November 2022

DIGITAL VEHICLE KEY ACCESS FOR PROVIDING RESTRICTED VEHICLE USAGE

Nick Miller

DIGITAL VEHICLE KEY ACCESS FOR PROVIDING RESTRICTED VEHICLE USAGE

ABSTRACT

A third party (e.g., a valet, a parking service, a vehicle rental customer, an acquaintance, etc.) may receive an anonymous digital key for operating a vehicle (e.g., an automobile, a motorcycle, a bus, etc.) owned by another person. For example, the owner of the vehicle may use a computing device (e.g., a cellular phone, a smartphone, a laptop computer, a tablet computer, etc.) to provide ownership information (e.g., an original digital key) to a computing system (e.g., a remote cloud server having a pre-negotiated certification with the vehicle manufacturer). Responsive to confirming ownership of the vehicle, the computing system may generate or otherwise provide an anonymous digital key for operating the vehicle. The third party may use a computing device to access the anonymous digital key and operate the vehicle. The anonymous digital key may be configured with various geographic restrictions, performance restrictions, time restrictions, etc., which may limit what an operator using the anonymous digital key may do with the vehicle. The anonymous digital key may expire (e.g., after a predetermined amount of time) and, once expired, the anonymous digital key may no longer be used to operate the vehicle.

DESCRIPTION

FIG. 1 below is a conceptual diagram illustrating a system 10 that includes a first computing device 100 (“first device 100”), a second computing device 102 (“second device 102”), a computing system 104, and a vehicle 106. Examples of first device 100 and second device 102 may include a cellular phone, a smartphone, a personal digital assistant (PDA), a laptop computer, a tablet computer, a portable gaming device, a portable media player, an e-book reader, a watch (including a so-called smartwatch), smart glasses, a gaming controller, etc. Examples of computing system 104 may include one or more desktop computers, laptop

computers, mainframes, servers, cloud computing systems, virtual machines, etc. Examples of vehicle 106 may include an automobile, a motorcycle, a bus, a recreational vehicle (RV), a semi-trailer truck, a tractor or other type of farm equipment, a boat, a personal transport vehicle, etc.

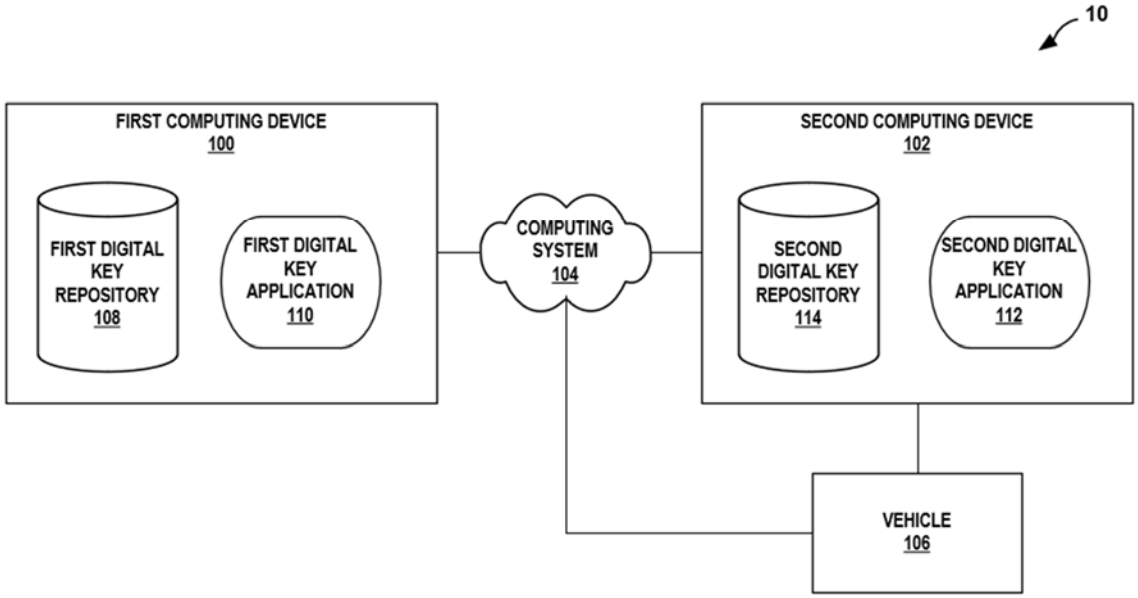

FIG. 1

First device 100, second device 102, computing system 104, and vehicle 106 may communicate with another component of system 10 via a network. Examples of a network may include a personal area network (PAN), such as a Bluetooth® network (including various versions or, in other words, profiles of Bluetooth®, such as Bluetooth Low Energy (BLE)), a local-area network (LAN), a wide-area network (WAN) (e.g., the Internet), an enterprise network, a cellular network, a telephone network, a Metropolitan area network (e.g., WiFi®, WAN, worldwide interoperability for microwave access (WiMAX), etc.), etc.

