



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
90/019,456	03/25/2024	11738659	185945.012900	7946
25920	7590	02/11/2025	EXAMINER CARLSON, JEFFREY D	
PENILLA IP, APC - PATENT LAW 5619 Scotts Valley Drive SUITE 280 Scotts Valley, CA 95066			ART UNIT	PAPER NUMBER
			3992	
			MAIL DATE	DELIVERY MODE
			02/11/2025	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

DO NOT USE IN PALM PRINTER

(THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS)

GREENBERG TRAUIG (NJ)
500 CAMPUS DRIVE, SUITE 400
P.O. BOX 677
FLORHAM PARK NJ 07932

***EX PARTE* REEXAMINATION COMMUNICATION TRANSMITTAL FORM**

REEXAMINATION CONTROL NO. 90/019,456.

PATENT UNDER REEXAMINATION 11738659.

ART UNIT 3992.

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above identified *ex parte* reexamination proceeding (37 CFR 1.550(f)).

Where this copy is supplied after the reply by requester, 37 CFR 1.535, or the time for filing a reply has passed, no submission on behalf of the *ex parte* reexamination requester will be acknowledged or considered (37 CFR 1.550(g)).

/JDC/

PTOL-465 (Rev.07-04)

EX PARTE REEXAMINATION OFFICE ACTION

The present reexamination proceeding, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA¹.

This is a reexamination of US Patent 11,738,659 (“the patent”). The Decision on Request mailed 4/15/2024 indicated that a substantial new question of patentability affecting patented claims 1–21 of the patent was raised by the request.

On 12/4/2024 Patent Owner filed arguments (“Remarks”) and a declaration by Dr. Sam Malek (“Malek Dec.”). These arguments and declaration have been considered in their entirety. Patent Owner has not proposed any claim amendments. Accordingly, claims 1–21 are pending in this reexamination.

Citations to the McNair declaration have been removed as they are not required for the thrust of the obviousness rejections provided previously and maintained in this action. Examiner does not necessarily disagree with any particular portion of the McNair declaration.

Priority

The patent (US Patent 11,738,659) resulted from application 17/461,959, filed 8/30/2021. This application includes a chain of domestic priority back to an earliest date of 4/22/2011. In this chain is application 14/063,638, filed 10/25/2013 which was a CIP of 13/842,158, filed 3/15/2013. The claims of the patent under reexamination here include subject matter first introduced in the ‘638 application and are therefore being examined with a benefit date no earlier than 10/25/2013. Furthermore, this reexamination proceeding is being examined under the first

¹ In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis (i.e., changing from AIA to pre-AIA) for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

inventor to file provisions of the AIA².

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

If Patent Owner argues that the claims are fully supported by a filing date earlier than 10/25/2013, a full mapping of each claim limitation to specific citation(s) in such a disclosure should be made of record.

Patent Owner “does not seek to traverse any prior art currently of record based on priority” (Remarks p. 3).

Claim Rejections - 35 USC § 103

In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis (i.e., changing from AIA to pre-AIA) for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

The following is a quotation of 35 U.S.C. 103 which forms the basis for all obviousness rejections set forth in this Office action:

A patent for a claimed invention may not be obtained,
notwithstanding that the claimed invention is not identically disclosed

² MPEP 2159 states: “AIA 35 U.S.C. 102 and 103 apply to any patent application that contains or contained at any time a claim to a claimed invention that has an effective filing date that is on or after March 16, 2013.”

as set forth in section 102, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1, 2 and 5–10 are rejected under 35 U.S.C. 103 as being unpatentable over US 2013/0099892 (Tucker) and US 2008/0275604 (Perry).

1. A sub-system of a vehicle, the vehicle having an on-board computer interfaced with the sub-system for processing instructions to enable use of an electronic key (eKey), the sub-system comprising:

Tucker's "vehicle access control system" is a sub-system of a "vehicle 106" having a "controller 304" that interfaces with various subsystems including components of the vehicle access control system, where the controller "can include one or more processors (e.g., microprocessors or microcontrollers) configured to execute machine-readable instructions," including those that enable the use of an electronic key (eKey), i.e., the vehicle access credential; see Ex. 1008 (Tucker), ¶¶ [0025], [0048], [0050], [0082]-[0083], [0106]-[0108], FIGS. 1, 3.

memory associated with the on-board computer of the vehicle having program instructions for instructing unlocking and starting of the vehicle; and

Tucker's "storage module 306" is memory and is associated with Tucker's controller because the controller is connected to it and able to execute "various software programs residing on storage module 306," including performing "various vehicle-related operations," which Tucker defines as including unlocking "a vehicle's doors," and "start[ing] a vehicle's engine," Ex. 1008 (Tucker), ¶¶ [0025], [0050], FIG. 3 (storage 306 associated with controller 304).

communications circuitry of the vehicle interfaced with the on-board computer of the vehicle and the sub-system,

Tucker's "Bluetooth module 302" is communications circuitry of vehicle (300) and is interfaced with the on-board computer-i.e., Tucker's controller 304—and Tucker's subsystem—i.e., "vehicle access control system," Ex. 1008 (Tucker), FIGS. 3 & 4, ¶¶ [0050], [0051], [0067], [0076] (describing Bluetooth and use of Bluetooth to perform vehicle-related operations).

the communications circuitry is configured to process program instructions to enable communication with a server,

Tucker's "Bluetooth circuitry 402," which is part of the "Bluetooth module 302," is configured to process program instructions because it includes "hardware and/or software elements" to enable Bluetooth communications, Ex. 1008 (Tucker), ¶¶ [0053]-[0054], FIGS. 3-4.

Tucker does not explicitly describe a configuration to enable communication with a server. Tucker does however provide the primary user (e.g. owner) with "operating and location information" including "movement", "vehicle-related operations accessed", "GPS coordinates", "speed information" etc., collected while the vehicle is in use by a secondary user (see ¶¶ 0094, 0110). This vehicle usage information "can be transmitted in any suitable manner" (Tucker ¶ 0110).

Perry monitors vehicle use and provides customized vehicle functions including:

"selectively monitoring one or more vehicle systems is disclosed herein and includes recognizing, at the vehicle, an activation device that is configured to trigger predetermined settings for the one or more vehicle systems. The telematics unit transmits to a secure server a signal indicative of the fact that the activation device is in use." (Perry ¶ 0003).

"the primary user may request that particular setting(s) (e.g., limitations on vehicle systems) be linked to secondary activation devices 76. It is to be understood that the settings for the secondary activation device 76 may be selected with a particular secondary user (e.g., a teenager, a disabled user, etc.) in mind. Secondary activation devices 76 may also be keys or key fobs, however, when these devices

76 are recognized by the vehicle 12, programs for setting the operating ranges are not accessible. Furthermore, when the secondary activation device 76 is recognized by the vehicle 12, settings that have been associated with the device 76 are triggered in the vehicle 12” (Perry ¶ 0022).

Perry uses activation devices (e.g. electronic key fobs) to access and operate a vehicle and monitors the usage of a vehicle when a secondary activation device is used by a secondary user (e.g. teenager, valet, etc.) with limitations on vehicle operation privileges (maximum speeds, geographics locations, etc.). Ex. 1009 (Perry), ¶¶ [0019]-[0020], [0023], [0054]-[0055].

Perry also describes techniques for monitoring usage of the vehicle over the Internet when, for example, a valet is using the vehicle. Ex. 1009 (Perry), ¶¶ [0023] (referring to “VALET KEY”), [0054]-[0055] (describing monitoring of vehicle operation when “secondary activation device” is being used to access the vehicle).

When Perry’s secondary key is being used, the telematics unit contacts a “secure server 72,” which determines whether the key being used to access the vehicle is a secondary key, returns an “encrypted identifier 38,” which, if deemed authentic activates outside access to the secure server to allow the owner of the vehicle to track usage of the vehicle via the Internet. See, e.g., Ex. 1009 (Perry), ¶¶ [0055]-[0056], [0061] (“Once the user's account is accessed, the user may monitor the vehicle location via the Internet-enabled program that is operatively connected to the secure server 72.” Id, ¶ [0061]. Perry discloses a “telematics unit 18” of a vehicle that can “send and receive radio transmissions from wireless carrier system 40,” to allow for vehicle tracking data to be provided to “secure server 72;” Ex. 1009 (Perry), ¶¶ [0002], [0014], [0045].

It would have been obvious to one of ordinary skill before the effective filing date to have modified Tucker's Bluetooth module 302 to also include communication circuitry configured to process program instructions to enable

communications with a server. This would have allowed communication with a server to thereby enable “various types of operating and location information” to be transmitted to a server so as to be accessible to, for example, the owner of the Tucker vehicle over the Internet—and not just at the primary portable device. Providing this information over the Internet while the secondary user was operating the vehicle would have further provided more timely information than after the trip was completed.

