

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

TOYOTA MOTOR CORP.

and

KIA CORPORATION,
Petitioners,

v.

EMERGING AUTOMOTIVE LLC,
Patent Owner.

Case IPR2026-00059
U.S. Patent 11,104,245

**EMERGING AUTOMOTIVE LLC'S
PATENT OWNER RESPONSE**

TABLE OF CONTENTS

I.	Introduction.....	1
II.	Innovations of U.S. Patent 11,104,245.....	2
III.	All Grounds fail because Petitioners failed to show that any reference, alone or in combination, discloses multiple limitations of independent claim 1.	3
A.	Grounds 1 and 2 fail because neither Kleve nor Kleve in combination is shown to disclose independent claim limitations 1[f], 1[g], 1[h] and 1[i].....	5
1.	Petitioners failed to show that any reference, alone or in combination, discloses “the coded data from the mobile device including a unique access code received by the mobile device from the server,” as recited by independent claim 1[f].	5
2.	Petitioners’ failure to show any reference, alone or in combination, that discloses “the unique access code functioning for the e-key,” as recited by independent claim 1[i], further highlights the Petition’s failure as to claim 1[f].	12
3.	Petitioners failed to show that any reference, alone or in combination, discloses the “privileges for the unique access code” or “the unique access code is associated with privileges set via the server,” as recited by independent claim 1[g].	13
4.	Petitioners failed to show that any reference, alone or in combination, discloses “the privileges are set via the server responsive to a restriction set by an administrator of the vehicle, the restriction is associated with a mode of allowed use of the vehicle ... privileges are for the unique access code” as recited by independent claim 1[g].....	15
5.	The Petition fails to demonstrate why a POSITA would have been motivated to modify or combine	

Kleve in view of Mottla.	22
6. Petitioners failed to show any reference, alone or in combination, discloses a “camera capturing video ... during a period of time in which the unique access code is to be active,” as recited by independent claim 1[h].	32
B. The Zaid Reference (EX1008)	33
C. For Grounds 3 and 4, Petitioners’ reliance on the Examiner’s findings is of no avail, as Zaid does not disclose the limitations of claim 1, and the Examiner agreed.	34
1. The Petition fails to identify any disclosure to satisfy claim 1[e]-[f]’s requirements of “coded data ... for unlocking and use of the vehicle, the coded data from the mobile device including a unique access code received by the mobile device from the server[.]”	35
2. Zaid’s “unique increment” fails to satisfy claim 1[e]-1[f]’s limitations requiring “coded data ... for unlocking and use of the vehicle, the coded data ... including a unique access code received by the mobile device from the server[.]”	37
3. The Petition fails to identify any disclosure to satisfy the recited limitations of claim 1[g]: “privileges are for the unique access code” and “privileges are set via the server responsive to a restriction set by an administrator of the vehicle, the restriction is associated with a mode of allowed use of the vehicle[.]”	41
4. The Petition fails to show that the combination of Zaid and Mottla renders obvious claim 1[i].....	44
5. The Petition fails to show that Zaid, or Zaid in combination with Kleve, teaches or suggests the recited elements of claim 1[h].....	47

IV.	Petitioners failed to present even a prima facie case of obviousness for either the Ground 1 or Ground 3 challenge to claim 6.....	48
A.	Petitioners’ Ground 1-claim 6 challenge fails because the Petition does not comply with 37 C.F.R. § 42.104(b)(4).	48
B.	Even if the Petition’s statutory deficiencies were not fatal to its Ground 1-claim 6 challenge, the Petition still fails to meet its burden as to claim limitation 6[a].	50
C.	The Petition’s Ground 3-claim 6 challenge is equally flawed.	54
V.	Each of the Petition’s claim 3 challenges fails because neither Kleve (Ground 1) nor Zaid (Ground 3) discloses “a unique access code generated by the server[.]”	59
A.	Kleve does not disclose any “unique access code generated by the server,” nor any “user account having privileges assigned by the administrator,” as recited by claim 3.	59
B.	The Petition’s Ground 3-claim 3 challenge fails because Zaid does not disclose “each request is associated with a unique access code generated by the server,” as recited by claim 3.	67
C.	The Petition’s Ground 3-claim 3 challenge fails because Zaid does not disclose “each unique access code is associated with a user account having respective privileges assigned by the administrator of the vehicle,” as recited by claim 3.	70
VI.	Additional deficiencies of Petitioners’ claim 15 challenge.....	72
A.	Petitioners fail to show Zaid’s server is part of any cloud processing system, and therefore cannot meet their burden as to claim 15.	73
B.	The identified “cloud processing system” managing Facebook®, Foursquare® and similar social networking	

	accounts is not alleged or shown to be <i>the same</i> “the cloud processing system configured to ... manage use of said e-key,” and therefore cannot meet the limitations of the challenged claim.....	74
C.	Zaid’s server is not “part of” the identified “cloud processing system” managing Facebook®, Foursquare® and similar social networking accounts and therefore Petitioners’ claim 15 challenge fails.	75
VII.	Conclusion	77

TABLE OF AUTHORITIES

Cases

<i>KSR Int’l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007).....	31
<i>Wasica Finance GmbH, et al. v. Continental Automotive Syst.</i> , 853 F.3d 1272 (Fed. Cir. 2017)	51
<i>Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.</i> , 821 F.3d 1359 (Fed. Cir. 2016)	31, 47, 49
<i>Medacta USA, Inc. et al. v. RSB Spine, LLC</i> , IPR2020-00264, Paper 46 (P.T.A.B. Apr. 15, 2021)	51

Statutes

37 C.F.R. § 42.104(b)(4).....	48-51
37 C.F.R. § 42.22(a)(2)	49-51
35 U.S.C. § 312(a)(3).....	49

PATENT OWNER’S UPDATED EXHIBIT LIST

Exhibit No.	Description
2001	Declaration of Sam Malek, Ph.D.
2002	Civil Docket Report for <i>Emerging Automotive LLC v. Toyota Motor Corp. et al.</i> , No. 2:23-cv-0437-JRG (lead case)
2003	Google Patents search, U.S. Patent No. 11,104,245, available at https://patents.google.com/patent/US11104245B2/en?q=11%2c104245#citedBy (identifying assignees of patents and patent applications which cited to U.S. Patent No. 11,104,245)
2004	Final Written Decision, IPR2024-00981
2005	Discovery Order for <i>Emerging Automotive LLC v. Toyota Motor Corp. et al.</i> , No. 2:25-cv-00782-JRG (lead case)
2006	Defendant’s Claim Construction Brief, <i>Emerging Automotive LLC v. Toyota Motor Corp. et al.</i> , No. 2:23-cv-0437-JRG
2007	Civil Docket Report for <i>Emerging Automotive LLC v. Toyota Motor Corp. et al.</i> , No. 2:23-cv-0434-JRG (member case)
2008	Civil Docket Report for <i>Emerging Automotive LLC v. Toyota Motor Corp. et al.</i> , No. 2:25-cv-0782-JRG (lead case)
2009	Civil Docket Report for <i>Emerging Automotive LLC v. Toyota Motor Corp. et al.</i> , No. 2:25-cv-0799-JRG (lead case)
2010	Order Denying Motion to Stay, <i>Digital Doors, Inc. v. Int’l Bus. Machines Corp.</i> , No. 2:22-cv-00457-JRG-RSP (E.D. Tex. July 24, 2023)
2011	<i>Curriculum Vitae</i> of Dr. Sam Malek
2012	“How are QR codes generated?”, QRcodeKit, available at https://qrcodekit.com/guides/how-are-qr-codes-generated/
2013 (new)	Declaration of Sam Malek, Ph.D. in Support of Patent Owner Response
2014 (new)	<i>Curriculum Vitae</i> of Dr. Sam Malek (June 7, 2026)

I. Introduction

Petitioners fail to show that any reference, alone or in combination, renders obvious any claim of U.S. Patent 11,104,245 (“the ’245 Patent”). The Petition fails, for all challenged claims, at least because:

(1) Petitioners concede that for the Kleve-based Grounds 1 and 2, there is no reference, alone or in combination, that discloses a “unique access code”—an element which is recited by no fewer than five different limitations in independent claim 1 (and by dependency, all challenged claims). Petitioners instead rely on expert testimony to incorrectly contend that Kleve’s “matrix barcode,” like “QR codes,” essentially “encode a unique access code” or “encode a unique value.” As anyone who has scanned a QR code for a restaurant menu can affirm, the QR codes at each table of a restaurant will reveal the same menu for each table, and therefore QR codes, like Kleve’s matrix barcode, do not “essentially” encode a “unique” value, as Petitioners’ expert contends. As detailed further below, the Petition’s failure on this point alone is fatal to both Kleve-based Grounds.

(2) For Grounds 1 and 2, the Petition’s failure to demonstrate any reference that discloses a “unique access code” means that the Petition also cannot sustain its burden as to independent claim elements 1[f], 1[g], 1[h], or 1[i]—each of which recite features or functions of the “unique access code.” And Grounds 1 and 2 fail regardless, as the Petition suffers from additional failures of proof as to independent

claim limitations 1[g], 1[h] and 1[i].

(3) Grounds 1 and 2 also fail because the Petition fails to show that Kleve and Mottla are properly combined, and even if they were, the combination still fails to satisfy the limitations of independent claim 1[i].

(4) Similarly deficient are the Petition's Zaid-based Grounds 3 and 4. Like Kleve, Zaid fails to disclose independent claim limitations 1[e]-1[f]. The identified "decrypted vehicle reservation" is neither shown to be a "unique access code," nor any "unique access code received by the mobile device from the server[.]"

(5) Even if claim limitations 1[e]-[f] were met, the Petition still suffers from additional deficiencies for independent claim limitations 1[g],1[h] and 1[i].

(6) Finally, the Petition fails to demonstrate why a POSITA would have been motivated to modify Zaid in view of Mottla for alleged disclosure of independent claim 1[i]. This failure is fatal to both Grounds 3 and 4 of the Petition.

II. Innovations of U.S. Patent 11,104,245

The '245 Patent issued on August 31, 2021. EX1001, Face Page. The '245 patent is titled "Vehicles and Cloud Systems for Sharing E-Keys to Access and Use Vehicles" and "relates to systems and methods for generating and sharing electronic keys (e-Keys) with users and cloud-based processing systems[.]" *Id.* at 1:1-3, 1:59-62. Companies like Apple, Ford, Samsung, Audi, General Motors, Volkswagen, and even Petitioner Toyota and Petitioner Kia's parent, Hyundai, have all cited to the

'245 Patent in their own patent applications. EX2003.

The '245 Patent describes innovations that allow a vehicle owner to assign, refine, and control the generation of any number of e-keys to any number of users for a vehicle—each unique e-key having its own privileges—privileges that are set responsive to a restriction set by the owner or administrator of the vehicle. EX1001, 43:26-40, 38:21-30.

The claims recite that the vehicle receives coded data from the mobile device for unlocking and use of the vehicle, that the coded data includes a unique access code including a unique access code received by the mobile device from the server. EX1001, independent claim 1. “The unique generation of access codes enables each electronic key[] to be different for each user and each e-key can be canceled at any time from a device having access to the Internet.” *Id.*, 43:49-53. Accordingly, each e-key is unique, and “being unique, can be cancelled and eliminated without affecting other issued e-keys.” *Id.*, 48:53-59, 47:57-61.

III. All Grounds fail because Petitioners failed to show that any reference, alone or in combination, discloses multiple limitations of independent claim 1.

The Petition fails to meet its burden for any claim, as the Petition relies on conclusory expert opinions to try to fill the glaring evidentiary gaps for multiple limitations required of independent claim 1 (and therefore required by dependency for all challenged claims 1-18).

Independent claim 1 recites no fewer than four different limitations to specify the “unique access code”:

(1) how the vehicle receives the unique access code and where it comes from, e.g., “the coded data from the mobile device including a unique access code received by the mobile device from the server” (EX1001, claim 1[f]);

(2) what the unique access code does and how it is managed, e.g., “the unique access code functioning for the e-key that is managed via one or more graphical user interface inputs rendered on a screen of the mobile device” (*id.*, claim 1[i]);

(3) specific features of the unique access code, e.g.:

(a) “privileges are for the unique access code” (*id.*, claim 1[g]);

(b) “the unique access code is associated with privileges set via the server responsive to a restriction set by an administrator of a vehicle” (*id.*, claim 1[g]); and

(4) components and operations when “the unique access code is to be active,” e.g., “a camera of the vehicle is used for capturing video of an area that includes the vehicle during a period of time in which the unique access code is to be active, such that actions taken by a user using an electronic key (e-key) is recorded” (*id.*, claim 1[h]).

Notwithstanding its integral role in the challenged claims, the Petition’s primary reference for Grounds 1 and 2—Kleve—fails to disclose any “unique access

code.” Equally deficient are Grounds 3 and 4, which both rely on Zaid as a primary reference, but fail to provide any disclosure of claim 1’s recited “unique access code,” much less “a unique access code received by the mobile device from the server.”

A. Grounds 1 and 2 fail because neither Kleve nor Kleve in combination is shown to disclose independent claim limitations 1[f], 1[g], 1[h] and 1[i].

While Petitioners point to Kleve’s matrix barcode as allegedly satisfying both the “coded data” and the “unique access code” limitations, it does not. The facts, and Kleve itself, show otherwise. And it is by this sleight of hand that the Petition seeks to evade its burden of proof as to *all the other independent claim limitations* that specify this “unique access code” required by claim 1[f], 1[g], 1[h], and 1[i]. This sophistry cannot sustain Petitioners’ burden, and Petitioners’ mere assertion is insufficient to render superfluous the claims’ requirements of the “unique access code.” Grounds 1 and 2 both fail.

1. Petitioners failed to show that any reference, alone or in combination, discloses “the coded data from the mobile device including a unique access code received by the mobile device from the server,” as recited by independent claim 1[f].

For Grounds 1-2, the Petition points to Kleve’s “matrix barcode” as the independent claim’s recited “coded data ... for unlocking and use of the vehicle.” Pet. 19. But even if Kleve’s matrix barcode were to meet each of the required

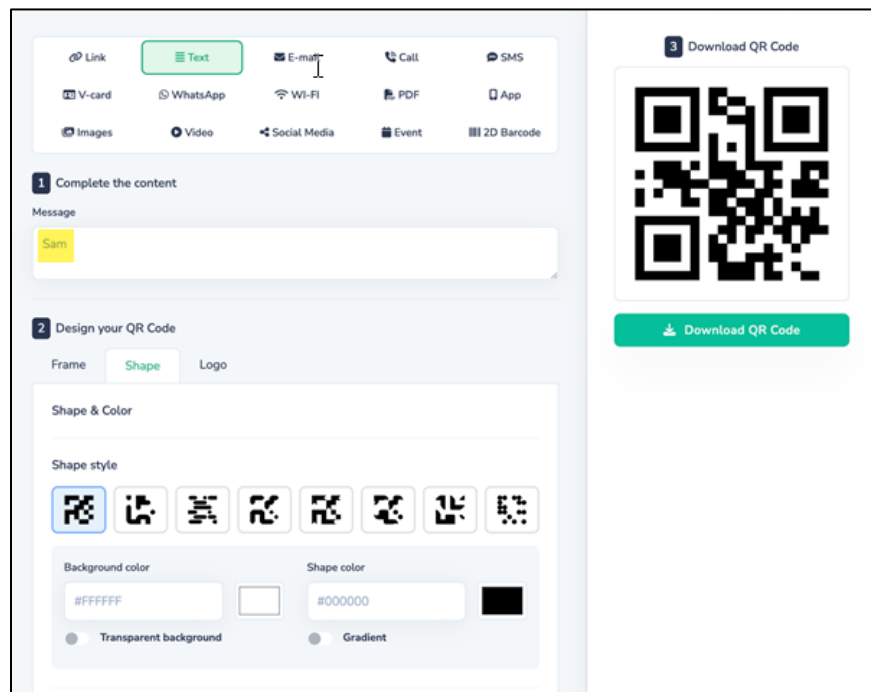
features of the claims’ recited “coded data,” neither Kleve nor any other reference discloses “**the coded data ... including a unique access code**”—let alone “the coded data from the mobile device including **a unique access code received by the mobile device from the server**,” as independent claim 1[f] requires. EX1001, claim 1[f] (emphases added).¹ To be clear, Petitioners do not make any inherency or modification arguments; instead, the Petition relies on Kleve as “disclos[ing] this limitation,” but there is no such disclosure. Pet. 20.

