UnifiedPatents

PATROLL Winning Submission

U.S. Patent 11,738,659

U.S. Patent 11,738,659 ("*Emerging Automotive*" or the "patent-at-issue") was filed on August 30, 2021 and claims an earliest priority date on April 22, 2011. Claim 1 of the patent-at-issue is generally directed to a sub-system within a vehicle, where the vehicle incorporates an on-board computer interfaced with the sub-system to process instructions for the utilization of an electronic key (eKey). The sub-system comprises memory associated with the vehicle's on-board computer, containing program instructions for unlocking and starting the vehicle. Additionally, the vehicle is equipped with communications circuitry that interfaces with the on-board computer and the sub-system. This communications circuitry processes program instructions for communication with a server, incorporating wireless communication circuitry for local connection with a mobile device. The mobile device is configured to utilize the eKey for unlocking and starting the vehicle. The wireless communications circuitry is designed to receive coded data from the mobile device when using the eKey. This coded data facilitates the functions of the eKey for unlocking and utilizing the vehicle, and it is associated with the eKey for use by the mobile device. Importantly, the coded data includes privilege settings, which restrict certain types of vehicle use when employing the eKey. Furthermore, the patent discloses that the use of the vehicle with the eKey is monitored to identify and log actions taken while the eKey is in use.

A primary reference, U.S. Pat. App. 2008/0150683 ("*Hyundai*"), was filed on December 21, 2006, and claims priority on the same date. The patent is directed to a method and wireless devices aimed at ensuring secure vehicle operation. The disclosed method involves detecting a key within a wireless device, like a cellular telephone, used for accessing the vehicle. Upon detection, the associated vehicle operation policy is retrieved, dictating the permissible operation of the vehicle. This policy encompasses access control rules that determine the enabling, partial enabling, or disabling of specific vehicle operation features. If the intended vehicle operation contradicts the access control rules, the operation is restricted, and enforcement actions, such as disabling certain vehicle features, may be implemented to maintain security.

A secondary reference, U.S. Patent 7,868,736 ("*Toshiba*"), was filed on July 25, 2006, and claims priority on January 26, 2004. The patent is directed to a system involving authentication processes beyond electronic key verification, extending to include the authentication of an ID card and user authentication information. Upon successful completion of these authentication steps, engine startup information is generated. This multifaceted authentication approach serves as a preventive measure against vehicle theft, as it ensures that even if electronic key data or the electronic key device is copied, unauthorized access to the vehicle is thwarted.

A secondary reference, JP2009293283 ("*Tokai Rika*"), was filed on June 5, 2008, and claims priority on the same date. The patent is directed to an electronic key system designed to maintain a high level of security in a vehicle with multiple electronic keys. The electronic key system comprises a master key and subkeys that perform wireless communication with the vehicle. The unlocking of the vehicle door is executed through a door lock mechanism based on the authentication of both the master key and subkeys via wireless communication. Notably, the system includes a provision to restrict the unlocking of the vehicle door based on the authentication of subkeys by the owner of the vehicle, who possesses the master key and can control this function through a car navigation apparatus. A case for storing the subkeys is provided in the vehicle, and the patent specifies the forceful prohibition of unlocking the vehicle door when the subkeys are stored in this case. The invention aims to enhance security in scenarios where multiple electronic keys are in use.

A sample claim chart comparing claim 1 of *Emerging Automotive* to *Hyundai*, *Toshiba*, and *Tokai Rika* is provided below.