A POSITA thus would have understood that Tucker's “various types of operating and location information” is provided to the portable device by the vehicle: “the information can include positioning information (e.g., GPS coordinates), speed information (e.g., speed measurements collected by an acceleration detection module), vehicle operating information (e.g., operational information received from vehicle 106), and/or the like. Ex. 1008 (Tucker), ¶ [0110]; Instead of having the vehicle send vehicle operating information to the second mobile device and then relaying that data to the primary portable device over a cellular communications network, Bluetooth connection, or WiFi connection, there were other known techniques of providing vehicle operation information from the vehicle to a server which can be accessed by Tucker's primary portable device – including the techniques of Perry. Providing communication circuitry to communicate vehicle operating information such as speed, location, etc. to the server would have enabled the owner of the vehicle to monitor usage not only on their own mobile device, but from any Internet-accessible device with access to Perry's secure server 72.

the communications circuitry includes wireless communication circuitry for enabling local connection with a mobile device,

Tucker's Bluetooth module is communications circuitry that includes wireless

communications circuitry for enabling local connection with a mobile device, Ex. 1008 (Tucker), ¶¶ [0048]-[0049] (“Bluetooth module 302 can include any suitable combinations of hardware for performing wireless communications with other Bluetooth enabled devices “), [0053]-[0062], FIGS. 3-4.

the mobile device is configured to use the eKey for said unlocking and said starting the vehicle;

Tucker's “secondary portable device 104” is configured to transmit an “activation message” that includes “a vehicle access credential,” thus permitting use of the eKey (vehicle access credential) for performing operations like “a door unlock command, an engine start command, etc.,” Ex. 1008 (Tucker), ¶¶ [0106], [0107], [0117].

wherein the wireless communications circuitry of the vehicle is configured to receive coded data from the mobile device when using the eKey,

Tucker's “Bluetooth module 302” is configured to receive coded data in the form of “an activation message” that includes “the vehicle access credential” and “usage parameters,” which can be encrypted and/or digitally signed, Ex. 1008 (Tucker), ¶¶ [0044], [0051], [0071], [0081], [0093], [0098], [0106], [0108].

the coded data enables functions of said eKey for said unlocking and use of the vehicle,

Tucker's coded data includes the vehicle activation message with its vehicle access credential and usage parameters, Ex. 1008 (Tucker), ¶¶ [0098] (“vehicle access credential can include ... other information such as the usage parameters”), [0106], [0108] (“activation message” can include “vehicle access credential”), and the coded data enables the functions of the eKey (the vehicle access credential) for unlocking and use of the vehicle because the vehicle access credential and usage parameters in the activation message allow for functions such as “unlock[ing] a vehicle's doors,” or “start[ing] a vehicle's engine,” Ex. 1008 (Tucker), ¶¶ [0025],

[0107].

the coded data is associated to the eKey for use by the mobile device, and

Tucker's "activation message" including the "vehicle access credential" and "usage parameters" are associated to the "vehicle access credential" (the eKey) for use by the mobile device because the mobile device generates and sends the activation message including the coded data to the vehicle to allow the vehicle to be activated via the eKey, see Ex. 1008 (Tucker), ¶¶ [0098] (vehicle access credential can "incorporate other information, such as usage parameters"), [0108] ("activation message can include the access credential" which is used to "authenticate secondary portable device 104 as a device permitted to activate the vehicle"), [0117] (if both "usage parameters" and "vehicle access credential" are authentic, the vehicle can be accessed).

the coded data includes privilege settings associated with the eKey for limiting types of use of the vehicle when using the eKey with the vehicle;

Tucker's coded data—i.e., the "activation message" including the "vehicle access credential" and "usage parameters," Ex. 1008 (Tucker), ¶¶ [0098], [0106]-[0107]—includes privilege settings (i.e., "usage parameters" and these parameters are for limiting the use of the vehicle when using the eKey with the vehicle because they can "limit the manner in which vehicle 106 can be operated when the vehicle is activated using secondary portable device 104," id., ¶ [0092].

wherein use of the vehicle using the eKey is tracked to identify and log actions taken using the vehicle while the eKey is used.

Tucker describes recording a "history" and recording "the vehicle-related operations that were accessed, etc." including tracking "positioning information," "speed information" and other information so that it can be provided to the user of the primary portable device, Ex. 1008 (Tucker), ¶ [0094].

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

Tucker explains that the “usage parameters can limit” access to a specific vehicle area like “the passenger compartment,” but not “a trunk or glove compartment,” thus disclosing that the usage parameters function as restrictions that enable access to specific vehicle areas that include one or more of vehicle door operation (“passenger compartment,” or “trunk,” Ex. 1008 (Tucker), ¶ [0097].

5. The sub-system of the vehicle of claim 1, wherein the wireless communication circuitry is associated with an NFC standard or a radio frequency standard for said local connection between the mobile device and the vehicle.

Tucker's “Bluetooth module 302” in combination with Perry's cellular communication circuitry is associated with a radio frequency standard for said local connection-namely the Bluetooth® standard, see, e.g., Ex. 1008 (Tucker), ¶ [0049].

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

Tucker explains that a “vehicle access application” can be associated with primary, secondary, and other mobile devices, see Ex. 1008 (Tucker), ¶¶ [0045], [0067], [0090], [0098], [0100], [0107], [0111], and that application is able to share the vehicle access credential (eKey) with a recipient user having a recipient mobile device, id, ¶¶ [0090] (“primary portable device 102 can ... launch or execute a

vehicle access application” and can “transmit a vehicle access credential to secondary portable device 104”), [0111] (“secondary portable device 104 can be configured to transmit the access credential and/or usage parameters to other portable devices” and “those portable devices can similarly transmit activation messages to vehicle 106 to activate the vehicle”), and the sharing is enabled via a message initiated from said mobile device (e.g., “email or MMS”), id, ¶¶ [0099] (“vehicle access credential can be sent as an MMS message to the mobile phone number associated with the secondary portable device”), [0100] (“email or MMS”).

7. The sub-system of the vehicle of claim 1, wherein the coded data is processed securely by the mobile device responsive to registering the e-Key to the mobile device, the registering being enabled by an owner of said vehicle or an administrator of said vehicle.

Tucker's activation message (coded data) is processed securely by a “portable device” because the activation message includes both encrypted vehicle access credential and usage parameters which are “decrypted and ... authenticity determined,” see Ex. 1008 (Tucker), ¶¶ [0081] (vehicle access credential decrypted), [0116] (usage parameters decrypted) and they are “securely stored” in the mobile device, id, ¶ [0044], and it is processed responsive to registering the eKey (i.e., registration performed by secondary device user entering a PIN, see id, ¶ [0100], to allow the credential to be decrypted and used, where the registering is enabled by the user of the primary portable device—i.e., one with “owner access level,” id, ¶¶ [0097]-[0099], [0100], [0125].

8. The sub-system of the vehicle of claim 1, wherein a mode of allowed use of the vehicle using the eKey is configured to monitor said use of the vehicle, and said on-board computer is configured to transmit one or more notifications when a violation of a restriction is detected.

Tucker's mode of allowed use of the vehicle access credential using the secondary portable device includes recording “a history” of the vehicle's movements and recording “the vehicle-related operations that were accessed, etc.,” Ex. 1008 (Tucker), ¶ [0094]. But Tucker does not explicitly state that a notification is transmitted when a violation of a restriction is detected.

Perry discloses that when “a secondary activation device 76” is used to access the vehicle, Ex. 1009 (Perry), ¶ [0035], the user is notified that usage is being monitored, id, ¶ [0053]. While the use of the vehicle is being monitored, “if a user with a secondary activation device 76 drives the vehicle beyond the associated geographic vehicle operating range, the vehicle 12 is able to leave the operating range, but a notification may be sent to the vehicle owner (e.g., via text messaging, phone messaging, email messaging, [or] the like).” Ex, 1009 (Perry), ¶ [0054]; see also id, ¶ [0028].

It would have been obvious to one of ordinary skill before the effective filing date to have modified Tucker's controller to define a mode of allowed use of the vehicle using the eKey that is configured to monitor said use of the vehicle to allow the vehicle owner to be notified if usage of the vehicle is attempted by the secondary driver in a manner that is inconsistent with the usage parameters defined by the user of the primary portable device—i.e., tracking and notification of a violation of the privileges. A POSITA would have seen a benefit in allowing for real time monitoring of vehicle usage and reporting of violations of usage parameters to give the owner of the vehicle more and current information about vehicle usage than Tucker's system otherwise provides.

9. The sub-system of the vehicle of claim 1, wherein the tracked use of the vehicle is configured to identify a violation, and the violation is associated with one or more of driving too fast, or driving out of an area, or accelerating too

fast, or stopping too fast, or parking too close to a structure or other vehicle, or coming in contact with a structure or another vehicle, or slamming a door of the vehicle, or turning on a radio, or texting while driving, or interfacing with vehicle controls while driving, or two or more thereof.

Perry discloses that tracked use of the vehicle is configured to identify a violation including driving too fast: exceeding a “maximum vehicle speed,” Ex. 1009 (Perry), ¶ [0026], driving out of an area: driving “the vehicle beyond the associated geographical vehicle operating range,” id, ¶ [0054], and texting while driving: a restriction on “outgoing and/or incoming communications with third parties,” id, ¶ [0026].

It would have been obvious to one of ordinary skill before the effective filing date to have modified Tucker to include an identification of a violation of any of the usage parameters, including those disclosed by Perry consistent with the reasons explained above in claim 8.

10. The sub-system of the vehicle of claim 1, wherein the tracked use of the vehicle is configured to identify a violation, and the violation is associated with exceeding a speed limit, or time limit, or an area limit.

Perry discloses that tracked use of the vehicle is configured to identify a violation including driving too fast: exceeding a “maximum vehicle speed,” Ex. 1009 (Perry), ¶ [0026], “limiting a speed of the vehicle to an upper limit” (Perry claim 5) driving out of an area: driving “the vehicle beyond the associated geographical vehicle operating range,” id, ¶ [0054].

It would have been obvious to one of ordinary skill before the effective filing date to have modified Tucker to include an identification of a violation of any of the usage parameters, including those disclosed by Perry consistent with the reasons explained above in claim 8.

Claims 1–3 and 5–7 are rejected under 35 U.S.C. 103 as being unpatentable over Tucker and US 2008/0150683 (Mikan).

1. A sub-system of a vehicle, the vehicle having an on-board computer interfaced with the sub-system for processing instructions to enable use of an electronic key (eKey), the sub-system comprising:

memory associated with the on-board computer of the vehicle having program instructions for instructing unlocking and starting of the vehicle; and

communications circuitry of the vehicle interfaced with the on-board computer of the vehicle and the sub-system,

The above limitations are addressed by the teachings of Tucker in the Tucker and Perry rejection above for claim 1.

the communications circuitry is configured to process program instructions to enable communication with a server,

Tucker's "Bluetooth circuitry 402," which is part of the "Bluetooth module 302," is configured to process program instructions because it includes "hardware and/or software elements" to enable Bluetooth communications, Ex. 1008 (Tucker), ¶¶ [0053]-[0054], FIGS. 3-4.

While Tucker's sub-system includes communications circuitry using Bluetooth communications, it does not describe configuring such circuitry for communication with a server.

Mikan describes "[m]ethods and wireless devices for providing secure operation of a vehicle." Ex. 1010 (Mikan), Abstract. When a key—which may be "embedded within a wireless device such as a cellular telephone"—is detected "a vehicle operation policy associated with the key is retrieved, and operation of the vehicle consistent with the operation policy is permitted." Id. The local database on

Mikan's vehicle may have certain records synchronized with the master database via the master application. For instance, Mikan explains that "local database 203 may mirror some of the data in master database 208 such that records within each database are consistent." Ex. 1010 (Mikan), ¶ [0054]. The local database 303 also includes the vehicle ID, key set, and policies. See Mikan FIG. 3B.

