Trials@uspto.gov
571-272-7822

Paper 30
Date: November 19, 2025

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

TOYOTA MOTOR CORP.,
Petitioner,

v.

EMERGING AUTOMOTIVE LLC,
Patent Owner.

IPR2024-00814
Patent 11,396,244 B2

Before GEORGIANNA W. BRADEN, FRANCES L. IPPOLITO, and JASON M. REPKO, *Administrative Patent Judges.*

IPPOLITO, *Administrative Patent Judge*.

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

I. INTRODUCTION

Toyota Motor Corp. ("Petitioner") filed a Petition (Paper 1, "Pet.") requesting *inter partes* review of claims 1, 2, and 4–20[1] of U.S. Patent No. 11,396,244 B2 (Ex. 1001, "the '244 patent"). Emerging Automotive LLC ("Patent Owner") filed a Preliminary Response (Paper 6, "Prelim. Resp."). With our authorization, Petitioner filed a Preliminary Reply (Paper 7, "Prelim. Reply") and Patent Owner filed a Preliminary Sur-reply (Paper 9, "Prelim. Sur-reply"). Applying the standard set forth in 35 U.S.C. § 314(a), we instituted an *inter partes* review. Paper 11 ("Inst. Dec.").

After institution, Patent Owner filed a Patent Owner Response (Paper 16, "PO Resp."), and Petitioner filed a Reply (Paper 18, "Pet. Reply"). Patent Owner filed a Sur-reply (Paper 20, "PO Sur-reply"). An oral hearing was held on August 25, 2025. Paper 29 ("Tr.").

We have jurisdiction pursuant to 35 U.S.C. § 6. This Decision is a Final Written Decision under 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73 as to the patentability of the Challenged Claims. Petitioner bears the burden of proving unpatentability of the Challenged Claims. *Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015). To prevail, Petitioner must prove unpatentability by a preponderance of the evidence. *See* 35 U.S.C. § 316(e) (2018); 37 C.F.R. § 42.1(d) (2021).

[1] The '244 patent issued with claims 1–20. In the Petition, Petitioner includes claims 21 and 22 that Patent Owner seeks to add in its Request for a Certificate of Correction ("COC"). *See* Pet. 1, n.1 (citing Ex. 1002, 620–660). That request was denied. Ex. 1027. Subsequently, Patent Owner filed an application for reissue, that reissue application has been suspended. *See* Paper 15 ("Joint Stipulation to Stay Reissue Application 18/977,798").

Having reviewed the arguments and the supporting evidence, we determine that Petitioner has shown, by a preponderance of the evidence, that claims 1, 2, and 4–20 are unpatentable.

A. Real Parties in Interest

Petitioner identifies Toyota Motor Corp., Toyota Motor North America, Inc., and Toyota Motor Sales, U.S.A., Inc. as the real parties-in-interest. Pet. 82. Patent Owner identifies Emerging Automotive LLC as the real party-in-interest. Paper 3 (Patent Owner's Mandatory Notices), 2.

B. Related Matters

The parties indicate that the '244 patent has been asserted in the following district court litigation: *Emerging Automotive LLC v. Toyota Motor Corp., et al.*, 2:23-cv-00434 (E.D. Tex.). Pet. 83; Paper 3, 2. Petitioner further indicates that this case has been consolidated for pretrial issues with: *Emerging Automotive LLC v. Kia Corp.*, No. 2:23-cv-00437-JRG (E.D. Tex.). Pet. 83. After the Petition was filed, the '244 patent was removed from the related district court litigation. Prelim. Reply 1; *see generally* Ex. 1029 (Second Amended Complaint).

C. The '244 patent

The '244 patent "relates to systems and methods for managing user profiles for vehicles and exchange of information with cloud-based processing systems." Ex. 1001, 1:37–39. The '244 patent discloses that a "user profile defines one or more settings that are preferred to be set in vehicles if the vehicles support the settings." *Id.* at 3:1–3. Furthermore, "applicable settings [are] those settings that are preferred to be set as identified from the user profile and are settable in the selected vehicle." *Id.* at 3:7–9. Figure 1, reproduced below, is a diagram showing how roles are associated with profiles settings for a vehicle. *Id.* at 6:15–16.

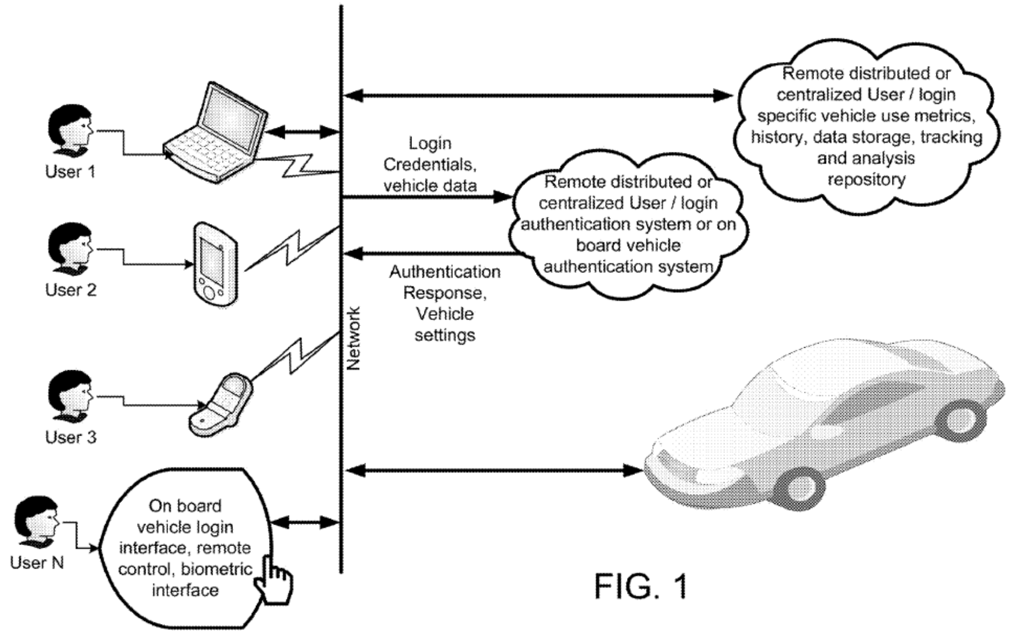

FIG. 1

Figure 1 above shows that different users can use different methods to interact with a vehicle login system. *Id.* at 15:62–63. After successful authentication or login, the user is allowed to operate the vehicle in which the vehicle "has [the user's] vehicle settings applied to it." *Id.* at 16:7–9.

The '244 patent further discloses that "the functions of the specific applications illustrated in the [vehicle] display will be monitored and restricted depending on safety considerations while driving." *Id.* at 9:66–10:1. For instance, "if a particular application requires entry of text, navigation of controls, or other activities that would distract the driver during operation of the vehicle, such vehicle controls or application controls for application interfaces can be temporarily disabled." *Id.* at 12:3–7. Also, "[e]ach login can be configured to provide or restrict access based on the user logged into the vehicle." *Id.* at 14:44–46.

D. Challenged Claims

1. Requests for Correction and Reissue

The ’244 patent issued with claims 1–20. Ex. 1001, 33:9–36:29. On January 17, 2024, Patent Owner filed a Request for a Certificate of Correction (“COC”). Ex. 1002, 627, 631–636. Patent Owner’s COC included amendments to independent claims 1 and 17, amendments to dependent claim 11, and further added claims 21 and 22 to the ’244 patent. *See* Ex. 1002, 631–637; *see* Pet. 1, n.1 (citing Ex. 1002, 620–660). Patent Owner’s COC was denied on September 23, 2024. Ex. 1027. On October 15, 2024, Patent Owner filed a Reconsideration of the Certificate of Correction. *See* Paper 10, Paper 12, 2. That Reconsideration was denied. Paper 12, 2. Patent Owner then filed a request for reissue. Paper 15. The request for reissue remains suspended, pending the outcome of this *inter partes* review. *Id.*; *see* Tr. 5 (“[O]n December 11th, 2024, the Patent Owner filed a request for reissue. That request for reissue is suspended, pending the outcome of this IPR. And so for the purposes of today’s discussion, we will address the claims as they stand, which do not include the language that was sought to be included.”). Thus, originally issued claims 1, 2, and 4–20 of the ’244 patent are subject to this *inter partes* review.

2. Independent Claim 1 and Claim 17

Petitioner challenges issued claims 1, 2, and 4–20. Pet. 1. Issued claims 1 and 17 are independent. Claims 1 and 17 are provided below:

Independent claim 1 is reproduced below:

> 1. A method executed by a server of a cloud services system that is configured to interface with vehicles, comprising:
>
> receiving, by the server, a request from electronics of a vehicle to access a profile for a user account, the request identifies user information for a user to use the vehicle;

> processing, by the server, at least part of the user information to verify the user for accessing the profile associated with the user account, the profile having a plurality of settings of the user for the vehicle, at least part of the plurality of settings for the profile being stored on storage accessible to the cloud services system; and
>
> transferring, by the server, upon verifying the user information, one or more settings of the plurality of settings to the vehicle, the transferring is configured to instruct software and/or hardware associated with said electronics of the vehicle to apply said one or more settings to the vehicle for customizing said vehicle to use said one or more settings associated with the profile,
>
> wherein the vehicle uses wireless communication for exchanging data with the cloud services system and for receiving said one or more settings for the profile.

Ex. 1001, 33:9–32.

Independent claim 17 is reproduced below:

> 17. A cloud-based system including one or more data centers, and each data center of the cloud-based system includes one or more servers, wherein some of said one or more servers have program instructions for enabling connections with vehicles and providing services to vehicles, wherein one service includes enabling access to settings associated with profiles of user accounts of the cloud-based system, comprising:
>
> receiving, by one of the servers, a request from a vehicle to access a profile for a user account associated with a user, the request identifies user information related to a user;
>
> processing, by one of the servers, at least part of the user information to verify the access for the user, the profile having a plurality of settings of the user for the vehicle, at least part of the plurality of settings of the profile being stored on storage accessible to said one or more servers; and
>
> transferring, by one of the servers, upon verification of the user information, one or more settings of the plurality of settings to the vehicle, the transferring is configured to instruct

> software and hardware associated the vehicle to enable said one or more settings for use on the vehicle to customize said vehicle for the user, the request and the transferring being via wireless communication of said vehicle.

Id. at 34:66–35:25.

E. Prior Art and Asserted Challenges to Patentability

Petitioner asserts that claims 1, 2, and 4–20 are unpatentable based on the following challenges:

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1, 9, 11–17, 19, 20	103	Rector,[2] Kleve[3]
2, 4, 10, 18	103	Rector, Kleve, Yassin[4]
5–7	103	Rector, Kleve, Yassin, Patenaude[5]
8, 21	103	Rector, Kleve, Faenger[6]
22	103	Rector, Kleve, Faenger, Yassin

Pet. 3. Petitioner also relies on the Declarations of Kevin C. Almeroth, Ph.D. (Exs. 1005, 1030). Patent Owner relies on the Declaration of Sam Malek, Ph.D. (Exs. 2001, 2003).

