

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 No. IPR2026-00059
U.S. Patent No. 11,104,245

PETITIONERS' REPLY TO PATENT OWNER'S RESPONSE

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. THE CLAIMS ARE OBVIOUS.....	1
A. Grounds 1 and 2: <i>Kleve</i> 's Matrix Barcode is Server-Generated Coded Data that Includes a Unique Access Code, Which Functions as the E-Key	1
1. <i>Kleve</i> discloses a unique access code encoded within its matrix barcode.....	1
2. <i>Kleve</i> 's unique access code functions as the e-key.....	3
3. <i>Kleve</i> discloses access and use privileges set by a server for the unique access code	4
4. <i>Kleve</i> 's administrator restricts the year, make, model, and availability of the rental vehicle; <i>Kleve</i> 's server only sets privileges subject to these restrictions	6
B. Grounds 1 and 2: A POSITA Would Have Combined the Analogous <i>Kleve</i> and <i>Mottla</i> References	8
C. Grounds 3 and 4: <i>Zaid</i> 's Vehicle Reservation is Server- Generated Coded Data that Consists of a Unique Access Code Which Functions as the E-Key.....	10
1. <i>Zaid</i> discloses a unique access code	10
2. <i>Zaid</i> 's time-based privileges are set responsive to the administrator's restricting of vehicle availability	12
D. Grounds 3 and 4: A POSITA Would Have Combined the Analogous <i>Zaid</i> and <i>Mottla</i> References, Which Disclose the Challenged Claims	14
1. <i>Zaid</i> 's decrypted vehicle reservation functions as the e-key	14
2. A POSITA would have combined <i>Zaid</i> and <i>Mottla</i>	15

E.	Grounds 1 and 3: <i>Kleve</i> Discloses a “Camera Capturing Video ... During a Period of Time in Which the Unique Access Code Is to Be Active”	16
F.	EA’s Remaining Arguments	16
1.	Ground 1 addresses Claim 6 in its entirety	16
2.	Claim 6: <i>Kleve</i> discloses sending instructions to the server to enable sharing	17
3.	Claim 6: <i>Zaid</i> discloses sending instructions to the server to enable sharing	18
4.	Claim 3: <i>Kleve</i> ’s matrix barcode and encoded unique access code are generated by the server.....	19
5.	Claim 3: <i>Kleve</i> discloses a user account having privileges assigned by the administrator.....	21
6.	Claim 3: <i>Zaid</i> ’s encrypted vehicle reservation is a unique access code generated by the server	22
7.	Claim 15: <i>Zaid</i> ’s server is part of a cloud processing system.....	23
III.	CONCLUSION.....	25

I. INTRODUCTION

The Board was right to institute *inter partes* review of the challenged claims. Emerging Automotive’s (“EA”) scattershot response fails because it relies on erroneous readings of the art, misrepresents the Petition, and contradicts its own expert. Worse, EA rehashes arguments that that the Board – and Director – already rejected, providing no additional reasoning or even acknowledgement of the Board’s prior decisions. Nothing sticks.

EA’s arguments cannot overcome the plain, express teachings of the prior art disclosing all the claimed features and motivations to combine them as claimed, while establishing a reasonable expectation of success in doing so. The Board should cancel all challenged claims.

II. THE CLAIMS ARE OBVIOUS

A. Grounds 1 and 2: *Kleve*’s Matrix Barcode is Server-Generated Coded Data that Includes a Unique Access Code, Which Functions as the E-Key

1. *Kleve* discloses a unique access code encoded within its matrix barcode

EA argues that “Petitioners point to *Kleve*’s matrix barcode as allegedly satisfying both the ‘coded data’ and the ‘unique access code’ limitations.” POR, 5. Not so. The Petition points to *Kleve*’s matrix barcode as the claimed “coded data.” Pet., 18-20. As EA and Dr. Malek admit, QR codes, like *Kleve*’s matrix barcode, “*store[] information* in a grid of typically black and white squares that can be read

by imaging devices.” POR, 6 (emphasis added).¹ The “unique Temporary User identification” stored in *Kleve*’s matrix barcode is the claimed “unique access code.” Pet., 20 (“The matrix barcode, i.e., coded data, encodes a unique access code within the two-dimensional matrix.”); *see also Kleve*, ¶¶[0037], [0063], [0069]; ’245 patent, 46:33-34 (“the unique access code . . . is then encrypted in a message and sent.”), claim 1 (“coded data . . . include[s] a unique access code”). As EA’s expert admits, for a unique individual, *Kleve*’s temporary user identification would be unique. EX1020, 19:17-20 (“if you're encoding someone's first and last name, date of birth, and the address, very likely that that is unique”).

EA rehashes its failed pre-institution argument regarding *Kleve*’s uniqueness. EA’s argument is a strawman because Petitioners do not contend that the data within *Kleve*’s barcode is unique simply because it is encoded in a QR code. Rather, the information encoded within *Kleve*’s matrix barcode is unique because it is designed to function as a key, and *Kleve* describes it as being unique. *Kleve*, ¶¶[0037], [0063], [0069]. The information encoded within *Kleve*’s matrix barcode, e.g., “unique Temporary User identification,” is the claimed “unique access code.”