Mikan discloses a "control unit 202" that "may be any combination of hardware/software that is in operative communication with vehicle 201," a "local database 203," and "wireless network 207," such as cellular network like a W-CDMA network, Ex. 1010 (Mikan), ¶¶ [0051]-[0052]; Mikan's control unit receives data from master database/application 208, 209, which can be implemented on "a server platform," id, ¶¶ [0054]-[0055], this allows for data related to "a collection of keys 205A-C" to be provided to the vehicle, id, ¶¶ [0058]-[0059].

It would have been obvious to one of ordinary skill before the effective filing date to have modified Tucker's communications circuitry to be able to communicate with the server to allow for Tucker's vehicle access credential to be provisioned by the manufacturer, a dealer, or other entity to the vehicle remotely. A POSITA would have found it obvious to modify Tucker to allow Tucker's "vehicle access credential" to be provided from a master application on a server based on Mikan. For instance, Tucker explains that a "vehicle access credential" is "provided to and locally stored in vehicle 106 at" a time before the primary portable device is authorized to access the vehicle. Ex. 1008 (Tucker), ¶ [0080]. The vehicle access credential can be provided "during manufacturing, prior to being sold by a dealer, etc." Ex. 1008 (Tucker), ¶ [0080]. Tucker does not specify how the stored vehicle access credential is provided by the manufacturer during manufacturing or at a later time by a dealer before selling it. A POSITA would

have understood that there were a number of ways for manufacturers and dealers to provide vehicles with data such as Tucker's vehicle access credential and one of those ways is disclosed by Mikan -to use communications circuitry on a vehicle to communicate with a server to receive the data. With such a modification, a manufacturer could provide various information to a vehicle to allow for not only providing the vehicle access credential to the vehicle, but also allowing things like software updates, or other data to be communicated to the vehicle from a server.

the communications circuitry includes wireless communication circuitry for enabling local connection with a mobile device,

the mobile device is configured to use the eKey for said unlocking and said starting the vehicle;

wherein the wireless communications circuitry of the vehicle is configured to receive coded data from the mobile device when using the eKey,

the coded data enables functions of said eKey for said unlocking and use of the vehicle,

the coded data is associated to the eKey for use by the mobile device, and

the coded data includes privilege settings associated with the eKey for limiting types of use of the vehicle when using the eKey with the vehicle;

wherein use of the vehicle using the eKey is tracked to identify and log actions taken using the vehicle while the eKey is used.

The above limitations are addressed by the teachings of Tucker in the Tucker and Perry rejection above for claim 1.

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

The above limitations are addressed by the teachings of Tucker in the

Tucker and Perry rejection above for claim 2.

3. The sub-system of the vehicle of claim 1, wherein the vehicle is configured to receive or securely store information from the server to perform authentication or verification that the coded data received from the mobile device should activate the eKey.

Tucker in view of Mikan as articulated above renders this limitation obvious because Tucker both receives the vehicle access credential because it “can be provided to and locally stored in vehicle 106” by a manufacturer or dealer, Ex. 1008 (Tucker), ¶ [0080], and it can be “encrypted or securely stored in any suitable manner,” id, ¶ [0051], additionally, the vehicle access credential is “used by vehicle 106 to authenticate a portable device,” id, ¶ [0071], [0116]-[0117]; Mikan discloses using authentication information (e.g., secure ID check from a server), and it would have been obvious to have modified Tucker such that the vehicle access credential is received from a server for the reasons discussed above, Ex. 1010 (Mikan), ¶¶ [0050]-[0052], [0055], [0059].

5. The sub-system of the vehicle of claim 1, wherein the wireless communication circuitry is associated with an NFC standard or a radio frequency standard for said local connection between the mobile device and the vehicle.

Tucker's “Bluetooth module 302” in combination with Mikan's cellular communication circuitry is associated with a radio frequency standard for said local connection-namely the Bluetooth® standard, see, e.g., Ex. 1008 (Tucker), ¶ [0049].

6. The sub-system of the vehicle of claim 1, wherein an application associated

with said mobile device is configured to enable sharing of said eKey with a recipient user having a recipient mobile device, the sharing is enabled via a message initiated from said mobile device.

The above limitations are addressed by the teachings of Tucker in the Tucker and Perry rejection above for claim 6.

7. The sub-system of the vehicle of claim 1, wherein the coded data is processed securely by the mobile device responsive to registering the e-Key to the mobile device, the registering being enabled by an owner of said vehicle or an administrator of said vehicle.

The above limitations are addressed by the teachings of Tucker in the Tucker and Perry rejection above for claim 7.

Claim 4 is rejected under 35 U.S.C. 103 as being unpatentable over Tucker, Mikan and US 2012/0254948 (Kleve).

4. The sub-system of the vehicle of claim 1, wherein the communications circuitry of the vehicle is configured to receive one or more additional requests from other mobile devices to use the vehicle,

Tucker's communications circuitry—the “Bluetooth module 302” in combination with Mikan's controller (as applied to claim 1)—is configured to receive requests to use the vehicle—i.e., activation messages—from “primary portable device,” “secondary portable device,” and “other portable devices,” Ex. 1008 (Tucker), ¶¶ [0111]; see also id, FIG. 1, ¶ [0032] (“a system 100 including a primary portable device 102, a secondary portable device 104 ...”).

each request is associated with coded data generated by the server,

Tucker's “primary portable device,” “secondary portable device,” and “other portable devices,” Ex. 1008 (Tucker), ¶¶ [0071], [0098], [0111], each send

activation messages to the vehicle that include a “vehicle access credential,” id., ¶¶ [0082], [0106], [0111]); Mikan discloses obtaining data related to eKeys from a server and it would have been obvious to have obtained Tucker's vehicle access credential—part of the coded data—from a server for the same reasons explained above.

such that each coded data is associated with a user account having privileges assigned by an administrator of the vehicle that enables assigning or use of eKeys to use the vehicle.

Tucker discloses that each “activation message” (coded data) from “secondary portable device” or “other portable devices,” Ex. 1008 (Tucker), ¶¶ [0082], [0106], has “usage parameters” assigned by the holder of the “primary portable device” with an “owner access level,” id., ¶¶ [0092], [0111], [0125], and because the vehicle access credential can be shared with “secondary portable device” or “other portable devices” and can be used to activate the vehicle, assigning or use of the eKeys to use the vehicle is enabled, id., ¶¶ [0106], [0111].

Tucker in view of Mikan does not disclose that each coded data (e.g., Tucker's vehicle access message) is associated with a user account having privileges assigned by an administrator. Kleve however describes “a system for authorizing use of a vehicle communication and information system” that includes the ability to “receive information associating one or more devices with a vehicle computer Ex. 1011 (Kleve), Abstract. Users can “request authorization to command one or more vehicle controls from the one or more devices associated with the vehicle computer.” Id., ¶ [0005]. A “nomadic device” is a “cellular phone” that can communicate using Bluetooth. Ex. 1011 (Kleve), ¶¶ [0031], [0037]. The cellular device can communicate with the vehicle through a remote server as well. See, e.g., id., ¶¶ [0031]-[0032]. According to Kleve, user devices need to “register” to use the system and once registered, the nomadic device can be used “to obtain

access to various vehicle-based services from the nomadic device 103” such as “remote lock and unlock, remote start, vehicle tracking, remote control of vehicle controls (e.g., and without limitation, radio and HVAC), data download, and others. Id, ¶¶ [0052]-[0053]. Kleveland's server can evaluate the identification information and “determine that a new account is requested. The owner can be notified when this happens, and the owner of the vehicle can accept or reject the request. Id, ¶ [0083]. “If authorization is accepted, the additional/substitute user(s) may only be permitted limited operation of the module 200,” and may be prevented from tracking the vehicle, locking or unlocking the vehicle, etc. Id, ¶ [0088]. Thus Kleveland discloses associating privileges with user accounts by explaining that “a vehicle user may register one or more devices ... to gain access to various vehicle-based services from the nomadic device 103 and/or personal computer,” Ex. 1011 (Kleveland), ¶ [0053], and this may require requesting “a new account,” which results in the notification of the “owner of the vehicle,” which may be approved by the owner, but may also permit “limited operation” of vehicle systems, Ex. 1011 (Kleveland), ¶¶ [0083], [0088].

It would have been obvious to one of ordinary skill before the effective filing date to have modified Tucker in view of Mikan further in view of Kleveland such that each coded data is associated with a user account having privileges. Kleveland teaches a technique of registering accounts before approval to use vehicle functions is granted by the owner of the vehicle. Requiring users of Tucker's secondary portable devices and other portable devices to register with the system and have accounts would have had multiple benefits including having the eKey functionality associated with the person that is operating the vehicle, thus enabling added security because in addition to the presence of the user's device use of the vehicle also requires a login procedure to be used as described by Kleveland. See, e.g., Ex.

1011 (Kleve), ¶¶ [0056], [0057]. Additionally because the login process would allow a user to gain access to a user account associated with the Tucker application, the login process would have better been able to prevent unauthorized use of the vehicle (i.e., requiring the user to have possession of the secondary mobile device and verify their identity through a login process).

Claims 8–10 are rejected under 35 U.S.C. 103 as being unpatentable over Tucker, Mikan and Perry.

8. The sub-system of the vehicle of claim 1, wherein a mode of allowed use of the vehicle using the eKey is configured to monitor said use of the vehicle, and said on-board computer is configured to transmit one or more notifications when a violation of a restriction is detected.

Tucker's mode of allowed use of the vehicle access credential using the secondary portable device includes recording “a history” of the vehicle's movements and recording “the vehicle-related operations that were accessed, etc.,” Ex. 1008 (Tucker), ¶ [0094]. But Tucker in view of Mikan does not explicitly state that a notification is transmitted when a violation of a restriction is detected.

Perry discloses that when “a secondary activation device 76” is used to access the vehicle, Ex. 1009 (Perry), ¶ [0035], the user is notified that usage is being monitored, id, ¶ [0053]. While the use of the vehicle is being monitored, “if a user with a secondary activation device 76 drives the vehicle beyond the associated geographic vehicle operating range, the vehicle 12 is able to leave the operating range, but a notification may be sent to the vehicle owner (e.g., via text messaging, phone messaging, email messaging, [or] the like).” Ex, 1009 (Perry), ¶ [0054]; see also id, ¶ [0028].

