PATROLL Winning Submission

U.S. Patent 9,365,188

U.S. Patent 9,365,188 ("*Emerging Automotive*" or the "patent-at-issue") was filed on June 12, 2014, and has an earliest priority date on April 22, 2011. Claim 1 of the patent-at-issue describes a method involving a server which receives a request from a user account linked to a vehicle to create an electronic key (e-key). The request includes specific conditions set by the user for the vehicle's use. The server generates this e-key and sends it to the recipient through electronic means, enabling the recipient's device to use the e-key. Additionally, the server transmits necessary data to the vehicle, allowing it to be used with the e-key. As the vehicle is utilized with this e-key, the server collects data on its usage, including any instances where the specified conditions for use are violated. This information is then analyzed by the server, which is accessible via the internet and communicates with the vehicle's wireless systems and other connected servers, facilitating the e-key generation and usage analysis.

The primary reference, JP2004190233 ("*Mitsui*"), was filed on December 6, 2002, and claims priority on the same date. The patent describes an on-vehicle device for managing automobile unlocking, a user terminal acting as an electronic key, and a key server issuing key data for this electronic key. The system operates as follows: the user terminal sends its ID, vehicle ID, and intended usage duration to the key server, requesting key data. Upon receiving this request, the key server sets the vehicle's usable period based on the reservation status and issues a terminal key and server key, both authenticated for this duration. The key server stores the server key and sends the terminal key to the user terminal. When the user wishes to use the car, the terminal key is transmitted to the vehicle-mounted device. If both the server and terminal keys are valid within the designated period, and the verification is successful, an unlock signal is sent to the in-vehicle device. Upon receiving this signal, the in-vehicle device unlocks the vehicle, having received both the terminal key from the user terminal and the server key from the key server.

A secondary reference, U.S. Patent 7,868,736 ("*Toshiba*"), was filed on July 25, 2006, and claims an earliest priority date on January 26, 2004. The patent describes a security device integrated into a vehicle authentication system, and operates within a vehicle to verify user access via an electronic key device containing electronic key data (K). The system includes storage for an encrypted engine master key derived from encrypting an engine master key in line with the electronic key data, a certificate information repository with an ID device certificate verification key, a user-specific key, and user-specific certificates. This device validates the ID device's certificate and, upon confirmation, prompts the ID device to authenticate user-inputted information based on personal details. It also verifies a digital signature applied to the electronic key data using a signature verification key, decrypts the encrypted engine master key once successful authentications occur, generates engine startup information using this key, and ultimately outputs this information. Essentially, it ensures secure vehicle operation by meticulously verifying both the ID device and the electronic key data before allowing engine startup.

A secondary reference, U.S. Pat. App. 2008/0150683 ("*Hyundai*"), was filed on December 21, 2006, and claims priority on the same date. The patent application describes a

vehicle access control process involving the detection of a key for vehicle access, retrieving a specific vehicle operation policy associated with that key, and allowing vehicle operation within the parameters of this policy. The key, embedded in a wireless device initiates access and applies a set of rules governing vehicle functionalities based on an access control rule. If the intended operation contradicts this rule, access may be denied, and enforcement actions, like feature disabling, could be implemented. Additionally, it describes database synchronization between two databases—one residing in the vehicle and the other communicating wirelessly. These databases contain access control rules to manage vehicle operations. The presented wireless device for secure vehicle operation encompasses a user interface, wireless communication capabilities for updating access control rules, a memory, processor, and a module enabling secure vehicle access via a secure identifier communicated through wireless networks.

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

US9365188 ("*Emerging Automotive* ")	**A. JP2004190233** (*"Mitsui"*) **B. US7868736** (*"Toshiba"*) **C. US20080150683** (*"Hyundai"*)
1.pre. A method, comprising, 1.a. **receiving, by a server, a request from a user via a user account that has a vehicle associated therewith to generate an electronic key (e-key) for an identified recipient to use the vehicle**, the **request includes identifying information for enabling sending of the e-key to the recipient via an electronic transmission**, the **request includes a condition of use of the vehicle as set by the user via the user account**;	**A. JP2004190233** "A terminal ID for specifying the user terminal, and a vehicle ID and **a desired use period of the vehicle input from a user who wants to use the vehicle**, are transmitted to the key server, so as to be distributed to the vehicle-mounted device. **An issuance request unit that requests issuance of an in-vehicle key that is key data and a terminal key that is key data for distribution for the user terminal**, **A key transmitting and receiving unit that receives the terminal key from the key server, and transmits the received terminal key to the in-vehicle device when the user uses the vehicle**, ..." *Mitsui* at p. 2 of the translation document **B. US7868736** "1. A security device 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 security device comprising: **key information storage device for storing an encrypted engine master key (E (EK)) obtained by encrypting an engine master key (EK) in accordance with the electronic key data (K)**; . . . ." *Toshiba* at claim 1 "The key information storage area 11 is provided as an area for storing in advance: **an encrypted engine master key EM (EK) that corresponds to electronic key data MK of an owner (purchaser)**, an electronic key data signature verification key VMK and an electronic key communication key KK at the time of vehicle delivery from a manufacturer; and an encrypted engine master key E (EK) that corresponds to the user's electronic key data K before use." *Toshiba* at col. 4:22-29 **C. US20080150683** "1. A method for providing secure operation of a vehicle comprising:

(cont.) 1.pre. A method, comprising, 1.a. **receiving, by a server, a request from a user via a user account that has a vehicle associated therewith to generate an electronic key (e-key) for an identified recipient to use the vehicle**, the **request includes identifying information for enabling sending of the e-key to the recipient via an electronic transmission**, the **request includes a condition of use of the vehicle as set by the user via the user account**;	**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**." *Hyundai* at claim 1 "3. The method of claim 1, wherein **the key is embedded in a wireless device in communication with the vehicle**." *Hyundai* at claim 3 "20. A wireless device for providing secure operation of a vehicle comprising: **a user interface module that receives a first request to gain access to a vehicle** and that receives a second request to update an access control rule; . . . ." *Hyundai* at claim 20 "**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 "In one embodiment, **vehicle record** 302 **may include key set** 310, policy set 313, and mapping 312. **Key set** 310 **may include data representing a collection of keys** 205A-C. Policy set 313 may include a collection of vehicle operation policies 311. **Mapping** 312 **may include a collection of one or more relationships linking individual keys from key set** 310 **with individual vehicle operation policies from policy set** 313. In one embodiment, there may be a one-to-one relationship between vehicle ID 301 and vehicle record 302. **Mapping** 312 **may include a one-to-many relationship between an individual key of key set** 310 **and vehicle operation policies** 311. It will be appreciated that other schema may be used to practice master database 300." *Hyundai* at par. 0058

1.b. **generating, by the server, the e-key, the e-key being assigned with the condition of use of the vehicle**;	**A. JP2004190233** "An **automobile electronic key system including** an in-vehicle device that controls unlocking of an automobile, a user terminal that functions as an electronic key that unlocks the automobile, and **a key server that issues key data of the electronic key**, ..." *Mitsui* at p. 1 of the translation document "The key server 50 can determine for each user the risk that the user will hinder the smooth operation of the vehicle by referring to such a usage record database 30. Thereby, **when the user requests the reservation of the car, the key server** 50 **can restrict the use conditions for each user** in order to reduce the degree of the risk." *Mitsui* at p. 6 of the translation document "First, when the user operates the user terminal 120 to request issuance of key data (S200), **the issuance requesting unit** 12 **transmits a desired use period, a terminal ID, and a vehicle ID to the key server** 50 (S202).). **When the key distribution unit** 18 **of the key server** 50 **receives the desired use period, the terminal ID, and the vehicle ID from the user terminal** 120, the key distribution unit 18 refers to the reservation unit 16 based on the received vehicle ID to reserve the corresponding vehicle. The situation is confirmed (S204)." *Mitsui* at p. 6 of the translation document "Next, **the key distribution unit** 18 **issues a** server key and a **terminal key for which authentication is established by collation in the set available period, available time zone, and available area** (S210), and stores the issued server key. On the other hand (S212), the terminal key is distributed to the user terminal 120 specified by the terminal ID (S214)." *Mitsui* at p. 6 of the translation document **B. US7868736** "Here, **the encrypted engine master key EM (EK) is produced when the engine master key EK is encrypted by means of electronic key data MK and a hash key MI** described later. An electronic key data signature verification key VMK is provided as a key for verifying a signature of electronic key data K." *Toshiba* at col. 4:30-35 **C. US20080150683** "In one embodiment, **vehicle record** 302 **may include key set** 310, policy set 313, and mapping 312. **Key set** 310 **may include data representing a collection of keys** 205A-C.