Petitioners attempt to fill Kleve’s gaps with expert testimony, but the Petition’s Grounds crumble after one look at that testimony. Pet. 19-20, citing EX1004, ¶¶ 121-22. For example, rather than point to any actual disclosure in Kleve, Petitioners’ expert provides the conclusory opinion that Kleve’s “matrix barcode,” like “QR codes, essentially encode a unique access code” or “encode a unique value[.]” EX1004, ¶ 122 (citing EX1005, ¶¶ 44, 69). This is simply wrong.

A QR code, or Quick Response code, also referred to as a matrix barcode, is a two-dimensional barcode that stores information in a grid of typically black and white squares that can be read by imaging devices, such as smartphone cameras. EX2013, ¶ 44, citing EX2012. As Dr. Malek explains, “a QR code is not inherently nor essentially unique; rather ‘a QR code becomes unique only when the data

¹ Emphasis herein added unless otherwise noted.

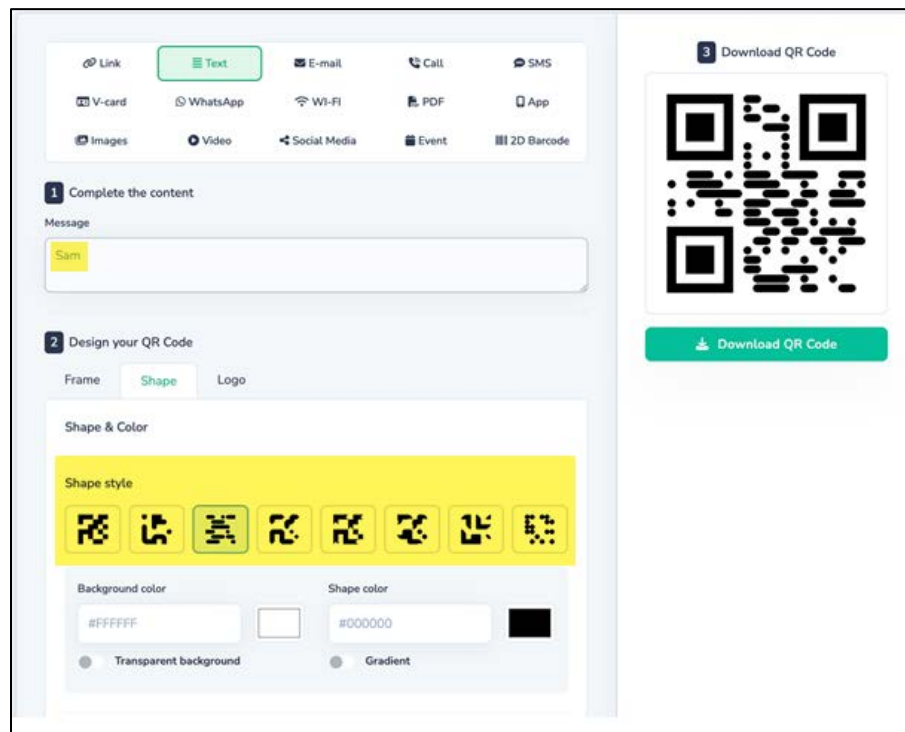
encoded within it is unique.” *Id.*, quoting EX2012. A QR code may be generated for arbitrary data, regardless of whether that data is unique. EX2013, ¶¶ 44-45. Indeed, publicly available online services, such as qr.io, allow users to generate QR codes for arbitrary input, without any requirement of uniqueness. *Id.* Dr. Malek demonstrates this point using the qr.io website to generate a QR code encoding his first name, “Sam,” which is not a unique name. *Id.*



Id.

A QR code is not even a unique representation of a given piece of information. *Id.*, ¶ 46. To illustrate this, Dr. Malek again used the qr.io service, this time altering the visual styling parameters of the QR code (e.g., shape style), and Dr. Malek generated a different QR code that still encodes the same underlying data—his first

name, “Sam.” *Id.*



Id.

By this illustration, Dr. Malek shows that “multiple distinct QR code symbols can encode identical information, further demonstrating that a QR code itself is not inherently or “essentially” unique, even with respect to a specific data value.” *Id.*

Accordingly, QR codes, like Kleve’s matrix barcode, do not “essentially encode a unique value” as Petitioners’ expert submits. *Id.*, ¶¶ 43-46; see EX2012. As demonstrated above, a matrix barcode, or QR code, is a way of encoding some information, but there is nothing essentially unique in that representation of data. *Id.*, ¶¶ 43-46; see EX2012. Petitioners’ reliance on expert testimony fails to fill the evidentiary gaps of the reference. A matrix barcode, like Kleve’s matrix barcode, is

not “well known [] to encode a unique value,” as Petitioners’ expert misstates, and therefore Kleve’s matrix barcode does not disclose claim 1[f]’s recited “coded data from the mobile device including a unique access code received by the mobile device...” EX1001, claim 1[f]; EX2013, ¶¶ 43-46; *see* EX2012.

Moreover, Kleve itself affirms this *lack of* “unique-ness,” likening its “matrix barcode” to a “code word that the Temporary User may enter/send to the vehicle when ready to begin the rental term.” EX1005, ¶ 69. In fact, Petitioners and Dr. Almeroth cite paragraph 69 of Kleve, misstating that

Kleve describes the matrix barcode as a type of “unique Temporary User identification” because, like a fingerprint or photo ID, the matrix barcode contains or encodes unique information (i.e., a unique access code) ...

Pet. 20, citing EX1004, ¶122 (verbatim). This is wrong. One look at Kleve paragraph 69 shows the opposite.

In a *first embodiment*, where the vehicle owner generates a virtual key using the “vehicle owner nomadic device,” Kleve states: “[a]t step 604, the vehicle Owner may then generate a virtual key based on a password generated by the vehicle Owner that may include a matrix barcode or a code word that the Temporary User may enter/send to the vehicle when ready to begin the rental term.” EX1005, ¶ 69; Fig. 6. The reference discloses “[a]nother exemplary embodiment of generating a virtual key [which] 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.” *Id.*, ¶ 69:

[0069] FIG. 6 is an exemplary embodiment of the vehicle rental micro-business distributing and controlling virtual keys using a nomadic device with a vehicle. The vehicle rental micro-business administrative system may consist of a computer system configured to host one or more websites for interaction with a vehicle Owner and Temporary User. In the illustration 600, a server 634 is used to communicate between a vehicle Owner nomadic device 601, a Temporary User nomadic device 611, and a vehicle computing system 621. Using a nomadic device, for example a smart phone, a Temporary User and vehicle Owner may set up user profiles, enter into an agreement and make a payment to initiate the vehicle rental process between the two parties at step 602 and 612. At step 604, the vehicle Owner may then generate a virtual key based on a password generated by the vehicle Owner that may include a matrix barcode or a code word that the Temporary User may enter/send to the vehicle when ready to begin the rental term. Another exemplary embodiment of 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. At step 616, the virtual key is generated and sent to the Temporary User. The Owner may deliver a virtual key to the vehicle for recognizing the Temporary User having authorization to enable a keyless drive-away at step 606.

Accordingly, the Petition misstates Kleve’s paragraph 69. There is no mention of a “unique Temporary User identification” for the first embodiment, at step 604,

to “generate a virtual key”—the embodiment that “may include a matrix barcode or a code word.” *Id.* In fact, paragraph 69 only discloses a “unique Temporary User identification” for “another exemplary embodiment of generating a virtual key,” but that embodiment *excludes* any mention of a “matrix barcode.” *Id.*; EX2013, ¶¶ 47-50.

Kleve simply does not disclose any “coded data ... *including a unique access code*,” or any “unique access code” at all, and Dr. Almeroth’s incorrect testimony about QR codes cannot cure the reference’s deficiency here. EX2013, ¶¶ 43, 51.

Because the Petition fails to identify any reference that discloses the independent claims’ required “unique access code,” the Petition likewise cannot show the remaining independent claim limitations requiring specific features and functionality of that recited “unique access code,” e.g.: (1) the “unique access code functioning for the e-key” (claim 1[i]); (2) “the unique access code is associated with privileges set via the server” (claim 1[g]); (3) the “privileges are for the unique access code” (claim 1[g]); or (4) the recited privileges set by the server being “responsive to a restriction set by an administrator of the vehicle” (claim 1[g]). EX1001; EX2013, ¶¶ 43-51.

The Petition’s failures as to claim 1[f] are, alone, fatal to Grounds 1 and 2. Additionally, because of this lack of the recited “unique access code,” the Petition cannot sustain its burden as to claim elements 1[g], 1[h], or 1[i].

Accordingly, Petitioners have failed to show any of the challenged claims of Grounds 1-2 are obvious over Kleve, alone or in combination. Because the Petition fails as to independent claim limitation 1[f], all claims must be upheld as valid.

2. Petitioners’ failure to show any reference, alone or in combination, that discloses “the unique access code functioning for the e-key,” as recited by independent claim 1[i], further highlights the Petition’s failure as to claim 1[f].

Petitioners cannot meet their burden for claim limitation 1[i], at least because claim 1[i] requires “the unique access code functioning for the e-key,” but the relied-upon “matrix barcode” does not disclose this limitation. As shown in Section III.A.1., for Grounds 1 and 2, the Petition failed to show any disclosure of the “unique access code” recited by independent claim 1 (and by dependency, all challenged claims). The Petition’s reliance on Kleve’s matrix barcode fails. *See* Section III.A.1., *supra*. As explained by Dr. Malek and the illustrative examples above, the identified matrix barcode does not encode a unique value, as Petitioners’ expert misstates. EX2013, ¶¶ 43-51.

In any event, Kleve actually discourages any “unique access code functioning for the e-key,” as claim 1[i] requires. Petitioners identify Kleve’s matrix barcode as the recited “coded data” and again point to this matrix barcode as allegedly encoding the recited “unique access code” of independent claim 1[e] and 1[f]. Pet. 19-20. But Kleve shows that its “matrix barcode” alone is “used as the virtual key.” EX1005, ¶

44. Kleve explains, “[o]nce the Temporary User has the matrix barcode scanned by the vehicle, the smart phone may be able to connect with the VCS and ***be used to enter and enable the vehicle drive away event.***” *Id.*

Kleve does not disclose any “unique access code,” let alone any “unique access code functioning for the e-key.” See Section III.A.1., *supra*; EX2013, ¶¶ 43-51. Nor would Kleve have any need to include such a disclosure, since Kleve already teaches that the matrix barcode alone is “used as the virtual key.” EX1005, ¶ 44. Accordingly, the Petition fails to identify any reference that discloses the recited “the unique access code functioning for the e-key.” Pet. 22-23.

The Petition’s failure to demonstrate that any reference discloses this limitation of independent claim 1 is, by itself, fatal to Grounds 1 and 2. All claims challenged in Grounds 1 and 2 must be upheld as valid.

3. Petitioners failed to show that any reference, alone or in combination, discloses the “privileges for the unique access code” or “the unique access code is associated with privileges set via the server,” as recited by independent claim 1[g].

As shown in Section III.A.1. above, the Petition does not identify any reference that discloses claim 1’s required “coded data from the mobile device ***including a unique access code,***” and therefore claim 1[g]’s requirements for that non-existent “unique access code” are likewise missing. EX1001, claim 1. However, even if a matrix barcode somehow “encodes a unique value” (it does not), and even

if Kleve had been shown to disclose a matrix barcode “including unique access code” (it was not), the Petition still fails because the relied-upon reference does not disclose the specific “privileges” limitations: “*privileges for the unique access code*” or “a unique access code associated with *privileges set via the server.*” EX1001, claim 1.

While the Petition makes the unhelpful and unexplained assertion that “[e]ach virtual key is tied to a time of use and so the privileges are for the unique access code,” these points are irrelevant to the Petition’s burden. Pet. 20-21. When Petitioners argue what must be “tied” to *a virtual key*, this wholly ignores the claim’s requirement that the privileges must be “*for the unique access code,*” with those “*privileges set via the server.*” EX1001, claim 1[g].

Indeed, to accept Petitioners’ argument is to render superfluous all of the independent claim’s requirements of the recited “unique access code.” EX1001, claim 1[f]-[i]. The Petition cannot render each of these recited elements meaningless by mere assertion. Pet. 20-21.

Because Petitioners have not identified any disclosure that Kleve’s server allegedly “set[s]” “*privileges [] for the unique access code,*” and have not even bothered to explain how anything “tied” to a virtual key could somehow satisfy these recited elements of independent claim 1, the Petition fails to meet its burden in showing any challenged claim unpatentable. The Petition’s failure as to independent claim limitation 1[g] means that all challenged claims of Grounds 1 and 2 must be

upheld as valid.

4. **Petitioners failed to show that any reference, alone or in combination, discloses “the privileges are set via the server responsive to a restriction set by an administrator of the vehicle, the restriction is associated with a mode of allowed use of the vehicle ... privileges are for the unique access code” as recited by independent claim 1[g].**

Even if Petitioners had shown some disclosure of the recited “unique access code,” and even if Petitioners had demonstrated the required “privileges *for* the unique access code,” the Petition is still deficient in its failure to show any privilege for the unique access code that is “*set via the server responsive to a restriction set by an administrator of the vehicle,*” where “*the restriction is associated with a mode of allowed use of the vehicle.*” EX1001, claim 1[g]; Pet. 20-21.

- a) **Neither paragraph 37 nor paragraph 40 of Kleve discloses the recited “a restriction” in claim 1[g]: “the privileges are set via the server *responsive to a restriction set by an administrator of the vehicle ... privileges are for the unique access code.*”**

For the alleged disclosure of the restriction of claim 1[g], the Petition points to Kleve, paragraph 37, which does not disclose any restriction at all. It also cites paragraph 40, which teaches that restrictions can be set at step 214, but that occurs *after* the virtual key with identified “privileges to unlock and drive the vehicle” has already been generated and distributed to the Temporary User. Pet. 20-21. Therefore, any restriction set after the distribution of this virtual key cannot be “privileges set

via the server **responsive to** a restriction set by an administrator of the vehicle,” as claim 1[g] recites. Accordingly, these failures as to independent claim limitation 1[g] are fatal to claims of Grounds 1 and 2, and all challenged claims therein must be upheld as valid.

(1) The Petition’s quotation from Kleve, paragraph 37, does not disclose any restriction.