EA suggests that *Kleve* discloses an embodiment in which the matrix barcode does not encode the unique Temporary User information. POR, 9-11. This is

¹ All emphasis original unless stated otherwise.

irrelevant, as *Kleve* expressly links the “matrix barcode” to “unique temporary user identification” throughout the reference, and EA’s expert admits that QR codes can be used to represent unique information. *Kleve*, ¶¶[0037], [0063] (“The Temporary User's information for vehicle authorization credential verification 516 may include . . . **matrix barcode . . . or other types of unique** Temporary User identification”) (emphasis added), [0069]; EX1020, 13:9-11. Even if EA’s allegation was correct, it does not nullify *Kleve*’s other disclosures. *Arthrocare Corp. v. Smith & Nephew, Inc.*, 406 F.3d 1365, 1372 (Fed. Cir. 2005) (“[I]t was error for the district court to limit the disclosure of the prior art reference to [one] embodiment.”).

In any event, EA’s allegation that paragraph [0069] “*excludes*” a matrix barcode is incorrect. POR, 11. The language EA highlights in blue specifies that “Temporary User’s credentials” are “unique.” *Kleve*, ¶[0069]. *Kleve* also teaches that “Temporary User's information for vehicle authorization credential” includes a “matrix barcode.” *Kleve*, ¶[0063]. Accordingly, the temporary user data underlying *Kleve*’s matrix barcode is consistently taught to be unique when the reference is read in its entirety.

2. *Kleve*’s unique access code functions as the e-key

According to EA, “*Kleve* [] discourages any ‘unique access code functioning for the e-key’” because “its ‘matrix barcode’ alone is ‘used as the virtual key.’” POR, 12. EA’s constraint, however, is absent from *Kleve*’s disclosure (which never recites

“alone”), contradicts its own expert’s concession (that QR codes, like *Kleve*’s matrix barcode, “store[] information”), and belies *Kleve*’s actual teachings, i.e., that “unique Temporary User identification” is necessary “to validate and pay for the rental service.” *Kleve*, ¶[0037]. As the Petition explained, “‘begin[ning] keyless vehicle rental authorization process’ [] includes receiving a barcode matrix with the unique access code to unlock and use the vehicle.” Pet., 22; *see also* EX1004, ¶122 (“the matrix barcode contains or encodes unique information . . . to ensure that the intended TU is being given access to the vehicle.”) (citing *Kleve*, ¶[0069]).

Kleve teaches that receipt of the matrix barcode involves “scann[ing] by the vehicle” (*Kleve*, ¶[0044])) using a “matrix barcode scanner” (*Kleve*, ¶¶[0066], [0067]), indicating that the matrix barcode is converted or decoded or to reveal its underlying data (i.e., the unique access code) before *Zaid*’s vehicle computer (VCS) “enable[s] the vehicle drive away event.” *Kleve*, ¶[0044]. Indeed, EA’s expert confirms that *Zaid*’s matrix barcode would first need to be converted to its unique access code before it can be interpreted by *Zaid*’s VCS and used as the ekey. EX1020, 17:14-16 (“if it’s already in the computer, it is also in binary format, because every piece of data is in binary format”).

3. *Kleve* discloses access and use privileges set by a server for the unique access code

Petitioners do not “wholly ignore[] the claim’s requirement that the privileges must be ‘*for the unique access code.*’” POR, 14. The Petition explains that “*Kleve*’s

unique access code, encoded within the virtual key . . . is associated with . . . privileges to unlock and drive a vehicle during a time of use.” Pet., 20. Again, *Kleve*’s virtual key (i.e., matrix barcode) *includes Kleve*’s unique access code. Because *Kleve* discloses a car sharing system, its matrix barcode and underlying unique access code limits access to a particular vehicle, for a particular user, for a particular time. *Kleve*’s barcode matrix thus has “privileges” for the unique access code encoded therein.

Further, the Board already concluded in related IPR2024-01167 that “*Kleve* teaches, or at least suggests, that the ‘coded data includes privilege settings . . .’ because [] *Kleve*’s virtual e-key includes a rental period, specifically the start of the rental period, which we find to constitute a privilege setting” *Kia Corp. v. Emerging Auto LLC*, No. IPR2024-01167, Paper 37 at 30 (P.T.A.B. Jan. 26, 2026). This finding clearly establishes that *Kleve*’s privileges, found within the virtual key, are “for the unique access code.” While the Board’s conclusion in IPR2024-01167 concerns the ’659 patent’s “coded data” and not the ’245 patent’s “unique access code,” the coded data is, as EA’s expert puts it, just “a way of encoding” *Kleve*’s unique access code. POR, 8. It follows that, if the matrix barcode “includes a rental period,” the unique access code encoded therein does also. This meets the “privileges for the unique access code” requirement.

