PATROLL Winning Submission

U.S. Patent 10,407,026

U.S. Patent No. 10,407,026 ("*Emerging Automotive*" or the "patent-at-issue") was filed on May 26, 2017 and claims an priority on April 22, 2011. Claim 1 of the patent-at-issue is generally directed to a vehicle designed for communication with a cloud system server to facilitate access through electronic keys. The vehicle includes electronics, subsystems for unlocking and starting the vehicle, and programmable communications circuitry. This circuitry is configured to receive unlocking requests from mobile devices, including a unique access code obtained from the server. The vehicle authenticates the request and, if valid, provides the mobile device with data for an electronic key. The electronics then instruct the vehicle subsystems to unlock and start the vehicle according to the specified privileges associated with the unique access code.

The primary reference, U.S. Pat. App. 2010/0293607 ("*Microsoft*"), was filed on May 14, 2009, and claims priority on the same date. The patent application is directed to a system and method for linking a web identity and a portable device to enable web access from a vehicle. The system comprises a presence agent to validate the portable device's presence by recognizing a device identifier. After validation, a security manager checks the user identifier against known values and sends a user identity secure proxy to a credential manager. The credential manager, in turn, passes credentials to the vehicle's onboard computing device, indicating authorization for the user to access web services.

A secondary reference, U.S. Patent 8,330,571 ("*Tokai Rika*"), was filed on October 13, 2009, and claims priority on October 14, 2008. The patent is directed to a vehicle electronic portable key system comprising a master key and sub-key, with a retainer in the vehicle to hold the sub-key. A control unit assesses the location of the keys in relation to the vehicle's wireless communicatable areas, permitting various operations based on their positions. If the sub-key is removed when the master key is inside, it's considered in a lent state. In such a state, the control unit restricts vehicle operations unless the sub-key is confirmed to be in the lent state.

A secondary reference, U.S. Pat. App. 2010/0073125 ("*GM Global*"), was filed on September 23, 2008, and claims priority on the same date. The patent application is directed to a system and methods for confirming the authorization of a user operating an electronic device to control a vehicle. The process involves receiving a vehicle-related request from the electronic device triggered by a user action, verifying the user's capability to initiate a specific vehicle operation, and allowing the request only if the vehicle successfully executes the predetermined operation.

A sample claim chart comparing claim 1 of *Emerging Automotive* to *Microsoft, Tokai Rika,* and *GM Global* is provided below.

US10407026 ("*Emerging Automotive*")	**A. US20100293607** (*"Microsoft"*) **B. US8330571** (*"Tokai Rika"*) **C. US20100073125** (*"GM Global"*)
1.pre. A vehicle configured to **communicate with a server of a cloud system to enable access to use the vehicle via one or more electronic keys**, comprising, electronics of the vehicle;	**A. US20100293607** "Each of the first, **second and/or third driver identifiers may enable access to different security levels, and therefore be granted access to different cloud services**." *Microsoft* at par. 0008 "**The portable device 14 may be any user 16 accompanying device. In some examples the portable device 14 may be a key fob coupled with a key 15. The key 15 may be associated with and/or able to unlock and start the vehicle 18, and may be a wireless electronic key and/or a mechanical key for starting the vehicle**. In many circumstances the primary driver of the vehicle 18 may be the exclusive user of a primary key fob." *Microsoft* at par. 0007 "1. **A system for linking a web identity and a portable device to provide web access to a user from a vehicle** . . . *Microsoft* at Claim 1 "In other examples, the credential manager 68, and/or the credential store 72, may be executed on a remote server in communication with the onboard computing device 54 via, for example, a communication agent 74. **The communication agent may be configured to establish a connection between the vehicle and the one or more web services. The remote server may be operated by one or more cloud vehicle services** 76**. The cloud vehicle services** 76 **may be part of a data network** 78**, for example the Internet**." Microsoft at par. 0014 **B. US8330571** "1. A **vehicle electronic portable key system comprising: an electronic portable key capable of performing wireless communication and comprising a plurality of keys including a master key and a sub-key** . . ." *Tokai Rika* at Claim 1 "**The master key control unit** 11 b **then transmits the response signal from a transmitter** 11 c **to the vehicle** 20**.**

