the time of the '659 patent." *Id.* (citing Ex. 1010, 11:15–31, 16:6–18 (describing an "automobile service server" and "automobile web service server" "associated with an automobile company")).

Petitioner makes similar arguments for claims 13 and 20. Pet. 31–33, 36.

Patent Owner disagrees with Petitioner's position and argues first that the printed matter doctrine is inapplicable because "printed matter must be

matter claimed for what it communicates." PO Resp. 81 (citing *C R Bard Inc. v. AngioDynamics, Inc.*, 979 F.3d 1372 (Fed. Cir. 2020)). According to Patent Owner, Petitioners offer no explanation how the limitations of claims 12, 13 and 20 meet this threshold inquiry of the "printed matter doctrine." *Id.*; PO Sur-Reply 31.

Patent Owner further argues that these limitations cannot implicate the printed matter doctrine where the specification provides numerous examples describing how applications, servers, and vehicles of the vehicle manufacturer are functionally related to the other claimed components of the system/vehicle. PO Resp. 81–82 (citing Ex. 1001, 15:15–37, 13:20–49, 13:50–14:2, 47:35–48:2). Therefore, Patent Owner concludes that reading the claims as a whole, the limitations of claims 12, 13 and 20 add functional characteristics to the claimed systems and vehicle. *Id.* at 82.

Regardless of whether the claims implicate the printed matter doctrine, we conclude the claims would have been obvious to an ordinarily skilled artisan. First, we agree with Petitioner that changing the server or the server's owner would not change the underlying functionality of the system. Second, we also agree with Petitioner that an ordinarily skilled artisan would have readily recognized that Kleve's server would likely be associated with the vehicle's manufacturer considering that Kleve is assigned to a major vehicle manufacturer. Third, we further agree with Petitioner that servers operated by vehicle manufacturers were well known by the time of the '659 patent. *See* Ex. 1004 ¶ 176 (citing Ex. 1010). Accordingly, we find that Petitioner has demonstrated by a preponderance of the evidence that Kleve alone or in combination with Hatton would have rendered dependent claims 12, 13, and 20 obvious to a person of ordinary skill in the art at the critical time.

C. Claim 2 Allegedly Rendered Obvious by Kleve and Hatton with Sekiyama

Claim 2 recites:

> The sub-system of the vehicle of claim 1, wherein said privileges function as restrictions that enable access to specific vehicle areas that include one or more of vehicle door operation, or trunk operation.

Ex. 1001, 52:40–43.

Petitioner provides arguments and evidence regarding dependent claim 2 in view of Kleve in combination with Hatton and with Sekiyama. Pet. 36–39 (citing Ex. 1004 ¶¶ 201–202). Specifically, Petitioner cites to Sekiyama for an "electronic key system" that enables "a subset of functions" while disabling "other functions." *Id.* at 38–39 (citing Ex. 1006 ¶ 8). Petitioner argues that the system may enable "a function of locking/unlocking a door lock of a vehicle" but disable "unlocking the trunk." *Id.* at 39 (citing Ex. 1006 ¶ 18).

According to Petitioner, a person of ordinary skill in the art would have been motivated to apply Sekiyama's teachings regarding restricting duplicate key access to vehicle functions such as the door lock and trunk to Kleve's vehicle rental system, because it would provide the vehicle owner with more control over the use of the vehicle, and thus offer more flexibility in providing access to the vehicle to temporary users. *Id.* at 39.

Patent Owner has not provided separate arguments regarding Kleve in combination with Hatton and with Sekiyama in regards to this challenged dependent claim. *See* PO Resp. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

We have reviewed the Petition's analysis and agree with it. Additionally, we credit Dr. Almeroth's testimony that an ordinarily skilled artisan would have been motivated to incorporate Sekiyama's eKey signal that allows execution of only a subset of functions to Kleve's vehicle rental system. Ex. 1004 ¶¶ 201–202. This would allow a user to restrict door locking and trunk access in Kleve's vehicle in order to "enhanc[e] security features and strengthen[] the protection of personal information." *Id.* ¶ 202 (citing Ex. 1006 ¶ 8).

Accordingly, based on the entire trial record, we determine that Petitioner has demonstrated by a preponderance of the evidence that dependent claim 2 would have been obvious over Kleve in combination with Hatton and with Sekiyama.