Kleve's "privileges are set via the server" (Pet., 21) because the virtual key encoding the unique access code including the privileges is "generate[d]" by the "system" (*Kleve*, ¶[0039]) and "[t]he owner may set user restrictions *by use of the website.*" (*Kleve*, ¶[0040]). Again, the Board already found in IPR2024-01167 that "*Kleve*'s 'virtual key'" originates "from a server" and "includes a rental period, specifically the start of the rental period, which we find to constitute a privilege." IPR2024-01167, Paper 37 at 30. EA provides no reasoning for the Board to depart from these findings.

4. *Kleve*'s administrator restricts the year, make, model, and availability of the rental vehicle; *Kleve*'s server only sets privileges subject to these restrictions

EA acknowledges that *Kleve*'s owner (i.e., administrator) sets up a profile by inputting information including, but not limited to, the make, model, and year of the vehicle available for rent. *See* POR, 16 (reproducing *Kleve*, ¶[0037]). EA does not dispute that *Kleve*'s server will only assign privileges that match the restricted year, make, model, and availability of the vehicle for rent. *Kleve* also discloses that its owner restricts the reservation to a specific vehicle subject to vehicle monitoring. Pet., 21 (citing *Kleve*, ¶¶[0037], [0042], [0053]). *Kleve*'s server will not set access and use privileges for any other vehicle because of the administrator's vehicle restriction. Thus, the "make, model and year of the vehicle available for rent" (POR, 16-17) plainly are restrictions.

Further, EA's step-210/step-214 argument (i.e., that privileges and/or restrictions are set after the virtual key is generated) has already been rejected by the Board because it conflates initial restrictions with a later control operation. *Kia Corp. v. Emerging Auto LLC*, No. IPR2024-00981, Paper 36 at 29-30 (P.T.A.B. Dec. 9, 2025) ("Contrary to Patent Owner's position, it appears that a rental start period is included prior to step 210"). Figure 2 places the owner's vehicle/profile and availability decisions before step 210, where the virtual key is generated and distributed for the approved rental; step 214 then describes additional control during the rental. *Kleve*, Fig. 2. *Kleve* confirms that the owner's make, model, year, and availability information is supplied in the profile, and time-limited privileges are set subject to the owner's make, model, year, and availability restrictions, all before step 214. *Kleve*, ¶¶[0037]-[0038], [0081], [0087] ("The vehicle rental authorization system may allow the Temporary User to be matched with a vehicle based on [] date, [and] scheduled number of hours needed"), [0088], [0090], Fig. 9 (Step 906).

Finally, *Kleve*'s privileges are not "unfettered" because they include a time restriction that "fetters" (limits) the user's access and use of the vehicle. *See Malek Tr.*, EX1020, 80:18-21 ("[I]f you have a time-limited use or access, then that would not be unfettered access, because it's limited by the amount of time that you have access."). Temporary Users have temporary access.

B. Grounds 1 and 2: A POSITA Would Have Combined the Analogous *Kleve* and *Mottla* References

In related IPR2024-00981, the Board already considered the combination presented here and “agree[d] with it.” IPR2024-00981, Paper 36 at 39. EA does not acknowledge the Board’s prior finding and provides no reason for the Board to diverge from that finding. Instead, EA misreads *Mottla* and Petitioners’ combination. *See* Pet., 22-25.

In claim 1, *Mottla* is relied on for its “on-demand unlocking via icon,” i.e., for its graphical user interface. Pet., 22-25. Petitioners do not propose combining *Mottla*’s “reservation” functionality in the proposed combination; only certain components of its GUI. Petitioner never contended that the entirety of *Mottla*’s functionality must be used, for wholesale “substitution of elements” is not required for obviousness. *In re Mouttet*, 686 F.3d 1322, 1333 (Fed. Cir. 2012) (“The test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference”).

Where *Mottla*’s reservation functionality is relied on, Petitioners explained that “[a] POSITA would further have been motivated to combine *Mottla*’s ‘reserve’ **button** to request use of the vehicle to receive an access code because it provides a user-friendly **example of a GUI** for selecting and requesting access to vehicles on a map.” Pet., 30 (emphasis added). Further, “**adding simple UI elements to a smartphone app** was well within the abilities of a POSITA.” Pet., 31 (emphasis

added). That is, *Mottla* is relied on for its reservation “button,” “GUI,” and “simple UI elements,” not any “direct ‘reserve’ actions.” Pet., 30-31. Indeed, *Kleve* teaches its own reservation scheme that discloses the claimed elements. The only element that *Kleve* does not explicitly disclose is the *graphical* portion of the user interface. See Pet., 14. In 2013, years after smartphone applications with GUIs had become commonplace, a POSITA would have easily been able to implement *Mottla*’s GUI elements on *Kleve*’s smartphone application. See Malek Tr., EX1020, 48:9-11 (“[Y]ou would expect in 2014 to involve a graphical user interface.”).