(cont.) 1.pre. A vehicle configured to **communicate with a server of a cloud system to enable access to use the vehicle via one or more electronic keys**, comprising, electronics of the vehicle;	The receiver 32 of the vehicle 20 receives the response signal and provides the response signal to the vehicle control unit 60. The vehicle control unit 60 compares and verifies the ID code included in the provided response signal with an ID code stored beforehand in a memory 60 a, which is incorporated in the control unit 60. **When determined that the ID code IDM of the master key** 11 **included in the response signal is authentic**, **the vehicle control unit** 60 **opens the door lock mechanisms** 41 **to** 45 **to unlock the doors** 21 a **to** 21 d **and trunk lid** 22." *Tokai Rika* at col. 6:65 through col. 7:1-9 "**When a vehicle occupant who is carrying an electronic portable key 10 (portable device) enters area A or B, various signals including a request signal and a response signal are transferred through wireless communication between the electronic portable key** 10 **and the vehicle** 20. The vehicle electronic portable key system verifies an identification (ID) code stored in the electronic portable key 10 with an ID code stored in the vehicle. When it is determined that the two ID codes are in conformance with each other, **the vehicle electronic portable key system unlocks the doors** 21 a **to** 21 d **and allows the execution of various controls, such as permitting the starting of the engine**. **When engine starting is permitted, the vehicle occupant may, for example, start the engine by pressing an engine start switch** 24 **arranged on an instrument panel** 23 **of the vehicle**." *Tokai Rika* at col. 4:26-40 **C. US20100073125** "15. The **system** of claim 9, wherein **the vehicle comprises a vehicular communication system** and the processor is further configured to: **detect a first network address corresponding to the request;** **instructing the user to direct the vehicular communication system to transmit a message to a presence server;** **detect a second network address corresponding to the message**; and **permit the request to proceed if the first network address and the second network address correspond to a same subnetwork**." *GM Global* at Claim 15 "17. The **vehicular communication system** of claim 16, wherein:

(cont.) 1.pre. A vehicle configured to **communicate with a server of a cloud system to enable access to use the vehicle via one or more electronic keys**, comprising, electronics of the vehicle;	the vehicular communication system further comprises a user interface and **has a private key that mathematically corresponds to a public key**; the input comprises receiving a credential value from the user via the user interface; and the **predetermined operation comprises generating a digital signature of the credential value using the private key**." *GM Global* at Claim 17
1.a. a **subsystem of the vehicle for enabling unlocking of the vehicle**, **the subsystem being interfaced with the electronics**;	**A. US20100293607** "**The portable device 14 may be any user 16 accompanying device. In some examples the portable device 14 may be a key fob coupled with a key 15. The key 15 may be associated with and/or able to unlock and start the vehicle 18, and may be a wireless electronic key and/or a mechanical key for starting the vehicle.** In many circumstances the primary driver of the vehicle 18 may be the exclusive user of a primary key fob. Accordingly, the key fob may be signify the presence of that individual, i.e. the user 16, when onboard the vehicle. In some example embodiments **a second, or a third key may also be associated with and/or able to unlock and start the vehicle** 18." *Microsoft* at par. 0007 "For example **the fob may be attached to a key that may be configured to unlock and/or start the vehicle**. Method 200 may be implemented using the systems and devices described above, or using other suitable hardware. **The method 200 may include, at 202, recognizing a presence of the vehicle fob when the vehicle fob is in the vehicle. The method 200 may include, at 204, retrieving a fob identifier from a memory on the vehicle fob**." *Microsoft* at par. 0019 **B. US8330571** "When a vehicle occupant who is carrying an electronic portable key 10 (portable device) enters area A or B, various signals including a request signal and a response signal are transferred through wireless communication between the electronic portable key 10 and the vehicle 20. The vehicle electronic portable key system verifies an identification (ID) code stored in the electronic portable key 10 with an ID code stored in the vehicle. **When it is determined that the two ID codes are in conformance with each other, the vehicle electronic portable key system unlocks the doors** 21 a **to** 21 d **and allows the execution of various controls, such as permitting the starting of the engine.** When engine starting is