(cont.) 1.b. **generating, by the server, the e-key, the e-key being assigned with the condition of use of the vehicle**;	Policy set 313 may include a collection of vehicle operation policies 311. Mapping 312 may include a collection of one or more relationships linking individual keys from key set 310 with individual vehicle operation policies from policy set 313. In one embodiment, there may be a one-to-one relationship between vehicle ID 301 and vehicle record 302. **Mapping** 312 **may include a one-to-many relationship between an individual key of key set** 310 **and vehicle operation policies** 311. It will be appreciated that other schema may be used to practice master database 300." *Hyundai* at par. 0058 "A vehicle operation feature may be associated with vehicle operation feature ID 316. **Access control rule** 317 **may include a criterion relating to associated vehicle operation feature ID** 316. For example, **access control rule** 317 **may operate to enable, partially enable, or disable the related vehicle operation feature**. **Access control rule** 317 **may include advanced criteria relating to the manner and conditions under which the vehicle may be operated**." *Hyundai* at par. 0060
1.c. **transmitting, by the server, the e-key to the recipient using the identifying information so that a device of the recipient is implemented to use the e-key**;	**A. JP2004190233** "Thereby, **the in-vehicle device** 10 **can transmit the operation status of the automobile** 200 **and the usage record of each user to the key server** 50. Thus, **the key server** 50 **can more smoothly operate the vehicle**." *Mitsui* at p. 5 of the translation document "Further, **the key server** 50 **has a use record database** 30 **that stores the use record of the automobile by the user in association with the terminal ID, and the key distribution unit** 18 **uses the use record database based on the terminal ID received from the user terminal** 120. The usage record of the user may be extracted from the record database 30, and the usable period may be set based on the extracted use record. The use record database 30 may acquire the use record for each user from the mobile phone operator 134 and the insurance company 136. Thereby, **the key server** 50 **can determine a user who has a high risk of hindering the vehicle operation based on the use record, and can set a usable period so as to reduce the risk**." *Mitsui* at p. 5 of the translation document "Next, the key distribution unit 18 issues a server key and a terminal key for which authentication is established by

(cont.) 1.c. **transmitting, by the server, the e-key to the recipient using the identifying information so that a device of the recipient is implemented to use the e-key**;	collation in the set available period, available time zone, and available area (S210), and stores the issued server key. On the other hand (S212), **the terminal key is distributed to the user terminal** 120 **specified by the terminal ID** (S214)." *Mitsui* at p. 6 of the translation document **B. US7868736** "In the case of an example shown in FIG. 4, unlike FIG. 3, **a linkage between information on an issued electronic key** 2 **and information specific to a user is established**. Thus, there is a need for the user's ID card 5 at the time of issuance of the electronic key 2. In addition, at the time of using the electronic key 2 (at the time of engine startup), there is a need for the ID card 5. In addition, **if an attempt is made to steal the electronic key** 2 **in order to obtain the internal electronic key data K, the electronic key is encrypted based on information I contained in the user's ID card** 5, thus making it difficult to illegally use the information without the user's ID card." *Toshiba* at col. 8:13-23 **C. US20080150683** "At 504, **a user attempt to access or operate vehicle** 201 **with a key** 205A-C **is detected, which may initiate the authentication the detection of key** 205A-C **may include receiving secure identifier** 407. Secure identifier 407 may be received, for example, at control unit 202. **Where key** 205A-C **is an electronic key, such as a key embedded in wireless device** 400 for example, key 205A-C **may transmit secure identifier** 407. Where key 205A-C is a metal key for insertion into a physical lock, the physical lock may authenticate the key—by the patterns of grooves and teeth, for example—and signal a secure identifier within vehicle 201 to control unit 202." *Hyundai* at par. 0070
1.d. **transmitting, by the server, data to the vehicle to enable use of the vehicle via the e-key**; and	**A. JP2004190233** "The **in-vehicle device** 10 **includes a transfer unit** 40 **that transfers the received terminal key to the key server** 50 **together with the vehicle ID when the terminal key is received from the user terminal** 120, **and an automobile that receives the unlock signal from the key server** 50 And an unlocking section 22 for unlocking the lock 200." *Mitsui* at p. 5 of the translation document "When the user is likely to violate the assigned availability condition, the in-vehicle device 10 warns the user to comply

(cont.) 1.d. **transmitting, by the server, data to the vehicle to enable use of the vehicle via the e-key**; and	with the availability condition. The **availability condition for each user may be included in the key data, or may be distributed from the key server** 50 **as separate data associated with the key data**." *Mitsui* at p. 7 of the translation document **C. US20080150683** "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
1.e. **receiving, by the server, use data regarding use of the vehicle for when the vehicle is used via the e-key**;	**A. JP2004190233** "When a terminal ID for specifying the user terminal, **a vehicle ID for specifying the vehicle, and a desired use period are received from a user terminal of a user who wants to use the vehicle, the terminal is specified by the vehicle ID**. A **usable period of the vehicle is set based on the reservation status of the vehicle and the desired use period, a server key and a terminal key for which authentication is established by collation in the usable period are issued, and the issued server key is issued**. A **key distribution unit that stores and distributes the issued terminal key to the user terminal specified by the terminal ID**; . . . ." *Mitsui* at p. 2 of the translation document "When the user is likely to violate the assigned availability condition, the in-vehicle device 10 warns the user to comply with the availability condition. The **availability condition for each user may be included in the key data, or may be distributed from the key server** 50 **as separate data associated with the key data**." *Mitsui* at p. 7 of the translation document **C. US20080150683** "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. Once control unit 202 has permitted a vehicle operation feature, monitoring ensures that the feature stays in conformance with policy 311." *Hyundai* at par. 0076