II. PRINCIPLES OF LAW REGARDING OBVIOUSNESS

In *Graham v. John Deere Co. of Kansas City*, 383 U.S. 1 (1966), the Supreme Court set out a framework for assessing obviousness under § 103 that requires consideration of four factors: (1) the "level of ordinary skill in

[2] U.S. Patent Application Publication No. 2011/0137520 A1, published June 9, 2011 (Ex. 1006) ("Rector").
[3] U.S. Patent Application Publication No. 2014/0129053 A1, published May 8, 2014 (Ex. 1007) ("Kleve").
[4] U.S. Patent No. 6,505,780 B1, issued Jan. 14, 2003 (Ex. 1008) ("Yassin").
[5] U.S. Patent Application Publication No. 2006/0136106 A1, published June 22, 2006 (Ex. 1009) ("Patenaude").
[6] U.S. Patent Application Publication No. 2011/0035031 A1, published Feb. 10, 2011 (Ex. 1010) ("Faenger").

IPR2026-00070
Emerging Auto EX2013

the pertinent art," (2) the "scope and content of the prior art," (3) the "differences between the prior art and the claims at issue," and (4) "secondary considerations" of non-obviousness such as "commercial success, long-felt but unsolved needs, failure of others, etc." *Id.* at 17–18. "While the sequence of these questions might be reordered in any particular case," *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 407 (2007), the Federal Circuit has "repeatedly emphasized that an obviousness inquiry requires examination of all four *Graham* factors and that an obviousness determination can be made only after consideration of each factor." *Nike, Inc. v. Adidas AG*, 812 F.3d 1326, 1335 (Fed. Cir. 2016).

We note that, with respect to the fourth *Graham* factor, the current record in this proceeding does not include any argument or evidence directed to objective indicia of nonobviousness. Therefore, the analysis below addresses the first three *Graham* factors.

III. LEVEL OF ORDINARY SKILL IN THE ART

In determining the level of skill in the art, we consider the type of problems encountered in the art, the prior art solutions to those problems, the rapidity with which innovations are made, the sophistication of the technology, and the educational level of active workers in the field. *Custom Accessories, Inc. v. Jeffrey-Allan Indus., Inc.*, 807 F.2d 955, 962 (Fed. Cir. 1986); *Orthopedic Equip. Co. v. U.S.*, 702 F.2d 1005, 1011 (Fed. Cir. 1983).

Petitioner contends that a person of ordinary skill in the art ("POSITA" or "POSA") at the time of the invention of the '244 patent "would have had at least a Bachelor's degree in electrical engineering, computer science, or closely related field, with at least two-to-four years' experience in cloud services for settings customization" and that "[a]dditional education (e.g., Master's degree in electrical engineering, computer science, or equivalent) could substitute for professional experience and vice-versa." Pet. 12 (citing Ex. 1005 ¶ 89).

Patent Owner does not address the level of ordinary skill in the art. *See, generally* PO Resp. Patent Owner's Declarant, Dr. Malek, adopts the definition proffered by Petitioner and its Declarant, Dr. Almeroth. Ex. 2001 ¶ 37.

We adopt Petitioner's proposal as it is reasonable and consistent with the prior art. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001) (the prior art may reflect an appropriate level of skill in the art).

IV. CLAIM CONSTRUCTION

We apply the same claim construction standard "used in the federal courts, in other words, the claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. [§] 282(b)," which is articulated in *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc). 83 Fed. Reg. 51,340, 51,358 (Oct. 11, 2018) (amending 37 C.F.R. § 42.100(b) effective November 13, 2018) (now codified at 37 C.F.R. § 42.100(b) (2019)). Under the *Phillips* standard, the "words of a claim are generally given their ordinary and customary meaning," which is "the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention, i.e., as of the effective filing date of the patent application." *Phillips*, 415 F.3d at 1312–13.

According to Petitioner, "[n]o terms of the patent need construction for the purposes of IPR because the claims read on the prior art below under any construction consistent with *Phillips*." Pet. 12.

Patent Owner asserts that the term "transferring is configured to instruct" should be construed according to its plain and ordinary meaning –

"designed, adapted or programmed to accomplish the specific objective of the limitation." PO Resp. 11. Patent Owner contends that the challenged claims require more than that the server is capable of the recited transferring (e.g., claims 1 and 17), and must be configured to accomplish the specific purpose of the claims. *Id.* at 12–17.

Our analysis and the outcome of this dispute, however, would not change even if we were to adopt Patent Owner's construction. Therefore, upon review of the entire record, including arguments by the parties and the relied upon evidence, we determine no terms require express construction to reach our decision. *See Realtime Data LLC v. Iancu*, 912 F.3d 1368, 1375 (Fed. Cir. 2019) ("The Board is required to construe 'only those terms . . . that are in controversy, and only to the extent necessary to resolve the controversy.'" (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))).

V. ANALYSIS

A. Summary of References

1. Rector (Ex. 1006)

Rector is a U.S. patent application publication titled "Devices, Systems and Methods for Controlling Permitted Settings on a Vehicle." Ex. 1006, code (54). Rector's Figure 1 is a diagram "show[ing] a system for controlling a driver's settings" and is reproduced below. *Id.* ¶ 12.

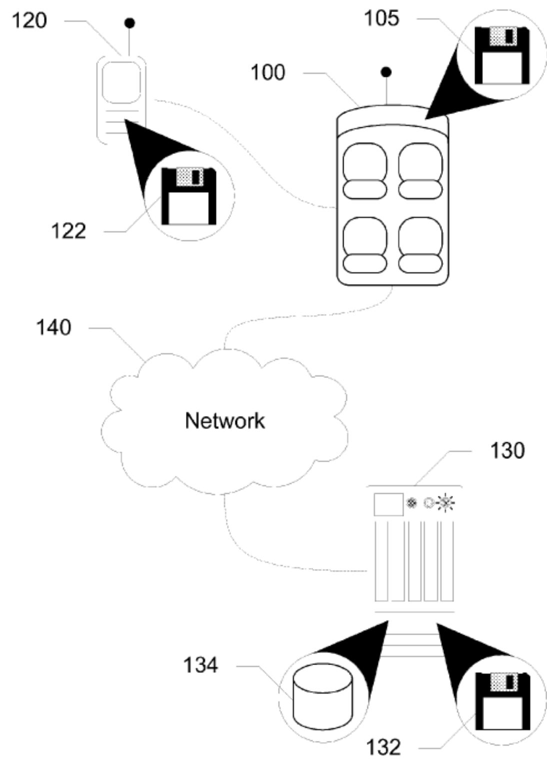

Figure 1

Figure 1, above, shows a system including smart vehicle 100 with client logic 105, wireless communication device 120 with wireless logic 122, network 140, and settings server 130 with server logic 132 and data base 134. *Id.* ¶ 30. Smart vehicle 100 is in communication with wireless communication device 120, and with settings server 130 via network 140. *Id.* Smart vehicle 100 can transmit a request to wireless communication device 120, and then wireless logic 122 may respond with a unique identifier of wireless communication device 120. *Id.* Client logic 105, on smart vehicle 100, may receive the unique identifier and determine the identity of the driver. *Id.* Client logic 105 then transmits the unique identifier through network 140 to settings server 130, which has settings for the driver that is associated with the unique identifier. *Id.* ¶ 31. "The settings, at least in part, are set by a controlling authority, such as a parent or superior of the driver." *Id.* Server logic 132 is used to match the driver's identity with corresponding settings from database 134. *Id.* "The settings may include driver created settings as well as controlling authority settings, such as parental controls, based upon the driver's identity." *Id.* For example, the controlling authority settings "may include a maximum speed of smart vehicle 100, radio controls, wireless communication device controls, passenger based controls, etc." *Id.*

Rector's Figure 3 is a flow chart "show[ing] a method of controlling a driver's settings on a smart vehicle" and is reproduced below. *Id.* ¶ 14.

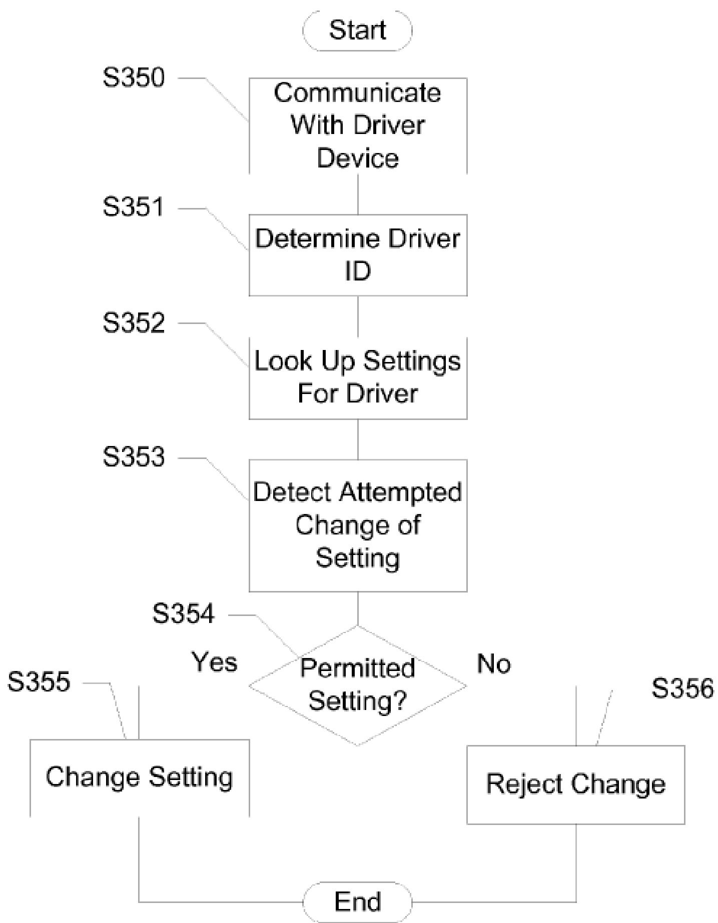

Figure 3

Figure 3, above, shows a method that starts at step S350 in which the smart vehicle communicates with a driver's device such as a wireless communications device when the driver enters or starts the smart vehicle.

Id. ¶ 43. The smart vehicle requests a unique identifier for the driver's wireless communication device to determine the identity of the driver at step S351. *Id.* "[T]he unique identifier may be compared with a set of unique identifiers on a server on a network." *Id.* At step S352, with the identity of the driver determined, the smart vehicle looks up settings for the driver. *Id.*

2. Kleve (Ex. 1007)

Kleve is a U.S. patent application publication titled "Credential Check and Authorization Solution for Personal Vehicle Rental." Ex. 1007, code (54). Kleve "relate[s] to a method and system for authorizing a vehicle rental microbusiness." *Id.* ¶ 2.