Next, EA and Dr. Malek fault Dr. Almeroth for not “explain[ing] how to combine *Kleve*’s matrix barcode with *Mottla*’s graphical user interface inputs, such that the barcode is being managed by some graphical user interface inputs.” EX2013, ¶[0062]. But no modification to *Kleve*’s matrix barcode is necessary because the combinations only propose on-demand unlocking “*after* the virtual key has been scanned and authorized.” Pet., 25 (emphasis added). The proposed handoff is sequential: (1) the Temporary User presents and scans *Kleve*’s matrix barcode; (2) the VCS decodes and authorizes it, establishing the rental/session; and (3) the combined mobile application presents *Mottla*’s GUI, whose lock/unlock input is relayed through *Kleve*’s existing communications to the VCS. *Kleve*, ¶[0061]. The GUI therefore acts on the authorization established by the scan; it does not rewrite the barcode, replace it, or supply a competing credential. This preserves *Kleve*’s

security while adding *Mottla*'s convenient controls, similarly to the '245 patent's disclosure that the device transfers the encrypted e-key and then accesses the vehicle. '245 patent, 45:3-20 (Bob's device "transfer[s] the encrypted e-keys 720 to the vehicle" (i.e., scans *Kleve*'s matrix barcode) and Bob's device "can now access the vehicle" (i.e., use *Mottla*'s GUI for the rental duration)).

There is no reason that *Kleve*'s matrix barcode-initiated functions could not have been implemented with *Mottla*'s GUI-based functionality. To be sure, *Mottla* is assigned to ZipCar, which allowed users to unlock vehicles by scanning their "access card" and utilizing the GUI on their mobile phone. *Mottla*, ¶[0004].

C. Grounds 3 and 4: *Zaid*'s Vehicle Reservation is Server-Generated Coded Data that Consists of a Unique Access Code Which Functions as the E-Key

1. *Zaid* discloses a unique access code

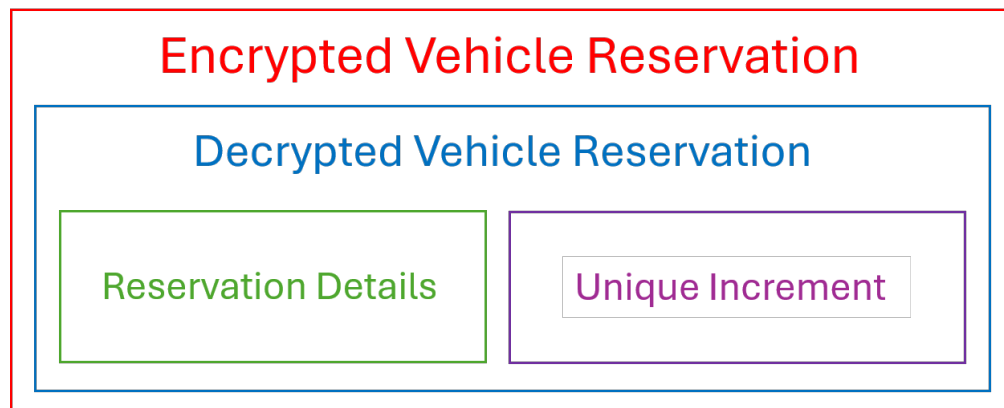
EA contends that *Zaid*'s unique access code is not "received by the mobile device from the server" because the encrypted vehicle reservation is decrypted using locally stored private keys. POR, 36. But the claim language does not require that the vehicle reservation is *decrypted* at the server, only that it is *received* from the server. EA admits that the encrypted vehicle reservation includes the decrypted vehicle reservation. POR, 39 (depicting "Reservation" within "Encrypted Message"). *Zaid* makes clear that the "central server managing vehicle reservation communicates the [encrypted] vehicle reservation to a wireless communication

device of a vehicle user.” *Zaid*, ¶[0126]. Thus, the decrypted vehicle reservation within the encrypted vehicle reservation is also communicated from the central server to the user’s communication device. Nothing more is required. Indeed, this is the same scheme disclosed in the ’245 patent. *See* ’245 patent, 3:2-12.

EA next argues that *Zaid*’s decrypted vehicle reservation is not a unique access code because it is not unique. POR, 36-40. EA bases its entire uniqueness argument on the belief that the unique increment is not included in *Zaid*’s vehicle reservation. POR, 38. But *Zaid* cannot be any clearer: “the vehicle reservation includes a unique increment,” *Zaid*, claim 21.

EA’s expert admits that, if “the message itself [] has the unique increment . . . [it] is unique.” EX2013, ¶79; *see also* EX1020, 76:13-17 (conceding that the “overall message would be unique if the unique increment is unique.”). Dr. Malek also opines that “encryption . . . merely converts the message from one form to another” (EX2013, ¶66), indicating that the decrypted vehicle reservation must include the unique increment that is included in the encrypted vehicle reservation. *See also* EX1020, 69:17-19 (“[W]hen you encrypt a unique number and then you decrypt the encrypted unique number, then you’re going to get back the same unique number.”). Because the encrypted vehicle reservation (i.e., coded data) includes a unique increment, which Dr. Malek admits renders the encrypted vehicle reservation unique, and the decrypted vehicle reservation (i.e., unique

access code) includes this “same number,” also admitted by Dr. Malek, the decrypted vehicle reservation must also be unique. Indeed, since *Zaid* (like *Kleve* and *Mottla*) discloses a car sharing system providing access to a particular vehicle, to a particular user, for a particular time, the vehicle reservation providing that access would also be unique:



Further, *Zaid*’s system could not possibly differentiate one decrypted vehicle reservation from another, such as to apply privileges, if reservations were not unique. Nonunique reservations would permit vehicles to be accessed by unauthorized users. EA’s read of *Zaid*’s disclosure renders the disclosed system unworkable, an interpretation which no POSITA would take.