D. Claims 1, 3, 5 and 8–10 Allegedly Anticipated and/or Rendered Obvious by Mikan

Petitioner contends that the disclosure of Mikan anticipated or renders obvious the subject matter of claims 1, 3, 5 and 8–10. Pet. 39–49; Pet. Reply 18–22. Patent Owner disagrees. PO Resp. 58–79; PO Sur-Reply 24–29. Patent Owner specifically challenges whether Petitioner has shown that Mikan discloses or teaches "coded date" that includes privilege settings and is "from a mobile device" as recited in limitations [d] and [e] of independent claim 1.

1. Analysis of Independent Claim 1

Claim 1 recites the following limitations:

> [1d] wherein the wireless communications circuitry of the vehicle is configured to receive coded data from the mobile device when using the eKey, the coded data enables functions of said eKey for said unlocking and use of the vehicle, the coded data is associated to the eKey for use by the mobile device,

> [1e] and the coded data includes privilege settings associated with the eKey for limiting types of use of the vehicle when using the eKey with the vehicle;

Ex. 1001, 52:28–36.

(i) Petitioner's Contentions

Petitioner contends that, for limitation [d], Mikan teaches wireless communications circuitry that receives coded data associated with an electronic key from a mobile device. Pet. 43–44 (citing Ex. 1004 ¶¶ 218–219). Petitioner asserts that, in Mikan, when "a user attempt[s] to access or operate vehicle 201 with a key 205A-C," the control unit initiates an authentication process where "[s]ecure identifier 407 may be received . . . at control unit 202." *Id.* at 44 (citing Ex. 1007 ¶¶ 67, 70). According to Petitioner, Mikan's "secure identifier comprises coded data, such as 'a digital signature associated with a key,' which may be 'the product of a public key encryption system.'" *Id.* (citing Ex. 1007 ¶ 59).

Petitioner relies on Dr. Almeroth's testimony to support its position. *See* Pet. 44. Dr. Almeroth testifies that "[a]uthenticating the electronic key using the secure identifier enables the key to perform vehicle functions, such as unlocking and using the vehicle." Ex. 1004 ¶ 219. Petitioner then explains that, in Mikan, "after the electronic key has been authenticated, the control unit may retrieve a 'vehicle operation policy . . . based on authenticated key 205A-C,' which enables the use of certain 'vehicle operation features,' including 'unlocking a door' and 'engaging an ignition.'" Pet. 44 (citing Ex. 1007 ¶¶ 60–61, 72).

Petitioner next contends that, for limitation [e], Mikan discloses privilege settings that limit the types of use of the vehicle as being included with the coded data associated with an electronic key. *Id.* (citing Ex. 1004

¶¶ 220–223). Petitioner specifically asserts Mikan teaches that electronic keys may be linked to vehicle operation policies and that "[a]s part of the electronic key authentication process, the vehicle receives the vehicle operation policy associated with the authenticated key." *Id.* (citing Ex. 1007 ¶¶ 60–61, 72, 76–77).

Petitioner lastly contends that a person of ordinary skill in the art at the critical time would have found it obvious "to transmit the vehicle operation policy as additional coded data along with Mikan's secure identifier" because it would "prevent a secondary user from tampering with the use restrictions associated with an electronic key." Pet. 45 (citing Ex. 1004 ¶ 221); Pet. Reply 18–19 (citing Ex. 1004 ¶¶ 221–222). Petitioner argues that an ordinarily skilled artisan "would have had a reasonable expectation of success because the vehicle operation policy could be encoded and transmitted using the same encryption and wireless communication techniques already implemented and used to transmit Mikan's secure identifier," and would have been "capable of applying these techniques to encode and transmit Mikan's vehicle operation policy." Pet. 45 (citing Ex. 1004 ¶ 222). Petitioner further argues that "Mikan's vehicle operation policy limits the types of use of the vehicle by the particular electronic key. *Id.* Petitioner then asserts that Mikan's teachings do not preclude sending the vehicle operation policy to the wireless device, and "Mikan itself acknowledges disadvantages in relying exclusively on the master database to provide virtual key information to the vehicle." Pet. Reply 19. Therefore, Petitioner concludes that a person of ordinary skill would have understood that "limiting access to different vehicle functions serves to limit the types of use of the vehicle." Pet. 45 (citing Ex. 1007 ¶¶ 60, 73–74; Ex. 1004 ¶ 223).