US11738659 (“*Emerging Automotive*”)	**A. US20080150683** (*“Hyundai”*) **B. US7868736** (*“Toshiba”*) **C. JP2009293283** (*“Tokai Rika”*)
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:	**A. US20080150683** “**Wireless vehicle security system** 200 **may secure access and operation of vehicle** 201. **Vehicle** 201 **may be a car, truck, boat, motorcycle or other mechanism for transporting people or things**. **Vehicle** 201 **may support various vehicle operation features such as unlocking a door, opening a trunk, opening a glove box, engaging an ignition, directing the vehicle from a one geographic location to a another geographic location, and accelerating the vehicle, for example. Any aspect of the control, use, or functionality of vehicle** 201 **may be considered a vehicle operation feature**. **The system may include one or more keys** 205A-C **control unit** 202 **and local database** 203**, for example. Keys** 205A-C **may be electronic keys, traditional metal keys, or a combination of both**. In one embodiment, keys 205A-C may be embedded in a wireless device such as a cellular telephone or Personal Digital Assistant (PDA), for example.” *Hyundai* at par. 0049-0050 “Control unit 202 may be any combination of hardware and/or software that is in operative communication with vehicle 201 and keys 205A-C. For example, the **control unit may be an onboard computer**.” *Hyundai* at par. 0051 **B. US7868736** 11. **A program for use in a computer of a vehicle authenticating device which is mounted on a vehicle** capable of running in accordance with engine startup information and **which authenticates a user of the vehicle based on an electronic key device having electronic key data (K) stored therein, the program stored in the vehicle authenticating device**” *Toshiba* at Claim 11

(cont.) 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:	**C. JP2009293283** “**A master key that can be collectively executed, and a sub key that can limit the execution of various processes relating to the vehicle control**, and based on a predetermined operation on the in-vehicle device, **An electronic key system for a vehicle in which execution of various processes related to vehicle control is restricted and the restriction is released** . . .” *Tokai Rika* at Claim 1 “Based on the transmission of such a request signal, the control device 21c of the **master key** 21 **generates a response signal including the ID code IDA** stored in the built-in memory and transmits the response signal to the transmission device 21b of the master key 21. This response signal is transmitted to the vehicle 10. When the response signal is transmitted in this manner, the vehicle receiving device 13 receives the response signal and transmits the received response signal to the vehicle-side control device 14. As a result, the **vehicle-side control device** 14 **collates the ID code IDA included in the transmitted response signal with the ID code registered in the ID code database** 14a **as described above. When the authentication is performed, the vehicle door is unlocked through the door lock mechanism** 15 which is a control target.” *Tokai Rika* at p. 4 of translated document
memory associated with the on-board computer of the vehicle **having program instructions for instructing unlocking and starting of the vehicle**; and	**A. US20080150683** “Vehicle 201 may receive a user request, such as an access request for example. **The access request may include unlocking a door, opening a trunk, opening a glove box, engaging an ignition, directing the vehicle from a first geographic location to a second geographic location, and accelerating the vehicle**, for example. To illustrate, the user may approach the vehicle 201, signal the secure ID 407 and an **access request to unlock a vehicle door**. To illustrate, **the user may be operating the vehicle and press the accelerator of the vehicle, signaling an access request to accelerate the vehicle**.” *Hyundai* at par. 0073 “**Control unit** 202 **may be any combination of hardware and/or software** that is in operative communication with vehicle 201 and keys 205A-C. For example, the control unit may be an onboard computer.” *Hyundai* at par. 0051 “Control unit 202 may interface with vehicle 201.

(cont.) **memory** associated with the on-board computer of the vehicle **having program instructions for instructing unlocking and starting of the vehicle**; and	**Control unit** 202 **may control vehicle functions** and may sense operation of vehicle 201. **For example, control unit** 202 **may signal to lock and unlock the vehicle doors**." *Hyundai* at par. 0053 **B. US7868736** 11. **A program for use in a computer of a vehicle** authenticating device which is mounted on a vehicle **capable of running in accordance with engine startup information** and which authenticates a user of the vehicle based on an electronic key device having electronic key data (K) stored therein, the program stored in the vehicle authenticating device, the program comprising: **a first program code for causing the computer to execute a processing operation of storing in a memory** an encrypted engine master key (E (EK)) produced when an engine master key (EK) is encrypted in accordance with the electronic key data (K) . . . *Toshiba* at Claim 11 "**The engine control device** 7 has a tamperproof area for storing the engine master key EK at the time of shipment from a manufacturer. **This device has a function of carrying out mutual authentication with the security device** 10 **by using this engine master key EK and a function of**, when mutual authentication has been successfully made and **if engine startup information S is received from the security device** 10, **controlling an engine**. **The engine master key EK is provided as an authenticating key for starting up an engine**." *Toshiba* at col. 7:1-9 **C. JP2009293283** "**The control device** 14 **collates the ID code of the electronic key 20 included in the received response signal with the ID code stored in the memory in the control device 14 in advance**. When the authentication is performed, **vehicle control such as unlocking the door lock mechanism** 15 **provided on the vehicle door or permitting the engine to start is executed**." *Tokai Rika* at p. 2 of translated document "As shown in FIG. 1, this electronic key system also **unlocks the aforementioned vehicle door or permits the engine to be started through wireless communication between the vehicle 10 and the electronic key** (portable device) 20." *Tokai Rika* at p. 3 of translated document