(cont.) 1.a. a **subsystem of the vehicle for enabling unlocking of the vehicle**, **the subsystem being interfaced with the electronics**;	permitted, the vehicle occupant may, for example, start the engine by pressing an engine start switch 24 arranged on an instrument panel 23 of the vehicle." *Tokai Rika* at col. 4:26-40 **C. US20100073125** "**As further described below, the processor** 100 **receives requests regarding the vehicle from electronic device** 54 **at the direction of the user. In response to these requests**, **processor** 100 **directs the user to cause the vehicle to perform certain actions to confirm that he or she is also an authorized user of the vehicle (e.g., that the user has access to, and control of, the vehicle**)." *GM Global* at par. 0026 "In one embodiment, a method is provided for confirming that a user of an electronic device is also an authorized user of a vehicle. **The method suitably comprises receiving a request regarding the vehicle from the electronic device in response to a user action, verifying that the user is able to cause the vehicle to perform an operation, and permitting the request to proceed only if the vehicle performs the operation**." *GM Global* at par. 0005
1.b. a **subsystem of the vehicle for enabling starting of the vehicle for use of the vehicle**; and	**A. US20100293607** "The portable device 14 may be any user 16 accompanying device. In some examples the portable device 14 may be a key fob coupled with a key 15. **The key 15 may be associated with and/or able to unlock and start the vehicle 18, and may be a wireless electronic key and/or a mechanical key for starting the vehicle**. In many circumstances the primary driver of the vehicle 18 may be the exclusive user of a primary key fob. Accordingly, the key fob may be signify the presence of that individual, i.e. the user 16, when onboard the vehicle. In some example embodiments **a second, or a third key may also be associated with and/or able to unlock and start the vehicle 18**." *Microsoft* at par. 0007 "For example **the fob may be attached to a key that may be configured to unlock and/or start the vehicle**. Method 200 may be implemented using the systems and devices described above, or using other suitable hardware. **The method 200 may include, at 202, recognizing a presence of the vehicle fob when the vehicle fob is in the vehicle. The method 200 may include, at 204, retrieving a fob identifier from a memory on the vehicle fob**." *Microsoft* at par. 0019

(cont.) 1.b. a **subsystem of the vehicle for enabling starting of the vehicle for use of the vehicle**; and	**B. US8330571** "When a vehicle occupant who is carrying an electronic portable key 10 (portable device) enters area A or B, various signals including a request signal and a response signal are transferred through wireless communication between the electronic portable key 10 and the vehicle 20. The vehicle electronic portable key system verifies an identification (ID) code stored in the electronic portable key 10 with an ID code stored in the vehicle. **When it is determined that the two ID codes are in conformance with each other, the vehicle electronic portable key system unlocks the doors 21 a to 21 d and allows the execution of various controls, such as permitting the starting of the engine.** When engine starting is permitted, the vehicle occupant may, for example, start the engine by pressing an engine start switch 24 arranged on an instrument panel 23 of the vehicle." *Tokai Rika* at col. 4:26-40 **C. US20100073125** "**As further described below, the processor** 100 **receives requests regarding the vehicle from electronic device** 54 **at the direction of the user. In response to these requests, processor** 100 **directs the user to cause the vehicle to perform certain actions to confirm that he or she is also an authorized user of the vehicle (e.g., that the user has access to, and control of, the vehicle**)." *GM Global* at par. 0026 "In one embodiment, a method is provided for confirming that a user of an electronic device is also an authorized user of a vehicle. **The method suitably comprises receiving a request regarding the vehicle from the electronic device in response to a user action, verifying that the user is able to cause the vehicle to perform an operation, and permitting the request to proceed only if the vehicle performs the operation**." *GM Global* at par. 0005
1.c. **communications circuitry of the vehicle interfaced with electronics of the vehicle**, **the communications circuitry being programmable to communicate with the server of the cloud system and communicate with a mobile device**;	**A. US20100293607** "For example, the **computing devices may be a** mainframe computer, personal computer, laptop computer, **portable data assistant (PDA), computer-enabled wireless telephone**, networked computing device, **enhanced mobile telephone device**, or other suitable computing device, **and may be connected to each other via computer networks, such as the Internet**." *Microsoft* at par. 0027