At paragraph 37, Kleve teaches that the Owner may set up a user profile by inputting information into the website or nomadic device about the vehicle:

[0037] At step 202, 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. The Owner may set up a user profile by inputting information into the website or nomadic device including, but not limited to the make, model and year of the vehicle available for rent. The 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.

EX1005, ¶ 37.

Petitioners *tell* the Board that Kleve, at paragraph 37, discloses that the “owner sets *when* vehicle is ‘available for rent’”—but this is not what the reference states. Pet. 21, citing EX1005, ¶ 37. Kleve’s *actual* disclosure at paragraph 37 shows no such restriction. The owner “inputting information ... including but not limited to ***the make, model and year of the vehicle available for rent***” (EX1005, ¶ 37) is not

a restriction.

The Petition’s nonsensical reliance on this disclosure is even more pronounced when that disclosure is considered in view of the required claim language. For example, the Petition leaves unanswered how Kleve allegedly teaches “privileges are for the unique access code,” “privileges set via the server **responsive to** [owner may set a user profile by inputting information ... the make, model and year of the vehicle available for rent].” Pet. 21, citing EX1005, ¶ 37.

And, as the district court construed the term, the required “privileges” cannot be merely “unfettered access.” EX1015, at 12-13. The Petition’s reliance on Kleve at paragraph 37 fails for this reason as well.

(2) **Kleve, paragraph 40, fails to disclose “privileges are set via the server responsive to a restriction set by an administrator of the vehicle ... privileges are for the unique access code,” as recited by claim 1.**

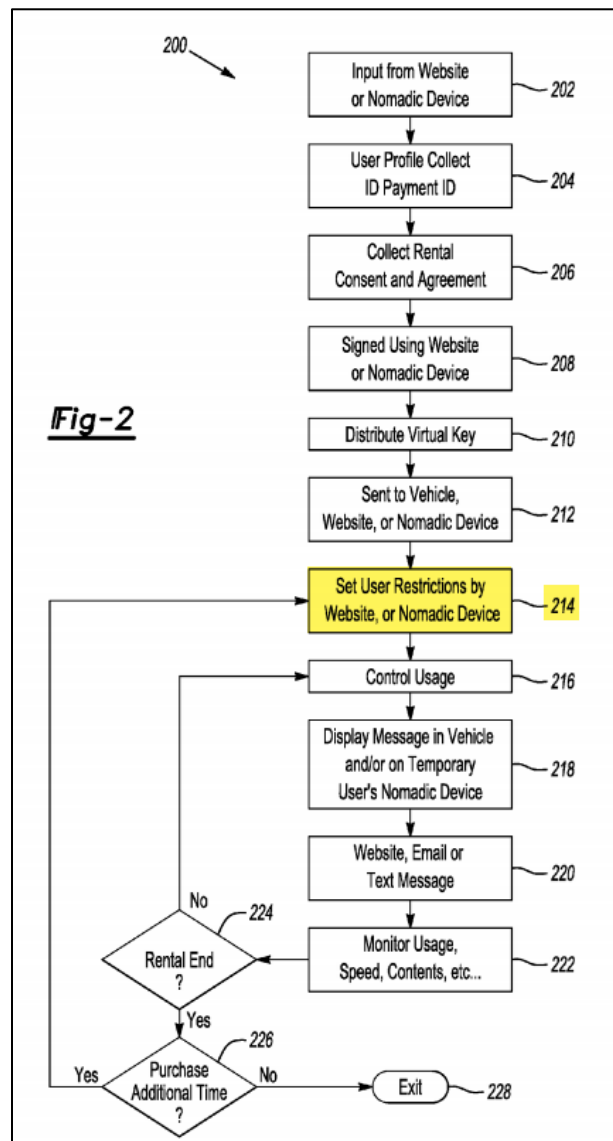
Petitioners’ reliance on paragraph 40 of Kleve also fails, but this disclosure fails based on the explicit **timing** disclosed therein. Petitioners point to Kleve’s matrix barcode virtual key as the alleged “coded data” and “unique access code” of limitations 1[e]-1[f] (Pet. 18-20), and further identify “privileges to unlock and drive a vehicle during a time of use” (Pet. 20-21)—but such “privileges” cannot be “set...responsive to” the Petition’s relied-upon “restrictions” of Kleve paragraph 40, because those “restrictions,” at step 214, are set **after** distribution of the virtual key

to the Temporary User (at step 210), **after** that Temporary User already has the virtual key with the identified “privileges to unlock and drive a vehicle.” Pet. 20-21. Accordingly, the Petition’s relied-upon “privileges” are not set “responsive to” the relied-upon “restrictions,” as claim 1[g] requires.

At paragraph 40 Kleve discloses: “[a]t step **214**, the Owner may have access to control usage of the vehicle being rented by the Temporary User.” EX1005, ¶ 40:

[0040] At step **214**, the Owner may have access to control usage of the vehicle being rented by the Temporary User. The Owner may set user restrictions by use of the website or nomadic device. The restrictions may be based on, but not limited to, the owner’s selection of parameters including, but not limited to, speed, global position coordinates, or load weight restrictions. At step **216**, the control parameters use restrictions may be monitored and if a restriction exceeds a limit the Temporary User and Owner may be notified. The monitoring information may be sent to the Owner through the website, with an email notification, or on the Owner’s nomadic device at step **220**. Email notification, text messages or an in-vehicle display message may be sent to notify the Temporary User if a restriction limit has been exceeded at step **218**.

But the owner cannot “set user restrictions” at step 214, until **after** Kleve’s virtual key has already been **distributed**, at step 210:



EX1005, Fig. 2. Accordingly, because Petitioners identify Kleve’s “virtual key as a matrix barcode” for both the “coded data” and the “unique access code” of limitations 1[e]-1[f], and Petitioners further rely on Kleve’s “restrictions” at step 214—a step *after* step 210’s distribution of the virtual key to the Temporary User—Kleve’s Temporary User already has the identified virtual key with the identified “privileges to unlock and drive a vehicle” *before* the Owner sets any restriction.

EX1005, Fig. 2; Pet. 20-21. Such privileges are therefore not the recited “privileges [] for the unique access code,” “privileges set via the server **responsive to a restriction** set by an administrator of the vehicle,” as claim 1 requires. EX1001, claim 1.

And, in case Kleve’s Figure 2 were not clear enough in showing that “step 214” does not occur until after Kleve’s virtual key has already been distributed, Kleve’s system explicitly directs that the Owner will have “control of the vehicle with the use of **vehicle restriction limits initially set by the Owner at the beginning of the rental term**,” which undisputably occurs after distribution of the virtual key (step 210). EX1005, ¶¶ 43, 40, Fig. 2. Again, when describing Figure 7, Kleve reiterates **when** a vehicle owner may assign “restrictions”: “**at the start of the rental period**”:

Once the Temporary User initiates the rental event, the system detects a rental time start at step **706**. The system may begin to download performance limitations and **restrictions assigned by the vehicle owner at the start of the rental period** at step **708**.

Id., ¶ 75.

Therefore, as taught by the Petition’s relied-upon reference, restrictions are “**initially** set by the Owner at the beginning of the rental term,” and indeed, the vehicle owner does not even “have access to control usage of the vehicle being rented by the Temporary User” until step 214, **after** a virtual key is distributed to the

Temporary User. *Id.*, Fig. 2, ¶¶ 43, 75, 40.

Because Petitioners’ identified “privileges to unlock and drive a vehicle”—privileges Kleve’s Temporary User already has when the virtual key is distributed at step 210—Kleve’s paragraph 40 (describing step 214, after distribution) cannot be the recited “restriction set by an administrator of the vehicle” to which “privileges set via the server [are] **responsive**.” EX1001, claim 1[g].

Therefore, even accepting as true Petitioners’ arguments that (1) Kleve discloses a matrix barcode that “encodes a unique value,” and that (2) alleged privileges “tied” to ***the virtual key*** can somehow satisfy the claim’s recited “privileges for the unique access code”—the Petition still fails in its burden of proof as to claim 1[g] because the identified “restriction” (Kleve’s “step 214” at paragraph 40) only ever ***occurs after the Temporary User already has the virtual key with the identified “privileges to unlock and drive a vehicle.”***

As with the Petition’s reliance on paragraph 37, paragraph 40 of Kleve cannot satisfy the recited limitations of claim 1: “privileges set via the server ***responsive to a restriction set by an administrator of the vehicle*** ... privileges are for the unique access code.” EX1001, claim 1.

Because the Petition fails as to independent claim limitation 1[g], all claims of Grounds 1 and 2 must be upheld as valid.

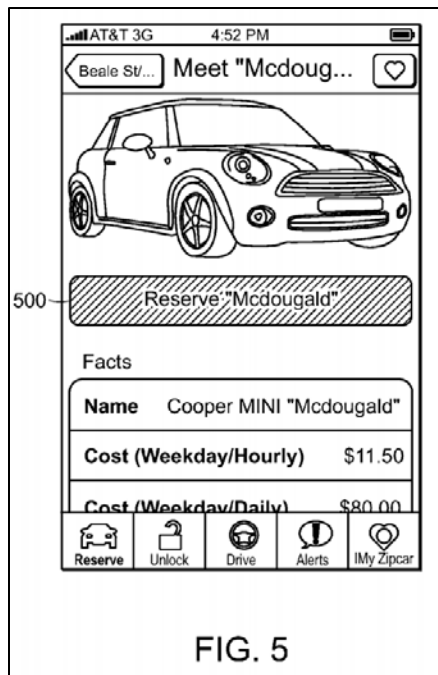
5. The Petition fails to demonstrate why a POSITA would have been motivated to modify or combine Kleve in view of Mottla.

To satisfy claim limitation 1[i], reciting “the unique access code functioning for the e-key that is managed via one or more graphical user interface inputs rendered on a screen of the mobile device,” the Petition proposes to combine Kleve and Mottla. Pet. 22-25. However, as demonstrated above, Kleve does not disclose any “unique access code,” let alone any “unique access code functioning for the e-key.” EX1001, claim 1; see Sections III.A.1.-2, *supra*. Petitioners do not allege that Mottla cures either of these deficiencies of Kleve. Pet. 22-25. Mottla does not disclose the recited “unique access code,” nor do Petitioners allege that it does. *Id.*; EX1006. Accordingly, the combination fails to meet the limitations of claim 1[i] regardless of whether the Petition’s proposed combination of references is proper.

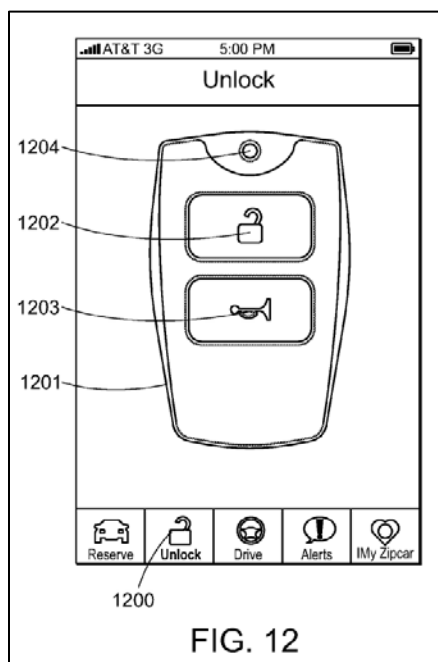
It is not, however. EX2013, ¶¶ 52, 58, 63. The Petition first proposes to combine Kleve’s “user interface” (EX1005, Figure 9) and Mottla’s Figure 5, which “illustrates a portion of the user interface for displaying information regarding a selected vehicle” (EX1006, ¶ 15, Figure 5) and Mottla’s Figure 12, which “illustrates a portion of the user interface for displaying an icon for unlocking a vehicle or for making a vehicle sound its horn” (*id.*, ¶ 22).

Mottla is a patent application that discloses mobile applications including a user interface allowing a user to browse reservable vehicles, a user interface to

reserve a vehicle, and a user interface which acts like a key-fob. EX1006, Figs. 5, 12, ¶ 33. Examples are shown below as Figures 5 and 12:



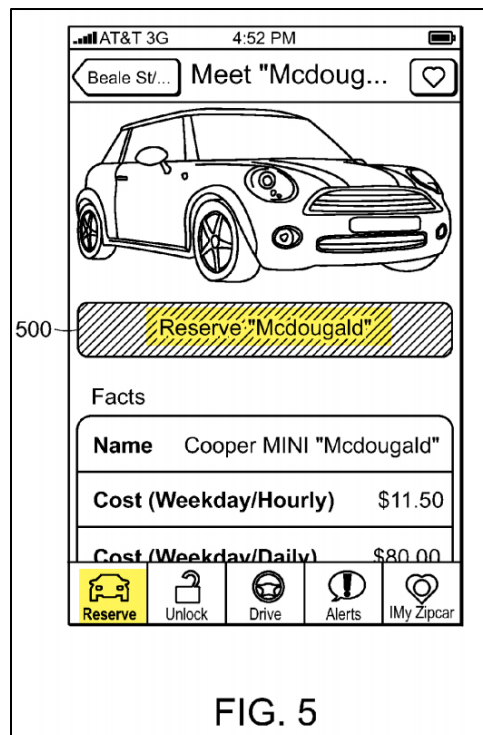
Id., Fig. 5.



Id., Fig. 12.

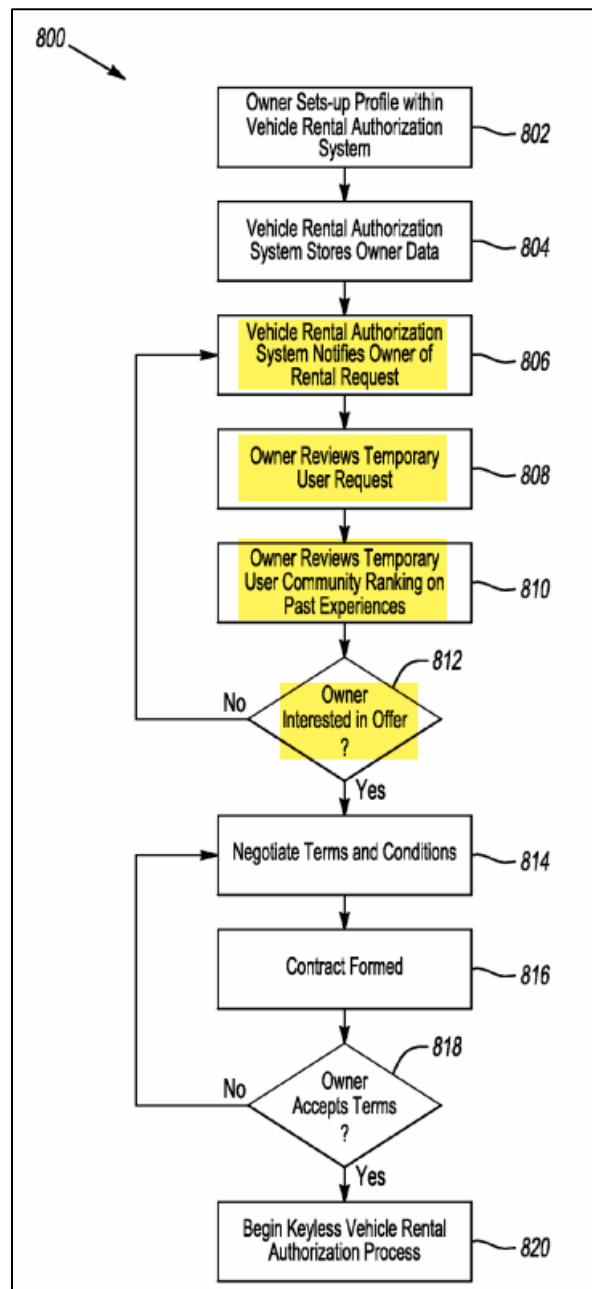
Kleve actually discourages the proposed modification in view of Mottla. EX2013, ¶¶ 52-55. Kleve's system is intentionally designed to require the vehicle owner to approve or decline any Temporary User's *request* to rent the vehicle. *Id.*, ¶¶ 55-57. Kleve does not allow, and in fact discourages, the direct "reserve" actions taught by Mottla's user interface. *Id.*, ¶ 58.