communications circuitry of the vehicle **interfaced with the on-board computer of the vehicle and the sub-system**,	**A. US20080150683** “**Control unit** 202 **may be any combination of hardware and/or software that is in operative communication with vehicle** 201 and keys 205A-C. For example, the **control unit may be an onboard computer.** In one embodiment, key 205A-C may communicate directly with control unit 202. **For example, key** 205A-C **and control unit** 202 **may communicate directly via a radio frequency transmission**.” *Hyundai* at par. 0051 “**Control unit** 202 **may be in communication with wireless network** 207.” *Hyundai* at par. 0052 **B. US7868736** “This vehicle authenticating device is mounted on a vehicle such as a car, **and an electronic key reader** 1**, a user information input device** 3**, an ID card reader** 4**, a communication device** 6**, and an engine control device** 7 **are connected to a security device** 10.” *Toshiba* at col. 3:10-14
the **communications circuitry** is **configured to process program instructions to enable communication with a server**	**A. US20080150683** “**Wireless communications module** 403 **may be a subsystem suitable to provide communications between wireless device** 400 **and wireless network** 207. Wireless communications module 403 may include a modulator, a transmitter, a receiver and an antenna, for example. In one embodiment, wireless communications module 403 may enable communication over a GSM or GPRS network for example. **Wireless communications module** 403 **may communicate the update request via wireless network** 207. Wireless communications module 403 may support telephony and data services.” *Hyundai* at par. 0064 “**Control unit** 202 **may be in communication with wireless network** 207. Wireless network 207 may be any system suitable for wirelessly sending and receiving data. Wireless network 207 may be a GSM network, a GPRS network, an EDGE network, Wideband Integrated Dispatch Enhanced Network (WilDEN), Wideband Code Division Multiple Access (W-CDMA) network, Wireless Local Area Network (WLAN), or a 802.11a/b/g/n network, for example. **In one embodiment, wireless network** 207 **may host master database** 208 **and application** 209. Wireless network 207 may interconnect with other networks, such as corporate extra nets, private networks, the Internet, or the public switched

(cont.) the **communications circuitry** is **configured to process program instructions to enable communication with a server**	telephone network (PSTN), for example." *Hyundai* at par. 0052 "Master application 209 may be any interface, software, or device suitable for managing communication to and from master database 208. For example, **master application** 209 **may be software resident on a server platform**, may be integrated into master database 208, may stand alone, etc. In one embodiment, master application 209 may include a hypertext transfer protocol (HTTP) server." *Hyundai* at par. 0055 **B. US7868736** "The computer according to the present invention executes the processes according to the present embodiment on the basis of the programs stored in the storage media. **The computer may be arbitrarily configured; it may comprise one apparatus similarly to a personal computer** or **may be a system in which a plurality of apparatuses are connected together via a network.**" *Toshiba* at col. 19:13-20
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**;	**A. US20080150683** "For example, **where key** 205B **is part of a mobile telephone, the user of the mobile telephone may use the mobile telephone to send updates to master database** 208 **via master application** 209." *Hyundai* at par. 0056 "Control unit 202 may be any combination of hardware and/or software that is in operative communication with vehicle 201 and keys 205A-C. For example, the control unit may be an onboard computer. In one embodiment, key 205A-C may communicate directly with control unit 202. For example, **key** 205A-C **and control unit** 202 **may communicate directly via a radio frequency transmission**." *Hyundai* at par. 0051 "1. A method for providing secure operation of a vehicle comprising: …. retrieving a vehicle operation policy from a first database, where the **vehicle operation policy is associated with the key**, and; **permitting operation of the vehicle consistent with the vehicle operation policy**." *Hyundai* at claim 1