Kleve discloses that a Temporary User may use vehicle rental services after setting up their user identity through a website. Ex. 1007 ¶ 47. Through the website, the Temporary User may agree to rental terms with a vehicle Owner. *Id.* Once this occurs, the Temporary User is provided with a virtual key that allows the Temporary User access to the Owner's vehicle. *Id.* ¶ 48. "The Temporary User may enter a virtual key outside or inside the vehicle, while credential authorization may be processed by the VCS [vehicle based computing system], a server and/or the vehicle Owner." *Id.* The virtual key can provide "additional security by requiring remote credential verification at the vehicle." *Id.* ¶ 49. "The remote credential verification may be done by the VCS, using a server, or allowing the Owner to verify the Temporary User's request." *Id.* Additionally, Kleve discloses that "the Temporary User may have vehicle preset settings applied when renting a vehicle." *Id.* ¶ 50.

Kleve's Figure 6, reproduced below, "is a flow-chart illustrating an example method of the authorization process between a vehicle owner and temporary user." *Id.* ¶ 16.

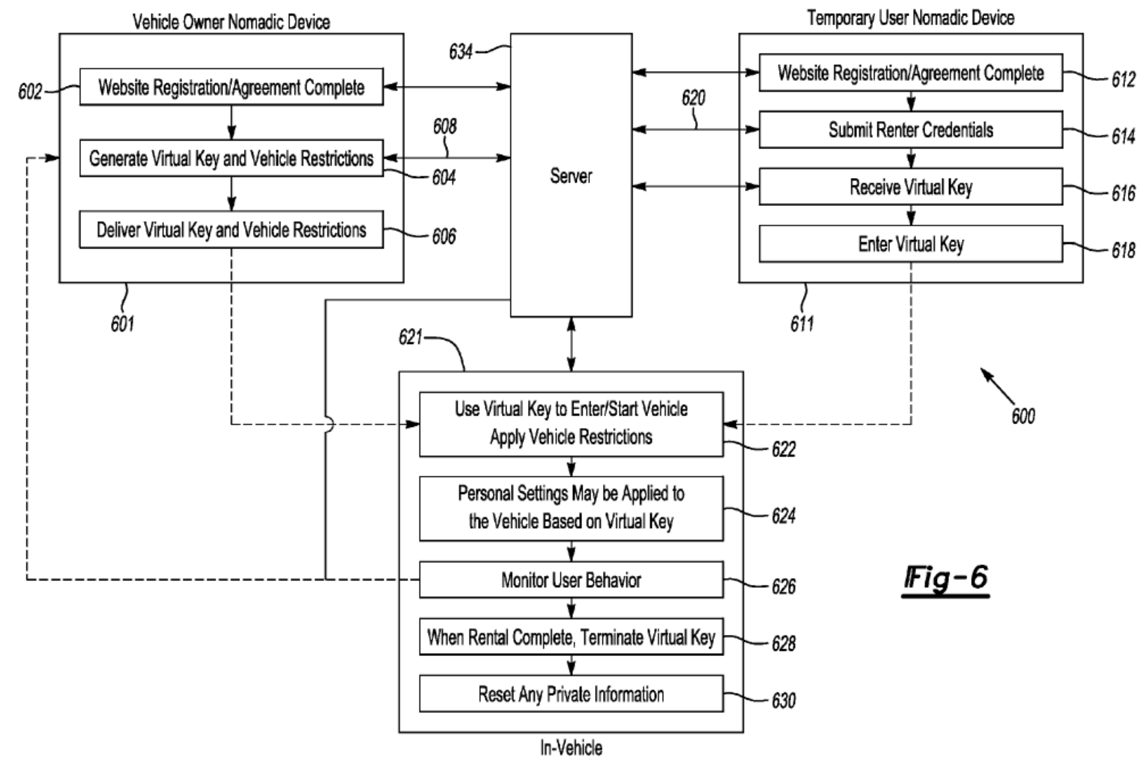

Figure 6 above shows communication between server 634, vehicle owner nomadic device 601, Temporary User nomadic device 611, and vehicle computing system 621. *Id.* ¶ 69. To receive a virtual key at step 616, a Temporary User's credential is used which can include "fingerprint recognition, photos of credit cards, photo of forms of ID, facial recognition, voice print recognition, phrase for speech recognition, temporary mobile web login IDs and password, or other type of unique Temporary User identification at step 614" via two-way communication 620 between Temporary User nomadic device 611 and server 634 as shown in Figure 6. *Id.*, Fig. 6. "At step 624, the Temporary User's nomadic device may be paired with the VCS and may send personal settings to the vehicle including, but not limited to, radio station presets, navigation routes, and/or preferred climate control settings." *Id.* ¶ 72. Kleve also discloses that "the Owner and Temporary User may set up a user profile using a website or a nomadic device communicating with the site that is stored in a database" in order to carry out some of the above-described steps. *Id.* ¶ 37.

3. *Yassin (Ex. 1008)*

Yassin is a U.S. patent titled "Personalize Vehicle Settings Using RF Tags." Ex. 1008, code (54). Yassin discloses "[a] method of and system for programming one or more personalized settings of a user for adjustable components of a vehicle, by using a communication device capable of communicating data to the vehicle." *Id.*, code (57). Yassin's Figure 4, reproduced below, "is a flowchart of the process of reading [a] RFID device and using its contents to retrieve driver vehicle preferences from a profile database over a communications network." *Id.* at 4:22–25.

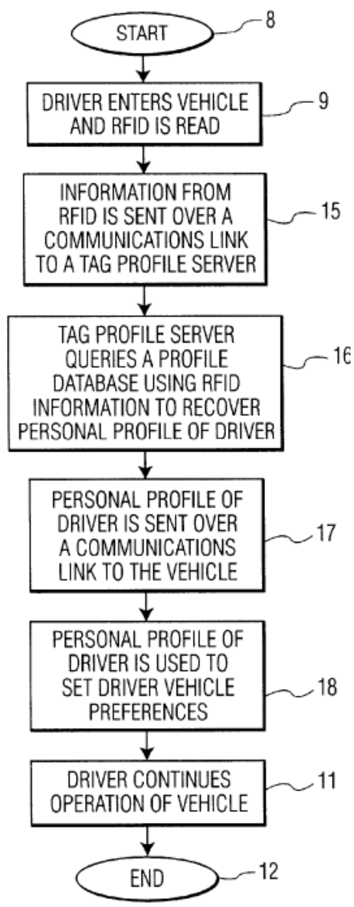

FIG. 4

Figure 4 above shows a process that starts at steps 8 and 9 in which the driver enters a vehicle and an RFID tag is read. *Id.* at 6:36–41. At the next step 15, information identifying the driver is read from the RFID tag to send over a communication link to a tag profile server. *Id.* at 6:42–51. Then at step 16, the tag profile server queries a profile database to recover a personal profile of the driver. *Id.* at 6:52–59. Finally, at steps 17 and 18, the personal profile is sent to the vehicle and is used to set driver vehicle preferences, respectively. *Id.* at 6:60–64.

4. Patenaude (Ex. 1009)

Patenaude is a U.S. patent application publication titled "Method of Determining and Predicting Entertainment Selections for Telematics Units." Ex. 1009, code (54). Patenaude "relates to providing entertainment in a vehicle by determining an entertainment selection profile." *Id.* ¶ 1. Patenaude's method includes using telematics unit 120 to monitor entertainment selections in a mobile vehicle communication system (MVCS) 100. *Id.* ¶¶ 18, 42. For example, an "algorithm searches the acquired data to determine if the FM radio is tuned to the same received FM frequency signal within a specified time frame each weekday for the specific user." *Id.* ¶ 70.

5. Faenger (Ex. 1010)

Faenger is a U.S. patent application publication titled "Personalized Entertainment System." Ex. 1010, code (54). Faenger's Figure 1 is a block diagram of a personalized entertainment system arrangement and is reproduced below. *Id.* ¶ 19.

IPR2026-00070
Emerging Auto EX2013

FIG. 1

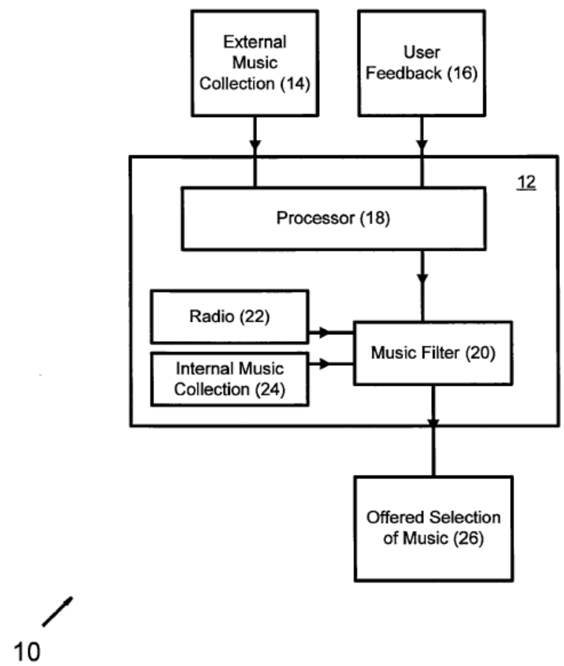

Figure 1 above shows arrangement 10 including entertainment system 12 coupled to a user's external music collection 14 in which system 12 may be "disposed within a vehicle." *Id.* ¶ 26. "System 12 may also actively or passively receive user feedback 16 regarding the user's musical likes and/or dislikes" as "information about the contents of collection 14 as well as user feedback 16 are received by an electronic processor 18 of system 12." *Id.* "Processor 18 may run one or more algorithms for creating a music filter 20 based on information gathered from collection 14 and/or from feedback 16" to offer a selection of music 26, which can also come from radio 22 or internal music collection 24. *Id.* ¶ 28.

B. Claims 1, 9, 11–17, 19, and 20 as Allegedly Obvious over Rector and Kleve

Petitioner contends that the combination of Rector and Kleve renders obvious claims 1, 9, 11–17, 19, and 20. Pet. 12–47. Patent Owner disagrees. PO Resp. 17–57.

1. Analysis of Claim 1

Petitioner contends that the combination of Rector and Kleve teaches or suggests every limitation of issued claim 1. Pet. 18–33.

a) receiving, by the server, a request from electronics of a vehicle to access a profile for a user account, the request identifies user information for a user to use the vehicle

Claim 1 recites a method executed by a server of a cloud services system that is configured to interface with vehicles. Ex. 1001, 33:9–11. This method includes the step of:

> receiving, by the server, a request from electronics of a vehicle to access a profile for a user account, the request identifies user information for a user to use the vehicle[.]

Ex. 1001, 33:12–15.