For example, Mottla's GUI inputs allow a user to make a reservation, i.e., by "select[ing] one or more of the reservable assets," and selecting the "reserve" element 500:



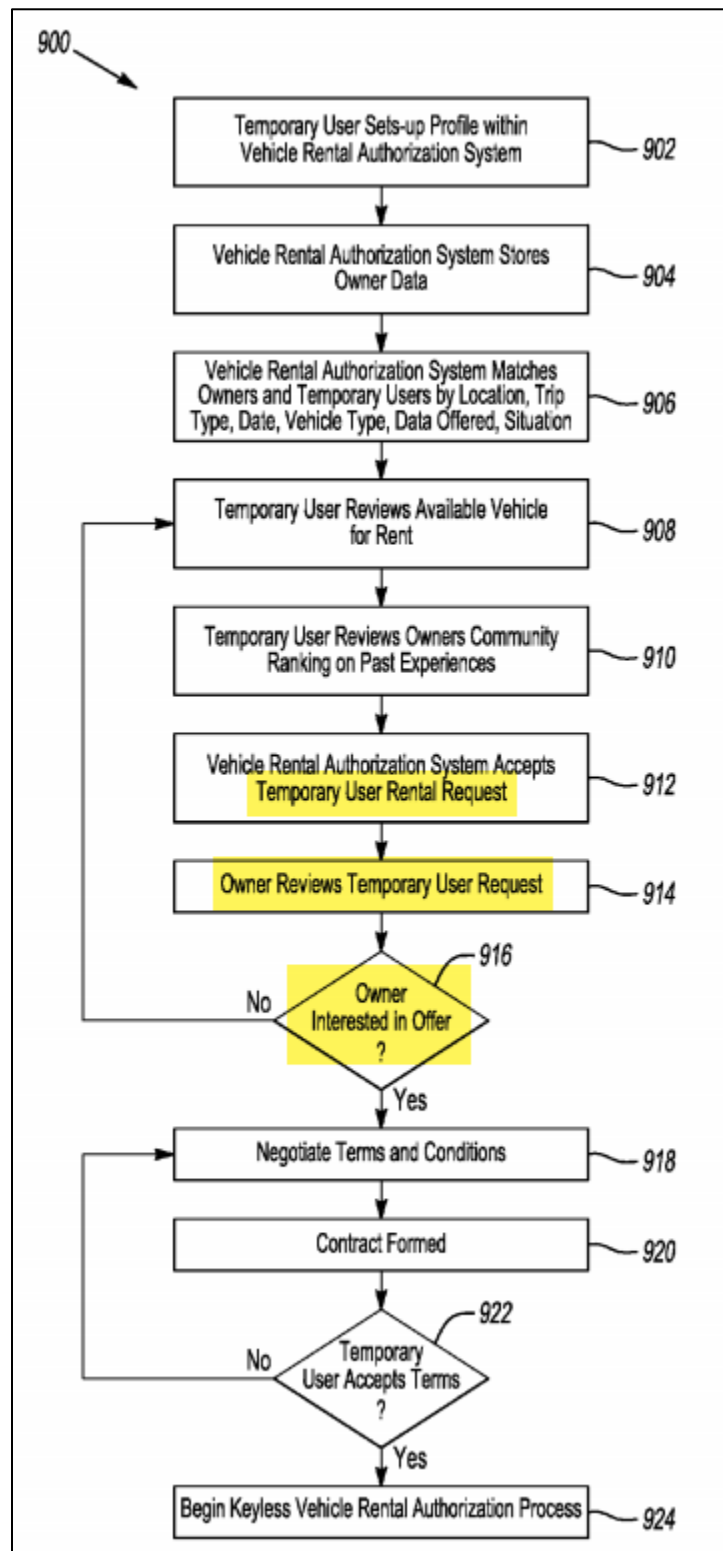
EX1006, Fig. 5, ¶ 27; EX2013, ¶¶ 54-55. Kleve, however, does not allow its "Temporary User" to take the reservation action that Mottla's Figure 5 permits.

EX2013, ¶¶ 55-57. Instead, the Temporary User of Kleve may only “*request*” to rent the owner’s vehicle, then the system will “notify the owner of a *rental request* at step 806,” and at step 808, the “owner reviews [a] Temporary User[’s] *request*,” at which point the owner may further review the “Temporary User Community Ranking” and, importantly, at step 812, the owner must take a specific action to either “decline and wait for the vehicle rental authorization system to notify of any other offers” or “accept the offer.” EX1005, ¶ 84, Figure 8:



As shown in Figure 8 above, and further explained at paragraphs 83 and 84, Kleve requires the owner to first “review the requested rental based on what the Temporary User is looking to use the vehicle for,” “when the requested use will be taking place, and where,” “review the Temporary User[’]s profile and rental history”

and Kleve teaches that ***the owner must ultimately undertake the active operation of accepting or declining the user's request.*** EX1005, ¶¶ 83-84, 89, Figs. 8, 9; EX2013, ¶¶ 55-56. Kleve's Figure 9, showing the "interface" available to the Temporary User, reiterates this point—the Temporary User may only "request" to rent a vehicle, which, as an initial matter, must be accepted by the "vehicle rental authorization system" at step 912. *Id.*, Fig. 9. Additionally, that "request" still requires later actions by the owner, i.e., review of the "request" and if the owner is "interested in offer," the owner may accept or decline the request. *Id.*, ¶¶ 83-84, 89, Figs. 8-9.



Id., Fig. 9; *see id.*, ¶ 89 (“If the owner has decided to accept the offer, he may begin the process of developing terms and conditions of the rental period.”). Accordingly, Kleve actually discourages the Temporary User from taking the direct “reserve” action taught by Mottla’s Figure 5. EX2013, ¶¶ 52, 55-58.

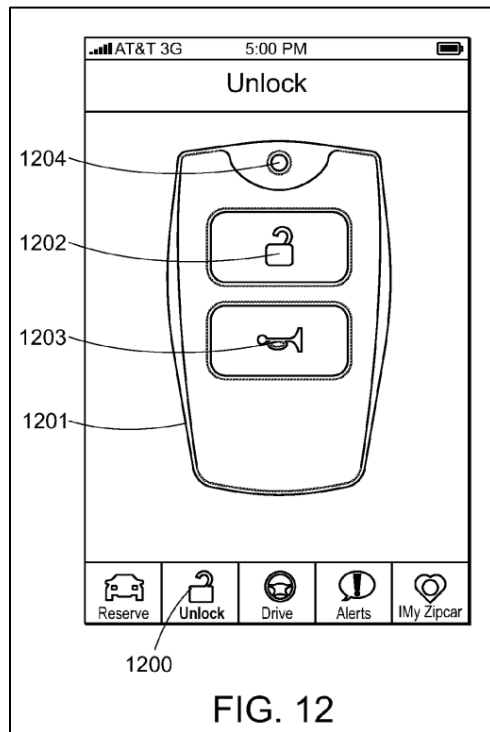
The Petition also fails to demonstrate why a POSITA would have been motivated to modify Kleve’s matrix barcode in view of Mottla’s GUI inputs, shown in Figure 12. EX2013, ¶¶ 52, 59, 62.

Kleve already teaches that (1) the “matrix barcode” *itself* is passively “used as the virtual key,” (2) this matrix barcode is simply scanned by the vehicle and (3) the matrix barcode is “used to enter and enable the vehicle drive away event,” without ever requiring that the Temporary User actively select any inputs to enter or start the vehicle. EX1005, ¶ 44 (“Once the Temporary User has the **matrix barcode scanned by the vehicle**, the smart phone may be able to connect with the VCS and be **used to enter and enable the vehicle drive away event.**”):

[0044] Another exemplary example of the vehicle rental micro-business system may include other enhancements including, but not limited to, **matrix barcode (ex. two-dimensional code) used as the virtual key being recognized by the VCS.** The smart phone may be used to communicate the matrix barcode information to the vehicle rental micro-business system directly. The system may be able to communicate information from the smart phone to the vehicle notifying the VCS of a virtual key. **Once the Temporary User has the matrix barcode scanned by the vehicle, the smart phone may be able to connect with the VCS and be used to enter and enable the vehicle drive away event.**

Id., EX2013, ¶ 60.

Mottla, by contrast, requires **active input** by the user to select certain buttons for executing certain operations, i.e., “a member selects a lock icon 1200 that causes the mobile device application to display a user interface with another icon 1201 that has a button 1203 for causing a vehicle 104 to sound its horn, or [] buttons 1202 to lock or unlock the vehicle doors.” EX1006, ¶ 33, Fig. 12:



Id.; EX2013, ¶ 61.

Petitioners fail to explain how the matrix barcode of Kleve would be combined with the graphical user interface of Mottla or how the two in combination would be expected to function. Pet. 22-25; EX2013, ¶¶ 62-63. Indeed, Kleve’s matrix barcode

is a passive mode of communication, scanned by the vehicle’s VCS, without any buttons for the user to select. EX1005, ¶ 44; EX2013, ¶¶ 60, 62. Moreover, by scanning Kleve’s barcode at the vehicle—without any interface input—the Temporary User can enter the vehicle and drive away. EX1005, ¶ 44; EX2013, ¶¶ 60, 62. Mottla, by contrast, requires the user to actively select buttons to unlock a door, sound a horn, etc. EX1006, ¶ 33, Fig. 12; EX2013, ¶ 61. Petitioners do not explain how to combine Kleve’s matrix barcode with Mottla’s selectable buttons, let alone why a POSITA would *add* buttons for “unlocking,” when Kleve’s matrix barcode *already* accomplishes this operation when scanned. Pet. 22-25; EX2013, ¶¶ 62-63.

Thus, Petitioners have failed to show that a POSITA would have had an “apparent reason to combine the known elements” and would have had a reasonable expectation of success in doing so. *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007) (requiring “articulated reasoning with some rational underpinning to support the legal conclusion of obviousness”); *Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1367–68 (Fed. Cir. 2016). A patent claim “is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art.” *KSR*, 550 U.S. at 418.

For this reason alone, the Petition cannot sustain its burden as to independent claim 1[i], and therefore both Grounds 1 and 2 fail.

Moreover, because neither reference discloses the recited “unique access code,” or “the unique access code functioning for the e-key,” as recited by claim [f] and 1[i], Grounds 1 and 2 fail regardless of whether the combination is proper.

6. Petitioners failed to show any reference, alone or in combination, discloses a “camera capturing video ... during a period of time in which the unique access code is to be active,” as recited by independent claim 1[h].

While Petitioners reduce independent claim 1 to requiring a “camera,” the Petition ignores the actual claim language recited by the limitation. Specifically, limitation 1[h] recites:

a camera of the vehicle is used for capturing video of an area that includes the vehicle ***during a period of time in which the unique access code is to be active***, such that actions taken by a user using an electronic key (e-key) is recorded[.]

EX1001, claim 1.

It is unsurprising that the Petition fails to identify any disclosure of “a camera of the vehicle [] used for capturing video ... ***during a period of time in which the unique access code is to be active***,” as Petitioners failed to identify any disclosure of any “unique access code” whatsoever. *Id.*; see Section III.A.1., *supra*. The Petition’s failures with respect to the required “unique access code” of limitation 1[f] are highlighted here as well. The Petition does not demonstrate any “unique access code,” let alone the recited element requiring a “period of time in which the unique

access code is to be active[.]” EX1001, claim 1[h].

Because the Petition fails to show any disclosure that satisfies either “the unique access code,” or “a camera of the vehicle [] used for capturing video ... during a period of time in which the unique access code is to be active,” as recited by claim 1[h], Grounds 1 and 2 both fail. All challenged claims must be upheld as valid.

B. The Zaid Reference (EX1008)

The inapplicability of Zaid is manifest in the reference itself. EX1008; EX2013, ¶¶ 65-66. Zaid is not directed to any vehicle configured to receive “a unique access code,” much less receive any unique access code that is “functioning for an e-key.” EX2013, ¶¶ 65-66; EX1001, claim 1. Nor does Zaid disclose or suggest privileges for the unique access code—privileges set via the server “responsive to” a specific “restriction” set by the administrator of the vehicle, where “the restriction is associated with a mode of allowed use of the vehicle.” *Id.* These deficiencies are unsurprising since Zaid does not even disclose the claim’s recited “unique access code received by the mobile device from the server.” *Id.*

Instead, Zaid discloses that a prospective vehicle *renter* can log into their Facebook® or a similar social networking site, view an ad for a vehicle—an ad placed by a vehicle owner—and, if interested, the renter can click on that ad and make a reservation. EX1008, ¶ 72; EX2004, 45. Once the renter makes the

reservation, that reservation may be relayed as an encrypted message. EX1008, ¶¶ 125-127. The reservation itself—encrypted or not—is not a “unique access code,” nor is its “unique increment” or “private key.” EX2013, ¶¶ 65-66. Zaid fails to disclose that the “unique access code [is] received by the mobile device from the server,” as claim 1 requires. *Id.*

Further, Zaid provides no disclosure of: an administrator of a vehicle that may set a restriction associated with a mode of allowed use of the vehicle, or that its server sets privileges for the reservation that are “responsive to” a restriction set by an administrator of the vehicle, as claim 1 requires. *Id.*

C. For Grounds 3 and 4, Petitioners’ reliance on the Examiner’s findings is of no avail, as Zaid does not disclose the limitations of claim 1, and the Examiner agreed.

For claim 1’s requirement of “a unique access code,” Petitioners offer three alternative theories, each relying solely on Zaid—but not one of them meets the recited limitations of claim 1[e]-1[f]: “coded data ... including a unique access code received by the mobile device from the server.” Further the identified disclosures fail to satisfy the recited “privileges set via the server responsive to a restriction set by an administrator of the vehicle,” as required of claim 1[g]. And neither of the Petition’s relied-upon combinations of art renders obvious claim limitations 1[h] or 1[i].

It is because Grounds 3 and 4 principally rely on Zaid—a fundamentally

deficient reference as to multiple limitations of independent claim 1—that the Petition relies heavily on the Examiner’s findings during prosecution, hoping to avoid having to explain Zaid’s shortcomings. However, the Petition’s reliance on the Examiner’s findings is of no avail. First, the Examiner agreed that Zaid did not teach limitations of [current] claim 1. EX1002, 124-25. Second, the Examiner proposed combinations with a reference—Joao—that is not even part of the Petition. *Id.* And, in any event, the disclosures of Zaid that the Examiner *did* rely upon do not support, and indeed undermine, Petitioners’ challenge to claim 1. *Id.*; Pet. 53.

As shown below, because of the Petition’s deficiencies as to independent claim 1, both Zaid-based Grounds 3 and 4 fail.

1. The Petition fails to identify any disclosure to satisfy claim 1[e]-[f]’s requirements of “coded data ... for unlocking and use of the vehicle, the coded data from the mobile device including a unique access code received by the mobile device from the server[.]”