2. *Zaid*’s time-based privileges are set responsive to the administrator’s restricting of vehicle availability

EA argues that *Zaid*’s privileges are not “responsive to a restriction set by an administrator of the vehicle” because “‘access’ is not a ‘privilege’ under the district court’s construction.” POR, 42. As explained in the Petition, *Zaid*’s access is

constrained or “*fettered*” by a specific time in which access is allowed. Pet., 53 (quoting *Zaid*, ¶[0069]). And as conceded by EA’s expert, time-limited access is a privilege. EX1020, 80:18-21.

EA further argues that “the owner or ‘administrator’ is [never] involved in the reservation’s ‘specified time period.’” POR, 43. The claim language, however, only requires that the “privileges [are] set [] responsive to *a restriction set by an administrator* of the vehicle.” EX1001, 52:21-22 (emphasis added). As the Petition makes clear, and as Dr. Malek admits, *Zaid* discloses a vehicle-availability restriction separate from the time-based privileges. Pet., 54 (citing *Zaid*, ¶[0079]); EX1020, 81:17-21 (“[T]he owner decides when the car is available for rent.”). Specifically, *Zaid*’s vehicle owners tell the server when the vehicles are available, i.e., when the time-based access and use privileges can be active. Pet., 54 (citing EX1004, ¶226).

Contrary to EA’s allegation that “the owner making a ‘vehicle availability’ update is just an advertisement or announcement” (POR, 43), *Zaid* actually teaches that “the dynamically updated vehicle location and availability information are *used by the backend vehicle sharing system to register the vehicle as available for sharing.*” *Zaid*, ¶[0079] (emphasis added). *Zaid* discloses that the “vehicle reservation system . . . retrieve[s] the list of nearby places (e.g., that the vehicle will be located or available for sharing),” indicating that *Zaid*’s reservation, and time-

based privileges, are set responsive to the administrator's vehicle availability restriction. *Zaid*, ¶[0078] (emphasis added). Nothing more is required.

D. Grounds 3 and 4: A POSITA Would Have Combined the Analogous *Zaid* and *Mottla* References, Which Disclose the Challenged Claims

1. *Zaid*'s decrypted vehicle reservation functions as the e-key

EA alleges that *Zaid*'s private key does not satisfy "the unique access code functioning for the e-key." POR, 44-45. This is irrelevant because the Petition mapped *Zaid*'s decrypted vehicle reservation to the "the unique access code," not solely the "private key." Pet., 52.

As cited in the Petition (Pet., 54), the '245 patent's own prosecution history explains that *Zaid*'s "server transmits the unique access code to the user's wireless device and then the user's wireless device transmits the unique access code to the vehicle to unlock and to operate the vehicle." EX1002, 124. The Petition further explains how *Zaid*'s unique access code would be managed via *Mottla*'s GUI. Pet., 58; *see also* Almeroth, ¶235. The Petition repeatedly explains how *Zaid*'s decrypted vehicle reservation functions as the e-key. *See, e.g.*, Pet., 51 (citing *Zaid*, ¶¶[0067], [0129]), 52 ("[T]he vehicle reservation is *decrypted* and authenticated at the vehicle access control system. At 604, *vehicle access is granted*." (quoting *Zaid*, ¶[0129]); *see also* *Zaid*, ¶[0090]. The limitation requires nothing more.

2. A POSITA would have combined *Zaid* and *Mottla*

EA questions “why *Zaid*’s operations for unlocking the vehicle somehow ‘[in]conveniently control the vehicle’” such that a POSITA would look to *Mottla* for improvement, and reiterates the same arguments “discussed in Section III.A.5.” POR, 46.

EA misinterprets the proposed combination. The proposed combination uses one element from *Mottla*: the “GUI[,] such that *Zaid*’s wireless device *provides graphics* for vehicle control.” Pet. 58 (emphasis added). Petitioners do not suggest replacing *Zaid*’s “operations for unlocking the vehicle” with those disclosed in *Mottla*. *Zaid*’s unlocking operation already discloses those claim limitations. Pet., 49-52; *Zaid*, ¶[0100] (“unlock doors, start engine, and/or other commands”); IPR2024-00785, Paper 13. In other words, *Zaid* *only* does not *explicitly* state that its mobile device “performs this unlocking function” *graphically*, i.e., rather than using text.

To answer EA’s question, *Mottla*’s GUI would be more convenient than a text-based interface because “unlocking via icon gives the user better control over vehicle access, and using an unlock icon (instead of text) is more user-friendly.” EX1004, ¶235. A POSITA would have easily replaced *Zaid*’s mobile interface with *Mottla*’s “because GUI icons were standard and implementation was within a

POSITA’s capabilities.” Pet., 58-59; *see also* EX1020, 48:9-11 (EA’s expert admitting the same).