For these limitations, Petitioner contends that Rector teaches a cloud system with a server that transmits driver settings, causing them to be implemented by a smart vehicle. Pet. 18–19 (citing Ex. 1006 ¶¶ 9, 11, 31, 38, 43, 57, claim 1). Petitioner further explains that Rector's server (e.g., settings server 130) may receive a request from the electronics of a vehicle (e.g., smart vehicle 100) over network 140. Pet. 19–20 (citing Ex. 1006 ¶¶ 30–31). Petitioner asserts that the communication between Rector's smart vehicle "may occur as the driver enters the smart vehicle, as the driver starts the smart vehicle, etc." *Id.* at 20 (quoting Ex. 1006 ¶ 43). According to Petitioner, the smart vehicle's client logic 105 may transmit a unique identifier to settings server 130 via network 140. *Id.* (citing Ex. 1006 ¶ 31). These unique identifiers, according to Petitioner, are associated with a driver (e.g., his/her device, smart card) detected by electronics (e.g., transceiver, smart card reader) of the smart vehicle, and then transmitted to a server in order to retrieve and implement driver settings on the vehicle. *Id.* at 20–21 (citing Ex. 1006 ¶¶ 31, 55, 57).

Patent Owner does not provide arguments specific to the preamble or this limitation. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378. Based on the complete record, we agree with and adopt Petitioner's arguments as our own, and further determine that Petitioner has explained sufficiently how Rector in combination with Kleve teaches or suggests this limitation. *See* Pet. 18–21.

b) processing, by the server, at least part of the user information to verify the user for accessing the profile associated with the user account, the profile having a plurality of settings of the user for the vehicle, at least part of the plurality of settings for the profile being stored on storage accessible to the cloud services system

Claim 1 further recites the step:

> processing, by the server, at least part of the user information to verify the user for accessing the profile associated with the user account, the profile having a plurality of settings of the user for the vehicle, at least part of the plurality of settings for the profile being stored on storage accessible to the cloud services system[.]

Ex. 1001, 33:16–22.

(1) Petitioner's Contentions

Referring to step S351 "Determine Driver ID" shown in Rector's Figure 3, Petitioner contends that Rector's smart vehicle determines the driver identity, which may be done by comparing the unique identifier "with a set of unique identifiers on a server." Pet. 23 (quoting Ex. 1006 ¶ 43).

Petitioner acknowledges that the claim limitation may require verification by the server. *Id.* As such, Petitioner asserts that "it would have been obvious to [a POSITA to] modify Rector such that verification is performed by the server, as in Kleve." *Id.* at 24 (citing Ex. 1007 ¶ 49; Ex. 1005 ¶¶ 120–125). Petitioner contends that

> Kleve teaches processing, by the server, (e.g., server 401, 506, or 634) at least part of the user information (e.g., credentials) to verify the user (e.g., performing remote credential verification) for accessing the profile associated with the user account, the profile having a plurality of settings (e.g., personal settings/radio presets) of the user for the vehicle.

Id. Petitioner directs us to Kleve's Figure 6 and steps 614/620 where renter credentials (e.g., login ID and password, fingerprint/facial recognition) are submitted to server 634. *Id.* at 24–25 (citing Ex. 1007 ¶ 69, Fig. 6). Petitioner contends that Kleve teaches a process of remote credential verification whereby the Temporary User enters a credential verification password and the server compares and verifies authorization. *Id.* at 24–25 (citing Ex. 1007 ¶ 49). Petitioner further argues that "[i]t would have been obvious to modify Rector's method of controlling driver settings to include server-side verification, as in Kleve, for additional security." Pet. 25 (citing Ex. 1005 ¶ 122; Ex. 1006 ¶ 49). Petitioner adds that a POSITA

> would have a reasonable expectation of success combining Rector and Kleve because both explain that the processing capabilities of servers can be used for various processes of connected systems; that is, implementing Kleve's server verification would have been within the capability of Rector's server.

Id. at 25–26 (citing Ex. 1005 ¶ 122).

Petitioner also contends that Rector discloses "at least part of the plurality of settings for the profile is stored on storage accessible to the cloud services system (e.g., database 134 on settings server 130)." Pet. 26 (citing Ex. 1006 ¶ 31). Petitioner contends that Rector discloses that settings may be stored on the smart vehicle's memory, which the cloud services system can access. *Id.* (citing Ex. 1006 ¶ 38).

(2) Patent Owner's Contentions

Patent Owner contends "Rector is explicit that 'the determination of a driver's identification and the subsequent initiation of the corresponding settings for the driver are performed by smart vehicle 200.'" PO Resp. 48–49 (citing Ex. 1006 ¶ 40; Ex. 2003 ¶¶ 72–75). Referring to Rector's Figure 3, Patent Owner adds that Rector's smart vehicle determines the identity of the driver at S351. *Id.* (citing Ex. 1006, Fig. 3; Ex. 2003 ¶¶ 72–77); *see id.* at 50 ("the disclosures of Rector only identify one component of the 'settings control system'—the 'smart vehicle'—'to verify that the correct party is determined to be the driver.'") (citing Ex. 1006 ¶¶ 9, 30, 40, 43, 47–48; Ex. 2003 ¶¶ 72–77).

Patent Owner further contends that a POSITA would not have had reason to modify Rector to include Kleve's server-side verification because a POSITA would have understood that Rector's client-side verification is more secure and would not have added the less secure server-side verification to Rector's more secure method. PO Resp. 51–53; PO Sur-reply 23 ("Petitioner leaves unrebutted Patent Owner's showing that the smart vehicle verification disclosed by Rector would be rendered less secure by modifying Rector's smart-vehicle-executed method to include Kleve's server-side verification, as Petitioners propose.") (citing Ex. 2003 ¶¶ 78–79).

In addition, Patent Owner contends, even if modified as Petitioner proposes, Kleve's server verifies credentials for accessing a vehicle, not verifying the user for accessing a user profile having settings. PO Resp. 54 (citing Ex. 1007 ¶¶ 48–49; Ex. 2003 ¶¶ 80–82). Patent Owner adds that

> [t]he Petition identifies disclosures of Kleve which describe a security feature available to a vehicle owner before a user is granted access to enter and/or drive away a vehicle. EX1007, ¶¶ 48-49; EX2003, ¶¶ 80-82. That is, *even after a "virtual key" is issued to a user to "unlock" and drive a vehicle, the user also undergoes remote credential verification at the vehicle itself*, before the user is allowed to enter and/or drive the vehicle. *Id.*

Id. (emphases added).

(3) Discussion

Turning to Rector, Figure 1 is reproduced below for convenience:

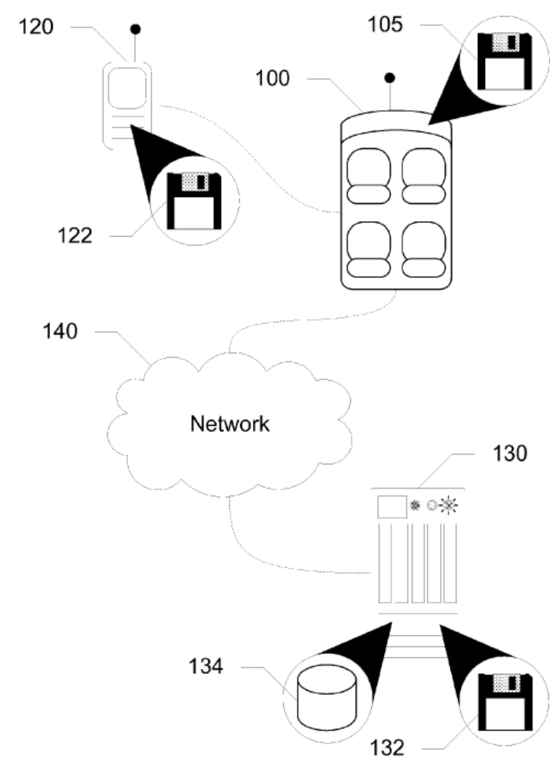

Figure 1

Figure 1 shows a system including smart vehicle 100 with client logic 105, wireless communication device 120 with wireless logic 122, network 140, and settings server 130 with server logic 132 and data base 134. Ex. 1006 ¶ 30. Smart vehicle 100 is in communication with wireless communication device 120, and with settings server 130 via network 140. *Id.* Rector teaches expressly that smart vehicle 100 can transmit a request to wireless communication device 120, and then wireless logic 122 can respond with a unique identifier of wireless communication device 120. *Id.* *Client logic 105,* on smart vehicle 100, *can receive the unique identifier and determine the identity of the driver.* *Id.* (emphases added). Client logic 105 then transmits the unique identifier through network 140 to settings server 130 which has settings for the driver that is associated with the unique identifier. *Id.* ¶ 31. Server logic 132 at settings server 130 matches the driver's identity with corresponding settings from database 134 on server 130. *Id.*

Rector teaches the smart vehicle may process user information (e.g., unique identifier) to identify the user for accessing the user's profile that contains user settings. *See* Ex. 1006 ¶¶ 30–31. For example, Rector teaches:

> Client logic 105 transmits the unique identifier and location to settings server 130 via network 140. This transmission may occur via WiFi, GPRS, or other protocols capable of communicating such information across a wide area network such as the Internet. Settings server 130 includes settings for the driver that is associated with the unique identifier transmitted from wireless communication device 120.

Id. ¶ 31. Furthermore, Rector teaches that the unique identifier (e.g., user information) may be used by server 130 to access user settings stored on server 130. *Id.* Rector's server then matches settings to a driver's identity. *Id.*

To Patent Owner's point, Rector teaches that the *smart vehicle* processes the unique identifier to identify the user before Rector's server 130 matches user settings to the driver's identity. PO Resp. 48–49; *see* Ex. 1006 ¶¶ 30–31. Nonetheless, Petitioner does not rely solely on Rector, but also directs us to Kleve's teaching that a verification step may take place on the server-side prior to accessing settings. Pet. 24.

We observe Kleve teaches that a Temporary User may use vehicle rental services after setting up their user identity through a website. Ex. 1007 ¶ 47. Through the website, the Temporary User may agree to rental terms with a vehicle Owner. *Id.* Once this occurs, the Temporary User is provided with a virtual key that allows the Temporary User access to the Owner's vehicle. *Id.* ¶ 48. "The Temporary User may enter a virtual key outside or inside the vehicle, while credential authorization may be processed by the VCS, a server and/or the vehicle Owner." *Id.*

We further observe that Kleve's Figure 6, reproduced below, provides a flow-chart illustrating the authorization process between a vehicle owner and temporary user. Ex. 1007 ¶ 16.