The recited “coded data” of claim limitation 1[e] is “for unlocking and use of the vehicle,” and 1[f] requires that the “coded data from the mobile device includ[es] a unique access code received by the mobile device from the server.” EX1001, claim 1. The Petition points to Zaid’s “vehicle reservation” as the claim’s recited “coded data” (Pet. 49) and further points to a “decrypted vehicle reservation” as the alleged “unique access code” that must be “include[ed]” in the “coded data from the mobile device” and must further be “received by the mobile device from the server” (Pet.

52).

First, Petitioners fail to provide any disclosure in Zaid that its reservation—encrypted or decrypted—is a “unique access code,” as recited by claim limitation 1[f]-1[i]. Pet. 51-52, citing EX1008, Fig. 5, ¶¶ 125-26, 128-130, EX1002, 387; EX2013, ¶¶ 67-71. “[T]he encryption disclosed by Zaid merely converts the message from one form to another.” EX2013, ¶ 66. Moreover, the “private key” utilized by Zaid’s encryption scheme is merely secret, as opposed to publicly known, but this private key does not disclose any “unique access code” either. *Id.*, ¶¶ 69-71.

But even if Zaid had disclosed a “unique access code”—Zaid does not—there is no showing of the recited “unique access code ***received by the mobile device from the server.***” EX1001, claim 1; EX2013, ¶¶ 69-70. Instead, Zaid’s first “encryption layer” is decrypted “**using a locally stored private key of the wireless communication device,**” and its second “encryption layer” is decrypted “**using a private key of the vehicle access kit.**” EX1008, ¶¶ 125-26. Zaid’s “vehicle access kit” is not “the mobile device” required by claim 1, but is instead “installed into an existing vehicle” either “during production” or “aftermarket.” EX1008, ¶ 85.

Accordingly, neither Zaid’s “locally stored private key of the wireless communication device” nor its “private key of the vehicle access kit” can be “a unique access code ***received by the mobile device from the server,***” as the challenged claim requires. EX1001, claim 1; EX2013, ¶¶ 67-72. The Petition’s cited

encryption/decryption disclosures do not satisfy the limitations of claim 1[f].

At bottom, Zaid does not disclose its decryption, its decrypted reservation, or its “private key” as “a unique access code,” and even assuming Zaid’s “private key” for decryption were somehow “unique,” Zaid shows that it is either “locally stored on the wireless communication device,” or is from “the vehicle access kit,” and is therefore not “received by the mobile device from the server,” as recited by 1[f].

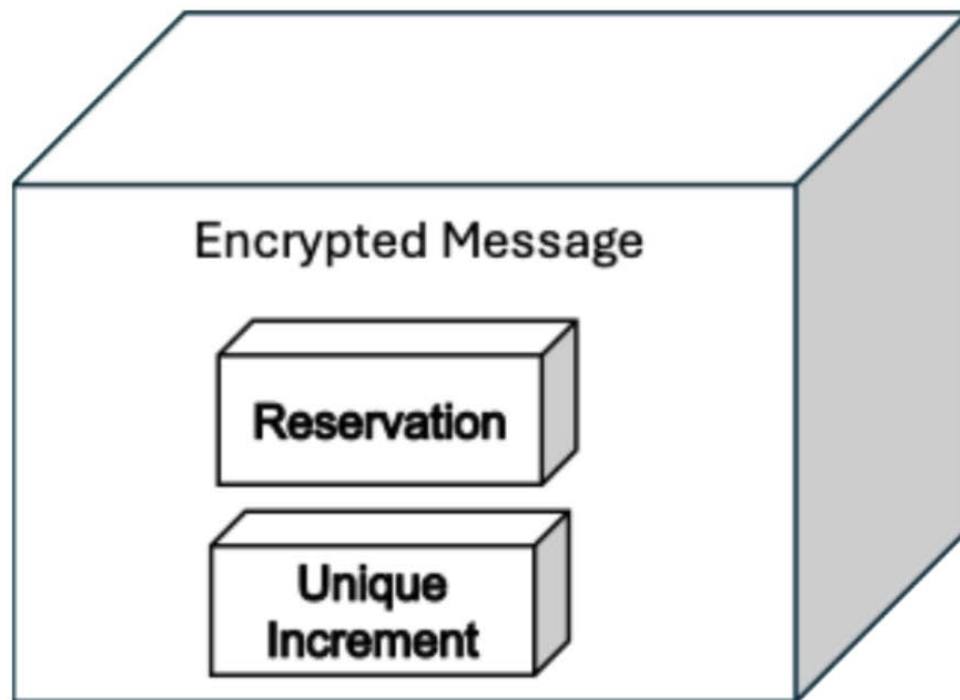
Accordingly, the Petition fails to show that the Zaid reference satisfies the elements of 1[e]-1[f], as none of the relied-upon encryption/decryption disclosures is “coded data ... for unlocking and use of the vehicle, the coded data ... including a unique access code,” much less “a unique access code received by the mobile device from the server.”

2. Zaid’s “unique increment” fails to satisfy claim 1[e]-1[f]’s limitations requiring “coded data ... for unlocking and use of the vehicle, the coded data ... including a unique access code received by the mobile device from the server[.]”

As an alternative “unique access code,” Petitioners point to Zaid’s disclosure of a unique increment for “each message,” which prevents repeat message attacks. Pet. 52, citing EX1008, ¶ 130. Zaid discloses “the unique increment is in the form of a counter and/or time stamp that indicate[s] the *uniqueness of the message* to avoid a repeat message attack.” EX1008, ¶ 130. However, this “unique increment”—included in “each message”—cannot satisfy the claim’s recited “coded data for

unlocking and use of the vehicle, the coded data ... including a unique access code received by the mobile device from the server,” at least because Zaid teaches that this “unique increment” is not included in Zaid’s “vehicle reservation”—the disclosure Petitioners identify as the claim’s recited “coded data” required by 1[e] and 1[f]. Pet. 49; EX2013, ¶¶ 72-82.

Claim 1 requires that a “unique access code” must be included in “the coded data”—the same coded data “for unlocking and use of the vehicle.” EX1001, claim 1. Zaid discloses that its “unique increment” is not “include[ed]” in the vehicle reservation, but is instead part of *each message*, each “communication,” thereby making each message **unique**, not the reservation itself. EX1008, ¶ 130; EX2013, ¶¶ 72-73. Zaid’s unique increment renders its message unique, ensuring that each valid message can only be accepted once. EX2013, ¶¶ 74-76. However, Zaid’s unique increment does not in turn render the message’s other payloads, such as the reservation, unique. *Id.*, EX2013, ¶¶ 77-79. The figure below illustrates Zaid’s disclosure:



Id., ¶ 77. Therefore, whether or not Zaid’s message includes a vehicle reservation, an update, or any other “communication,” Zaid is clear that it is only *the message* itself that has this “unique increment.” EX1008, ¶¶ 81, 130; EX2013, ¶¶ 77-79.

Because Zaid’s unique increment is not “included” in the vehicle reservation itself—which Petitioners identify as the alleged “coded data” (Pet. 49)—Zaid’s “unique increment” cannot meet claim 1[f]’s recited “the coded data ... including a unique access code.” EX1001, claim 1.

Petitioners do not contend that Zaid’s message is the recited “coded data” of claim 1[e]-1[f]. In any event, it is not. Zaid’s unique increment is for *message security*, included in the message “to avoid a repeat message attack,” accordingly, that message is not “***coded data ... for unlocking and use of the vehicle***, the coded

data ... including a unique access code.” EX1008, ¶¶ 81, 130. A POSITA would understand from Zaid’s disclosures that Zaid’s “message” with a unique increment is not the required “coded data ... for unlocking and use of the vehicle, the coded data ... including a unique access code,” as claim 1 requires. EX2013, ¶¶ 79-82; Pet. 49-53. Therefore, the fact that Zaid’s message itself includes a “unique increment” cannot satisfy “*the* coded data ... including a unique access code,” as recited by claim 1.

Accordingly, the “uniqueness of the message” is of no avail to Petitioners, both because Zaid’s unique increment is not included in its vehicle reservation (alleged “coded data”), and because what does include the unique increment—the message itself—is not alleged to be the recited “*the* coded data” “for unlocking and use of the vehicle,” nor would a POSITA understand it to be. Pet. 49-53; EX2013, 80.

Likewise unavailing are Zaid’s disclosures of paragraph 81 regarding a “new private key,” because “the server update includ[ing] a new private key” is not “coded data ... for unlocking and use of the vehicle,” nor do Petitioners allege it to be. Pet. 52, citing EX1002, 387; EX2013, ¶ 81. Thus, whether unique or not, neither Zaid’s “unique increment,” nor its “server update includes a new private key,” meets the recited limitations of “coded data ... for unlocking and use of the vehicle, the coded data ... including a unique access code[.]” EX1001, claim 1; EX2013, ¶ 82.

The Petition fails to meet its burden as to independent claim limitation 1[f], and therefore all challenged claims must be upheld as valid.

3. The Petition fails to identify any disclosure to satisfy the recited limitations of claim 1[g]: “privileges are for the unique access code” and “privileges are set via the server responsive to a restriction set by an administrator of the vehicle, the restriction is associated with a mode of allowed use of the vehicle[.]”

For each of the alleged disclosures for a “unique access code”—whether it be a “decrypted vehicle reservation,” a “unique increment” or a “server update includes a private key”—not one is shown to have “privileges for the unique access code,” or “privileges [that] are set via the server responsive to a restriction set by an administrator of the vehicle, the restriction is associated with a mode of allowed use of the vehicle.” Pet. 53-55; EX1001, claim 1; EX2013, ¶ 83.

Neither the “unique increment” nor the “server update includes a new private key” has anything to do with privileges “responsive to a restriction,” as limitation 1[f] requires, and Petitioners do not even allege there to be any “privileges for” these identified disclosures. Pet. 53-55. Because there aren’t any. EX1008, ¶¶ 81, 130; EX2013, ¶ 84.

As for the identified reservation, Petitioners allege “Zaid’s privileges that limit (1) vehicle access and (2) use for a period of time.” Pet. 53-54, citing EX1008, ¶ 69. But here, too, the requisite disclosure is lacking. Neither Zaid’s vehicle access

nor its “specified time period” is shown to be “privileges set via the server responsive to a restriction set by an administrator of the vehicle” nor “a restriction set by an administrator of the vehicle,” as claim 1[g] requires. EX1008, ¶¶ 69, 77; Pet. 53-55; EX2013, ¶¶ 85-88. First, mere vehicle “access” is not a “privilege” under the district court’s construction of the “plain and ordinary meaning” of “privileges”—a claim construction order which Petitioners concede as applicable to the ’245 patent. Pet. 14; EX2013, ¶ 85; EX1015, 12-13:

From Defendants’ perspective, the dispute centers on whether the “privileges” or “conditions of use” can allow what they call “unfettered access.” They say Plaintiff’s “non-construction of these terms invites the incorrect possibility that mere (unrestricted) access alone might be a privilege within the context of the . . . patents.” Dkt. No. 134 at 5. For support, they cite prosecution-history and IPR statements purportedly distinguishing cited references that allow such access.

The Court agrees with Defendants. The patents use “privileges” and “conditions” similarly, and there appears to be no dispute about what “conditions” are. For example, the specification explains various drivers can each have their own user account, “which provides specific privileges (use capabilities, restrictions, limits, parameters, etc.).” ’026 Patent at 36:46–50. Elsewhere, the patents explain conditions of use “define[] one or more privileges associated to use of the e-key.” *Id.* at 4:65–66; *see also id.* at 6:60–63 (describing “use of the vehicle in accordance with conditions defined in the privilege settings”).

Id. (internal citations omitted). Plaintiff then emphasized its prosecution remarks that Zaid did not disclose “a unique access code that includes privilege settings set for additionally limiting types of use of the vehicle.” *Id.* at 17. In other words, Plaintiff equated “unfettered access” with the absence, not presence, of “privileges.” Given that, the Court agrees with Defendants that “privileges for use of the vehicle” cannot simply be “unfettered access” to the vehicle, which is the “plain and ordinary meaning” of these phrases on this record.

Second, Zaid’s “use for a period of time” is not a “privilege set via the server responsive to a restriction set by an administrator ...” EX2013, ¶ 86; EX1008, ¶¶ 69, 72, 77. Indeed, Zaid never discloses or suggests that the owner or “administrator” is even involved in the reservation’s “specified time period.” *Id.*; EX2004, 45.

Petitioners further rely on Zaid’s owner updating “various vehicle related information such as vehicle availability and vehicle location”—at paragraph 79—but Zaid teaches these are not “privileges [] set via the server responsive to a restriction” or “a restriction set by an administrator of the vehicle,” as required by claim 1. EX1008, ¶¶ 77, 79. Instead, as Zaid explains, the owner making a “vehicle availability” update is just an advertisement or announcement. *Id.*, ¶ 77 (“advertise or announce when the vehicle will be available for sharing”). Zaid’s owner advertising or announcing when the vehicle is available for sharing is just what Zaid says it is, an advertisement or announcement—and that vehicle availability can of course be a year (or more), or months within a year, or weeks within a month, or days within a week, etc. *Id.*; EX2013, ¶ 87. Zaid does not disclose an owner setting

a restriction for the reservation to which any “privileges set via the server [are] responsive,” much less setting a “reservation period” as asserted in the Petition. *Id.*

As a further deficiency, Petitioners fail to make any connection between Zaid’s reservation having a “specified time period,” a vehicle owner announcing “vehicle availability,” and some specific action of Zaid’s server that is “set” “responsive to” the owner’s announcement of vehicle availability. Pet. 54-55; EX1001, claim 1[g]; EX2013, ¶ 88.

Accordingly, the Petition fails to meet its burden of proof as to independent claim 1[g] and therefore all challenged claims of Grounds 3 and 4 must be upheld as valid.

4. The Petition fails to show that the combination of Zaid and Mottla renders obvious claim 1[i].

a) Petitioners provide no prior art disclosure for claim 1[i]’s recited “the unique access code functioning for the e-key[.]”

For Grounds 3 and 4, the Petition does not point to any disclosure, *from any reference*, which allegedly satisfies the recited “the unique access code functioning for the e-key[.]” Pet. 56-59; EX1001, claim 1. Merely stating what “[t]he Office determined” does not satisfy Petitioners’ burden, especially where the Examiner cited to a “unique private key” as the alleged “unique access code.” Pet. 56-59, citing EX1002, 124. There is no disclosure in Zaid, and no allegation from Petitioners, as

to how Zaid’s “private key” allegedly satisfies the element—“the unique access code functioning for the e-key”—as claim 1[i] recites. *Id.* But, in any event, Zaid does not disclose the recited “unique access code,” and Zaid does not even disclose a “unique private key.” See Sections III.C.1.-2., *supra*. Accordingly, Zaid’s disclosures neither meet the “unique access code” requirement of limitation 1[f], nor “the unique access code functioning for the e-key,” as recited by limitation 1[i]. EX2013, ¶¶ 89-90.

As an additional failure, neither Zaid’s message nor the message’s “unique increment” is alleged to be “functioning for the e-key,” as claim 1[i] requires. Pet. 56-59. Petitioners do not allege that Mottla somehow cures Zaid’s deficiencies to this element of 1[i], but instead rely on Mottla solely for alleged disclosure of “one or more graphical user interface inputs rendered on a screen of the mobile device.” Pet. 56.