It would have been obvious to one of ordinary skill before the effective filing date to have modified Tucker's controller to define a mode of allowed use of

the vehicle using the eKey that is configured to monitor said use of the vehicle to allow the vehicle owner to be notified if usage of the vehicle is attempted by the secondary driver in a manner that is inconsistent with the usage parameters defined by the user of the primary portable device—i.e., tracking and notification of a violation of the privileges. A POSITA would have seen a benefit in allowing for real time monitoring of vehicle usage and reporting of violations of usage parameters to give the owner of the vehicle more and current information about vehicle usage than Tucker's system in view of Mikan otherwise provides.

9. The sub-system of the vehicle of claim 1, wherein the tracked use of the vehicle is configured to identify a violation, and the violation is associated with one or more of driving too fast, or driving out of an area, or accelerating too fast, or stopping too fast, or parking too close to a structure or other vehicle, or coming in contact with a structure or another vehicle, or slamming a door of the vehicle, or turning on a radio, or texting while driving, or interfacing with vehicle controls while driving, or two or more thereof.

Perry discloses that tracked use of the vehicle is configured to identify a violation including driving too fast: exceeding a “maximum vehicle speed,” Ex. 1009 (Perry), ¶ [0026], driving out of an area: driving “the vehicle beyond the associated geographical vehicle operating range,” id, ¶ [0054], and texting while driving: a restriction on “outgoing and/or incoming communications with third parties,” id, ¶ [0026].

It would have been obvious to one of ordinary skill before the effective filing date to have modified Tucker in view of Mikan to include an identification of a violation of any of the usage parameters, including those disclosed by Perry consistent with the reasons explained above in claim 8.

10. The sub-system of the vehicle of claim 1, wherein the tracked use of the

vehicle is configured to identify a violation, and the violation is associated with exceeding a speed limit, or time limit, or an area limit.

Perry discloses that tracked use of the vehicle is configured to identify a violation including driving too fast: exceeding a “maximum vehicle speed,” Ex. 1009 (Perry), ¶ [0026], “limiting a speed of the vehicle to an upper limit” (Perry claim 5) driving out of an area: driving “the vehicle beyond the associated geographical vehicle operating range,” id, ¶ [0054].

It would have been obvious to one of ordinary skill before the effective filing date to have modified Tucker in view of Mikan to include an identification of a violation of any of the usage parameters, including those disclosed by Perry consistent with the reasons explained above in claim 8.

Claims 11–21 are rejected under 35 U.S.C. 103 as being unpatentable over Tucker and US 8,977,408 (Cazanas).

11. A system of a vehicle, the vehicle having an on-board computer for processing and communicating with the system for use of an electronic key (eKey), the system comprising:

Tucker's “vehicle access control system” is a system of “vehicle 106” having a “controller 304” (on-board computer) that interfaces with various subsystems including components of the vehicle access control system, where the controller “can include one or more processors (e. g., microprocessors or microcontrollers) configured to execute machine-readable instructions,” including those that enable the use of an electronic key (eKey)—i.e., Tucker's “vehicle access credential”—by, among other things, communicating with the system; see Ex. 1008 (Tucker), ¶¶ [0025], [0048], [0050], [0082]–[0083], [0106]–[0108], FIGS. 1, 3.

memory associated with the on-board computer of the vehicle having program instructions for controlling unlocking and starting of the vehicle;

and

Tucker's "storage module 306" is memory and is associated with Tucker's controller because the controller is connected to it and able to execute "various software programs residing on storage module 306," including performing "various vehicle-related operations," which Tucker defines as including unlocking "a vehicle's doors," and "start[ing] a vehicle's engine," Ex. 1008 (Tucker), ¶¶ [0025], [0050], FIG. 3 (storage 306 associated with controller 304).

communications circuitry of the vehicle interfaced with the on-board computer of the vehicle,

Tucker's "Bluetooth module 302" is communications circuitry of vehicle (300) and is interfaced with the on-board computer—i.e., Tucker's controller 304, Ex. 1008 (Tucker), FIGS. 3 & 4, ¶¶ [0050], [0051], [0067], [0076] (describing Bluetooth and use of Bluetooth to perform vehicle-related operations.

the communications circuitry includes wireless communication circuitry for enabling local connection with a mobile device,

Tucker's Bluetooth module is communications circuitry that includes wireless communications circuitry for enabling local connection with a mobile device, Ex. 1008 (Tucker), ¶¶ [0048]-[0049] ("Bluetooth module 302 can include any suitable combinations of hardware for performing wireless communications with other Bluetooth enabled devices"), [0053]-[0062], FIGS. 3-4.

the mobile device is configured to use the eKey for said unlocking and said starting of the vehicle;

Tucker's "secondary portable device 104" is configured to transmit an "activation message" that includes "a vehicle access credential," thus permitting use of the eKey (vehicle access credential) for performing operations like "a door unlock command, an engine start command, etc.," Ex. 1008 (Tucker), ¶¶ [0106], [0107], [0117].

wherein the wireless communications circuitry of the vehicle is configured to receive coded data from the mobile device,

Tucker's "Bluetooth module 302" is configured to receive coded data in the form of "an activation message" that includes "the vehicle access credential" and "usage parameters," which can be encrypted and/or digitally signed, Ex. 1008 (Tucker), ¶¶ [0044], [0051], [0071], [0081], [0093], [0098], [0106], [0108].

the coded data is unique for said eKey, and

Tucker's "vehicle access credential can include a uniquely generated value," Ex. 1008 (Tucker), ¶ [0071], and because that uniquely generated value is provided in the vehicle activation message, see, e.g., id., ¶ [0108], the coded data is unique for the eKey.

the coded data includes privilege settings set for limiting types of use of the vehicle when using the vehicle via the eKey;

Tucker's coded data—i.e., the "activation message" including the "vehicle access credential" and "usage parameters," Ex. 1008 (Tucker), ¶¶ [0098], [0106]-[0107]—includes privilege settings (i.e., "usage parameters" and these parameters are for limiting the use of the vehicle when using the eKey with the vehicle because they can "limit the manner in which vehicle 106 can be operated when the vehicle is activated using secondary portable device 104," ¶ [0092].

wherein the eKey is associated with a user account,

Tucker's eKey (i.e., the vehicle access credential) is not described as being associated with a user account. Cazanas provides various embodiments to "allow transfer of a driver's profile with one or more settings for user configurable features of a vehicle to and/or from a server via network communications." Ex. 1012 (Cazanas), 1:44-48. Functionality of a mobile device can also be incorporated into a telematics unit of a vehicle. Id., 5:9-23, 5:40-42. "Data from the vehicle 14 may

be transmitted from the telematics unit 16 to the network. Data may also be transmitted from the network 10 to the vehicle 14 from the telematics unit 16.” Id, 12:13-16. Drivers can establish profiles with “settings stored in the IPR Multimedia Subsystem (IMS) server 42, or web server 41 in communication with the IMS server 42, or web server 41 in communication with the IMS server “ Id, 6:1-5. “The web server 41 provides the user interface for account related functions, e.g., via a mobile or Internet web session from a personal computer (PC) or mobile station” and “stores the driver profile and the IMS server transfers the profile ...”. Ex. 1012 (Cazanas), 6:17-25. These profiles may be associated with a user account. See, e.g., id, 12:13-30 (“The account information thus includes the profile as well as the various identifiers associated with the driver, e.g., key fob identifiers, MDN, email address, etc.”). Drivers can establish profiles with “settings stored in the IPR Multimedia Subsystem (IMS) server 42, or web server 41 in communication with the IMS server 42, or web server 41 in communication with the IMS server “ Id, 6:1-5. “The web server 41 provides the user interface for account related functions, e.g., via a mobile or Internet web session from a personal computer (PC) or mobile station” and “stores the driver profile and the IMS server transfers the profile ... “. Ex. 1012 (Cazanas), 6:17-25. These profiles may be associated with a user account. See, e.g., id, 12:13-30 (“The account information thus includes the profile as well as the various identifiers associated with the driver, e.g., key fob identifiers, MDN, email address, etc.”).

It would have been obvious to one of ordinary skill before the effective filing date to have modified Tucker to associate the eKey with a user account, such that Tucker's mobile device vehicle access application (i.e., Tucker's “application that enables a user of portable device 200 to activate and control a vehicle 106” that operates as an eKey, Ex. 1008 (Tucker), ¶ [0045]), is tied to a user account for

the user of the mobile device based on Cazanias. This would have permitted the monetization of the eKey system if the provider of that system wanted to monetize it; Ex. 1012 (Cazanias), 11:36-46 (describing a “My Account” interface (now “My Verizon”)). Additionally, a POSITA would have appreciated that setting up user accounts corresponding the vehicle access applications on the Tucker portable devices to associate them with the eKeys to use one or more vehicles would have had multiple benefits including having the eKey functionality associated with the person that is operating the vehicle, thus proving more robust association with the user and requiring not just the presence of the user's device but also a login procedure to be used. A POSITA would have also found it obvious to make that account accessible through the user interface associated with the Tucker application to allow the user to manage things like shared eKeys, and usage parameters because it would have been convenient and providing access to user accounts for use in connection with vehicle electronics systems was a known way to make access and modification of settings and preferences and undertaking certain actions convenient and accessible anywhere a mobile device can be used. **the user account is accessible via a user interface of an application executed by the mobile device,**

Tucker discloses “software programs” or “apps” including “an application that enables a user of a portable device to activate and control vehicle 106,” with a “graphical user interface for the application,” Ex. 1008 (Tucker), ¶¶ [0045], [0047]; Cazanias describes a user account, such as “user's account on the web server 41,” Ex. 1012 (Cazanias), 13:64-67, that can be accessed through “a profile service specific device application,” id, 14:4-16; it would have been obvious to make the user account accessible via the user interface of Tucker's vehicle access application for the reasons discussed above.

the eKey when active enables said unlocking of the vehicle and said starting of the vehicle.