(ii) Patent Owner's Contentions

Patent Owner disputes Petitioner's position and contends that Mikan fails to teach any "coded data" with "privilege settings" and that none of the "coded data" is "from the mobile device." PO Resp. 67–79. According Patent Owner, there is no disclosure in Mikan that its vehicle receives any privilege settings (allegedly included in "vehicle operation policies") that are "from the mobile device." *Id.* at 73–75 (citing Ex. 1007 ¶¶ 59, 60–61, 72–74, 81, 84, Figs. 3A–B; Ex. 2021 ¶¶ 126–128).

Patent Owner argues that Mikan's vehicle operation policies are stored in a master database on a wireless network, which syncs with the vehicle in order to send/update the vehicle operation policies that are then stored on the vehicle's local database. PO Resp. 59 (citing Ex. 1007 ¶¶ 58–59, 72, 81, Figs. 3A–B; Ex. 2021 ¶ 67). Next, according to Patent Owner, the master database records a "vehicle ID," that includes a key set, which is "data representing a collection of keys 205A-C," as well as "a policy set of vehicle operation policies 311," and that is stored on the vehicle's local database. *Id.* at 60 (citing Ex. 1007 ¶¶ 58–60, Fig. 3A; Ex. 2021 ¶¶ 68–69). Patent Owner explains that the master database also includes a "mapping 312," which relates individual keys from the records of the key set 310 with specific vehicle operation policies 311. *Id.* (citing Ex. 1007 ¶ 58, Fig. 3A).

Patent Owner argues that, in Mikan, "the synchronization between the databases precedes a vehicle's detection and authentication of a key 205A-C" so that the vehicle control unit "need only access locally stored records, e.g. vehicle operation policy 311 and any included access control rule 317, to process and permit/block specific access requests." *Id.* at 62 (citing

Ex. 1007 ¶¶ 54, 68–69, Fig. 5; Ex. 2021 ¶ 72). Patent Owner then argues that Mikan's vehicle local database also includes a "secure ID check 315" associated with a key in the key set 205A-C in order to authenticate the key. *Id.* (citing Ex. 1007 ¶¶ 59, 70–71; Ex 2021 ¶ 73).

Patent Owner assert that, in Mikan, when a user attempts to access the vehicle, the vehicle receives secure key identifier 407 from the wireless device and is used by the vehicle to authenticate the user's wireless device as a key 205A-B to access the vehicle. *Id.* at 63 (citing Ex. 1007 ¶¶ 60, 70, Fig. 5; Ex. 2021 ¶ 74). Patent Owner explains that secure key identifier 407 is stored in memory of the wireless device or does not include any vehicle operation policy or any access control rule. *Id.* at 63–64 (citing Ex. 1007 ¶ 70, Fig. 4; Ex. 2021 ¶¶ 74–75). Thus, Patent Owner concludes that due to the syncing between the master database and the local database that provides updated vehicle operation policies, in Mikan, the only information that comes from the mobile device is secure key identifier 407, which is insufficient to meet the claim limitations. *Id.* at 64–67 (citing Ex. 1007 ¶¶ 59, 64, 71–72, Figs. 2, 3B, 4, 5; Ex. 2021 ¶ 76); PO Sur-Reply 24.

Patent Owner relies on the testimony of Dr. Malek to support its position. Dr. Malek testifies that a person of ordinary skill at the critical time have understood that Mikan does not disclose or teach sending any vehicle operation policies from a user's mobile device. Ex. 2021 ¶ 75. Dr. Malek further testifies that the vehicle database's mapping 312 relates any locally stored vehicle operation policy 311 that may be in effect with relation to the authenticated key. *Id.* ¶ 76 (citing Ex. 1007 ¶¶ 71–72). According to Dr. Malek, this mapping 312 function would be unnecessary were the vehicle operation policy 311 already included in the secure ID 407 that had already been transmitted from the wireless device to the vehicle. *Id.*

Additionally, Dr. Malek opines that by avoiding storing on or sending from the user's phone any vehicle operation policies, Mikan's solution to store vehicle operation policies on the master database and the local database is already more secure, and less vulnerable to Dr. Almeroth's concerns of a user "tampering with" or circumventing use restrictions. *Id*. ¶¶ 127–133. Therefore, Dr. Malek concludes Mikan discourages a vehicle receiving any privilege settings from a mobile device. *Id*.