(cont.) 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**;	"7. The method of claim 5, wherein the **vehicle operation feature corresponds to** any one of: **unlocking a door**, opening a trunk, opening a glove box, **engaging an ignition**, directing the vehicle from a first geographic location to a second geo graphic location, and accelerating the vehicle." *Hyundai* at claim 5 **B. US7868736** "In addition, **the ID card** 5 **can be changed to an arbitrary ID device such as a cellular phone**, an electronic notebook, a personal computer, an ID tag, a pendant, a badge, or an electronic book, without being limited to a card shaped ID device. In this case, similarly, it is a matter of course that the ID card reader 4 can be changed to a reader of an arbitrary ID device without being limited to an ID card reader." *Toshiba* at col. 3:58-64 "**A specific configuration is featured in that an electronic key registering device** 1 r **and a registration ID card reader** 4 r **having functions similar to those of the electronic key reader** 1 **and the ID card reader** 4 described previously are connected to a security device. **In the security device** 10**, a vehicle information storage area** 13 **is eliminated, and a private key information storage area** 18 **is provided**." *Toshiba* at col. 8:55-61 "10. A vehicle authenticating method for use in a vehicle authenticating device which is mounted on a vehicle capable of running in accordance with engine startup information and which authenticates a user of the vehicle based on an electronic key device having electronic key data (K) stored therein, the method comprising: ... **producing the engine startup information by using the engine master key** (EK)**, and** **outputting the obtained engine startup information**." *Toshiba* at claim 10 **C. JP2009293283** "That is, **when the vehicle owner having the electronic key** 20 **enters the communicable area A or the communicable area B, a response signal is transmitted from the electronic key** 20. In this system, **the response signal transmitted from the electronic key** 20 **is received by the receiving device** 13 **provided in the vehicle compartment and transmitted to**

(cont.) 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**;	**the vehicle-side control device** 14 **that executes various controls on the vehicle** 10. The control device 14 collates the ID code of the electronic key 20 included in the received response signal with the ID code stored in the memory in the control device 14 in advance. **When the authentication is performed**, **vehicle control such as unlocking the door lock mechanism** 15 **provided on the vehicle door or permitting the engine to start is executed**” *Tokai Rika* at p. 2 of translated document
wherein the **wireless communications circuitry** of the vehicle **is configured to receive coded data from the mobile device when using the eKey**,	**A. US20080150683** “Next, mobile subscriber 119 establishes a user session with the destination network, corporate network 136, by going through a Packet Data Protocol (“PDP”) activation process. Briefly, in the process, **mobile subscriber** 119 **requests access to the Access Point Name (“APN”), for example, UPS.com (e.g., which can be corporate network** 279**) and SGSN** 130 **receives the activation request from mobile subscriber** 119**. SGSN** 130 **then initiates a Domain Name Service (“DNS”) query to learn which GGSN node has access to the UPS.com APN. The DNS query is sent to the DNS server within the core network** 124**, such as DNS** 131**, which is provisioned to map to one or more GGSN nodes in the core network** 124. Based on the APN, the mapped GGSN 132 can access the requested corporate network 279. The SGSN 130 then sends to GGSN 132 a Create Packet Data Protocol (“PDP”) Context Request message that contains necessary information. The GGSN 132 sends a Create PDP Context Response message to SGSN 130, which then sends an Activate PDP Context Accept message to mobile subscriber 119.” *Hyundai* at par. 0027 1. **A method for providing secure operation of a vehicle comprising**: **detecting a key for accessing a vehicle**; **retrieving a vehicle operation policy from a first database, where the vehicle operation policy is associated with the key**, and; permitting operation of the vehicle consistent with the vehicle operation policy. 2. The method of claim 1, **wherein said detecting comprises receiving a secure key identifier from a wireless device**. *Hyundai* at Claims 1 and 2