When Tucker's "vehicle access credential" is authenticated it enables unlocking and starting of the vehicle because the vehicle access credential and usage parameters in the activation message allow for functions such as "unlock[ing] a vehicle's doors," or "start[ing] a vehicle's engine," Ex. 1008 (Tucker), ¶¶ [0025], [0107].

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

Associating a server with the manufacturer of a vehicle is not a structural or functional limitation on the claim and is not entitled to patentable weight, see *Catalina Mktg. Int'l v. Coolsavings.com, Inc.*, 289 F.3d 801, 809 (Fed. Cir. 2002) ("The patentability of an apparatus claim 'depends on the claimed structure, not on the use or purpose of that structure "); *In re Schreiber*, 128 F.3d 1473, 1477 (Fed. Cir. 1997) ("It is well settled that the recitation of a new intended use for an old product does not make a claim to that old product patentable."); but, even if it is a limitation, it would have been obvious over Tucker in view of Cazan's; Tucker discloses "vehicle access applications" for use with eKeys, Ex. 1008 (Tucker), ¶¶ [0045], [0067], [0100]; Cazan's discloses a "web server 41" and an "IP Multimedia Subsystem (IMS) server 42," Ex. 1012 (Cazan's), 12:16-21, thus disclosing a plurality of servers; Cazan's web server 41 can be provided by "an automobile manufacturer," *id.*, 6:27-34, an account on the server is linked to "a profile specific device application," *id.*, 14:4-16, showing that the server is configured for communication with Cazan's application; it would have been

obvious to modify Tucker to allow communication between Cazan's server and Tucker's application for the reasons explained above.

13. The system of a vehicle as recited in claim 11, wherein the eKey is securely generated on the mobile device, and

Tucker's "vehicle access application can generate a vehicle access credential for the secondary portable device," Ex. 1008 (Tucker), ¶ [0098], and that vehicle access credential may be securely generated because "the credential itself can be encrypted prior to transmission" to the secondary or "other portable devices," id, ¶¶ [0100] [0111].

wherein a server associated with a manufacturer of the vehicle is configured to communicate with the application, the application further being associated with a manufacturer of the vehicle.

Associating a server with the manufacturer of a vehicle is not a structural or functional limitation on the claim and is not entitled to patentable weight, see *Catalina Mktg. Int'l v. Coolsavings.com, Inc.*, 289 F.3d 801, 809 (Fed. Cir. 2002) ("The patentability of an apparatus claim 'depends on the claimed structure, not on the use or purpose of that structure "); *In re Schreiber*, 128 F.3d 1473, 1477 (Fed. Cir. 1997) ("It is well settled that the recitation of a new intended use for an old product does not make a claim to that old product patentable."); but, even if it is a limitation, it would have been obvious over Tucker in view of Cazan's; Tucker discloses "vehicle access applications" for use with eKeys, Ex. 1008 (Tucker), ¶¶ [0045], [0067], [0100]; Cazan's discloses a "web server 41" and an "IP Multimedia Subsystem (IMS) server 42," Ex. 1012 (Cazan's), 12:16-21, thus disclosing a plurality of servers; Cazan's web server 41 can be provided by "an automobile manufacturer," id, 6:27-34, an account on the server is linked to "a profile specific device application," id, 14:4-16, showing that the server is

configured for communication with Cazan's application; it would have been obvious to modify Tucker to allow communication between Cazan's server and Tucker's application for the reasons explained above.

14. The system of a vehicle as recited in claim 11, wherein said on-board computer includes logic for processing encryption operations of said eKey in coordination with logic of said mobile device.

Tucker explains that the secondary mobile device decrypts a vehicle access credential received from a secondary portable device, Ex. 10008 (Tucker), ¶ [0100], and this process would have been understood to be performed by the on-board computer—i.e., Tucker's controller 304; decryption by the on-board computer is logic that works in coordination with the encryption operation when sending an encrypted eKey to the vehicle, see Ex. 1008 (Tucker), ¶¶ [0100] (credential from primary portable device encrypted, decrypted by secondary portable device), [0081] (credential decrypted by the vehicle).

15. The system of a vehicle as recited in claim 14, wherein said encryption operations use secure public/private key pair encryption operations.

Tucker explains that “primary portable device 102 can provide a cryptographic key (e.g., ... one of a public/private key pair) to vehicle,” Ex. 1008 (Tucker), ¶ [0096].

16. The system of a vehicle as recited in claim 11, wherein said wireless communication circuitry facilitates one or more of Bluetooth, near field communication (NFC), WiFi, or radio communication.

Tucker describes the use of “Bluetooth module,” which can communicate “based on the Bluetooth and/or Bluetooth LE standard,” Ex. 1008 (Tucker), ¶

[0053].

17. The system of a vehicle as recited in claim 11, wherein said eKey is validated and securely bound to the mobile device to prevent unauthorized transfers of the ekey.

Tucker discloses validating the eKey (vehicle access credential) by a user entering a “personal identification code” to allow decryption of an encrypted eKey transmitted by the primary portable device to the secondary portable device, Ex. 1008 (Tucker), ¶ [0100], and Tucker teaches that the eKey is securely bound to the portable devices because it is (1) transmitted in an encrypted form, id., ¶¶ [0081]-[0082], [0100], (2) securely stored in the portable devices, id., ¶ [0044], and (3) decrypted by the vehicle to validate it originated from the primary portable device, id., ¶ [0082]; by requiring the eKey be decrypted before it can be used by the secondary portable device or be used to activate the vehicle, unauthorized transfers of the eKey are prevented.

18. A vehicle having an on-board computer for processing and communicating an electronic key (eKey), the vehicle comprising:

Tucker teaches a “vehicle 106” having a “controller 304” that includes “one or more processors (e.g., microprocessors or microcontrollers) configured to execute machine-readable instructions” and communicating an electronic key, e.g., by sending an eKey to a “primary portable device”; see Ex. 1008 (Tucker), ¶¶ [0025], [0048], [0050], [0071] (“primary portable device 102 can receive a vehicle access credential from vehicle 106”), [0081][0083], [0106]-[0108], FIGS. 1, 3.

memory associated with the on-board computer of the vehicle having program instructions for controlling unlocking and starting of the vehicle; and

Tucker's "storage module 306" is memory and is associated with Tucker's controller because the controller is connected to it and able to execute "various software programs residing on storage module 306," including performing "various vehicle-related operations," which Tucker defines as including unlocking "a vehicle's doors," and "start[ing] a vehicle's engine," Ex. 1008 (Tucker), ¶¶ [0025], [0050], FIG. 3 (storage 306 associated with controller 304).

communications circuitry of the vehicle interfaced with the on-board computer of the vehicle,

Tucker's "Bluetooth module 302" is communications circuitry of vehicle (300) and is interfaced with the on-board computer—i.e., Tucker's controller 304—and Tucker's subsystem—i.e., "vehicle access control system," Ex. 1008 (Tucker), FIGS. 3 & 4, ¶¶ [0050], [0051], [0067], [0076] (describing Bluetooth and use of Bluetooth to perform vehicle-related operations).

the communications circuitry includes wireless communication circuitry for enabling local connection with a mobile device,

Tucker's Bluetooth module is communications circuitry that includes wireless communications circuitry for enabling local connection with a mobile device, Ex. 1008 (Tucker), ¶¶ [0048]-[0049] ("Bluetooth module 302 can include any suitable combinations of hardware for performing wireless communications with other Bluetooth enabled devices"), [0053]-[0062], FIGS. 3-4.

the mobile device is configured to use the eKey for said unlocking and said starting of the vehicle;

Tucker's "secondary portable device 104" is configured to transmit an "activation message" that includes "a vehicle access credential," thus permitting use of the eKey (vehicle access credential) for performing operations like "a door unlock command, an engine start command, etc.," Ex. 1008 (Tucker), ¶¶ [0106], [0107], [0117].

wherein the wireless communications circuitry of the vehicle is configured to receive coded data from the mobile device,

Tucker's "Bluetooth module 302" is configured to receive coded data in the form of "an activation message" that includes "the vehicle access credential" and "usage parameters," which can be encrypted and/or digitally signed, Ex. 1008 (Tucker), ¶¶ [0044], [0051], [0071], [0081], [0093], [0098], [0106], [0108].

the coded data is unique for said eKey to be used via the mobile device, and

See discussion of this limitation for claim 11, where the vehicle activation message from the secondary portable device includes both the "vehicle access credential" that was uniquely generated and the "usage parameters" assigned to the secondary portable device, thus producing a unique eKey to be used via the mobile device, Ex. 1008 (Tucker), ¶¶ [0092], [0098].

the coded data includes privilege settings for use of the vehicle when using the eKey with the vehicle;

Tucker's coded data-i.e., the "activation message" including the "vehicle access credential" and "usage parameters," Ex. 1008 (Tucker), ¶¶ [0098], [0106]-[0107]-includes privilege settings (i.e., "usage parameters") and these parameters are for use of the vehicle when using the eKey with the vehicle because they can "limit the manner in which vehicle 106 can be operated when the vehicle is activated using secondary portable device 104," id, ¶ [0092].

wherein the eKey is associated with a user account,

Tucker's eKey (i.e., the vehicle access credential) is not described as being associated with a user account. Cazanas provides various embodiments to "allow transfer of a driver's profile with one or more settings for user configurable features of a vehicle to and/or from a server via network communications." Ex. 1012 (Cazanas), 1:44-48. Functionality of a mobile device can also be incorporated into

a telematics unit of a vehicle. Id, 5:9-23, 5:40-42. “Data from the vehicle 14 may be transmitted from the telematics unit 16 to the network. Data may also be transmitted from the network 10 to the vehicle 14 from the telematics unit 16.” Id, 12:13-16. Drivers can establish profiles with “settings stored in the IPR Multimedia Subsystem (IMS) server 42, or web server 41 in communication with the IMS server 42, or web server 41 in communication with the IMS server “ Id, 6:1-5. “The web server 41 provides the user interface for account related functions, e.g., via a mobile or Internet web session from a personal computer (PC) or mobile station” and “stores the driver profile and the IMS server transfers the profile ...”. Ex. 1012 (Cazanas), 6:17-25. These profiles may be associated with a user account. See, e.g., id, 12:13-30 (“The account information thus includes the profile as well as the various identifiers associated with the driver, e.g., key fob identifiers, MDN, email address, etc.”). Drivers can establish profiles with “settings stored in the IPR Multimedia Subsystem (IMS) server 42, or web server 41 in communication with the IMS server 42, or web server 41 in communication with the IMS server “ Id, 6:1-5. “The web server 41 provides the user interface for account related functions, e.g., via a mobile or Internet web session from a personal computer (PC) or mobile station” and “stores the driver profile and the IMS server transfers the profile ... “. Ex. 1012 (Cazanas), 6:17-25. These profiles may be associated with a user account. See, e.g., id, 12:13-30 (“The account information thus includes the profile as well as the various identifiers associated with the driver, e.g., key fob identifiers, MDN, email address, etc.”).