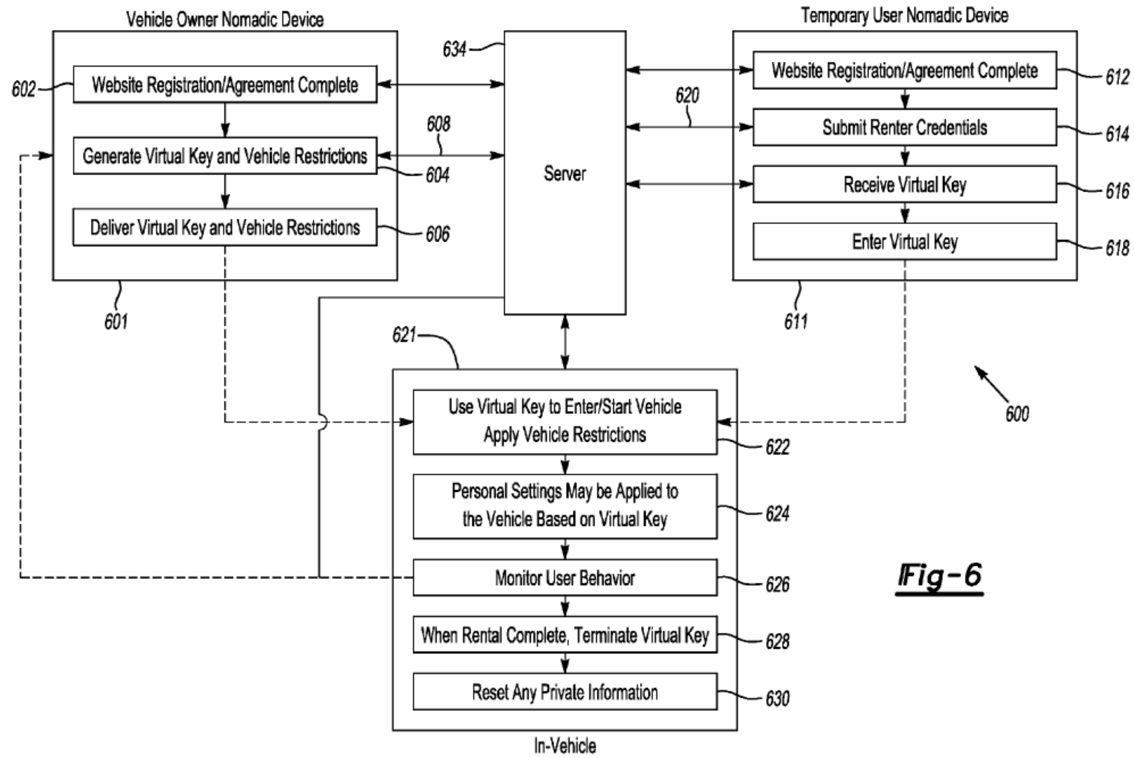

Figure 6 shows communication between server 634, vehicle Owner nomadic device 601, Temporary User nomadic device 611, and vehicle computing system 621. *Id.* ¶ 69. Referring to Figure 6, Kleve teaches that a Temporary User and vehicle Owner may set up user profiles and enter into an agreement for vehicle rental. *Id.* A virtual key may be generated and sent to the Temporary User for access to the rental vehicle. *Id.* Kleve further teaches explicitly that the server may authorize the Temporary User's access to the vehicle. *Id.* ¶ 70. In particular, Kleve teaches that

> *generating a virtual key may be done by using Temporary User's credentials* including fingerprint recognition, photos of credit cards, photo of forms of ID, facial recognition, voice print recognition, phrase for speech recognition, temporary mobile web login IDs and password, or other type of unique Temporary User identification at step 614.

Ex. 1007 ¶ 69 (emphasis added). As shown in Figure 6, the server may receive the renter credentials (Step 614) and generate the virtual key (Step 616). *Id.* Additionally, Kleve provides that

> [t]he system may be further extended to facilitate the virtual key with *additional security* by requiring remote credential verification at the vehicle. . . . The remote credential verification may be done by the VCS, *using a server*, or allowing the Owner to verify the Temporary User's request. For example, but not limited to, the Temporary User entering a credential verification password at the vehicles touchscreen visual display while having the VCS, *server*, or owner compare and verify authorization.

Id. ¶ 49 (emphases added).

With these disclosures in mind, we agree with Petitioner that Kleve teaches "processing, by the server, at least part of the user information to verify the user" because Kleve's server performs credential verification. Ex. 1007 ¶ 69. Furthermore, we determine the complete record better supports Petitioner's position that it would have been obvious to modify Rector's client-side (e.g., smart vehicle) user identification process with Kleve's server-side verification of user information to "facilitate . . . additional security by requiring remote credential verification." Pet. 22 ("[O]ne would have considered Kleve for improving security in Rector, and would have a reasonable expectation of success doing so."), 25; Ex. 1005 ¶¶ 114–126; *see* Ex. 1007 ¶ 49.

We note Patent Owner and Dr. Malek contend that Kleve only uses remote credential verification for vehicle access and that the profile in Kleve has no user settings to access. *See* PO Resp. 55 ("The Petition-identified disclosures of Kleve never mention or suggest verification by any server for accessing a user profile, let alone accessing a user profile having settings of a user for a vehicle."); *see also* Ex. 2003 ¶ 81 ("But the server in Kleve only verifies credentials for accessing a vehicle (e.g., enter/drive away); the server in Kleve is not verifying the user for accessing a profile having settings, which is required by all challenged claims.”).

We do not understand Petitioner to rely upon Kleve for verifying the user for accessing a profile having settings. Rather, Petitioner asserts that *Rector* discloses a user profile containing user settings. Pet. 26–27. Petitioner explains “the Petition never contends that Kleve’s verifying is ‘for accessing a profile with a plurality of settings.’ Rather, as conceded by Patent Owner, Kleve discloses ‘verifying [a user identity] to grant access to a vehicle.’” Pet. Reply 24. Consistent with Petitioner’s position, Dr. Almeroth testifies that

> Rector states it is the server that “associate[s] the unique identifier with the user account, [and then] determine[s] the permitted settings for the user.” *Id.*, ¶ [0009], claim 1. Rector’s method comprises “look[ing] up settings for the driver.” *Id.*, ¶ [0043]. And such settings include “driver created settings as well as controlling authority settings, such as parental controls, based upon the driver’s identity . . . .” *Id.*, ¶ [0031].

Ex. 1005 ¶ 118. Dr. Almeroth further opines that “before ‘implementing settings based upon the driver’ in *Rector*, one would have been motivated and found it obvious to verify the driver’s credentials using the server, as in *Kleve*.” *Id.* ¶ 122 (citing Ex. 1006 ¶ 49). Thus, we agree with Petitioner that, as presented in the Petition, Petitioner’s “proposed combination is not to substitute Rector’s ‘settings’ with some other ‘settings’ disclosed in Kleve, but rather to perform Kleve’s server-side ‘verifying’ in the invention disclosed by Rector.” Pet. Reply 24 (citing Pet. 30).

Patent Owner further takes issue with Petitioner’s asserted rationale for combining the disclosures of Rector and Kleve. Patent Owner contends that server-side verification over client-side verification would be disfavored by a POSITA. PO Resp. 51–53 (citing Ex. 2001 ¶¶ 65–66). Patent Owner relies on the testimony of Dr. Malek who testifies

> [i]t is common knowledge in computer science that distributed software systems are less secure than local software systems. Indeed, computer security was not a major concern until the advent of the Internet and the increased popularity of distributed software systems, such as client-server software systems. *A system in which authentication (verification) is performed locally on the client is typically more secure than a system in which the authentication is performed remotely on the server.* That is because server-side authentication relies on computer networks to transmit messages for verifying credentials. Computer networks are the major source of security attacks. Systems relying on computer networks for authentication must deal with a myriad of security attacks, including spoofing and replay attacks.

Ex. 2003 ¶ 78 (emphases added).

With regard to this testimony, we note that Dr. Malek does not provide an underlying basis for these statements to support his conclusion that it is "common knowledge" that distributed software systems are less secure than local software systems. *Id.* In fact, when viewed with Kleve, Dr. Malek's testimony appears to contradict Kleve's express teaching that the "system may be further extended to *facilitate the virtual key with additional security by requiring remote credential verification at the vehicle* . . . by the VCS, *using a server*, or allowing the Owner to verify the Temporary User's request." Ex. 1007 ¶ 49 (emphases added).

With regard to Kleve's disclosure, Dr. Malek further testifies that

> [a] POSITA would understand that in Kleve credential authorization can be performed by: (1) VCS, (2) server, or (3) owner . . . . While Kleve discloses the verification can be performed by any of these entities, it states the *client-side verification* at the vehicle using VCS provides additional security. *A POSITA would not have been motivated to modify*

> *Rector's method of controlling driver settings to include server-side verification. Rector already uses the more secure client-side verification.*

Ex. 2003 ¶ 79 (emphases added). Dr. Malek, however, does not explain how Kleve's express teachings limit "additional security" to client-side verification with VCS. *Id.* In fact, Kleve expressly discloses the opposite. Kleve teaches that the additional security may be provided by a remote credential certification that "may be done by the VCS, *using a server*, or allowing the Owner to verify the Temporary User's request." Ex. 1007 ¶ 49 (emphasis added). Kleve further teaches that the Temporary User may enter "a credential verification password at the vehicles touchscreen visual display *while having the VCS, server, or owner compare and verify authorization*." *Id.* (emphasis added). Even Dr. Malek acknowledges that the verification can be performed by "any of these entities," including the server. *Id.*

We further note Dr. Almeroth testifies that "[t]he server-side verification may be done above and beyond any verification that takes place locally. The server-side verification could also be done as a check on local verification." Ex. 1005 ¶ 122. This testimony is consistent with and supported by Kleve's disclosure, which expressly states that "additional security" includes remote credential verification at the vehicle using a server. Ex. 1007 ¶ 49. As such, we credit Dr. Almeroth's testimony as his testimony better supported by prior art disclosure.

In addition, Patent Owner argues that Kleve teaches two server-side credential checks. Patent Owner argues that "Kleve is not introducing server-side verification as 'additional security' to a local, client-side verification system as Petitioner argues, but is instead merely repeating the teaching that a server can be used for both the initial 'credential authorization,' and, for 'additional security' a server may likewise perform a second credential verification." PO Sur-reply 24 (citing Ex. 1007 ¶¶ 48–49). Patent Owner contends that "[i]t is only after, and in addition to, teaching that a server may already perform the initial credential authorization that Kleve further teaches a server may perform a second credential verification as 'additional security.'" *Id.* at 25 (citing Ex. 1007 ¶ 49).

We understand Patent Owner's position to be that Kleve teaches a first and second server-side authorization and verification. Even assuming that is correct, it is then conceded by Patent Owner that Kleve's provides a *second* credential verification for additional security. PO Sur-reply 25. As such, Patent Owner's arguments are consistent with Petitioner's position that Kleve teaches additional security may be provided via server-side verification.