(cont.) wherein the **wireless communications circuitry** of the vehicle **is configured to receive coded data from the mobile device when using the eKey**,	**B. US7868736** “Here, **the electronic key reader** 1 has: **a function of inserting and removing a portable electronic key** 2**, and then, transmitting the data read from the electronic key** 2 **to the security device** 10**; and a function of inputting the data received from the security device** 10 **to the electronic key** 2.” *Toshiba* at col. 3:15-19 **C. JP2009293283** “A response signal including is transmitted. **On the other hand, the vehicle** 10 **transmits the request signal to the outdoor transmission device** 11 **for transmitting the above request signal to the communicable area A set around the vehicle door, and to the communicable area B set in the vehicle interior**. And **a receiving device** 13 **for receiving response signals transmitted from the master key** 21 **and the sub keys** 22 **and** 23.” *Tokai Rika* at p. 3 of translated document
the **coded data enables functions of said eKey for said unlocking and use of the vehicle**	**A. US20080150683** “At 516, the control unit 202 may block and/or limit operation of vehicle 201 may occur when an access request does not conform with vehicle operation policy 311 or may occur when a vehicle operation feature being monitored no longer conforms with vehicle operation policy 311. In such a situation, and in one embodiment, control unit 202 may disallow the operation. For example, **where key** 205A-C **signals an access request to vehicle** 201 **to unlock a door and the access request is not allowed by vehicle operation policy** 311 **retrieved for that specific key** 205A-C**, blocking operation may include maintaining the locked condition of the doors, or if the doors were previously unlocked, blocking may include locking the doors**.” *Hyundai* at par. 0077 **B. US7868736** “In addition, in the case where a plurality of users use a vehicle, **an electronic key is newly issued for each user without producing a duplicate electronic key, making it possible to use a vehicle**. In addition, an electronic key is revoked for each user, making it impossible to use a vehicle. **In this manner, the use of a vehicle is enabled or disabled for each user**. Thus, a theft at the time of car rental can be prevented while in operation such as car rental, enabling safe vehicle rental.” *Toshiba* at col. 13:62-67 through col. 14:1-3

(cont.) the **coded data enables functions of said eKey for said unlocking and use of the vehicle**	"10. A vehicle authenticating method for use in a vehicle authenticating device which is mounted on a vehicle capable of running in accordance with engine startup information and which authenticates a user of the vehicle based on an electronic key device having electronic key data (K) stored therein, the method comprising: ... **producing the engine startup information by using the engine master key** (EK)**, and** **outputting the obtained engine startup information**." *Toshiba* at claim 10 **C. JP2009293283** "That is, **when the vehicle owner having the electronic key** 20 **enters the communicable area A or the communicable area B, a response signal is transmitted from the electronic key** 20. In this system, **the response signal transmitted from the electronic key** 20 **is received by the receiving device** 13 **provided in the vehicle compartment and transmitted to the vehicle-side control device** 14 **that executes various controls on the vehicle** 10. The control device 14 collates the ID code of the electronic key 20 included in the received response signal with the ID code stored in the memory in the control device 14 in advance. **When the authentication is performed**, **vehicle control such as unlocking the door lock mechanism** 15 **provided on the vehicle door or permitting the engine to start is executed.**" *Tokai Rika* at p. 2 of translated document
the **coded data** is **associated to the eKey for use by the mobile device**	**A. US20080150683** "As illustrated here, core network 124 may comprise **Mobile Switching Center ("MSC")** 125, Service Control Point ("SCP") 126, gateway MSC 127, SGSN 130, Home Location Register ("HLR") 129, **Authentication Center ("AuC")** 128, Domain Name Server ("DNS") 131 and GGSN 132. Interconnect network 137 also comprises a host of various networks and other network elements. **As illustrated in FIG. 1B, interconnect network** 137 **comprises Public Switched Telephone Network ("PSTN")** 133, Fixed-End System ("FES") or Internet 134, firewall 135 and Corporate Network 136." *Hyundai* at par. 0021 1. **A method for providing secure operation of a vehicle comprising**: **detecting a key for accessing a vehicle**;