(iii). Analysis

We agree with Patent Owner that Petitioner's analysis of the "coded data" to be received "from the mobile device when using the eKey" as required by claim 1 is insufficient. *See* Pet. 44–45; Pet. Reply 18–22. Mikan discloses the following:

(i) wireless vehicle security system where wireless devices may include a cellular telephone (Ex. 1007 ¶¶ 4, 11),

(ii) Mikan's system also includes local and master databases that maintain information about vehicles, keys, and vehicle operation policies associated with different vehicles and keys (*id.* ¶¶ 51, 54),

(iii) a "vehicle operation policy" may assign specific "vehicle operation features" (*e.g.*, "unlocking a door," "opening a trunk," or "engaging an ignition") that are accessible to different electronic keys (*id.* ¶¶ 49, 51),

(iv) Mikan's system also includes a control unit that uses the vehicle operation policies to "block and/or limit operation of vehicle 201 . . . when an access request does not conform with vehicle operation policy," (*id.* ¶ 77),

(v) the system may include multiple keys, which may be "electronic keys" that are "embedded in a wireless device" (*id.* ¶ 50), (vi) the eKeys may include a secure ID check that may be an encrypted digital signature (*id.* ¶ 59), then

(vii) when a user attempts to access or operate the vehicle, this may initiate the authentication of the eKey, which may include receiving a secure identifier that is transmitted from an eKey that is embedded in a wireless device (*id.* ¶ 70), after which

(viii) a vehicle operation policy may be retrieved by, for example, querying the vehicle's local database (*id.* ¶ 72).

We understand this disclosure in Mikan to mean that the vehicle operation policy that includes the vehicle privileges, restrictions, and/or conditions are found on the vehicle's local database. *See* Ex. 1007 ¶ 72. We do not understand the vehicle operation policy to be included as encrypted data on the electronic key that is embedded on the wireless mobile telephone. Therefore, we find that Mikan fails to provide a disclosure or teaching that the "vehicle is configured to receive coded data from the mobile device when using the eKey" where "the coded data includes privilege settings associated with the eKey for limiting types of use of the vehicle when using the eKey with the vehicle. Additionally, we do not discern a sufficient suggestion in Mikan that its coded data with privilege settings would emanate from the embedded eKey in the mobile device. *See id.* ¶¶ 49, 51, 54, 59, 70, 72.

To the extent Petitioner argues that Patent Owner's arguments rely on exemplary embodiments in Mikan and treats such embodiments as limiting (*see* Pet. Reply 19–20), we find Petitioner has not shown sufficiently that Mikan teaches or suggests other embodiments where the coded data with

privilege setting come from the mobile device. Petitioner's argument that "Mikan does not preclude including the vehicle operation policy with the associated electronic key in a wireless device" (*id.* at 19), appears to be premised on hindsight analysis and fails to sufficiently point out where Mikan indicates or suggests that the coded data with privilege settings would be located anywhere other than the vehicle's local drive.

Petitioner argues that "transmit[ting] the vehicle operation policy as additional coded data along with Mikan's secure identifier" would "prevent a secondary user from tampering with the use restrictions associated with an electronic key." Pet. 45 (citing Ex. 1004 ¶ 221). But Petitioner's assertion here is not to explain why it would have been obvious to send the privilege settings from the mobile device to the vehicle; rather it is to explain why it would have been obvious to encrypt such data, which assumes that such data are sent in the first place. *See* Ex. 1004 ¶ 221 ("If the vehicle operation policy is transmitted in unencrypted form, a user may be able to access the policy and modify it to enable unauthorized access to certain vehicle features. A POSITA would thus have been motivated to encrypt or otherwise encode the vehicle operation policy for transmission so that users cannot tamper with the vehicle operation policies and associated access control rules."). Petitioner's contentions already assume that Mikan teaches sending privilege settings from the mobile device to the vehicle, a contention with which we disagree as explained above. *See* Pet. 44 ("Mikan discloses that the coded data associated with an electronic key includes privilege settings that limit the types of use of the vehicle."); Ex. 1004 ¶ 220 ("In my opinion, Mikan discloses that the coded data includes privilege settings for the electronic key that limit the types of use of the vehicle").