We also are not persuaded by Patent Owner's contention that a POSITA would not have reason to add server-side verification to Rector's local verification because local verification is more secure without server-side verification. PO Sur-reply 25–26. Dr. Almeroth has explained in detail the advantages and benefits of additional server-side verification. Ex. 1005 ¶ 122. Specifically, Dr. Almeroth testifies that

> [i]n contrast to local verification, a server may be kept more up-to-date, and may be better protected from security attacks. For example, there may be a situation where a vehicle is in a location where it is unable to communicate with a centralized authority (like a server or data center that administers a settings-applying system).

Ex. 1005 ¶ 122. Dr. Almeroth also opines that "[t]he server-side verification may be done above and beyond any verification that takes place locally. The server-side verification could also be done as a check on local verification."

Id. Although tradeoffs may be required in balancing the benefits and drawbacks of type of additional security selected, such tradeoffs do not necessarily prevent the proposed combination or negate the obviousness of the claimed subject matter. *See Medichem, S. A. v. Rolabo, S.L.*, 437 F.3d 1157, 1165 (Fed. Cir. 2006) ("a given course of action often has simultaneous advantages and disadvantages, and this does not necessarily obviate motivation to combine"). We observe that Dr. Almeroth's testimony takes into consideration these exact tradeoffs:

> A POSA would have recognized the tradeoffs associated with client–side and server-side verification. In my opinion, a POSA would recognize that any potential security-related disadvantages of implementing Kleve's server-side verification would be outweighed by the advantages, including those I detailed in my first declaration. Further, I do not believe Dr. Malek's generalized security concerns would lead a POSA away from utilizing Kleve's server-side verification in the context of Rector's invention, which also expressly teaches server-side functionality.

Ex. 1030 ¶ 20.

Based on the complete record, we determine that Petitioner's arguments on this issue are well-reasoned and supported by the evidence of record. Therefore, we determine Petitioner has explained sufficiently how the asserted combination of Rector and Kleve teaches or suggests this limitation.

> *c) transferring, by the server, upon verifying the user information, one or more settings of the plurality of settings to the vehicle, the transferring is configured to instruct software and/or hardware associated with said electronics of the vehicle to apply said one or more settings to the vehicle for customizing said vehicle to use said one or more settings associated with the profile*

Claim 1 further recites the step:

> transferring, by the server, upon verifying the user information, one or more settings of the plurality of settings to the vehicle, the transferring is configured to instruct software and/or hardware associated with said electronics of the vehicle to apply said one or more settings to the vehicle for customizing said vehicle to use said one or more settings associated with the profile[.]

Ex. 1001, 33:23–29.

(1) Petitioner's Contentions

For these limitations, Petitioner asserts that Rector's server "transmit[s] the permitted settings to the client logic [on the smart vehicle], wherein the client logic limits functions of the smart vehicle based upon the permitted settings." Pet. 27–28 (quoting Ex. 1006 ¶ 9). Petitioner further asserts that Rector only transmits the settings after the verification of the driver identity. Pet. 28 (citing Ex. 1006 ¶ 10, 43, 57).

Petitioner adds that to the extent Patent Owner may argue that Rector does not disclose the server verification of the user information, that it would be obvious to modify Rector in view of Kleve to meet this limitation. Referring to Kleve's Figure 3B and Figure 6, Petitioner argues that Kleve teaches personal settings are applied after a user is verified in, for example, Step 624 "Personal Settings May be Applied to the Vehicle Based on Virtual Key"; or in Step 324 "Apply Enhancements" (e.g., personalization of settings) that takes place after remote credential verification in Step 304. Pet. 29 (citing Ex. 1007 ¶¶ 49–50, Figs. 3B, 6). Petitioner asserts that "[i]t would have been obvious to modify Rector's method of controlling driver settings to transmit settings upon verifying user information by the server, as in Kleve, as it would be a natural consequence of adding security by including the server-side verification of Kleve." *Id.* at 30 (citing Ex. 1005 ¶ 131).

Furthermore, Petitioner argues that Rector uses client logic to implement settings instructions via software, hardware, or both. Pet. 31 (citing Ex. 1006 ¶ 25). Petitioner asserts "Rector discloses numerous examples of the ways software or hardware of the smart vehicle is instructed to apply the settings for customizing the vehicle." *Id.* (citing Ex. 1006 ¶¶ 31–34, 38, 43, 57, 59).

(2) Patent Owner's Contentions

In its Response, Patent Owner contends that Petitioner has engaged in improper hindsight and "cherry-picked" features from Rector's different embodiments "without any explanation or evidence of motivation." PO Resp. 18. Patent Owner further contends that Petitioner uses the '244 patent claims as a roadmap and rewrites Rector's "method of controlling permitted settings on a smart vehicle" by incorporating server functions into a different embodiment where the smart vehicle performs those functions. *Id.* at 19–20. Patent Owner contends that

> [u]nlike each of the server-executed steps of the independent claims of the '244 Patent (EX1001, claims 1, 17), Rector's "method of controlling a driver's settings on a smart vehicle" does not contemplate a server at any step (EX1006, Figure 3, ¶ 43). This is unsurprising, since the import of Rector as a whole is centered around the operations of a "smart vehicle." EX1006; EX2003, ¶¶ 56-60. Indeed, *Rector actually requires the "smart vehicle," as the lone operator, to execute each of the steps depicted in Figure 3—illustrating an embodiment of "a method of controlling a driver's settings on a smart vehicle*." EX1006, ¶ 43, Fig. 3; EX2003, ¶¶ 56-60, 66.

Id. at 20 (emphases added). Patent Owner acknowledges that Rector also teaches an embodiment, "system for controlling a driver's settings," that does include a server and that the server can "associate the unique identifier with the user account, determine the permitted settings for the user, and transmit the permitted settings to the client logic" of a smart vehicle. *Id.* (citing Ex. 1006 ¶ 9, claim 1). Nonetheless, Patent Owner contends that these are "incompatible" embodiments with fundamental differences, which the Petitioner has not addressed. *See* PO Resp. 21, 34 ("Neither Petitioner nor Dr. Almeroth pointed to any suggestion in Rector that its method remains operable if its steps are swapped or supplemented with the system embodiment components selectively plucked by the Petition."), 35 ("Rector's method embodiment already achieves the very same determining of settings that the system embodiment achieves, but the Petition never justifies nor explains the nonsensical redundancies of combining the two embodiments."); PO Sur-reply 13–14.

In addition, Patent Owner contends Petitioner has not explained how a POSITA would have had a reasonable expectation of success in combining the embodiments of Rector. PO Resp. 38–40. Patent Owner asserts that the Petition does not explain when after Rector's step S351 Rector's server would transmit settings. *Id.* at 39. Patent Owner contends that adding server transmission after step S351 and before S354 would render steps of Rector "nonsensical." *Id.*

Furthermore, Patent Owner contends that Petitioner has not shown how Rector teaches or suggests "transferring is configured to instruct" required by claims 1 and 17 of the '244 patent. PO Resp. 41 ("Missing from the Petition and Rector is any suggestion of the server's transferring of settings to the vehicle that 'is configured to instruct' the vehicle according to the limitations of claim 1[c] and 17[c].") (citing Ex. 2003 ¶¶ 65–71), 44 ("[M]ere capability does not teach the recited 'configured to' limitations.") Patent Owner adds that Rector does not teach transmitted settings "cause" the smart vehicle to implement settings. *Id.* at 42–43 ("Rector repeatedly emphasizes that it is the smart vehicle itself, using its client logic, that determines what functions to limit on the vehicle according to the permitted settings.") (citing Ex. 1006 ¶ 9; Ex. 2003 ¶ 69).

(3) Discussion

Based on the complete record, we determine that Petitioner has the better position. To start, Rector does not teach "incompatible" embodiments as Patent Owner proposes. Rector generally teaches a system for controlling a driver's settings. Ex. 1006 ¶ 12. Rector's Figure 1 is again reproduced below. *Id.*

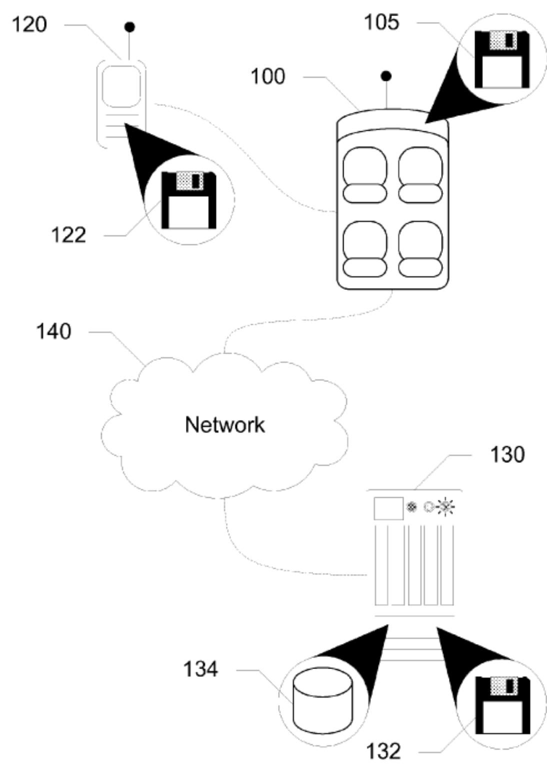

Figure 1

Figure 1 above shows a system with smart vehicle 100, wireless communication device 120, network 140, and settings server 130. *Id.* ¶ 30. Smart vehicle 100 communicates with wireless communication device 120 and settings server 130 via network 140. *Id.* Smart vehicle 100 can transmit a request to wireless communication device 120, and then wireless logic 122 may respond with a unique identifier of wireless communication device 120. *Id.* Client logic 105, on smart vehicle 100, may transmit a unique identifier through network 140 to settings server 130, which has settings for the driver that is associated with the unique identifier. *Id.* ¶ 31.

Rector teaches variations on how these driver settings may be transmitted and implemented by this system for vehicles. Rector expressly discloses that

> the settings may be stored on the driver's wireless communication device or on the memory of the smart vehicle. In these embodiments, *the settings may be uploaded from the settings server to the driver's wireless communication device or the smart vehicle's memory*. Alternatively, the settings may be directly set or uploaded by a second wireless communication device, such as that of a parent of the driver. In this alternative embodiment, *the settings server may not be necessary to the system*. The driver's wireless communications device would communicate with client logic of the smart vehicle and create settings which are stored on the memory of the wireless communications device or the smart vehicle.