(cont.) the **coded data** is **associated to the eKey for use by the mobile device**	**retrieving a vehicle operation policy from a first database, where the vehicle operation policy is associated with the key**, and; permitting operation of the vehicle consistent with the vehicle operation policy. 2. The method of claim 1, **wherein said detecting comprises receiving a secure key identifier from a wireless device**. *Hyundai* at Claims 1 and 2 “In one embodiment, **keys** 205A-C **may be embedded in a wireless device such as a cellular telephone** or Personal Digital Assistant (PDA), for example.” *Hyundai* at par. 0050 **C. JP2009293283** “And **a receiving device** 13 **for receiving response signals transmitted from the master key**” *Tokai Rika* at p. 3 of translated document
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**;	**A. US20080150683** “**Mapping** 312 **may link vehicle operation policy** 311 **and keys** 205A-C. To illustrate this point, **one embodiment may include two keys, first with greater access than the second**. **The first key**, in this example illustration, **may be related via mapping** 312 **to access control rule** 317 **that enables all vehicle operation features**. **The second key**, in this illustration, **may be a “valet key” with limited functionality.** For example, **the second key may be related to three access control rules** 317**: a first rule that disables access to the trunk and glove box, a second rule that limits the maximum speed to 35 miles per hour, and a third rule that limits the total allowed distance traveled to one mile**.” *Hyundai* at par. 0061 **B. US7868736** “**The ID card (ID device)** 5 **has a general IC card function** and is capable of communicating with the security device 10 via the ID card reader 4. **This ID card stores personal information for specifying an individual user, a hash key (user specific key) I generated from this personal information, license classification information L issued on the receipt of a driver's license, and a certificate C issued from a specific authorized organization**. Here, **the privacy information, the hash key I, the license classification information L, and certificate C are stored at the time of**

(cont.) 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**;	**ID card issuance. The data contained in the ID card** 5 **can be read/written only by a person having a specific privilege**. **The ID card owner can read the data, but cannot write it**." *Toshiba* at col. 3:45-57 "**The registrant's ID card** 5 r **is similar to the user's ID card** 5 described previously. In addition, **the data contained in the ID cards** 5M **and** 5 r **can be read/written by only a person having a specific privilege, and the ID card owner can read the card, but cannot write to it**, in the same manner as that described previously." *Toshiba* at col. 9:25-30 **C. JP2009293283** "Since it is **possible to prevent unauthorized use such as operation of the in-vehicle device during the absence, the security level as a system can be improved**. Moreover, **if the restriction of the execution of various processes related to vehicle control based on the authentication of the subkey and the release of the restriction are performed based on a predetermined operation with respect to the in-vehicle device, the vehicle owner can respond to the usage status of the subkey**. As described above, **it is possible to appropriately limit the functions of the subkeys and to appropriately prevent unauthorized use of the subkey by a third party**." *Tokai Rika* at p. 2 of translated document
wherein **use of the vehicle using the eKey is tracked to identify and log actions taken using the vehicle while the eKey is used**.	**B. US7868736** 10. A vehicle authenticating method for use in a vehicle authenticating device which is mounted on a vehicle capable of running in accordance with engine startup information and **which authenticates a user of the vehicle based on an electronic key device having electronic key data (K) stored therein**, the method comprising: ... **outputting the obtained engine startup information**. *Toshiba,* Claim 10 "At 514, the **control unit** 202 **may monitor the status of a particular vehicle operation feature and confirming its conformance with vehicle operation policy** 311 **associated with the key** 205A-C **that is currently in use**." *Hyundai* at par. 0076 **C. JP2009293283**

(cont.) wherein **use of the vehicle using the eKey is tracked to identify and log actions taken using the vehicle while the eKey is used**.	"Therefore, **the vehicle owner can validate / deactivate the function appropriately according to the usage status of the sub key, such as validating the ID code when renting the sub key and invalidating the ID code when returning the sub key.** Thus, unauthorized use of the subkey by a third party as described above can be suitably prevented." *Tokai Rika* at p. 2 of translated document