(cont.) 1.c. **communications circuitry of the vehicle interfaced with electronics of the vehicle**, **the communications circuitry being programmable to communicate with the server of the cloud system and communicate with a mobile device**;	"**The credential manager may be configured to receive the user identity secure proxy, and in response, pass one or more credentials to a computing device onboard the vehicle**. **The credentials may indicate that the user is authorized to access one or more web services from the computing device**." *Microsoft* at par. 0002 "**In other examples, the credential manager** 68**, and/or the credential store** 72, **may be executed on a remote server in communication with the onboard computing device** 54 **via, for example, a communication agent** 74. **The communication agent may be configured to establish a connection between the vehicle and the one or more web services. The remote server may be operated by one or more cloud vehicle services** 76**. The cloud vehicle services** 76 **may be part of a data network** 78**, for example the Internet.**" *Microsoft* at par. 0014 **C. US20100073125** "FIG. 2 is a block diagram of an exemplary system 50 for confirming that **a user of an electronic device has access to, and control of, a vehicle (e.g., the vehicle** 10 **of FIG. 1). The system** 50 **includes a VCS** 52**, an electronic device** 54**, a remote device** 56**, a network access point** 58**, and a gateway** 60." *GM Global* at par. 0021 "**The gateway** 60 **provides connectivity between devices on the subnetwork** 110 **and devices on a wide area network** 124 **such as the Internet**. For example, in one embodiment the **gateway** 60 **is a router that provides connectivity between the electronic device** 54 **and the network access point** 58 **operating on a local area network (LAN) and the remote device** 56 **over the Internet**. In some embodiments, the network access point 58 may be integrally formed with the gateway 60. It should be noted that because **the electronic device** 54 **and the VCS** 52 **(via the network access point** 58**) each access the wide area network** 124 **via the gateway** 60**, the network addresses for these devices will correspond to subnetwork** 110." *GM Global* at par. 0032

1.d. wherein **the communications circuitry of the vehicle is configured to receive a request from the mobile device for unlocking of the vehicle**, **the request from the mobile device including a unique access code obtained by the mobile device from the server to enable sending the request to the vehicle**,	**A. US20100293607** "The method 200 may also include, at 222, **recognizing a request from a specified web service for one or more authenticating credentials with the password input mechanism**. The method 200 may also include, at 224, based on the request, passing a predetermined authenticating credential to the specified web service to enable the user to have access to the specified web service. In some examples, **the password input mechanism may be served by a program executed on a remote server. In other examples, the password input mechanism may be executed by the onboard computing device.**" *Microsoft* at par. 0020 **B. US8330571** "**The master key control unit** 11 b **then transmits the response signal from a transmitter** 11 c **to the vehicle** 20**.** The receiver 32 of the vehicle 20 receives the response signal and provides the response signal to the vehicle control unit 60. The vehicle control unit 60 compares and verifies the ID code included in the provided response signal with an ID code stored beforehand in a memory 60 a, which is incorporated in the control unit 60. **When determined that the ID code IDM of the master key** 11 **included in the response signal is authentic**, **the vehicle control unit** 60 **opens the door lock mechanisms** 41 **to** 45 **to unlock the doors** 21 a **to** 21 d **and trunk lid** 22." *Tokai Rika* at col. 6:65 through col. 7:1-9 "**When a vehicle occupant who is carrying an electronic portable key** 10 **(portable device) enters area A or B**, **various signals including a request signal and a response signal are transferred through wireless communication between the electronic portable key** 10 **and the vehicle** 20. **The vehicle electronic portable key system verifies an identification (ID) code stored in the electronic portable key** 10 **with an ID code stored in the vehicle**. When it is determined that the two ID codes are in conformance with each other, **the vehicle electronic portable key system unlocks the doors** 21 a **to** 21 d **and allows the execution of various controls, such as permitting the starting of the engine. When engine starting is permitted, the vehicle occupant may, for example, start the engine by pressing an engine start switch** 24 **arranged on an instrument panel** 23 **of the vehicle."** *Tokai Rika* at col. 4:26-40 **C. US20100073125**