In its Reply, Petitioner argues that "[p]roviding the vehicle operation policy through the mobile device allows the vehicle to receive this information even when it cannot communicate with the master database." Pet. Reply 22 (citing Ex. 1004 ¶ 274). Petitioner's cited support for this belatedly raised rationale is Dr. Almeroth's testimony as to why a person of ordinary skill in the art would have combined certain teachings of Sekiyama related to sharing keys with Mikan's teachings for claims 6 and 7. Petitioner, therefore, did not propose this combination of features to address the limitations of sending privileges from the mobile device to the vehicle. *Cf.* 22 ("Mikan identifies a problem in relying on the master database for vehicle operation policies that is solved *by the proposed combination*." (emphasis added)).

Thus, Petitioner fails to explain why an ordinarily skilled artisan would have modified Mikan to provide coded data via a mobile device rather than the recently updated local drive. Petitioner must articulate a *reason why* a person of ordinary skill in the art would have modified the prior art reference. The fact that an ordinarily skilled artisan was not "precluded" from modifying the prior art or that they "may" modify the art is insufficient to demonstrate that they would have done so. *Belden Inc. v. Berk-Tek LLC*, 805 F.3d 1064, 1073 (Fed. Cir. 2015) ("[O]bviousness concerns whether a skilled artisan not only *could have made* but *would have been motivated to make* the combinations or modifications of prior art to arrive at the claimed invention."). Conclusory statements alone, even those provided by a declarant, are inadequate to demonstrate a rationale for why a person of ordinary skill in the art would modify the teachings of the prior art references. *In re NuVasive*, 842 F.3d 1376, 1383 (Fed. Cir. 2016). Instead, Petitioner's arguments must be supported by a "reasoned explanation" and

"must articulate a *reason why* the [person of ordinary skill in the art] would have been motivated to modify" the cited art. *Id.* at 1383–84 (citing *In re Lee*, 277 F.3d 1338, 1342, 1345 (Fed. Cir. 2002)). We understand that a person of ordinary skill is a person of ordinary creativity, not an automaton, but without any explanation as to how or why the references would be modified to arrive at the claimed invention, we are left with only hindsight bias that *KSR* warns against. *See Metalcraft of Mayville, Inc. v. The Toro Co.*, 848 F.3d 1358, 1367 ("'[T]he obviousness analysis cannot be confined by a formalistic conception of the words teaching, suggestion, and motivation,' we also recognize that we cannot allow hindsight bias to be the thread that stitches together prior art patches into something that is the claimed invention" (quoting *KSR*, 550 U.S. at 420–21)).

We also find that the teachings of Mikan's e-key embedded in a wireless device fail to meet the claim limitation because the secure ID stored as coded data in the wireless device does not include privilege settings and at no time does Mikan suggest that the secure ID would include such privilege settings. Again, Petitioner's argument that it would have been obvious to provide the vehicle operation policy as coded data (*see* Pet. Reply 21–22) appears to be based on hindsight analysis and not on the actual teachings or suggestions found in Mikan.

Accordingly, based on the entirety of the trial record, we determine Petitioner failed to demonstrate by a preponderance of the evidence that Mikan anticipates or renders obvious the required limitations of claim 1[d]/[e] for a "receive coded data from the mobile device" where "the coded data include privilege settings."

2. Analysis of Dependent Claims 2, 3, 5, and 8–10

Petitioner asserts that dependent claims 2, 3, 5, and 8–10 are anticipated by or rendered obvious by the disclosures of Mikan. Pet. 46–49; Pet. Reply 18–22.

For this challenge, Patent Owner relies on the same arguments presented for claim 1. PO Resp. 58–79; PO Sur-Reply 24–29.