Ex. 1006 ¶ 38 (emphases added). In this way, Rector contemplates that the servers in the disclosed systems may transmit settings to a wireless communication device or smart vehicle. *Id., see, e.g.,* ¶ 9, claim 1. Moreover, Rector discloses that the server *may* not be necessary where the settings are directly set or uploaded by a wireless communication device. *Id.* ¶ 38. In our view, Rector's disclosure does not, as Patent Owner proposes, describe categorically incompatible embodiments, but provides examples of how the system may permissively use various components, including the server to store and transmit settings. *Id.* Indeed, Rector states that "[v]arious other settings are possible and would be apparent to one of ordinary skill in the art in light of this disclosure." *Id.*

IPR2026-00070
Emerging Auto EX2013

With this in mind, we note Rector describes one such variation as a method of controlling a driver's settings on a smart vehicle. *See* Ex. 1006 ¶ 43. As discussed, Rector's Figure 3 is a flow chart of this method, reproduced below. *Id.* ¶ 14.

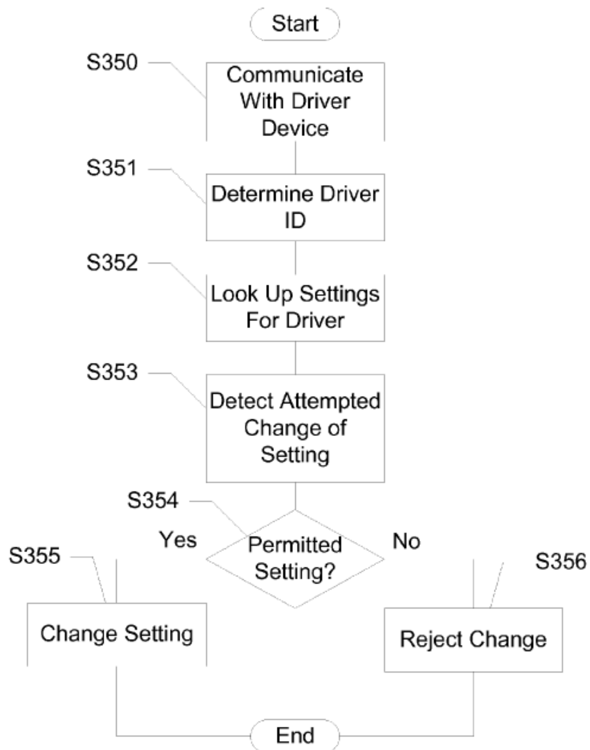

Figure 3

Figure 3 above shows a method that starts at step S350 in which the smart vehicle communicates with a driver's device such as a wireless communications device when the driver enters or starts the smart vehicle. *Id.* ¶ 43. The smart vehicle requests a unique identifier for the driver's wireless communication device to determine the identity of the driver at step S351. *Id.* "[T]he unique identifier may be compared with a set of unique identifiers on a server on a network." *Id.* At step S352, with the identity of the driver determined, the smart vehicle looks up settings for the driver. *Id.* Rector further teaches that

> [w]ith the identity of the driver determined, the smart vehicle looks up settings for the driver S352. These settings may include driver created settings, controlling authority settings, etc. *The settings are determined by comparing the driver's identity with a database of identities with corresponding settings*. *This database may be on the network*, on the driver's device, on the smart vehicle's memory, etc.

Ex. 1006 ¶ 43 (emphases added).

While Rector teaches that the smart vehicle may perform these steps, as shown in Figure 3, Rector also teaches that the smart vehicle is part of a system (e.g., Figure 1) and that the settings may be stored on a network database. Ex. 1006 ¶ 43. Furthermore, we observe that Rector explicitly teaches that the unique identifier may be compared on the server via the network. *Id.* As such, we understand Rector's disclosure to broadly disclose that the server may be accessed via the network, as part of the system such as the one shown in Figure 1. *Id.* ("[T]he unique identifier may be compared with a set of unique identifiers on a server on a network.").

Patent Owner contends that Rector's method described in Figure 3 does not teach that the server does this comparison or that the server transmits settings from the database. PO Resp. 22–28. Patent Owner argues that the smart vehicle performs all the steps of Figure 3. *Id.* Even so, we understand Petitioner relies upon Rector's broader disclosure of the entire system, e.g., Figure 1, that includes a network and a server, and various options for the operation of that system. Pet. 27–28 (citing Ex. 1006 ¶ 9, claim 1). As such, we do not agree that Petitioner has mixed and matched *incompatible* embodiments disclosed in Rector, or that the Petition is deficient on this basis. Rector expressly discloses that various options exist for operating the system, including storing the settings in the server and transmitting the settings from the server. Ex. 1006 ¶¶ 9, 38, 43, claim 1.

In addition, even assuming Petitioner relies on different embodiments, we determine Petitioner has not unfairly combined features from different embodiments disclosed in Rector. Dr. Malek testifies that Rector's smart vehicle performs all the steps shown in Figure 3, which is not reflected in the embodiment of paragraph 9. *See* Ex. 2003 ¶¶ 53–59. Yet, that testimony and Patent Owner's arguments do not take into account all of Petitioner's arguments and evidence. Here, Petitioner has explained how a POSITA could and would implement additional server-side functionality by directing us to Rector's express disclosure of server transmission (Ex. 1006 ¶ 9, claim 1), and to Kleve's disclosure of server-side verification. Dr. Almeroth testifies that "[i]t would have been obvious to modify Rector's method of controlling driver settings to transmit settings upon verifying user information by the server, as in Kleve*, as it would be a natural consequence of adding security by including the server-side verification of Kleve*." Ex. 1005 ¶ 131 (emphasis added). In other words, Petitioner proposes to modify Rector's method, shown in Figure 3, to perform server-side verification (as taught in Kleve) and then to have the server transmit the settings to the vehicle (as taught in Rector) because it would have been a "natural consequence of adding security" by using server-side verification of Kleve disclosed in Kleve. Pet. 30 (citing Ex. 1005 ¶ 131).

Separately, it bears mentioning that in *Boston Scientific Scimed, Inc. v. Cordis Corp.*, 554 F.3d 982, (Fed. Cir. 2009), one reference disclosed all of the asserted claim's elements, but those elements were taught by two different embodiments that were pictured side-by-side in the patent. The Federal Circuit nonetheless found that claim obvious because "[c]ombining two embodiments disclosed adjacent to each other in a prior art patent does not require a leap of inventiveness." *Id.* at 991. Our reviewing court noted that as long as a POSITA "can implement a predictable variation, § 103 likely bars its patentability." *Id.* (quoting *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007)).

Like the combination of two side-by-side embodiments in *Boston Scientific*, we view the combination of elements from the embodiments in Rector as a "predictable variation" that does not "require a leap of inventiveness." *Boston Sci.*, 554 F.3d at 991. As discussed, Rector describes a general system that includes a server and provides examples of how the server may operate in that system. Ex. 1006 ¶¶ 9, 38, 43, Fig. 3, claim 1); *see* Pet. Reply 12 ("Rector's invention includes systems involving both a smart vehicle and a server, and how they interact."). Petitioner has explained that the various options are compatible alternatives, as expressly taught be Rector. Pet. Reply 14–15 (citing Ex. 1006 ¶ 43, Fig. 3).

Furthermore, we determine that Petitioner has explained sufficiently whether a POSITA would have had a reasonable expectation of success for the asserted combination. Patent Owner contends that Petitioner's arguments result in duplicative and "nonsensical" steps for the method shown in Rector's Figure 3. PO Resp. 38–39; PO Sur-reply 13–14. Patent Owner contends, for example, that

> if the Petition's system embodiment were added before step S354, such that Rector's system server determines and transmits settings before Rector's method step S354, Rector's method is still going to require (at S354) that the smart vehicle check the database of permitted settings each time it detects an attempted change of setting. *Id.*, ¶ 43. This confounding result is left completely unaddressed by the Petition. Pet. 27-28, 30-31.

PO Resp. 40. But, Patent Owner's position appears to miss the point. Petitioner explains that Rector's embodiments are compatible, and Rector does not teach away from the alternative options where the server transfers the settings after the verification is done on the server-side. Pet. Reply 17. Petitioner does not argue, however, that S354 of Figure 3 is performed by the settings server. Nor, are we persuaded that Rector's smart vehicle cannot continue to perform S354 in Petitioner's proposed modification. Again, Rector itself teaches that various options "are possible and would be apparent to one of ordinary skill in the art in light of this disclosure." Ex. 1006 ¶ 38. Moreover, as Petitioner has reasoned "a POSA would have a reasonable expectation of success combining Rector and Kleve because both explain that the processing capabilities of servers can be used for various processes of connected systems[.]" Pet. 26 (citing Ex. 1005 ¶ 122). Thus, demonstrating the point that the servers *can* be used for various processes optionally.

Patent Owner further contends that Petitioner has not shown how Rector teaches or suggests "transferring is configured to instruct" because Petitioner merely argues that Rector's server is capable of this limitation. PO Resp. 41 ("Missing from the Petition and Rector is any suggestion of the server's transferring of settings to the vehicle that 'is configured to instruct' the vehicle according to the limitations of claim 1[c] and 17[c].") (citing Ex. 2003 ¶¶ 65–71), 44 ("[M]ere capability does not teach the recited 'configured to' limitations."). Patent Owner adds that Rector does not teach transmitted settings "cause" the smart vehicle to implement settings. *Id.* at 42–43. Dr. Malek also testifies that Dr. Almeroth's citations do not support the opinion that Rector discloses "numerous examples of the ways that software or hardware of the smart vehicle is instructed to apply the settings for customizing the vehicle." Ex. 2003 ¶ 71 (citing Ex. 1005 ¶ 136; Ex. 1006 ¶¶ 31–34, 38, 43, 57, 59).

We observe Rector's claim 1 recites a system for controlling a driver's settings, the system including "a settings server on the network" and "a server logic on the settings server to associate the unique identifier with the user account, determine the permitted settings for the user, and transmit the permitted settings to the client logic" on the smart vehicle. Ex. 1006, claim 1. Rector also explains that

> "Logic" as used herein and throughout this disclosure, refers to any *information having the form of instruction signals and/or data that may be applied to direct the operation of a processor.* Logic may be formed from signals stored in a device memory. Software is one example of such logic. Logic may also be comprised by digital and/or analog hardware circuits, for example, hardware circuits comprising logical AND, OR, XOR, NAND, NOR, and other logical operations. Logic may be formed from combinations of software and hardware. *On a network, logic may be programmed on a server, or a complex of servers.* A particular logic unit is not limited to a single logical location on the network.

Id. ¶ 25 (emphases added). Dr. Almeroth further testifies that Rector "discloses that the client 'logic' which implements the setting instructions can be 'software' or 'hardware,' or both," and that Rector's server makes a transmission to the vehicle where the vehicle follows instructions to implement the driver's settings. Ex. 1005 ¶ 135 (citing Ex. 1005 ¶ 25).