E. Grounds 1 and 3: *Kleve* Discloses a “Camera Capturing Video ... During a Period of Time in Which the Unique Access Code Is to Be Active”

Concerning both the *Kleve* and *Zaid*-based grounds (Grounds 1 and 3), EA argues that “[t]he Petition does not demonstrate . . . a ‘period of time in which the unique access code is to be active[.]’” POR, 32-33. The Petition, relying on the disclosures of *Kleve* in both grounds, demonstrates that *Kleve*’s camera captures video of the vehicle “interior” (*Kleve*, ¶¶[0042], [0073]) and temporary user “continuous[ly]” (Pet., 21 (quoting *Kleve*, ¶[0076]); Pet., 55) while they operate the vehicle, which would necessarily include “time in which the unique access code is to be active,” and that “[d]ata is collected while the unique access code is active, because it occurs while the [TU] uses the vehicle, i.e., the time when the unique access code is active” (Pet., 22 (citing *Kleve*, ¶¶[0079], [0080]); Pet. 55). EA ignores this evidence.

F. EA’s Remaining Arguments

1. Ground 1 addresses Claim 6 in its entirety

The Petition addresses claim 6 in its entirety. *See* Pet., ix (List of Challenged Claims). Claim 6 depends from claim 1, so its repeated e-key/GUI relationship in

6[b] carries forward the mapping already made for claim 1[i]. Petitioners need not restate identical evidence in full for a dependent claim.

Specifically, the petition explains how the combination of *Kleve* and *Mottla* discloses “wherein the e-key has functions enabled via graphical user interfaces of the application of the mobile device” (EX1001, 52:58-59), mapping that functionality to *Mottla*’s GUI illustrating on-demand unlocking via an icon. Pet., 22-25 (“A POSITA would have been motivated to incorporate *Mottla*’s GUI into *Kleve* by the benefits of a user-friendly GUI, as *on-demand unlocking via icon* gives the user better control over vehicle access, and using an unlock icon (instead of text) is more user-friendly.”). Nothing more is required by this language of claim 6.

Further, in the *Zaid*-based ground (Ground 3), the Petition expressly addresses this language of Claim 6, relying on the same elements of *Mottla*. EA does not dispute that this subject matter is disclosed by *Mottla*.

2. Claim 6: *Kleve* discloses sending instructions to the server to enable sharing

For Ground 1, EA alleges that “Petitioners do not even mention or address the claim’s requirement that an application is ‘*configured to enable sending instructions to said server.*’” POR, 51. But the Petition explains that *Kleve*’s “TU uses the application to ‘input profile information’ ‘including details about the vehicle he intends to rent’” which is stored in, i.e., sent to, “‘the vehicle rental authorization system,’” a server. Pet., 32; *Kleve*, ¶[0035] (“Such a system may include . . . a remote

computing system (e.g., and without limitation, a server)"). *Kleve*'s server uses the TU's instructions to "begin the keyless vehicle rental authorization process without [TU] physically meeting the owner." Pet., 32 (citing *Kleve*, ¶[0090]). EA never explains what more it believes is required by "to enable sharing said vehicle with the user to enable use of the e-key." Nothing more is. See *ParkerVision, Inc. v. Qualcomm Inc.*, 903 F.3d 1354, 1361 (Fed. Cir. 2018).

EA resorts to tacit claim construction to distinguish the art, arguing that "the identified application [is not] 'configured to enable' sending *the kind* of 'instructions' to said server" POR, 51. But the claim does not require a specific "kind" of instructions. Because EA has not identified any disclaimer of claim scope or even enlightened the Board as to what "kind" of instruction it believes is required, the Board should decline to construe this claim narrowly.

3. Claim 6: *Zaid* discloses sending instructions to the server to enable sharing

For Ground 3, EA restates the same arguments as above, arguing that *Zaid* is not "configured to" send the right "kind" of instructions to the server. POR, 54. But, as the Petition explains, *Zaid*'s "vehicle reservation application enables 'communicat[ion] with backend server(s)' to permit vehicle 'sharing.'" Pet., 65 (quoting *Zaid*, ¶¶[0077], [0080]). Further, *Zaid*'s "vehicle reservation is 'booked at the server 110 via a user interface' . . . for providing access and usage via an electronic key." Pet., 65 (quoting *Zaid*, ¶¶[0077], [0080]).

Indeed, EA even admits that “Zaid makes explicit that the ‘vehicle reservation **application**’ ‘enables a vehicle user (e.g., renter and owner) to communicate with [i.e., send instructions to] 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**,” which enables sharing of the vehicle and use of an e-key. POR, 56 (emphasis added). EA never explains what more it believes is required by the claim. The plain language is met.

4. Claim 3: *Kleve*’s matrix barcode and encoded unique access code are generated by the server

EA alleges that *Kleve*’s matrix barcode is not “***generated by the server***” because it “***already exists***” before *Kleve*’s vehicle rental micro-business begins. POR, 60-1. As explained, it is the data encoded within *Kleve*’s barcode, and not the barcode itself, that corresponds to the claimed unique access code. In any event, both the matrix barcode and underlying data are generated by the server. EA’s position contradicts *Kleve*, the Board’s prior findings, and its own expert.