It would have been obvious to one of ordinary skill before the effective filing date to have modified Tucker to associate the eKey with a user account, such that Tucker's mobile device vehicle access application (i.e., Tucker's “application that enables a user of portable device 200 to activate and control a vehicle 106”

that operates as an eKey, Ex. 1008 (Tucker), ¶ [0045], is tied to a user account for the user of the mobile device based on Cazanias. This would have permitted the monetization of the eKey system if the provider of that system wanted to monetize it; Ex. 1012 (Cazanias), 11:36-46 (describing a “My Account” interface (now “My Verizon”)). Additionally, a POSITA would have appreciated that setting up user accounts corresponding the vehicle access applications on the Tucker portable devices to associate them with the eKeys to use one or more vehicles would have had multiple benefits including having the eKey functionality associated with the person that is operating the vehicle, thus proving more robust association with the user and requiring not just the presence of the user's device but also a login procedure to be used. A POSITA would have also found it obvious to make that account accessible through the user interface associated with the Tucker application to allow the user to manage things like shared eKeys, and usage parameters because it would have been convenient and providing access to user accounts for use in connection with vehicle electronics systems was a known way to make access and modification of settings and preferences and undertaking certain actions convenient and accessible anywhere a mobile device can be used. **the user account is accessible via a user interface of an application executed by the mobile device,**

Tucker discloses “software programs” or “apps” including “an application that enables a user of a portable device to activate and control vehicle 106,” with a “graphical user interface for the application,” Ex. 1008 (Tucker), ¶¶ [0045], [0047]; Cazanias describes a user account, such as “user's account on the web server 41,” Ex. 1012 (Cazanias), 13:64-67, that can be accessed through “a profile service specific device application,” id, 14:4-16; it would have been obvious to make the user account accessible via the user interface of Tucker's vehicle access

application for the reasons discussed above.

the eKey when active enables said unlocking of the vehicle and said starting of the vehicle.

When Tucker's "vehicle access credential" is authenticated, it enables unlocking and starting of the vehicle because the vehicle access credential and usage parameters in the activation message allow for functions such as "unlock[ing] a vehicle's doors," or "start[ing] a vehicle's engine," Ex. 1008 (Tucker), ¶¶ [0025], [0107].

19. The vehicle of claim 18, wherein the privilege settings being unrestricted for an owner of the vehicle and restricted for a shared user of the vehicle,

Tucker teaches that a portable device can be associated with "an owner access level" that enables the user to "activate the vehicle such that any supported vehicle related operation can be accessed," and "guest user" privileges can be assigned to use a "limited number of vehicle-related operations," Ex. 1008 (Tucker), ¶ [0125].

the shared user of the vehicle receives a shared eKey responsive to said owner of the vehicle causing the shared eKey to be sent for shared use of the vehicle.

In Tucker, the "guest user"—i.e., a shared user—receives the vehicle access credential in response to the holder of the primary portable device—i.e., owner of the vehicle—causing the application on their device to share the key with the secondary portable device, see Ex. 1008 (Tucker), ¶¶ [0090], [0092]; see also id, ¶¶ [0097]-[0099].

20. The vehicle of claim 18, wherein the eKey is securely generated on the mobile device, and

Tucker's "vehicle access application can generate a vehicle access credential

for the secondary portable device,” Ex. 1008 (Tucker), ¶ [0098], and that vehicle access credential may be securely generated because “the credential itself can be encrypted prior to transmission” to the secondary or “other portable devices,” id., ¶¶ [0100], [0111].

wherein a server associated with a manufacturer of the vehicle is configured to communicate with the application, the application further being associated with a manufacturer of the vehicle.

Associating a server with the manufacturer of a vehicle is not a structural or functional limitation on the claim and is not entitled to patentable weight, see *Catalina Mktg. Int'l v. Coolsavings.com, Inc.*, 289 F.3d 801, 809 (Fed. Cir. 2002) (“The patentability of an apparatus claim 'depends on the claimed structure, not on the use or purpose of that structure “); *In re Schreiber*, 128 F.3d 1473, 1477 (Fed. Cir. 1997) (“It is well settled that the recitation of a new intended use for an old product does not make a claim to that old product patentable.”); but, even if it is a limitation, it would have been obvious over Tucker in view of *Cazanas*; Tucker discloses “vehicle access applications” for use with eKeys, Ex. 1008 (Tucker), ¶¶ [0045], [0067], [0100]; *Cazanas* discloses a “web server 41” and an “IP Multimedia Subsystem (IMS) server 42,” Ex. 1012 (*Cazanas*), 12:16-21, thus disclosing a plurality of servers; *Cazanas*'s web server 41 can be provided by “an automobile manufacturer,” id., 6:27-34, an account on the server is linked to “a profile specific device application,” id., 14:4-16, showing that the server is configured for communication with *Cazanas*'s application; it would have been obvious to modify Tucker to allow communication between *Cazanas*'s server and Tucker's application for the reasons explained above.

21. The vehicle of claim 18, wherein encryption operations are associated with use of said eKey, and

Tucker's vehicle access credential (eKey) is encrypted and decrypted, encryption operations are associated with the use of the eKey, see Ex. 1008 (Tucker), ¶¶ [0081], [0099]-[0100], [0116].

said encryption operations use public/private key pair encryption, and

Tucker explains that “primary portable device 102 can provide a cryptographic key (e.g., ... one of a public/private key pair) to vehicle,” Ex. 1008 (Tucker), ¶ [0096].

wherein said wireless communication circuitry uses one or more of Bluetooth, or near field communication (NFC), or WiFi, or radio communication.

Tucker describes the use of “Bluetooth module,” which can communicate “based on the Bluetooth and/or Bluetooth LE standard,” Ex. 1008 (Tucker), ¶ [0053].

Response To Arguments

Tucker and Perry – using the eKey

Patent Owner states:

“Tucker fails to teach or suggest a vehicle "configured to receive coded data from the mobile device when using the eKey" as required by Claim 1” (Remarks p. 6).

“The Office Action alleges that the alleged "coded data" in Tucker is "an activation message." But Tucker's "activation message" is not received "when using the eKey." Tucker's "activation message" merely activates the car. As recited in Tucker, after the car is activated, a user can use the "eKey" (e.g., press a button to unlock)” (Remarks p. 6). See also Malek Dec., ¶ 72–75.

Examiner disagrees that Tucker fails to receive coded data “when using the eKey”. The broadly claimed phrase “when using the eKey” can apply to not only the activation message but also to subsequent operation commands. Tucker’s

vehicle access credential (“credential”) has been interpreted to represent the eKey and the activation message includes the credential. Therefore, sending the eKey as part of the activation message represents a use of the eKey. The eKey is also used for operation commands (e.g. unlock) as Patent Owner recognizes.

Tucker and Perry – adding a server

Patent Owner states:

“Tucker recites a direct, device-centric, architecture that does not use or require server or vehicle telematics infrastructure; a POSITA would not consider it amenable to the server-oriented approach disclosed” (Remarks p. 7).

“the disclosures of Tucker actively preclude the use of, and purposely omit, a server-based architecture and the resulting need for an in-vehicle telematics unit, user accounts, and the like” (Remarks p. 7). See also Malek Dec. ¶ 78–80.

“That understanding is further confirmed by Tucker's prosecution history, wherein the Tucker applicants emphasized that Tucker involves "direct connection between the personal communications device and the vehicle" without an intermediary device” (Remarks p. 9). See also Malek Dec. ¶ 81.

“My opinion is that a POSITA, considering the Tucker reference as a whole, would understand Tucker to purposely omit, and to discourage the use of a server-oriented architecture and the resulting need for an in-vehicle telematics unit, user accounts, etc. This is reinforced by the fact that the Tucker reference is assigned to Apple Inc., a company that a POSITA would expect to know of the availability of such alternative arrangements, server-oriented solutions, and the like. It is also reinforced by my understanding that during prosecution of the Tucker application, the Tucker applicants emphasized the direct nature of communications between a "portable device" and the vehicle, without any intermediary device” (Malek Dec. ¶ 80).

Regarding a server, examiner disagrees that Tucker “actively precludes”, “purposely omit[ted]” or “discourage[d]” the use of a server. Examiner and Patent Owner are in agreement that Tucker does not require a server. However, nowhere

has Tucker been shown to disparage the use or consideration of a server. Silence regarding a server is neither a disparagement of nor a teaching away from a server.

The prosecution history (13/278,027) of the Tucker reference lacks any preclusion or discouragement against a server and sheds no light on why Tucker did not employ a server. No mention of a “server” has been located by Examiner in this prosecution history. Patent Owner and declarant point to arguments³ by the Tucker applicants addressing the phrase of claim 7 at the time: “a first direct connection between the secondary portable device and a vehicle”. The applicants argued that the applied anticipatory Sultan reference did not meet this language because Sultan had an intermediary key fob – Sultan was not “equivalent to claim 7”. That Sultan may not anticipate claim 7 is not a disparagement against use of a server. Further, this claimed direct connection is associated with the activation of the Tucker vehicle and is unrelated to the subsequent communication of vehicle usage data.

Declarant states that “a POSITA would understand those assertions [Tucker’s remarks re: Sultan] to distinguish the Tucker disclosures from arrangements in which there was an intermediary server as well” (Malek Dec. ¶ 80, annotated). These remarks were limited to Sultan’s teachings and the claims of Tucker. No reasons have been provided why they would extend to Tucker’s “disclosures” – or further, Tucker’s reasonings why a server was never disclosed, especially for transmission of vehicle usage history.