Accordingly, because Petitioners failed to make any showing of “the unique access code functioning for the e-key,” the Petition fails as to limitation 1[i], and this failure is fatal to all challenged claims of Grounds 3 and 4. Pet. 56-59.

b) The Petition fails to demonstrate why a POSITA would have been motivated to modify Zaid in view Mottla.

The Petition’s rationale for modifying Zaid with Mottla is facially deficient. For example, Petitioners argue that a POSITA would have been motivated to use Mottla’s system “*instead of scanning the virtual key*—providing a better user

experience while maintaining security.” Pet. 58. But Zaid does not disclose “scanning the virtual key.” EX1008. This argument makes no sense. EX2013, ¶ 91.

Equally nonsensical is Petitioners’ piggybacking on the Examiner’s use of Mottla “to conveniently control the vehicle.” Pet. 56, citing EX1002, 124-25. Petitioners already told the Board that Zaid’s mobile device is used to perform “unlocking requests,” i.e., “the vehicle receives a request from a mobile device that unlocks the vehicle[.]” Pet. 49. Petitioners fail to explain, therefore, why Zaid’s operations for unlocking the vehicle somehow “[in]conveniently control the vehicle,” such that a POSITA would be motivated to look to Mottla for alleged improvement as to “convenience.” Pet. 56-59; EX2013, ¶ 92.

And, as discussed in Section III.A.5., with respect to the unsupported combination of Kleve and Mottla, here too, the Petition does not explain why a POSITA would be motivated to add Mottla’s GUI inputs, e.g., for unlocking the vehicle (Pet. 56-59), when Petitioners concede that Zaid’s mobile device already performs this unlocking function (Pet. 49). EX2013, ¶ 93.

The alleged combination also fails because Petitioners do not show any reasonable expectation of success in making this proposed modification. Pet. 56-59; EX2013, ¶ 94. Petitioners merely repeat the Examiner’s conclusion—that Zaid’s “unique increment” satisfies the recited “unique access code functioning for the e-key”—but neither the Examiner nor Petitioners demonstrate *how to combine* the

“unique increment” of Zaid with Mottla’s graphical user interface inputs, let alone *how* this undescribed combination *would function*. EX2013, ¶ 95.

Petitioners’ cursory treatment of the Examiner’s findings fails to meet their required burden to show “both that a skilled artisan would have been motivated to combine the teachings of the prior art references to achieve the claimed invention, and that the skilled artisan would have had a reasonable expectation of success in doing so.” *Intelligent Bio-Sys., Inc.*, 821 F.3d at 1367–68.

Accordingly, the Petition fails to meet its burden of obviousness, as there is no showing that a POSITA would have been motivated to modify Zaid in view of Mottla, and no showing that a POSITA would have had a reasonable expectation of success in doing so. EX2013, ¶ 95.

Even if proper, the combination still fails to satisfy limitation 1[i], for the reasons set forth in Section III.C.4.a., above.

5. The Petition fails to show that Zaid, or Zaid in combination with Kleve, teaches or suggests the recited elements of claim 1[h].

Petitioners do not even allege that Zaid’s “camera” is one which, as claim 1[h] recites, “is used for capturing video during a period of time in which the unique access code is active.” Pet. 55-56. Instead, Petitioners propose to modify Zaid with Kleve, relying on the same deficient disclosures for the Petition’s Kleve-based Grounds. *Id.* However, as shown above, Kleve also fails to disclose this

limitation 1[h]. *See* Section III.A.6., *supra*. The Petition's combination of Zaid and Kleve does not cure the numerous deficiencies of Kleve, nor do Petitioners allege that it does. *Id.*; Pet. 55-56.

Petitioners do not show that any prior art combination renders obvious claim limitation 1[h]. Accordingly, the Petition's Grounds 3 and 4 fail for at least the same reasons as set forth in Section III.A.6.

IV. Petitioners failed to present even a prima facie case of obviousness for either the Ground 1 or Ground 3 challenge to claim 6.

A. Petitioners' Ground 1-claim 6 challenge fails because the Petition does not comply with 37 C.F.R. § 42.104(b)(4).

For Ground 1, the Petition does not even address claim limitation 6[b], let alone present any argument or evidence as to its alleged unpatentability. These deficiencies are fatal to the Petition's claim 6 challenge presented in Ground 1.

The Petition addresses only the first limitation of claim 6, completely ignoring the remaining limitation (6[b]):

7. Claim 6

6: “The vehicle of claim 1, wherein an application accessed by said mobile device is configured to enable sending instructions to said server to enable sharing said vehicle with the user to enable use of the e-key or another e-key on said vehicle,”

Kleve’s application is accessed by TU’s mobile device. *Kleve*, [0036]. The TU uses the application to “input profile information” “including details about the vehicle he intends to rent.” *Id.* [0086]. This is stored in “the vehicle rental authorization system” so that the owner can be notified about “the requested vehicle rental.” *Id.* [0088]. The application enables sharing the key with the user to enable use of the e-key, because once agreement terms are accepted between VO and TU, “the vehicle rental authorization system may begin the keyless vehicle rental authorization process without [TU] physically meeting the owner.” *Id.*, [0090].

Accordingly, *Kleve* discloses this limitation. Almeroth, ¶¶149-50.

8. Claim 7

Pet. 32; see EX1004, ¶¶ 149-50 (discussing *only* limitation 6[a]). However, claim 6[b] further recites: “wherein the e-key has functions enabled via graphical user interfaces of the application of the mobile device.” EX1001, claim 6.

By ignoring limitation 6[b], the Petition fails to “specify where each element of the claim is found in the prior art patents or printed publications relied upon.” 37 CFR § 42.104(b)(4); see 37 C.F.R. § 42.22(a)(2); and see 35 U.S.C. § 312(a)(3); EX2013, ¶¶ 96-97. Indeed, the Petition is wholly devoid of *any* “prior art patents or printed publications relied upon” for limitation 6[b], and certainly lacks any “detailed explanation of the significance of the [non-existent] evidence.” 37 C.F.R. §§ 42.22(a)(2), 42.104(b)(4).

By failing to comply with these basic statutory requirements, the Petition has not only flouted the governing Rules, but also denied Patent Owner the opportunity to demonstrate each of the flaws in its challenge to claim 6’s patentability. *See Intelligent Biosys. Inc.*, 821 F.3d at 1369 (“It is of the utmost importance that petitioners identify ‘with particularity’ the ‘evidence that supports the grounds for the challenge to each claim’”). Accordingly, claim 6 must be upheld as valid.

B. Even if the Petition’s statutory deficiencies were not fatal to its Ground 1-claim 6 challenge, the Petition still fails to meet its burden as to claim limitation 6[a].

The Petition’s argument as to limitation 6[a] is facially deficient, omitting *any* explanation or evidence as to how Kleve allegedly discloses “an application...*configured to enable sending instructions to said server to enable sharing said vehicle with the user to enable use of the e-key...*” EX1001, claim 6; EX2013, ¶ 98.

What *is* addressed by the Petition is woefully deficient. At most, Petitioners argue that Kleve discloses an “application” that is “accessed by TU’s mobile device” (Pet. 32, citing EX1005, at ¶ 36), and further allege that this “application enables sharing the key with the user to enable use of the e-key” (Pet. 32, citing EX1005, at ¶ 90). Even if the Petition’s characterizations of Kleve’s application were accurate, the Petition still lacks any explanation or evidence as to how each of the elements of claim 6[a] are allegedly disclosed. Pet. 32; EX2013, ¶ 99.

First, Petitioners do not even mention or address the claim’s requirement that an application is “***configured to enable sending instructions to said server,***” and second, the Petition does not identify where, or explain how, the identified application is allegedly “configured to enable” sending *the kind* of “instructions” to said server *to enable* the recited functions of the claim: “***to enable sharing said vehicle with the user to enable use of the e-key[.]***” Pet. 32. By failing to even address each of the elements of the limitation 6[a], Petitioners’ challenge to claim 6 again fails to “specify where each element of the claim is found in the prior art patents or printed publications relied upon.” 37 C.F.R. §42.104(b)(4); 37 C.F.R. § 42.22(a)(2); EX2013, ¶ 100.

Moreover, the law does not allow Petitioners to simply ignore the recited claim element “***configured to enable sending instructions to said server***”—doing so would improperly render the phrase superfluous. *Medacta USA, Inc. et al. v. RSB Spine, LLC*, IPR2020-00264, Paper 46 at 13 (P.T.A.B. Apr. 15, 2021) (rejecting petitioner’s interpretation of claim limitation that “renders the term ‘primarily’ superfluous”); see *Wasica Finance GmbH, et al. v. Continental Automotive Syst.*, 853 F.3d 1272, 1288-89, fn.10 (Fed. Cir. 2017) (Board erred by failing to give effect to express claim terms, as doing so would render other limitations meaningless). The ’245 patent shows that the claim’s inclusion of an application configured to enable sending “instructions” is far from superfluous. The specification offers numerous

examples wherein “instructions” are utilized to enable various functions. *E.g.*, EX1001, 44:55-59 (“... code, logic, or program instructions that will request that the device ID ... should be transferred”); *see id.*, 8:1-3 (“the server ... sends deactivation instructions to one or both of the devices”).

Accordingly, the Petition’s failure to argue or show that Kleve’s “application” is allegedly “configured to enable sending instructions to said server to enable sharing said vehicle with the user to enable use of the e-key or another e-key on said vehicle” is, on its own, a dispositive deficiency, and therefore claim 6 must be upheld as valid. 37 C.F.R. §§ 42.22(a)(2), 42.104(b)(4).

The Petition’s omissions are alone fatal to its claim 6 challenge. Moreover, even what *is* argued in the Petition is of no avail. First, Kleve at paragraph 36 describes only a “smart phone application ... that an Owner or Temporary User may use to manage their assets and/or user profile.” EX1005, ¶ 36. Likewise, Petitioners do not ever explain how either Kleve at paragraph 88 or 90 somehow supports the notion that the “application accessed by the Temporary User” (Pet. 32, citing EX1005, ¶¶ 36, 88, 90) is an application that is “***configured to enable sending instructions to said server to enable sharing said vehicle with the user to enable use of the e-key or another e-key on said vehicle,***” as claim 6 requires. Pet. 32.

[0036] In the illustrative embodiment as shown in FIG. 2 is an overview of the several steps that may contribute to the process of a vehicle rental micro-business integrated with a VCS. The process of a vehicle rental micro-business integrated with a computing system may be applied, but not limited to, automobiles, boats, machinery, and equipment rentals. The vehicle rental micro-business 200 may include a website, smart phone application or other nomadic device that an Owner and Temporary User may use to manage their assets and/or user profile. The following elements within a vehicle rental micro-business 200 may include a process for collecting identification and payment from Temporary User 204, collecting rental consent and agreement 206, distributing a virtual key to the Temporary User and VCS 210, giving the Owner a selection of vehicle parameters to monitor usage of the vehicle including vehicle speed, load capacity, etc. . . . 222, control temporary user's usage 216, and other features that may assist the Owner and Temporary User with the virtual rental experience.

EX1005, at ¶ 36.

[0088] At step 912, the vehicle rental authorization system may accept the Temporary User's selection of which vehicle he would like to rent. The system may output a notification to the owner of the requested vehicle rental by a Temporary User. The owner may review the Temporary User's request based on several factors including, but not limited to, the use, trip type, and date the Temporary User is requesting to rent the vehicle at step 914. The owner may also review the Temporary User community ranking to determine if he should rent to the interested Temporary User.

Id., ¶ 88.

[0090] At step 920, once the contract (e.g. without limitation, a rental contract) is formed, the owner and Temporary User may use the vehicle authorization rental system to accept the terms and conditions. The Temporary User may review the contract and accept the term using the vehicle authorization rental system at step 922. Once the contract is accepted, the vehicle authorization rental system may begin the keyless vehicle rental authorization process at step 924. The Temporary User may complete the entire vehicle rental process using the vehicle rental authorization system without physically meeting the owner.

Id., at ¶ 90.

The Petition’s failures in addressing all elements of the claim, as well as its failure to present any prior art disclosure of the elements, are independent bases for upholding claim 6 as valid. Kleve does not disclose claim limitation 6[a], and Petitioners do not contend that Mottla cures these deficiencies.

Accordingly, claim 6 must be upheld as valid.

C. The Petition’s Ground 3-claim 6 challenge is equally flawed.

Turning to Ground 3, the Petition’s challenge to claim 6 is again deficient because Petitioners fail to identify any disclosure that allegedly meets the claim’s requirement of an application “configured to enable sending instructions to said server,” or otherwise explain how Zaid’s “application” is allegedly “configured to enable sending instructions to said server to enable sharing said vehicle with the user to enable use of the e-key or another e-key on said vehicle,” as recited by claim limitation 6[a]. Pet. 65; EX1001, claim 6. On its face, the Petition’s argument is

deficient—leaving entirely unaddressed specific requirements of the claim. *Id.*

What Petitioners do offer is hindsight analysis, based on the teachings of the '245 patent, to argue that “it would have been obvious to a POSITA to implement Zaid’s vehicle reservation application to enable both geolocation [] and requesting use of the vehicle[.]” Pet. 65. But even if such modifications were proper, neither an “application to enable [] geolocation” nor one “requesting use of the vehicle” discloses the claim’s element requiring an application that is “**configured to enable sending instructions to said server**” “to enable sharing said vehicle with the user to enable use of the e-key,” and Petitioners do not contend that it does. Pet. 64-65. Petitioners fail to show that an “application to enable [] geolocation” or “requesting use of the vehicle” somehow discloses an application “configured to enable sending instructions to said server,” or one that is “configured to enable” sending *the kind of* “instructions to said server” recited by claim 6. *Id.*; EX2013, ¶¶ 101-104. Petitioners do make any kind of inherency argument to support these bare assertions. Therefore, neither proposed modification, even if proper, is shown to satisfy the recited limitations of claim 6[a].

Petitioners leave it to the Board to dig through the relied-upon disclosures to try to map the prior art to the claim’s limitation. Pet. 64-65. But, in any event, this is a wild goose chase—Zaid does not teach an application “configured” to achieve what the claim requires.

For example, the Petition cites to paragraph 77, but there Zaid makes explicit that the “vehicle reservation application” “enables a vehicle user (e.g., renter and owner) to communicate with backend server(s)” to “advertise or announce” vehicle location, user location, or when the vehicle is available for sharing, and/or to retrieve a list of nearby vehicles available for sharing. EX1008, ¶ 77:

[0077] In various embodiments, the wireless communication device includes a vehicle reservation application or other software function (e.g., an iPhone or Droid application) that enables a vehicle user (e.g., renter and owner) to communicate with backend server(s) (e.g., an online vehicle reservation system) to (a) advertise or announce the location of the vehicle, (b) advertise or announce the location of the user, (c) advertise or announce when the vehicle will be available for sharing (e.g., vehicle owner announces when the vehicle is available for sharing, and/or vehicle user announcing when the vehicle is returned and is available for sharing by others), and/or (d) retrieving a list of nearby vehicles available for sharing.

Not one of Zaid’s application “communications” to “advertise or announce” locations, availability, or to “retrieve a list” (*id.*) describes an application “configured to enable sending instructions to said server to enable sharing said vehicle with the user to enable use of the e-key or another e-key on said vehicle” (EX1001, claim 6), and in any event, Petitioners do not even argue otherwise. Pet. 64-65; EX2013, ¶ 102. Instead, the Petition merely plucks from Zaid words like “sharing” and “enable,” then intersperses the recited language of claim 6, to suggest disclosures that are non-existent in the reference itself. Pet. 64-65; EX1008, ¶¶ 77,

80, 125.