EA has already raised its timing argument, and lost, on three occasions. First, in IPR2024-00981, EA argued that the “e-key is generated and distributed” before “any alleged ‘restrictions’” are requested. IPR2024-00981, Paper 36 at 25 (citing Paper 16 at 4). The Board disagreed, finding that “the virtual key is only generated ***after*** the Vehicle Owner has ‘already setup a user profile’” (*id.* at 28 (emphasis added)) and ultimately concluding that *Kleve* discloses “generating, by the server,

the e-key” (*id.* at 33-36). Similarly, in IPR2024-01167, EA argued that *Kleve*’s virtual key is “already generated” prior to setting of the rental period. IPR2024-01167, Paper 37 at 29 (citing Paper 17 at 44-45). The Board again disagreed: “*Kleve* specifically teaches that ‘[t]he Owner and Temporary User may agree to terms and conditions for the rental period,’ *after which its ‘system may generate a virtual key to distribute to the Temporary User and VCS.’*” *Id.*, 31-32 (emphasis added); *see also id.* at 30 (“[W]e are persuaded that *Kleve*’s ‘virtual key’ is coded data because it is wirelessly communicated from a server to a Temporary User’s nomadic device in an encrypted format.”). And third, EA again raised this argument in a Request for Director Review, which was denied. IPR2024-00981, Paper 39. Indeed, *Kleve* makes clear that “the system may generate a virtual key to distribute to the Temporary User and VCS.” *Kleve*, ¶¶[0039], [0044], [0048], [0069]. While *Kleve* may disclose using barcodes for other purposes, “mere disclosure of alternative designs does not teach away.” *In re Fulton*, 391 F.3d 1195, 1201 (Fed. Cir. 2004).

Additionally, *Kleve*’s teaching of generating a virtual key on its server does not “*exclude[]* any mention of a matrix barcode,” as EA states. POR, 64. The very paragraph that EA relies on explicitly *includes* “other type[s] of unique Temporary User identification,” (*Kleve*, ¶[0069]) which “may include . . . [a] **matrix barcode** (ex. two-dimensional code)” (*Kleve*, ¶[0063]) (emphasis added).

The unique access code within *Kleve*'s matrix barcode is also generated by the server because it based on information "input[] into the website" (*Kleve*, ¶[0037]) for future reading by the VCS computer (*Kleve*, ¶[0044]). Indeed, EA's expert confirms that this unique access code would be "in binary format, because every piece of data [read by a computer] is in binary format." EX1020, 17:14-16. No POSITA would have read *Kleve* to require its users to generate and input their own binary code, as EA suggests. *Kleve*'s server plainly accomplishes this task.

5. Claim 3: *Kleve* discloses a user account having privileges assigned by the administrator

PO acknowledges that "Petitioners identify a Temporary User's 'user account'" but dispute whether "the *user account itself*" has "privileges assigned by the administrator[.]" POR, 67. The Petition explains that "[t]hrough website accounts, [users] negotiate conditional rental agreements." Pet., 9. This includes a "rental period . . . assigned by the vehicle owner" to a specific renter. Pet., 27 (citing *Kleve*, ¶[0039]). Because the rental agreement is "negotiated" through the user account (profile), it follows that the rental period would be including in the user account. To be sure, *Kleve* notes that "[t]he user profile" (i.e., account) includes "details about the vehicle [the TU] intends to rent," suggesting that the account includes the rental time limitation. *Kleve*, ¶[0086].

6. Claim 3: *Zaid*'s encrypted vehicle reservation is a unique access code generated by the server

Concerning claim 3, EA disputes whether *Zaid*'s unique access code is “generated by the server.” POR, 68-69. But EA's argument addresses the wrong object. Petitioners identify the unencrypted vehicle reservation as the unique access code generated by the server; the encrypted reservation is the coded data. *See, e.g.*, Pet., 52 (“[T]he [unencrypted] vehicle reservation . . . was generated by the server and encrypted *after* the reservation was booked.”) (emphasis added).

Specifically, at step 502, the reservation is booked at the central server; that booking creates the unencrypted reservation. *Zaid*, ¶¶[0072], [0125]. At step 504, the central server encrypts that already-booked reservation, and at step 506 the server communicates the encrypted reservation to the wireless device. *Zaid*, ¶¶[0125]-[0126], Fig. 5; *see also* EX1020, 62:15-24 (admitting that this sequence is disclosed). Thus, the server generates the unencrypted reservation (i.e., the unique access code) while the later encrypted form is the coded data for transmission. *Zaid*, claim 21, ¶[0130]; *see also* Malek Tr., EX1020, 67:17 (“Encrypted data can be coded data.”). EA's belated construction of “encrypt” is irrelevant, and EA's representation that this impermissibly narrow construction is “admitted by Petitioners” is incorrect.