Regarding telematics, examiner disagrees that Tucker precludes the use of “the resulting need for an in-vehicle telematics unit”. Tucker already includes

³ Patent Owner and Declarant both mis-identify prosecution history statements as being filed on 5/19/2014. They were filed on 5/29/2014.

telematics functionality – such as monitoring and logging of particular drivers’ vehicle usage history, vehicle sensor outputs as well as the reporting of this data to remote devices and users. See Tucker e.g. ¶¶ 0025, 0092, 0094. The lack of a server is addressed above.

Patent Owner states:

“Perry's reference to "activation devices" diverges significantly from, and does not relate to "eKeys" as described in the '659 Patent, nor even to Tucker's recited "vehicle access credential." Rather, Perry refers to a traditional, physical "key" or "key fob" that is pre-programmed for use of the vehicle.” (Remarks p. 11). See also Malek Dec., ¶ 82.

“Perry also does not relate to controlling access or use of a vehicle, or even to a more dependable or comprehensive means for monitoring use of a vehicle; it is more concerned with privacy and whether monitoring should be permitted” (Remarks p. 11). See also Malek Dec., ¶ 83.

“Perry does not relate to allowing or restricting access to vehicles; access and use of the vehicle is unrestricted, even when known to be stolen” (Remarks p. 14). See also Malek Dec., ¶ 83.

“Perry's reference to "encrypted identifiers" is not about controlling access to, or use of the vehicle; they ensure that an owner's ability to access the "secure server" via an "Internet-enabled program" is limited to the periods when certain "secondary activation devices" (i.e., key fobs) are in active use” (Remarks p. 12–13). See also Malek Dec., ¶ 86.

The rejection relies on Perry’s teachings to communicate with a server in order to transmit vehicle usage data of a secondary user. The eKeys of the claims are addressed using Tucker. One cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Perry is absolutely related to controlling access and use of a vehicle and monitoring its use. The rejection states:

“Perry uses activation devices (e.g. electronic key fobs) to access and operate a vehicle and monitors the usage of a vehicle when a secondary activation device is used by a secondary user (e.g. teenager, valet, etc.) with limitations on vehicle operation privileges (maximum speeds, geographics locations, etc.) ... Perry also describes techniques for monitoring usage of the vehicle over the Internet when, for example, a valet is using the vehicle”.

The privacy and permission-to-monitor aspects noted by Patent Owner do not demonstrate that Perry is from a different field or is unfit to be considered for a combination with Tucker.

Patent Owner’s argument that Perry does not restrict access to a vehicle because it can be stolen is not convincing. Each of the patent, Tucker and Perry provide vehicles that can be stolen, even though they control access.

Patent Owner states:

“a POSITA would not be motivated to abandon the serverless, device-centric approach of Tucker to adopt the disparate architecture of Perry, particularly given that it would achieve little or no benefit.” (Remarks p. 16).

“Far from a mere swap of a component, it would require the addition and implementation of a vehicle telematics system, along with attendant supporting backend infrastructure that conflict with Tucker's explicitly serverless and device-centered approach.” (Remarks p. 16).

“Researchers also demonstrated that, even in 2011, the presence of a vehicle telematics unit grossly expanded the attack vector, which would dissuade a POSITA from making a modification to Tucker to include the telematics and server dependencies of Perry (or other references) absent a compelling reason do so” (Remarks p. 17).

The argument that Tucker cannot reasonably be modified to include a server because Tucker has no server is circular and not convincing, especially in view of

Tucker's lack of server disparagement, addressed above. Tucker, although not specifying a server, also states that vehicle usage information "can be transmitted in any suitable manner" (Tucker ¶ 0110). Patent Owner fails to substantively actually address the benefits articulated in the rejection, but instead merely labels them as little. As also addressed above, Tucker already employs telematics functionality. Tucker and a POSITA were well aware of security techniques of the time that would enable operations in a secure manner for the asserted combination. Tucker specifically addresses "any suitable security mechanisms" (¶ 0122) while Perry touts a secure server throughout the disclosure.

Tucker and Mikan – adding a server

Patent Owner states:

"As discussed above, Tucker discloses a device-centric approach that requires no intermediate server infrastructure, eliminating the need for a telematics unit in the vehicle itself" (Remarks p. 22). See Malek Dec., ¶ 107.

"a POSITA would not have been motivated to modify Tucker in view of Mikan because Tucker discloses doing so without the need for the divergent server-based architecture of Mikan." (Remarks p. 22). See Malek Dec., ¶ 108.

These arguments asserting Tucker's lack of server and telematics unit have been addressed above.

Patent Owner states:

"The Office Action ... relies on McNair, whose basis for modifying Tucker to include Mikan rests on Tucker's use of the word "etc."" (Remarks p. 22). See Malek Dec., ¶ 112–113.

"Considered in context, Tucker recites that the "vehicle access credential" is either created by the vehicle itself, [or] "can be provided to and locally stored in the vehicle at a previous time," listing examples of when the vehicle access

credential can be provided to the vehicle at a prior time, "during manufacturing, prior to being sold by a dealer, etc." (Remarks p. 23, annotated).

Examiner agrees that the "etc" in Tucker relates to other times when the credential can be provided to the vehicle for local storage at the vehicle. The rejection was not solely based upon the single word of "etc", nor was the "etc" term a substitute for a teaching to remotely provision a key to a vehicle. The rejection was based upon what a POSITA would have recognized given Tucker in combination with Mikan's express teachings for remotely transmitting electronic keys to a vehicle.

Patent Owner states:

"Mikan is unrelated to the creation or provisioning of eKeys; it is focused on syncing database records to map policies with a given vehicle key" (Remarks p. 24). See Malek Dec., ¶ 114.

Examiner disagrees. Mikan clearly teaches more than the syncing of policies. Mikan indeed teaches downloading of all records (including keys from a key set) of the master database to the local database for storage at the vehicle. For vehicle ID 1 these records include a key set including key 1, key 2 ... key n (See FIG. 3B showing synchronization of records between the databases). Mikan also describes transmitting the entirety of records for a vehicle requesting a full data set: "local database 203 may initiate the synchronization to pull updated data from master database 208 ... The synchronization may be a partial or complete refresh of the data. For example, the updated data may represent only the changes in the master database made since the last synchronization in a partial refresh. In a complete refresh, the updated data may represent the entire contents of master database 208 that are relevant to vehicle 201" (Mikan ¶ 0069).

Patent Owner states:

“Mikan does not suggest storing the credential used to gain access to the vehicle in its database; it actively avoided doing so” (Remarks p. 24). See Malek Dec., ¶ 115–116.

“in Mikan, the secure identifier-i.e., the purported eKey discussed in the Office Action-is not stored in the database(s) ... Instead, Mikan only discloses that the Secure ID is stored in the mobile device (see Fig. 4); the databases

store a different value to associate a key with a vehicle operation policy: a "secure ID check." ... The vehicle does not communicate with the server to receive the "secure ID,"” (Remarks p. 25).

Mikan clearly shows the storage of a key in both the server’s master database and the vehicle’s local database (see FIG. 3B). The locally stored key is obtained from the server as explained above. The rejection relied upon Tucker’s credential to address the claimed eKey. The combination of Tucker and Perry was used to establish the obviousness to have downloaded Tucker’s key to local storage in the car.

Patent Owner states:

“A POSIT A would have been disinclined to provision the "vehicle access credential" of Tucker via remote connection given serious security and privacy concerns, including the expanded attack surface that remote connectivity would create, and demonstrated vulnerabilities in such systems even prior to 2013.” (Remarks p. 25). See Malek Dec., ¶ 117.

Tucker and a POSITA were well aware of security techniques of the time that would enable operations in a secure manner for the asserted combination. Tucker specifically addresses “any suitable security mechanisms” (¶ 0122) while Mikan touts a Secure ID Check and Security Module (FIG. 4) when using its key.

Patent Owner states:

“Claim 3 is not obvious because there is no disclosure of a vehicle "configured to receive or securely store information from the server to perform authentication or verification that the coded data received from the mobile device should activate the eKey," as recited in Claim 3” (Remarks p. 26–27).

“While the Office Action refers to the alleged disclosure in Mikan of "using authentication information (e.g., secure ID check from a server)," authenticating an eKey (e.g., verifying that a received key is authentic) is different from "activating an eKey," (e.g., provisioning the eKey via a server)” (Remarks p. 27).

“In such a combination (the proposed server-centric model), it may not be possible to open/start a vehicle in remote areas with poor cellular network coverage because the vehicle would not be able to receive the information from the server to perform authentication or verification that the coded data received from the mobile device should activate the eKey” (Malek Dec., ¶ 121).

Patent Owner improperly equates “activate the eKey” with “provisioning the eKey via a server”. The words of claim 3 itself include “verification that the coded data received from the mobile device should activate the eKey”. An eKey that successfully interacts with a vehicle and allows control of vehicle functions represents an eKey that is broadly “activated”.

The rejection does not suggest that a server would be needed during use of eKeys such as opening/starting the vehicle.

Tucker, Mikan and Kleve – user account having privileges

Patent Owner states:

“Tucker discloses a self-contained, device-centric solution in which portable devices (mobile phones) directly interface with a vehicle without the need for a vehicle to have telematics capabilities or to interact with a server” (Remarks p. 29).

These arguments asserting Tucker’s lack of server and telematics unit have been addressed above.

Patent Owner states:

“A POSITA would understand Tucker not to require the added complexity of server and account-based registration, and to advocate for the different approach recited in its disclosures. For example, contrary to the supposed need for account registration expressed by McNair, Tucker discloses an alternative device-centric registration approach” (Remarks p. 29).

“Properly considered, there would have been no motivation for the purported combination, as Tucker itself disclosed a means to achieve the purported benefits espoused by McNair without the need for a server or account-based administration. Malek ¶ 130. Account-based administration is a product of server-based architecture, which Tucker expressly did not adopt” (Remarks p. 30). See (Malek Dec., ¶ 130).

The argument that Tucker cannot reasonably be modified to include an account registration feature because Tucker has no account registration or server is circular and not convincing. That Tucker already allows a first device to authorize a second device does demonstrate error with the articulation of obviousness presented in the rejection.

Patent Owner states:

“a POSITA would understand that a "user account" does not verify identity; but even to the extent that something more than mere presence of the device would be desirable (e.g., something known, like a password,) Tucker addresses that concern. Tucker recites in its discussion of Fig. 9, "a flow diagram of a process 900 for accessing a vehicle," that "the connection procedure can be initiated and performed manually or semi-automatically (e.g., a user must provide a PIN, etc.).”” (Remarks p. 30).