Nor are any of these “advertise or announce” communications from Zaid’s application to or from a server showing the application to be “configured to enable” sending *the kind* of “instructions to said server” to enable the recited functions of the claim: “to enable sharing said vehicle with the user to enable use of the e-key or another e-key on said vehicle[.]” EX1008, ¶ 77; EX2013, ¶ 102. And again, Petitioners do not even allege that they do. Pet. 64-65.

Equally unavailing to Petitioners is Zaid’s teaching that “the vehicle reservation is booked by a user at a central server via a user interface displayed on a computing device” or “booked at the server 110 via a user interface 116” (EX1008, ¶¶ 80, 125). Petitioners fail to argue, let alone show, that Zaid’s reservation, “booked” via a user interface, is an application “configured to enable sending instructions to said server.” Pet. 64-65; EX2013, ¶ 103. Likewise missing from the Petition is any explanation as to how these disclosures show an application configured to enable sending *the specific kind* of “instructions” to said server to enable the recited functions of the claim: “to enable sharing said vehicle with the user to enable use of the e-key or another e-key on said vehicle[.]” EX1001, claim 6; EX2013, ¶ 103. In sum, Petitioners do not demonstrate how this reservation being “booked at the server” is somehow sufficient meet the elements of claim 6. Pet. 64-65; EX1008, ¶ 80:

[0080] The vehicle reservation is booked at the server **110** via a user interface **116** displayed on a computing device **118**. The server may be configured to interact with a plurality of vehicle access control systems for providing access control to a plurality of vehicles. The plurality of vehicle access control systems may be geographically distributed across different locations. In various embodiments, the computing device **118** can be any suitable computing device that has connection to the server **110** and can support the user interface **116**. In various embodiments, the computing device **118** is the same wireless computing device **108** used by a user to access the vehicle.

See *id.*, ¶ 125:

[0125] FIG. 5 is a flowchart illustrating an example flow for receiving vehicle reservation from a wireless communication device in accordance with some embodiments. At **502**, a vehicle reservation is booked. In various embodiments, the vehicle reservation is booked by a user at a central server via a user interface displayed on a computing device. The computing device can be any suitable computing device that has network access and can support the user interface. In various embodiments, the computing device is the same wireless communication device the reservation is sent to. At **504**, the vehicle reservation is encrypted. In various embodiments, the central server encrypts the message containing the vehicle reservation. In various embodiments, the encryption includes multiple layers. In various embodiments, the vehicle reservation is encrypted in a first layer of encryption using a public key of the wireless communication device the vehicle reservation will be sent to. The first layer of encryption can be decrypted using a private key of the wireless communication device. The vehicle reservation is further encrypted in a second layer of encryption using a public key of a vehicle access kit that provides access control to the vehicle. The second layer of encryption can be decrypted using a private key of the vehicle access kit.

Petitioners' Ground 3-claim 6 challenge fails because the Petition does not show that Zaid's application is somehow "configured to enable sending instructions

to said server,” or how the relied-upon disclosures render obvious an “application configured to enable sending” *the specific kind* of “instructions” claim 6 requires. Pet. 64-65; EX1001, claim 6; EX2013, ¶¶ 104-105.

The Petition’s proposed combination with Mottla does not cure the numerous deficiencies of Zaid’s disclosures, nor do Petitioners allege that it does. Pet. 64-66.

Claim 6 must be upheld as valid.

V. Each of the Petition’s claim 3 challenges fails because neither Kleve (Ground 1) nor Zaid (Ground 3) discloses “a unique access code generated by the server[.]”

A. Kleve does not disclose any “unique access code generated by the server,” nor any “user account having privileges assigned by the administrator,” as recited by claim 3.

Ground 1 relies on Kleve for alleged disclosure of claim 3’s requirement that the recited “unique access code” is “generated by the server.” Pet. 27. As established above, Kleve neither discloses any “unique access code” nor the alleged “unique access code embedded in a virtual key,” as Petitioners allege. *See* Section III.A.1., *supra*. The Petition repeats its mischaracterization of Kleve’s matrix barcode in its claim 3 challenge, misstating that “[e]ach of Kleve’s requests is associated with a unique access code embedded in a virtual key that can be expressed as a matrix barcode.” Pet. 27. But, as explained above, Kleve’s matrix barcode is neither taught to be a “unique access code,” nor does Kleve disclose any “embedded” unique access

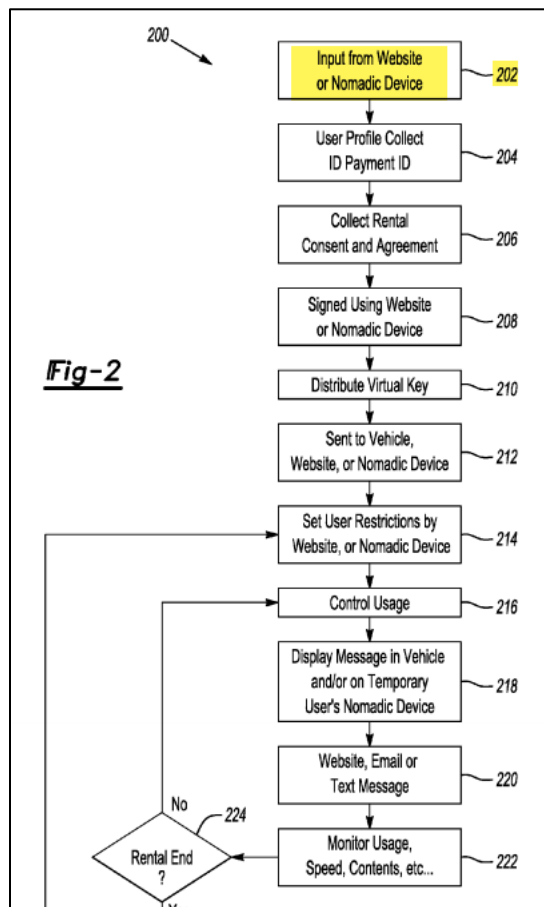
code in a matrix barcode. See Section III.A.1., *supra*.

But even if Kleve's matrix barcode were a "unique access code"—it is not—the matrix barcode is not "a unique access code ***generated by the server***" as claim 3 requires. EX1001, claim 3; EX2013, ¶¶ 106-107.

Instead, Kleve teaches that its matrix barcode ***already exists*** as part of the temporary user's "user profile" ***before*** the temporary user can even use the vehicle rental service. EX1005, ¶¶ 37, 47; EX2013, ¶ 107. For example, "[a]t step 202," Kleve teaches that the "Temporary User may set up a user profile using a website or nomadic device" "to include a ... matrix barcode":

[0037] At step 202, 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. The Owner may set up a user profile by inputting information into the website or nomadic device including, but not limited to the make, model and year of the vehicle available for rent. The 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.

EX1005, ¶ 37; *see id.*, Fig. 2:



Because Kleve teaches the matrix barcode is already *included* in the temporary user’s user profile at step 202—and step 202 *precedes* the generation and distribution of a virtual key—the matrix barcode cannot be the virtual key “generated by the server” at any subsequent step, as Petitioners allege. *Id.*; EX2013, ¶¶ 107-108.

It is only “[a]fter a Temporary User set[s] up[] their user identity within the website” that “the Temporary User may begin to use the vehicle rental services.” *Id.*, ¶¶ 47, 86.

[0047] After a Temporary User setups their user identity within the website, the Temporary User may begin to use the vehicle rental services. The Temporary User may establish a community rating 306 based on past experiences and services with other vehicle owners that use the site. The Temporary User can log-in to the website to begin browsing the database of available vehicles to rent at step 308. Once the Temporary User is logged-in they may browse existing rental offers available, which may include, but not limited to, one sided rentals, swaps, offset swaps, trades, and custom swaps at step 310. At step 312, the Temporary User may also post offers of offset swaps, one sided rentals, and trades. The Temporary User may also browse other users and proposes an offer directly at step 314. When the Temporary User and vehicle Owner agree to terms 316 the website may generate the exchange or propose a rental agreement 318. The agreement between the Owner and Temporary User can be signed and payment made through the website at step 320. The agreement to rental terms and conditions between the parties may be done with the website using smart phones or a smart phone application, or any other type of nomadic device. Rental conditions may also be displayed on the vehicle's touch-screen visual display and accepted or rejected through the touchscreen visual display. Acceptance may be sent back to the Owner over the wireless network. A Temporary User may also access the Owner's web page to view and accept rental terms and conditions online at step 320.

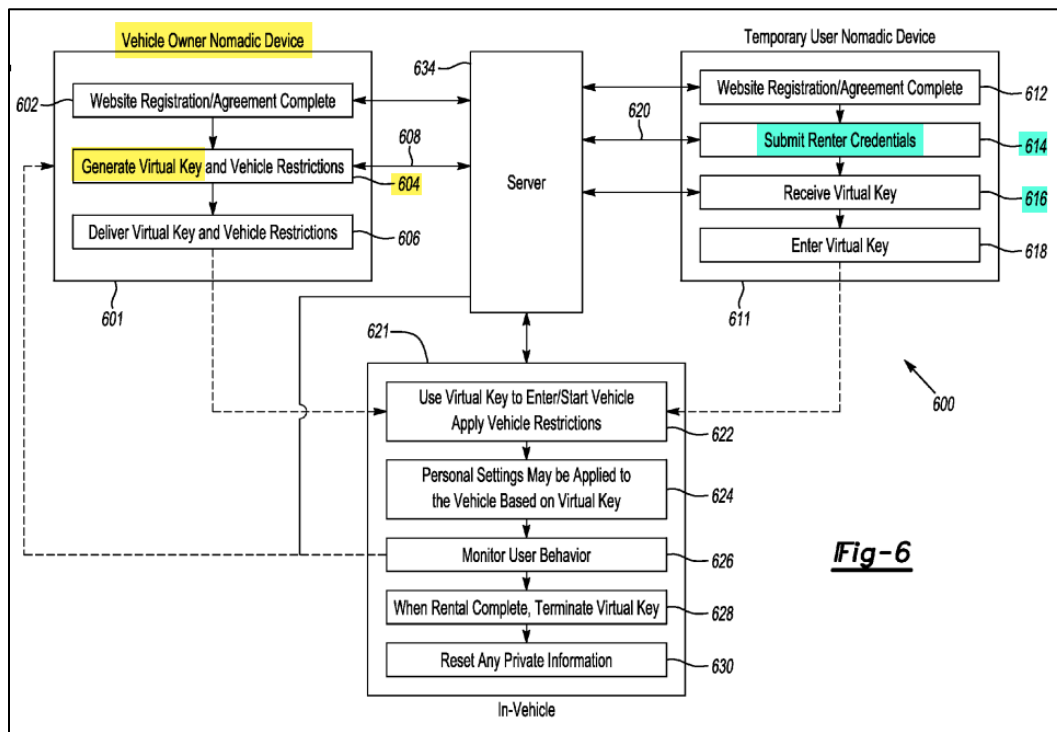
Id., ¶ 47.

As another example, Kleve teaches that before “step 502”—the step in which the vehicle owner may “set up a virtual key”—the Temporary User has “**already setup a user profile** within the database.” *Id.*, ¶ 62. Therefore, the “user profile”—that “include[s]...a matrix barcode”—already exists before the owner may “set up a virtual key.” *Id.*, at ¶ 37; EX2013, ¶ 109. Figure 5 shows that Kleve’s matrix barcode is not “generated by the server,” as Petitioners allege; instead, the **matrix barcode**

While Petitioners cite to paragraph 69 for alleged support that a “server” is used to generate the matrix barcode—this is flatly contradicted by Kleve at paragraph 69 and Figure 6. Pet. 19 (citing EX1005, ¶ 69), 26 (same); EX2013, ¶ 110. As shown in Section III.A.1., Kleve distinguishes between two “exemplary embodiment[s]” of “generating a virtual key.” EX1005, ¶ 69. Kleve is unambiguous that the server is not involved in generating the virtual key for the first embodiment, wherein only “the vehicle owner may generate a virtual key” using a “vehicle owner nomadic device” to generate a virtual key “based on a password that may include a matrix barcode.” *Id.*, ¶ 69, Fig. 6. By contrast, Kleve teaches “another exemplary embodiment of generating a virtual key,” at step 616, that *excludes* any mention of a matrix barcode, and certainly fails to disclose any server generating any matrix barcode. *Id.*, ¶ 69:

[0069] FIG. 6 is an exemplary embodiment of the vehicle rental micro-business distributing and controlling virtual keys using a nomadic device with a vehicle. The vehicle rental micro-business administrative system may consist of a computer system configured to host one or more websites for interaction with a vehicle Owner and Temporary User. In the illustration 600, a server 634 is used to communicate between a vehicle Owner nomadic device 601, a Temporary User nomadic device 611, and a vehicle computing system 621. Using a nomadic device, for example a smart phone, a Temporary User and vehicle Owner may set up user profiles, enter into an agreement and make a payment to initiate the vehicle rental process between the two parties at step 602 and 612. At step 604, the vehicle Owner may then generate a virtual key based on a password generated by the vehicle Owner that may include a matrix barcode or a code word that the Temporary User may enter/send to the vehicle when ready to begin the rental term. Another exemplary embodiment of 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. At step 616, the virtual key is generated and sent to the Temporary User. The Owner may deliver a virtual key to the vehicle for recognizing the Temporary User having authorization to enable a keyless drive-away at step 606.

See *id.*, Fig. 6:



Likewise unavailing is the Petition’s citation to Kleve’s “authorization code,” as Petitioners leave unexplained how this code allegedly satisfies some element of the challenged claim. EX2013, ¶ 111. While Petitioners contend that “[e]ach of Kleve’s requests is associated with a unique access code embedded in a virtual key that can be expressed as a matrix barcode” (Pet. 27), Kleve teaches that its authorization code is simply a code that is (1) manually “typed in a touchscreen” to “authorize” an authorized user, and (2) is separate and apart from Kleve’s “matrix barcode.” EX1005, ¶ 59. Accordingly, Kleve shows this manually-typed code is *not* somehow “embedded” in any virtual key, as Petitioners allege, and Petitioners do not even contend that this manually-inputted code is “a unique access code.” Pet. 27; EX2013, ¶ 110.

In any event, the Petition’s claim 3 challenge fails regardless, as Petitioners do not provide any disclosure that satisfies “a user account having respective privileges assigned by the administrator of the vehicle[.]” Pet. 27; EX1001, claim 3. At most, Petitioners identify a Temporary User’s “user account” and alleged privileges for “the unique access code,” but such allegations—even if true—are insufficient, as the *user account itself* must have “privileges assigned by the administrator[.]” *Id.*; EX2013, ¶¶ 112.

Petitioners failed to show that Kleve discloses the recited elements of claim 3, and therefore claim 3 must be upheld as valid.

B. The Petition’s Ground 3-claim 3 challenge fails because Zaid does not disclose “each request is associated with a unique access code generated by the server,” as recited by claim 3.