Further, *Zaid*'s owner's retained “control” operates on the user, not merely on an abstract reservation. *Zaid*'s renter first logs into a social-networking account and requests the vehicle, but the owner retains control over “the type of user the owner

is lending/sharing/renting vehicle to.” *Zaid*, ¶¶[0072], [0097], [0114]; EX1004, ¶¶276, 289. The owner’s acceptance of the user is the gate that allows the server to activate the requested duration and issue the reservation/access code for that identified user. Because the account supplies the identity being approved—and *Zaid* tracks the user’s driving history and reputation—the resulting time-limited access and use privileges are assigned to the user account; the reservation is the mechanism through which that account exercises them. *See* Pet., 61; EX1004, ¶¶247-248.

EA’s account-versus-reservation objection therefore misses the sequence *Zaid* discloses. The logged-in account identifies the renter; the owner’s acceptance determines whether that account may use the vehicle and for what duration; and the server’s reservation/access code implements that account-level authorization. Pet., 61; EX1004, ¶¶247-248. Nothing in claim 3 requires a particular implementation or excludes privileges implemented through a reservation tied to the approved account.

7. Claim 15: *Zaid*’s server is part of a cloud processing system

First, EA argues that *Zaid*’s server is not a part of a cloud processing system. POR, 75-76. As explained in the Petition, *Zaid*’s Server 110 is connected to Network 114, which is purposefully depicted as a cloud, i.e., a cloud processing system. Pet., 72-73 (“showing ‘Network’ in cloud”). EA ignores this disclosure, never addressing *Zaid*’s figure 1.

EA also ignores the '245 patent's broad definition of "cloud processing system": a "network . . . virtual or physical" that "facilitate[s] communication." '245 patent, 11:61-12:3. *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1316 (Fed. Cir. 2005) ("claims must be . . . consistent with the specification, of which they are a part") (citations omitted); *see also* Malek Tr., EX1020, 83:15-91:18 (being unable to define the boundaries of "cloud computing system"), 91:24-93:19 (being unable to decipher what the "cloud" icon in *Zaid*'s figure 1 indicates).

Zaid's "data network 114" facilitates communications between the vehicle, the user's device, and the server system using, for instance, a "cellular communication link." *Zaid*, ¶[0076] ("a central server 110 sitting on a data network 114"), Fig. 1. *Zaid* also stresses "Internet connectivity" (*Zaid*, ¶[0092]) and explains that "the Internet . . . can be used to communicate the vehicle reservation" (*Zaid*, ¶[0126]). This limitation is clearly met.

EA next contends that "Petitioners offer no explanation as to how *that same cloud processing system* is also 'configured to' 'manage' use of said e-key" (POR, 75) and that "*Zaid*'s server is [not] 'part of' the [identified] 'cloud processing system [] managing the user social media accounts.'" POR, 75-76. The Petition, however, explains that "*Zaid*'s server is part of a cloud processing system" (Pet., 73), for instance, the internet, and "manag[es the] vehicle reservation" (Pet., 71-72). *See also Zaid*, ¶¶[0125-26], [0130]. Indeed, *Zaid* explains that "the vehicle reservation

system is configured to . . . retriev[e information] directly from a social network.”

Zaid, ¶[0078]. Because the key management and social media servers are on same cloud network (e.g., the internet), they are part of the same cloud processing system.

The claim is met.

III. CONCLUSION

For these reasons, the Board should find the challenged claims unpatentable.

Respectfully submitted,

Dated: September 4, 2026

By: /Joshua L. Goldberg/
Joshua L. Goldberg, Reg. No. 59,369
Counsel for Petitioner Toyota

CERTIFICATE OF COMPLIANCE

Pursuant to 37 C.F.R. § 42.24(c)(1), the undersigned hereby certifies that the foregoing PETITIONERS' REPLY TO PATENT OWNER'S RESPONSE contains 5,585 words, excluding the parts exempted under 37 C.F.R. § 42.24(c), as measured by the word-processing system used to prepare this paper.

Dated: September 4, 2026

/Joshua L. Goldberg/
Joshua L. Goldberg, Reg. No. 59,369
Counsel for Petitioner Toyota

CERTIFICATE OF SERVICE

The undersigned certifies that a copy of the foregoing **PETITIONERS’
REPLY TO PATENT OWNER’S RESPONSE** was served on September 4, 2026
via email directed to counsel of record for Patent Owner at the following.

Lead Counsel	Backup Counsel
Brenda Entzminger (Reg. No. 76,896) bentzminger@bdiplaw.com BDIP_EmergingAuto@bdiplaw.com BUNSOW DE MORY LLP 701 El Camino Real Redwood City, CA 94063 Telephone: 650-351-7248 Facsimile: 415-426-4744	Aaron R. Hand (Reg. No. 80,694) ahand@bdiplaw.com BUNSOW DE MORY LLP 701 El Camino Real Redwood City, CA 94063 Telephone: 650-351-7248 Facsimile: 415-426-4744

Dated: September 4, 2026

By: /Daniel E. Doku/
Daniel E. Doku
Senior Litigation Paralegal
FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, LLP