Patent Owner points to a PIN that is not only an optional feature, but is only used for vehicle connection, not for administrative granting or limiting of privileges.

Tucker and Cazanans

Patent Owner states:

“The art of record does not teach that "the coded data is unique for said eKey," as required by independent Claims 11 and 18” (Remarks p. 31).

“Tucker recites that a vehicle access credential is not unique, but rather is the same between primary and secondary devices (e.g., Tucker, [0022]),” (Remarks p. 32). See (Malek Dec., ¶¶ 137–139).

“The Office Action does not address this express disclosure of non-uniqueness” (Remarks p. 32).

The action addresses the claimed uniqueness of the coded data by pointing to the portions of Tucker which clearly specify uniqueness in Tucker’s own words (“[i]n some embodiments, the vehicle access credential can include a uniquely generated value,” Tucker ¶¶ 0071).

Rather than accepting or rebutting Tucker’s explicit teaching for uniqueness, Patent Owner diverts the discussion towards other statements by Tucker. In this case, Patent Owner points asserts examples where an access credential may be a copy of another access credential. However, a full reading of Tucker also shows that in this scenario Tucker also contemplates a unique secondary access credential:

“in some embodiments, the access credential provided to a primary portable device (designated as the primary access credential) from a vehicle might not be the same as the access credential provided to a secondary portable device (designated as the secondary access credential) from the primary portable device” (Tucker ¶¶ 0126).

Patent Owner states:

“Patent Owner incorporates by reference its discussion of the device-oriented architecture of Tucker and its incompatibility with server-based architectures discussed above” (Remarks p. 34).

Examiner has addressed the server vs. no server arguments above and these positions also apply to Tucker in view of Cazan as.

Patent Owner states:

“a POSITA would not be motivated to do so, as there would be little to no benefit achieved from the addition of Cazan as given Tucker's own (and different) approach for "personalization operation.” (Remarks p. 34). See (Malek Dec., ¶ 144).

“Cazan as stands in stark contrast to Tucker, and a POSITA would find their divergent approaches to be incompatible with one another. The references have differing objectives that a POSITA would not see as complimentary given the need for significant modifications to both systems to combine them, particularly given the architectural mismatch (e.g., Cazan as's centralized web server for user account management and profile storage, while Tucker operates in a decentralized manner, without user accounts)” (Remarks p. 35). See (Malek Dec., ¶ 145).

Admitting benefit from the combination but asserting it to be little is not effective to overcome the articulation of obviousness.

Tucker and Cazan as are not incompatible and both provide electronic access to vehicles via Tucker’s mobile device sending a credential to a vehicle and Cazan as’s keyless entry token or key fob (6:61–62). Both also contemplate multiple users having electronic access to the same vehicle according to different stored elements in such a vehicle (see Cazan as 7:25–41), including a primary and secondary user. Examiner is not proposing to modify both, but rather modify Tucker in view of Cazan as as articulated in the rejection.

Patent Owner states:

“a POSITA would also have understood (and been dissuaded by) significant security concerns related to the addition of a vehicle telematics unit and

server infrastructure under the potential Tucker-Cazanas combination”
(Remarks p. 35). See (Malek Dec., ¶ 145).

Tucker and a POSITA were well aware of security techniques of the time that would enable operations in a secure manner for the asserted combination. Cazanas having provided a telematics unit in communication with a server also represents the notion that they can be provided, despite security “concerns”.

Patent Owner states:

“Claim 13 recites: "wherein a server associated with a manufacturer of the vehicle is configured to communicate with the application, the application further being associated with a manufacturer of the vehicle." As discussed in detail above and acknowledged in the Office Action, Tucker does not disclose communication with a server, much less a plurality of servers, or of a server associated with a manufacturer of the vehicle” (Remarks p. 38).

“Tucker also does not teach that an application is "associated with a manufacturer of the vehicle."” (Remarks p. 38).

Tucker’s lack of server has been addressed above. The rejection addresses a server associated with a manufacturer, a plurality of servers and user applications and accounts that are associated with such servers when used with the service.

Patent Owner states:

“Claim 17 recites: "wherein said eKey is validated and securely bound to the mobile device to prevent unauthorized transfers of the ekey."” (Remarks p. 38).

“Office Action, citing McNair, states that the vehicle of Tucker validates that the vehicle access credential "originated from the primary portable device., id. ¶ [0082]... " But Tucker does not teach verifying that a vehicle access credential "originated from the primary portable device." Tucker only discloses "determining the authenticity of the vehicle access credential included in the activation message."” (Remarks p. 38). See (Malek Dec., ¶ 150).

As discussed above (see, e.g., discussion beginning at page 32), Tucker recites that the same "vehicle access credential" used for the "primary portable device," the "secondary portable device," and other "primary portable devices" (e.g., transfer from one device to another)." (Remarks p. 38–39).

Patent Owner fails to show why any of the three elements used to reject the claim are faulty. The rejection addresses how Tucker validates and securely binds the eKey to the mobile device to prevent unauthorized transfers. Patent Owner's arguments that determining authenticity is not validating is not convincing, especially in view of the fact that Tucker indeed teaches uniqueness for an eKey (also addressed above).

Secondary Considerations

Patent Owner states:

"Failure of Others and Long-Felt Need" (Remarks p. 41).

"The work of the Consortium circa 2018 to develop technology for electronic keys-and the desire for a standardized solution-demonstrates that the problem was significant and not easily solved. Despite the extensive resources of industry leaders, the problem of integrating OEM servers for secure mobile phone access to vehicles remained unresolved" (Remarks p. 41).

Alleged work by others after Patent Owner's invention is not dispositive of nonobviousness. Nor is alleging that a "problem" remains unsolved after Patent Owner's invention. Patent Owner fails to provide any timeline before the invention or any long-felt need as part of that pre-invention timeline.

Patent Owner states:

"Industry Adoption and Standardization" (Remarks p. 42).

"The Consortium, which includes almost all automakers, is actively working toward standardizing digital keys for use with mobile phones. This industry-wide effort to create a uniform standard reinforces the notion that the

solution to the problem of physical key limitations, security, and provisioning by servers to mobile phones was not obvious. The fact that the consortium turned to standardization and collaboration among major players in the industry further supports the uniqueness and non-obviousness of the claims of the '659” (Remarks p. 42).

Ongoing standardization says little about nonobviousness, especially when there is no nexus established to any claimed invention.

Patent Owner states:

“Commercial Success and Industry Recognition” (Remarks p. 42).

“The interest of the world's leading automakers in standardizing digital keys further supports the commercial success of the claimed inventions of the '659 Patent and their importance to the industry. The widespread recognition and pursuit of a similar solution through industry collaboration highlights the innovative nature of the work by the inventors of the” (Remarks p. 42).

Patent Owner provides no evidence of success, identifies no particularly defined “success” and identifies no nexus to any of the claimed inventions. Interest in standardizing among automakers after Patent Owner’s invention says nothing about success or recognition of the invention, per se.

Conclusion

The patent owner is reminded of the continuing responsibility under 37 CFR 1.565(a) to apprise the Office of any litigation activity, or other prior or concurrent proceeding, involving Patent No. US Patent 11,738,659 throughout the course of this reexamination proceeding. The third party requester is also reminded of the ability to similarly apprise the Office of any such activity or proceeding throughout the course of this reexamination proceeding. See MPEP §§ 2207, 2282 and 2286.

THIS ACTION IS MADE FINAL.

A shortened statutory period for response to this action is set to expire TWO MONTHS from the mailing date of this action.

Extensions of time under 37 CFR 1.136(a) do not apply in reexamination proceedings. The provisions of 37 CFR 1.136 apply only to “an applicant” and not to parties in a reexamination proceeding. Further, in 35 U.S.C. 305 and in 37 CFR 1.550(a), it is required that reexamination proceedings “will be conducted with special dispatch within the Office.”

Extensions of time in reexamination proceedings are provided for in 37 CFR 1.550(c). A request for extension of time must specify the requested period of extension and it must be accompanied by the petition fee set forth in 37 CFR 1.17(g)(1). Any request for an extension in a third party requested ex parte reexamination must be filed on or before the day on which action by the patent owner is due, and the mere filing of a request will not effect any extension of time. A request for an extension of time in a third party requested ex parte reexamination will be granted only for sufficient cause, and for a reasonable time specified. Any request for extension in a patent owner requested ex parte reexamination (including reexamination ordered under 35 U.S.C. 257) for up to two months from the time period set in the Office action must be filed no later than two months from the expiration of the time period set in the Office action. A request for an extension in a patent owner requested ex parte reexamination for more than two months from the time period set in the Office action must be filed on or before the day on which action by the patent owner is due, and the mere filing of a request for an extension for more than two months will not effect the extension. The time for taking action in a patent owner requested ex parte reexamination will not be extended for more

than two months from the time period set in the Office action in the absence of sufficient cause or for more than a reasonable time.

The filing of a timely first response to this final rejection will be construed as including a request to extend the shortened statutory period for an additional two months. In no event, however, will the statutory period for response expire later than SIX MONTHS from the mailing date of the final action. See MPEP § 2265.

All correspondence relating to this ex parte reexamination proceeding should be directed:

By Mail to: Mail Stop *Ex Parte* Reexam
Central Reexamination Unit
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

By FAX to: (571) 273-9900
Central Reexamination Unit

By hand: Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Information regarding the status of reexamination proceedings may be obtained from Patent Center. To file and manage patent submissions in Patent Center, visit: <https://patentcenter.uspto.gov>. Visit <https://www.uspto.gov/patents/apply/patent-center> for more information about Patent Center and <https://www.uspto.gov/patents/docx> for information about filing in DOCX format. For additional questions, contact the Electronic Business Center

Application/Control Number: 90/019,456
Art Unit: 3992

Page 55

(EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Any inquiry concerning this communication should be directed to **the Central Reexamination Unit** at telephone number **517-272-7705**.

/JEFFREY D CARLSON/
Primary Examiner, Art Unit 3992

Conferees:

/C. Michelle Tarae/
Reexamination Specialist, Art Unit 3992
/MICHAEL FUELLING/
Supervisory Patent Examiner, Art Unit 3992