First, as established above, Zaid’s vehicle reservation—encrypted or not, or unique or not—is not “a unique access code received by the mobile device from the server,” as required by claim 1. *See* Section III.C.1., *supra*. Second, Zaid’s vehicle reservation is not shown to be “a unique access code generated by the server,” as claim 3 recites. EX2013, ¶¶ 113-116. The Petition mischaracterizes Zaid’s disclosures, telling the Board that “[a]s in 1[e], each vehicle reservation in Zaid is associated with an encrypted unique access code generated by the server ...” Pet. 61. But “as in 1[e]” and 1[f], the Petition is incorrect that Zaid discloses “encrypted ‘vehicle reservations,’ *generated by the server...*” (Pet. 49), and likewise incorrect

that such reservations somehow disclose “*a unique access code generated by the server*,” as the challenged claim requires. *Id.*, ¶ 113. Again, Zaid does not disclose the features of the “unique access code” recited by claim limitations 1[f]-1[i]. See Sections III.C.1.-4., *supra*.

Turning to the Petition’s analysis of claim 1[e], Petitioners “compare” Zaid’s disclosures with the teachings of the ’245 patent, which only highlights the deficiencies of the Petition’s challenge to claim 3. For example, Petitioners point to the ’245 patent’s teaching that “[c]loud services 120 can generate the unique access code which *is then encrypted* in a message and sent as encrypted e-keys 720 to the recipient.” Pet. 49 (citing EX1001, 46:32-35) (emphasis in Petition). Here, Petitioners drive home the point that the function to “generate the unique access code” is a *separate and distinct* function from the next two functions quoted from the specification: (1) the unique access code is “*then encrypted* in a message” and (2) is “sent as encrypted e-keys[.]” *Id.* These distinctions lay bare the deficiencies of Zaid’s disclosures.

As an additional deficiency, the reservation identified by the Petition not a “unique access code generated by *the server*”—*the* server identified for claim 1. EX2013, ¶ 114. For claim 3, Petitioners point to a reservation “booked through one or more social networking websites, such as FourSquare® and Facebook®[.]” where “[a] user must first log into the social networking website before he/she can view the

advertisement and make [a] reservation.” EX1008, ¶ 72; Pet. 61 (citing *id.*). But Zaid provides no disclosure that its server (“*the server*” identified for claim 1) somehow generates the reservation that Zaid describes as “booked” or “ma[de]” through FourSquare® or Facebook®, and Petitioners do not explain how Zaid’s server somehow ***generates a unique access code*** when a user books this Facebook® reservation. Pet. 61. EX1008, ¶ 72; EX2013, ¶ 114.

The fact that Zaid’s server does perform *other functions* is of no utility to Petitioners’ challenge. EX2013, ¶ 115. For example, the Petition cites to paragraph 128, in which Zaid’s system encrypts the message containing a vehicle reservation. Pet. 61 (citing EX1008, ¶128). But this function of encrypting data, as admitted by Petitioners, is *separate and distinct* from the recited function of “generating” the unique access code, as claim 3 requires. Pet. 49 (citing EX1001, 46:32-35).

Likewise insufficient is Zaid’s disclosure that its server “***communicates*** the vehicle reservation to a wireless communication device.” EX1008, ¶126; EX2013, ¶ 115. Again, it is Petitioners who argue that the function to “send” data is *separate and distinct* from the function to “generate” that data. Pet. 49 (citing EX1001, 46:32-35) (“[c]loud services 120 can generate the unique access code which *is then encrypted* in a message and sent as encrypted e-keys...”) (emphasis in Petition).

[0126] At 506, the vehicle reservation is communicated to a wireless communication device of the user. In various embodiments, a central server managing vehicle reservation communicates the vehicle reservation to a wireless communication device of a vehicle user. A wired network, such as the Internet and/or a wireless network, such as cellular network that uses long-range wireless communication link/protocol, can be used to communicate the vehicle reservation. At 508, the wireless communication device receives and caches the reservation. In various embodiments, the wireless communication device decrypt the first layer of encryption encrypted using the public key of the wireless communication device using a locally stored private key of the wireless communication device. In various embodiments, decryption is used to ensure and authenticate that the intended wireless communication device is receiving the vehicle reservation rather than one that intercepts the vehicle reservation. At 510, the wireless communication device establishes a communication link with a vehicle access kit.

EX1008, ¶ 126.

The Petition fails to show that Zaid’s vehicle reservation—encrypted or not—is: (1) a unique access code (Section III.C.1., *supra*), much less (2) “a unique access code generated by the server,” as claim 3 requires. EX2013, ¶ 116.

Accordingly, the Petition’s Ground 3-claim 3 challenge fails. Claim 3 must be upheld as valid.

C. The Petition’s Ground 3-claim 3 challenge fails because Zaid does not disclose “each unique access code is associated with a user account having respective privileges assigned by the administrator of the vehicle,” as recited by claim 3.

As the recited “user account,” the Petition identifies Zaid’s disclosure that a prospective vehicle renter can log into Facebook® or a similar social networking

site, view an ad for a vehicle placed by a vehicle owner, and if interested, the renter can click on that ad and make a reservation. Pet. 61 (citing EX1008, ¶ 72). But Zaid’s Facebook® or similar social networking account has no “respective privileges assigned by the administrator of the vehicle,” as recited by the challenged claim. EX1008, ¶ 72; EX2013, ¶ 117.

While Zaid’s vehicle owner can *advertise* their vehicle on social networking sites, like Facebook®, it is *the renter*—and not the vehicle owner—that “must first log into the social networking website before he/she can view the advertisement and make [a] reservation.” EX1008, ¶ 72; EX2004, 45. Indeed, it is the renter *alone* that makes this reservation using their Facebook® or other social networking account. *Id.* Claim 3 requires the “user account” itself to have “privileges assigned by the administrator of the vehicle,” but Zaid provides no disclosure that the *renter’s Facebook® or other social networking account* has “privileges assigned by” the vehicle owner or any “administrator of the vehicle.” *Id.*; EX2013, ¶ 118.

Petitioners’ argument that the reservation made by the renter is “time-limited,” this does not aid the Petition’s cause. First, assuming this time limitation were a “privilege,” Zaid does not teach that it is the vehicle owner or “administrator” that “assigns” such a “privilege.” EX1008, ¶ 72; EX2013, ¶ 119; see Section III.C.3., *supra*. Zaid teaches that it is only the renter that “make[s]” the reservation and that the reservation itself may be “for a specified time period.” EX1008, ¶¶ 72, 69.

Second, and more fundamentally, the claim requires that *the user account itself* must have “privileges assigned by the administrator of the vehicle,” not merely the reservation, as Petitioners allege. EX1001, claim 3. Here, Zaid offers no disclosure of the renter’s Facebook® or other social networking account itself “having privileges assigned by the administrator of the vehicle,” as the challenged claim requires. EX1008, ¶ 72; EX2013, ¶ 119.

Accordingly, this deficiency provides yet another reason claim 3 must be upheld as valid.

VI. Additional deficiencies of Petitioners’ claim 15 challenge.

Claim 15 requires that “the server is part of *a* cloud processing system and *the* cloud processing system is configured to”: (1) “manage user accounts and” (2) “manage use of said e-key.” EX1001, claim 15. The Petition fails to show that: (a) the server is part of any cloud processing system, much less “part of” (b) *the same* “*the* cloud processing system [] configured to manage user accounts and manage use of said e-key.” EX1001, claim 15; EX2013, ¶¶ 120-123.

Petitioners try to conflate Zaid’s server (Pet. 71-72, citing server functions at EX1008, ¶¶ 125-26, 129-30) with a cloud processing system that manages the user accounts of Facebook®, Foursquare® or similar social networking accounts (Pet. 72, citing EX1008, ¶ 72). The Petition’s challenge to claim 15 fails because Petitioners do not even allege that Zaid’s server is “part of” the same “*the* cloud

processing system” alleged to be managing Facebook® or a similar social networking account—it is not—nor do Petitioners even allege that a POSITA would be motivated to make such a modification. Pet. 71-73. In any event, Petitioners’ challenge also fails because Zaid’s server is not even shown to be part of “a” cloud processing system at all.

A. Petitioners fail to show Zaid’s server is part of any cloud processing system, and therefore cannot meet their burden as to claim 15.

Petitioners allege that “Zaid’s server is part of *a* cloud processing system,” but the relied-upon disclosures do not mention or show that Zaid’s server is part of any cloud processing system. Pet. 71-73 (citing EX1008, Fig. 1); EX2013, ¶ 120. Instead, Zaid’s Figure 1, described at paragraphs 75 and 76, shows that “[t]he wireless communication device is connected *to a data network 114* via a long-range communication link 112,” and the “vehicle reservation is received by the wireless communication device 106 from *a central server 110 sitting on a data network 114* via a long-range wireless communication link 112 or a wired link (not shown).” EX1008, ¶¶ 75-76.

[0075] FIG. 1 is a block diagram illustrating an embodiment of a system 100 for vehicle access control in accordance with some embodiments. In various embodiments, the system for vehicle access control includes a vehicle access component 102 configured to provide access to a vehicle 104 when a vehicle reservation is received from a wireless communication device 106 via a communication link 108.

[0076] The wireless communication device is connected to a data network 114 via a long-range wireless communication link 112, such as cellular communication link and/or satellite communication link. The vehicle reservation is received by the wireless communication device 106 from a central server 110 sitting on a data network 114 via a long-range wireless communication link 112 or a wired link (not shown).

Id. Zaid does not describe this “data network 114” as a cloud processing system, and Petitioners do not even allege that this “data network 114” functions as a cloud processing system. *Id.*; Pet. 71-73; EX2013, ¶ 120. For this deficiency alone, Petitioners’ Ground 3 challenge to claim 15 fails.

B. The identified “cloud processing system” managing Facebook®, Foursquare® and similar social networking accounts is not alleged or shown to be *the same* “the cloud processing system configured to ... manage use of said e-key,” and therefore cannot meet the limitations of the challenged claim.

Petitioners *allege*, though Zaid does not mention, “a cloud processing system is managing the user social media accounts” such as Facebook® and Foursquare®. Pet. 72. What Zaid *does* disclose is that a prospective vehicle renter can log into their own Facebook® or a similar social networking site, view an ad for a vehicle and, if interested, the renter can click on that ad and make a reservation. EX1008, ¶ 72. Zaid

fails to disclose a cloud processing system that is managing Facebook®, Foursquare® and similar social networking accounts, nor does Zaid disclose that this *unmentioned* cloud processing system is somehow “configured to” *both* “manage user accounts *and* manage use of said e-key,” as claim 15 recites. *Id.*; EX1001, claim 15; EX2013, ¶ 121.

Even assuming there is a cloud processing system managing the Facebook® or similar social networking accounts, and even assuming it is “configured to” do so, Petitioners offer no explanation as to how ***that same cloud processing system*** is also “configured to” “manage use of said e-key,” as required by the challenged claim. Pet. 71-73; EX1001, claim 15. Petitioners do not even argue that *the same* “cloud processing system” that is allegedly managing Facebook®, Foursquare® and similar social networking accounts is also “configured to” manage ***the e-key of claim 1***. EX1001, claim 15 (“...manage use of *said* e-key”); EX2013, ¶ 121.

This deficiency is fatal to Petitioners’ challenge to claim 15. Claim 15 must be upheld as valid.

C. Zaid’s server is not “part of” the identified “cloud processing system” managing Facebook®, Foursquare® and similar social networking accounts and therefore Petitioners’ claim 15 challenge fails.

As yet another deficiency, Zaid does not disclose, and Petitioners do not even allege, that Zaid’s server (Pet. 71-72, citing server functions at ¶¶ 125-26, 129-30)

is somehow “part of” the alleged “cloud processing system [] managing the user social media accounts” (Pet. 72, citing EX1008, ¶ 72), as would be required to meet the limitations of claim 15. EX1001, claim 15 (“***the server is part of a cloud processing system*** and ***the*** cloud processing system is configured to manage user accounts ...”).

But even assuming, *arguendo*, Zaid’s server were part of “a” cloud processing system—it is not shown to be—Petitioners still fail to allege that Zaid’s server is “part of” the identified “***the*** cloud processing system [] managing the user social media accounts.” Pet. 72; EX2013, ¶ 122. Accordingly, whether or not “Zaid’s server is part of ***a*** cloud processing system,” as alleged (Pet. 73), and whether or not Zaid discloses a “cloud processing system is managing user accounts”—it does not—Zaid’s server is still not part of the same “***the*** cloud processing system [that] is managing the user social media accounts” for Facebook®, Foursquare®, and similar social networking accounts. EX2013, ¶¶ 122-23. For this reason alone, Petitioners’ challenge to claim 15 cannot be sustained.

Notwithstanding the additional deficiencies recited above, Petitioners still cannot meet their burden to show that Zaid either discloses or renders obvious the limitations of claim 15 because first, Zaid’s server is not part of ***the same*** “the cloud processing system” that “is configured to manage user accounts and manage use of said e-key,” as recited by the claim, and second, Petitioners do not even allege that

a POSITA would be motivated to make such a modification—let alone what motivation would prompt such a modification to Zaid’s system. Pet. 71-73; EX2013, ¶ 123.

Accordingly, the identified disclosures cannot satisfy the limitations of claim 15, requiring that “the server” is “part of” *the same “the* cloud processing system configured to manage user accounts and manage use of said e-key.” EX1001, claim 15. Zaid’s server is not part of the identified “*the* cloud processing system [] managing the user social media accounts” and Petitioners do not allege that it is.

Claim 15 must be upheld as valid.

VII. Conclusion

For the foregoing multitude of reasons, all challenged claims should be upheld as valid.

Dated: June 12, 2026

/Brenda Entzminger/
Brenda Entzminger, Reg. No. 76,896

CERTIFICATE OF WORD COUNT

The undersigned certifies that the foregoing PATENT OWNER'S RESPONSE complies with the type-volume limitation in 37 C.F.R. § 42.24(d). According to the word-processing system's word count, the brief contains 13,995 words, excluding the parts of the brief exempted by 37 C.F.R. § 42.24(a).

Dated: June 12, 2026

/Brenda Entzminger/
Brenda Entzminger
Reg. No. 76,896 (Lead counsel)
Aaron R. Hand
Reg. No. 80,694 (Back-up
counsel)
BUNSOW DE MORY LLP
701 El Camino Real
Redwood City, CA 94063
Telephone: 650-318-6774
Facsimile: 415-426-4744
bentzminger@bdiplaw.com
ahand@bdiplaw.com

Counsel for Patent Owner

CERTIFICATE OF SERVICE

Petitioners have consented to e-mail service in this proceeding. Pursuant to 37 C.F.R. §42.6, the undersigned certifies that, on the date indicated below, a copy of the foregoing document was served by email upon the following counsel at the below email addresses:

Finnegan, Henderson, Farabow, Garrett & Dunner LLP
Joshua L. Goldberg – joshua.goldberg@finnegan.com
James R. Barney - james.barney@finnegan.com
Aidan Skoyles - aidan.skoyles@finnegan.com
Nicholas Eitsert - nicholas.eitsert@finnegan.com

QUINN EMANUEL URQUHART & SULLIVAN, LLP
James M. Glass – jimglass@quinnemanuel.com
Quincy Lu - quincylu@quinnemanuel.com
Joseph Milowic - josephmilowic@quinnemanuel.com

Dated: June 12, 2026

/Brenda Entzminger/
Brenda Entzminger
Reg. No. 76,896 (Lead counsel)
Aaron R. Hand
Reg. No. 80,694 (Back-up
counsel)
BUNSOW DE MORY LLP
701 El Camino Real
Redwood City, CA 94063
Telephone: 650-318-6774
Facsimile: 415-426-4744
bentzminger@bdiplaw.com
ahand@bdiplaw.com

Counsel for Patent Owner