For the reasons discussed above with regards to independent claim 1, and because no additional arguments remedy the deficiencies of Mikan, we determine Petitioner has failed to demonstrate by a preponderance of the evidence that claims 2, 3, 5, and 8–10 are anticipated by or would have been obvious in view of Mikan.

E. Alleged Obviousness of Claims 4, 11–18, and 20–21 in View of Mikan and Xiao

Petitioner contends the combined teachings of Mikan and Xiao would have rendered claims 4, 11–18, and 20–21 obvious. Pet. 2, 49–63. Claims 11 and 18 recite substantially similar elements for limitations [d] and [e]. *See id.* 53:35–40, 54:27–32. For this challenge, as to the disputed limitations discussed above, Petitioner does not rely on Xiao for additional teachings that remedy the deficiencies discussed above. *See* Pet. 57, 62. Patent Owner relies on the same arguments presented for claims 1, 11, and 18 in view of Mikan alone. *See* PO Resp. 58–79. For the reasons discussed above, we agree with Patent Owner.

Accordingly, based on the entirety of the trial record, we determine Petitioner has failed to demonstrate by a preponderance of the evidence that Mikan in combination with Xiao would have rendered claims 4, 11–18, and 20–21 obvious to an ordinarily skilled artisan at the critical time.

F. Alleged Obviousness of Claims 6, 7, and 19 in View of Mikan, Xiao, and Sekiyama or Mikan and Sekiyama

Petitioner contends the combined teachings of Mikan, Xiao, and Sekiyama would have rendered obvious claim 19 and that the combined teachings of Mikan with Sekiyama would have rendered claims 6 and 7obvious. Pet. 2, 63–68. For this challenge, Patent Owner relies on the same arguments presented for claims 1, 11, and 18 in view of Mikan alone. *See* PO Resp. 58–79. For the reason discussed above, we agree with Patent Owner.

Accordingly, based on the entirety of the trial record, we determine Petitioner failed to demonstrate by a preponderance of the evidence that claims 6, 7, and 19 would have been obvious to an ordinarily skilled artisan at the critical time.

IV. CONCLUSION[8]

For the reasons discussed above, we determine that Petitioner has proven, by a preponderance of the evidence, that claims 1–5 and 7–21 of the ’659 patent are unpatentable, as summarized in the following table:

[8] Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this decision, we draw Patent Owner’s attention to the April 2019 *Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding*. *See* 84 Fed. Reg. 16,654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. *See* 37 C.F.R. § 42.8(a)(3), (b)(2).

Claim(s)	35 U.S.C. §	Reference(s)/Basis	Claims Shown Unpatentable	Claims Not Shown Unpatentable
1, 3–21	103	Kleve, Hatton	1, 3–5, 7–21	6
2	103	Kleve, Hatton, Sekiyama	2	
1–3, 5, 8–10	102	Mikan		1–3, 5, 8–10
1–3, 5, 8–10	103	Mikan		1–3, 5, 8–10
4, 11–18, 20, 21	103	Mikan, Xiao		4, 11–18, 20, 21
6, 7	103	Mikan, Sekiyama		6, 7
19	103	Mikan, Xiao, Sekiyama		19
Overall Outcome			1–5, 7–21	6

V. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that claims 1–5 and 7–21 of the ’659 patent have been shown to be unpatentable;

FURTHER ORDERED that claim 6 of the ’659 patent has not been shown to be unpatentable;

FURTHER ORDERED that, because this is a Final Written Decision, parties to the proceeding seeking judicial review of the Decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

For PETITIONER:

James Glass
Quincy Lu
Brett Watkins
Ron Hagiz
QUINN EMANUEL URQUHART & SULLIVAN, LLP
jimglass@quinnemanuel.com
quincylu@quinnemanuel.com
brettwatkins@quinnemanuel.com
ronhagiz@quinnemanuel.com

Joshua Goldberg
James Barney
Aidan Skoyles
Nicholas Eitsert
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, LLP
joshua.goldberg@finnegan.com
james.barney@finnegan.com
aidan.skoyles@finnegan.com
nicholas.eitsert@finnegan.com

For PATENT OWNER:

Brenda Entzminger
Aaron Hand
Jerry Tice
BUNSOW DE MORY LLP
bentzminger@bdiplaw.com
ahand@bdiplaw.com
jtice@bdiplaw.com