1.f. wherein **the use data identifies information regarding the use of the vehicle, and the information identifies a violation of the condition of use**;	**A. JP2004190233** "The **key server** 50 **can determine for each user the risk that the user will hinder the smooth operation of the vehicle by referring to such a usage record database** 30. Thereby, when the user requests the reservation of the car, **the key server** 50 **can restrict the use conditions for each user in order to reduce the degree of the risk**." *Mitsui* at p. 6 of the translation document "When the user is likely to violate the assigned availability condition, the in-vehicle device 10 warns the user to comply with the availability condition. The **availability condition for each user may be included in the key data, or may be distributed from the key server** 50 **as separate data associated with the key data**." *Mitsui* at p. 7 of the translation document **C. US20080150683** "The **vehicle operation policy may include an access control rule that may indicate to enable, partially enable, or disable a vehicle operation feature**. Where the intended operation of the vehicle is not consistent with the access control rule, the operation may not be permitted and an enforcement action may be taken, such as disabling a feature of the vehicle for example." *Hyundai* at par. 0005 "At 508, **control unit** 202 **may process the access request and compare the access request with retrieved vehicle operation policy** 311. **Where the access request is consistent with retrieved vehicle operation policy** 311, **control unit** 202 **may permit the operation of the vehicle** at 510. Where the access request is inconsistent with the with the retrieved vehicle operation policy 311, then at 516 control unit 202 may block and/or limit the operation of the vehicle." *Hyundai* at par. 0074
1.g. wherein **the server processes logic for generating the e-key and processes logic for analyzing the data regarding use of the vehicle when the e-key is used for the vehicle**, **the server or other servers connected to the server being accessible over the Internet**, **the**	**A. JP2004190233** "**The key distribution unit** 18 **confirms the usage record of the user by referring to the use record database** 30 based on the received terminal ID (S206). Then, **based on the desired use period received from the user terminal** 120 **and the confirmed reservation status and use results, the available period and available area for the user are set** (S208)." *Mitsui* at p. 6 of the translation document

vehicle having wireless communication systems for communicating with the server or other servers and for communicating with devices local to the vehicle.	"In step 208, **the key distribution unit** 18 **limits the usable period for the user to a certain period**, for example, when the payment ability as the usage record is lower than a predetermined standard. When the user's ability to pay is low enough to make the service unsuitable, the key distribution unit 18 may set the usable period to zero. As a result, the risk of non-payment by the user is reduced." *Mitsui* at p. 6 of the translation document "In step 208, **when the key distribution unit** 18 **determines that the accident by the user is biased to a specific time zone based on, for example, an accident history as a use record, the key distribution unit** 18 **determines a time zone excluding the specific time zone**. Set as available period. As a result, the possibility of an accident by the user can be reduced, and the risk that the operation of the vehicle is disabled due to the accident can be reduced." *Mitsui* at p. 6 of the translation document "In step 208, if the key distribution unit 18 determines that the accident by the user is biased to a specific area based on, for example, an accident history as a use record, the key distribution unit 18 extracts the area excluding the specific area. Is set as an area that can be used by users. **The key distribution unit** 18 **may set the usable area of the user within a predetermined distance from the home based on the number of times of use, the total mileage, or the skill level as the use result**." *Mitsui* at p. 6 of the translation document **C. US20080150683** "2. The method of claim 1, wherein said **detecting comprises receiving a secure key identifier from a wireless device**." *Hyundai* at claim 2 "3. The method of claim 1, wherein **the key is embedded in a wireless device in communication with the vehicle**." *Hyundai* at claim 3 "**Key** 205B **and computer** 210 **may be in communication with wireless network** 207. In one embodiment, **key** 205B **and computer** 210 may communicate with application 209, with master database 208, or, **via wireless network** 207, with control unit 202 and/or local database 203. Both **computer** 210 **and key** 205B **may provide a user interface with wireless**

(cont.) 1.g. wherein **the server processes logic for generating the e-key and processes logic for analyzing the data regarding use of the vehicle when the e-key is used for the vehicle**, **the server or other servers connected to the server being accessible over the Internet**, **the vehicle having wireless communication systems for communicating with the server or other servers and for communicating with devices local to the vehicle**.	**vehicle security system** 200 **to enable a user to manage and monitor system** 200. 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