(cont.) 1.d. wherein **the communications circuitry of the vehicle is configured to receive a request from the mobile device for unlocking of the vehicle**, **the request from the mobile device including a unique access code obtained by the mobile device from the server to enable sending the request to the vehicle**,	"1. A method for confirming that a user of an electronic device is also an authorized user of a vehicle, the method comprising: **receiving a request regarding the vehicle from the user from the electronic device in response to a user action** . . ." *GM Global* at Claim 1 "In one embodiment, a method is provided for confirming that a user of an electronic device is also an authorized user of a vehicle. **The method suitably comprises receiving a request regarding the vehicle from the electronic device in response to a user action, verifying that the user is able to cause the vehicle to perform an operation, and permitting the request to proceed only if the vehicle performs the operation**." *GM Global* at par. 0005 "As further discussed below, **the manufacturer or trusted entity receives a request from the user, via the electronic device, to perform an action with respect to the vehicle**. **The request may be to register a vehicle identification number (VIN) with a unique identifier for the user (e.g., a UserID), to obtain information regarding the vehicle (e.g., mileage or operation information), or to enable or provision certain configurable options on the vehicle (e.g., navigation services or on-call support).**" *GM Global* at par. 0013
1.e. **wherein the unique access code is associated with privileges for use of the vehicle, the privileges are defined for the unique access code, the vehicle is configured to receive information from the server to authenticate the request by the mobile device**,	**A. US20100293607** "In some examples, **the system** 10 **may be configured to manage various levels of security, and/or to provide various credentials to various applications and/or services when requested**. For example, **a remote server, such as a web based service may prompt for additional credentials, such as a username, and/or password in order to grant the user** 16 **access to a higher level of service than initially granted**. For example, **initially the user** 16 **may be given access to a news service, or a calendaring application, or the like. However, if the user** 16 **would like access to, for example, personal banking information, additional credentials may be requested**. Accordingly, various examples may include a password input mechanism 84. **The password input mechanism** 84 **may have a store of authenticating credentials** 86 **and may be onboard the vehicle and/or in the cloud vehicle services** 76." *Microsoft* at par. 0017

1.f. **and if the request is authentic** and **the mobile device is provided with data to enable an electronic key to use the vehicle and the electronics of the vehicle instructs the subsystem of the vehicle to enable unlocking of the vehicle and enable starting of the vehicle for use of the vehicle via the electronic key consistent with the privileges of the unique access code**.	**A. US20100293607** "The method 200 may also include, at 222, **recognizing a request from a specified web service for one or more authenticating credentials with the password input mechanism**. The method 200 may also include, at 224, **based on the request, passing a predetermined authenticating credential to the specified web service to enable the user to have access to the specified web service**. In some examples, **the password input mechanism may be served by a program executed on a remote server.** In other examples, **the password input mechanism may be executed by the onboard computing device.**" *Microsoft* at par. 0020 "1. A system for linking a web identity and a portable device to provide web access to a user from a vehicle, the system comprising: . . . **a security manager configured to receive the device identifier, and further configured to receive a user identifier, the security manager configured to verify if the user identifier corresponds with a known user value, upon receipt of the device identifier, and upon verifying the user identifier, the security manager configured to send a user identity secure proxy to a credential manager**; and **the credential manager configured to receive the user identity secure proxy from the security manager and to pass one or more credentials to a computing device onboard the vehicle, the one or more credentials indicating that the user is authorized to access one or more web services from the computing device onboard the vehicle**." *Microsoft* at Claim 1 **C. US20100073125** "In one embodiment, a method is provided for confirming that a user of an electronic device is also an authorized user of a vehicle. **The method suitably comprises receiving a request regarding the vehicle from the electronic device in response to a user action, verifying that the user is able to cause the vehicle to perform an operation, and permitting the request to proceed only if the vehicle performs the operation**." *GM Global* at par. 0005