We find Dr. Almeroth's testimony is consistent and supported by Rector's disclosure that settings, such as a speed limits, may be implemented on the vehicle. For example, Rector teaches that a parent may upload a speed setting to the settings server and then the smart vehicle limits the maximum speed the vehicle travels when a child is driving. Ex. 1006 ¶ 32. Rector further discloses that the setting server may transmit the settings to the smart vehicle, and doing so causes the client logic to limit the operation of the smart vehicle. *Id.* ¶ 9 ("[S]erver logic on the settings server to associate the unique identifier with the user account, determine the permitted settings for the user, and *transmit the permitted settings to the client logic, wherein the client logic limits functions of the smart vehicle based upon the permitted settings*.") (emphasis added). As such, we determine that Rector's disclosure and Dr. Almeroth's testimony based on this disclosure support Petitioner's position that "transferring," by Rector's server, "is configured," e.g., adapted/designed/programmed, to instruct software or hardware (e.g., Rector's vehicle client logic) to apply one or more settings to the vehicle. We are further persuaded by Petitioner that Rector's transmitting of settings causes the vehicle to implement the settings because Rector's settings are, in fact, implemented on receipt of the transmission. Pet. Reply 18–20; Ex. 1006 ¶¶ 31–34, 38, 43, 57, 59, claim 1; Ex. 1005 ¶¶ 134–137.

Based on the complete record, we determine that Petitioner's arguments on this issue are well-reasoned and supported by the evidence of record. Therefore, Petitioner has explained sufficiently how the asserted combination of Rector and Kleve teaches or suggests this limitation. *See* Pet. 27–32.

d) wherein the vehicle uses wireless communication for exchanging data with the cloud services system and for receiving said one or more settings for the profile.

Claim 1 also recites the step:

> wherein the vehicle uses wireless communication for exchanging data with the cloud services system and for receiving said one or more settings for the profile.

Ex. 1001, 33:30–32.

For this limitation, Petitioner asserts that in Rector "[s]mart vehicle 100 is in communication with wireless communication device 120 and with settings server 130 over network 140." Pet. 32 (quoting Ex. 1006 ¶ 30). Petitioner contends that such communication is for, in part, transmitting the settings to the vehicle. *Id.* (citing Ex. 1006 ¶ 9).

Patent Owner does not provide arguments specific to limitation [1e]. PO Resp.; PO Sur-reply. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

Based on the complete record, we agree with and adopt Petitioner's arguments as our own, and further determine that Petitioner has explained sufficiently how Rector in combination with Kleve teaches or suggests these limitations. *See* Pet. 32–33.

e) Conclusion

After review of the arguments and evidence, we determine that Petitioner has demonstrated by a preponderance of the evidence that independent claim 1 would have been rendered obvious to an ordinarily skilled artisan at the critical time by Rector in combination with Kleve.

2. Analysis of Claim 17

Petitioner contends that the combination of Rector and Kleve teaches or suggests every limitation of claim 17. Pet. 41–46. Petitioner largely relies on arguments discussed with regard to claim 1. *See* Pet. 42–46.

Patent Owner relies on the same arguments presented for claim 1. *See* PO Resp. 17–57; PO Sur-reply.

Based on the complete record, we agree with and adopt Petitioner's arguments as our own, and further determine that Petitioner has established by a preponderance of the evidence that claim 17 would have rendered obvious to an ordinarily skilled artisan at the critical time by Rector in combination with Kleve. *See* Pet. 42–46.

3. Analysis of Claims 9 and 11–16

Claims 9 and 11–16 depend from claim 1. Ex. 1001, 34:10–13, 34:16–65. Petitioner asserts that Rector in combination with Kleve teaches or suggests all the limitations recited in dependent claims 9 and 11–16. Pet. 33–41.

Patent Owner relies on the same arguments presented for claim 1. *See* PO Resp. 17–57; PO Sur-reply.

Based on the complete record, we agree with and adopt Petitioner's arguments as our own, and further determine that Petitioner has established by a preponderance of the evidence that claims 9 and 11–16 would have been rendered obvious to an ordinarily skilled artisan at the critical time by Rector in combination with Kleve. *See* Pet. 33–41.

4. Analysis of Claims 19 and 20

Claims 19 and 20 depend from claim 17. Ex. 1001, 35:27–36:29. Petitioner asserts that dependent claims 19 and 20 of the '244 patent are rendered obvious by Rector in combination with Kleve. Pet. 46–47.

Patent Owner relies on the same arguments presented for claim 1. *See* PO Resp. 17–57; *see, generally* PO Sur-reply.

Based on the complete record, we agree with and adopt Petitioner's arguments as our own, and further determine that Petitioner has established by a preponderance of the evidence that claims 19 and 20 would have been rendered obvious to an ordinarily skilled artisan at the critical time by Rector in combination with Kleve. *See* Pet. 46–47.

C. Claims 2, 4, 10, and 18 as Allegedly Obvious over Rector, Kleve, and Yassin

Petitioner contends that the combination of Rector, Kleve, and Yassin renders obvious claims 2, 4, 10, and 18. Pet. 50–58.

Patent Owner does not specifically address these challenged dependent claims apart from the arguments presented for the independent claims discussed above. PO Resp. 57. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

Based on the complete record, we agree with and adopt Petitioner's arguments as our own, and further determine that Petitioner has established by a preponderance of the evidence that claims 2, 4, 10, and 18 would have been rendered obvious to an ordinarily skilled artisan at the critical time by Rector in combination with Kleve and Yassin. *See* Pet. 50–58. For example, for claim 2, Petitioner asserts that "[i]t was well-known in the art, at the time of the patent, for cloud services systems to transfer a driver's settings to multiple vehicles, as demonstrated by Yassin, which would provide more opportunities for reducing distractions and enhancing safety." *Id.* at 50–51 (citing Ex. 1008, 3:24–40, 3:54–57, 6:60–67, Figs. 1, 4; Ex. 1005 ¶¶ 213–214), *see id.* at 57–58 (applying arguments made for claim 2 to claims 10 and 18). For claim 4, Petitioner contends:

> One would have sought to improve convenience and safety of Rector by capturing user changes to settings made during use and communicating them to a server, as in Yassin, which would have the predictable result of carrying forward the driver's changed settings and further reducing driver distractions (i.e., preventing the need for readjusting components to implement the driver's changed settings the next time he/she uses the same/different vehicle). Ex. 1005, ¶ 216. One would have a reasonable expectation of success doing so because Yassin demonstrates its methods are broadly applicable, Ex. 1008, 4:55-5:5, and usable to set desired settings "whenever" or wherever the driver choses to drive, *id.*, 6:65-7:8.

Id. at 54.

**IPR2026-00070
Emerging Auto EX2013**

As discussed previously, we are persuaded by Petitioner's position, as supported by the evidence of record.

D. Claims 5–7 as Allegedly Obvious over Rector, Kleve, Yassin, and Patenaude

Petitioner contends that the combination of Rector, Kleve, Yassin, and Patenaude renders obvious claims 5–7. Pet. 58–68.

Patent Owner does not specifically address the challenged dependent claims apart from the arguments presented for the independent claims discussed above. PO Resp. 57. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

Based on the complete record, we agree with and adopt Petitioner's arguments (Pet. 60–68) as our own, and further determine that Petitioner has established by a preponderance of the evidence that claims 5–7 would have been rendered obvious to an ordinarily skilled artisan at the critical time by Rector in combination with Kleve, Yassin, and Patenaude. *See* Pet. 60 ("[O]ne would have been motivated to further improve Rector (as modified by Kleve and Yassin), which aims to reduce preventable distractions and improve convenience, by implementing the learning engine of Patenaude, which provides the improvement of being able to automatically predict and apply user settings from determined patterns. Ex. 1006, ¶¶ [0001]-[0008]; Ex. 1009,¶¶ [0001]-[0005]."), 64–65 ("A POSA would have been motivated to send a recommended setting to the user account so that it could be applied in the vehicle, as taught by Yassin, to reduce distractions, as taught by Rector, and to improve upon the existing art that did not automatically apply settings, as taught by Patenaude. Ex. 1005, 2:30-41, 4:64-65; Ex. 1006, ¶¶ [0002]-[0007]; Ex. 1009, ¶¶ [0001]-[0006]; Ex. 1005, ¶ 247."), 67–68 ("In combining Patenaude with Rector, Kleve, and Yassin as discussed above with respect to claim 5, implementing Patenaude's learning engine would have included having the patterns be correlated to one or more conditions (e.g., factors), which include one or more of the recited alternatives. *Id.*, ¶¶ 252-253. One would also have been motivated to have the patterns be correlated to one or more conditions so that the determined patterns are more predictive of the user's desired intent, as taught by Patenaude. Ex. 1009, ¶¶ [0054]-[0057].").

E. Claims 8 and 21 as Allegedly Obvious over Rector, Kleve, and Faenger

Petitioner contends that the combination of Rector, Kleve, and Faenger renders obvious claims 8 and 21. Pet. 68–78. Claim 21 is not part of the issued claims for the '244 patent. Pet. 75 n.10; Ex. 1001, 33:9–36:29. We address claim 8. *See* Pet. 75–78.

Patent Owner does not specifically address the challenged dependent claims apart from the arguments presented for the independent claims discussed above. PO Resp 57. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

Based on the complete record, we agree with and adopt Petitioner's arguments as our own, and further determine that Petitioner has established a by a preponderance of the evidence that claim 8 is rendered obvious by Rector in combination with Kleve and Faenger. *See* Pet. 68–75. We do not reach the challenge of claim 21 as this claim is not an issued claim in the '244 patent. Ex. 1001, 33:9–36:29.

F. Claim 22 as Allegedly Obvious over Rector, Kleve, Faenger, and Yassin

Petitioner contends that the combination of Rector, Kleve, Faenger, and Yassin renders obvious claim 22. Pet. 78–79. We do not reach the challenge of claim 22 as this claim is not an issued claim in the '244 patent. Ex. 1001, 33:9–36:29; Pet. 78 n.11.

VI. CONCLUSION[7]

After considering the complete record, we conclude that Petitioner has demonstrated by a preponderance of the evidence, that challenged claims 1, 2, and 4–20 of the '244 patent are unpatentable.

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis	Claim(s) Shown Unpatentable	Claims(s) Not Shown Unpatentable
1, 9, 11–17, 19, 20	103	Rector, Kleve	1, 9, 11–17, 19, 20	
2, 4, 10, 18	103	Rector, Kleve, Yassin	2, 4, 10, 18	
5–7	103	Rector, Kleve, Yassin, Patenaude	5–7	
8, 21	103	Rector, Kleve, Faenger	8	21[8]
22	103	Rector, Kleve,		22

[7] 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).

[8] We do not speculate on the patentability of claims 21 and 22, which are not part of the issued claims of the '244 patent. Ex. 1001, 33:9–36:29.

IPR2026-00070
Emerging Auto EX2013

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis	Claim(s) Shown Unpatentable	Claims(s) Not Shown Unpatentable
		Faenger, Yassin		

VII. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that based on a preponderance of the evidence, claims 1, 2, and 4–20 of the '244 patent are unpatentable; and

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

FOR PETITIONER:

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

FOR PATENT OWNER:

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

IPR2026-00070
Emerging Auto EX2013