First device 100, second device 102, and vehicle 106 may each include communication components for receiving and transmitting various types of information over a network. Examples of the COMM components may include an ultra-wideband (UWB) radio, a cellular

radio, a third-generation (3G) radio, a fourth-generation (4G) radio, a fifth-generation (5G) radio, a Bluetooth® radio (or any other personal area network (PAN) radio), a near-field communication (NFC) radio, a WiFi® radio (or any other wireless local area network (WLAN) radio), etc.

In general, an owner of vehicle 106 may want to allow another person (e.g., a valet) to operate vehicle 106 (e.g., to park vehicle 106). However, the owner of vehicle 106 may be reluctant to transfer a physical key for operating vehicle 106 to the other person. Additionally, in some cases, the owner of vehicle 106 may operate vehicle 106 using an original digital key stored in, for example, a first digital key repository 108 of first device 100 (which may belong to the owner of vehicle 100). The owner of vehicle 106 may be similarly reluctant to transfer first device 100 to the other person.

In accordance with techniques of this disclosure, system 10 may grant another person a digital key for operating vehicle 106. For example, the owner of vehicle 106 may provide a first digital key (e.g., an original digital key associated with vehicle 106) in first digital key repository 108 to computing system 104 via a first digital key application 110. Computing system 104 may use the first digital key to confirm ownership of vehicle 106. Responsive to confirming ownership of vehicle 106, computing system 104 may generate or otherwise provide a second digital key for temporarily operating vehicle 106. Second computing device 102 (which may belong to an authorized person, such as a valet of a parking service) may receive the second digital key from computing system 104 and use the second digital key to operate vehicle 106. Responsive to satisfaction of a condition (e.g., passage of a predetermined amount of time, shutting off of vehicle 106, etc.), the second digital key may expire. Once expired, the second digital key may no longer be used to operate vehicle 106.

As noted above, the owner of vehicle 106 may use first digital key application 110 to grant another person access to vehicle 106. For example, the owner of vehicle 106 may (e.g., via a presence-sensitive display of first device 100) provide a user input (e.g., tapping a graphical element, scanning a QR code, responding to a push notification prompt, etc.) to first digital key application 110 to initiate the process for generating or otherwise providing a second digital key. In some examples, the owner of vehicle 106 may select restrictions for the usage of the second digital key. For example, the owner of vehicle 106 may use first digital key application 110 to set geographic restrictions, performance restrictions, time restrictions, etc., on the usage of the second digital key.

Responsive to the user input, first digital key application 110 may transmit an encrypted request that includes the first digital key to computing system 104. In some examples, computing system 104 may be associated with a third party (e.g., a parking service) or the manufacturer of vehicle 106 ("vehicle manufacturer"). In examples where computing system 104 is associated with a third party, computing system 104 may have a pre-negotiated certification with the vehicle manufacturer.

Computing system 104 may use the first digital key included in the request to confirm ownership of vehicle 106. For example, responsive to the first digital key matching the digital key for vehicle 106 provided by the vehicle manufacturer, computing system 104 may determine that the request was initiated by the owner of vehicle 106 (in this way indicating consent from the owner to provide another person access to vehicle 106). Computing system 104 may use a certifying authority provided by the vehicle manufacturer to determine whether the first digital key matches the digital key for vehicle 106 provided by the vehicle manufacturer. Responsive to the first digital key not matching the digital key for vehicle 106 provided by the vehicle

manufacturer, computing system 104 may deny the request from first digital key application 110.

Responsive to determining that the request from first digital key application 110 was initiated by the owner of vehicle 106, computing system 104 may generate or otherwise provide a second digital key. The second digital key may be different from the first digital key. Further, the second digital key may be anonymized and configured to be limited based on the request from first digital key application 110. For example, the second digital key may only be used to operate vehicle 106 in a geographic area, for certain operations, and for a predetermined amount of time specified in the request. In some examples, computing system 104 may communicate with vehicle 106 via a network to provide vehicle 106 with information about the existence and restrictions associated with the second digital key. Vehicle 106 may use this information to verify against the original equipment manufacturer (OEM) specific certifying authority for additional safety.

A user of second device 102 may obtain the second digital key from computing system 104 via a second digital key application 112. For example, the user may use second digital key application 112 to request the second digital key for vehicle 106 from computing system 104. The request may include identifying information for vehicle 106 that second device 102 may receive from vehicle 106. In some examples, second digital key application 112 may require second device 102 to be within a threshold distance of vehicle 106 to send the request to computing system 104 via second digital key application 112 (as well as to receive the identifying information for vehicle 106).

For example, second device 102 and vehicle 106 may perform distance-based measurements based on time-of-flight (ToF) values (which may be correlated with distance).

Second device 102 and vehicle 106 may determine ToF values by sending and receiving (e.g., via COMM components) UWB signals (which may include one or more packets of information). A UWB signal may be defined as a signal with a bandwidth higher than 20% of its center frequency, or a signal with a bandwidth higher than 0.5 gigahertz (GHz). In some examples, UWB technology may operate over a frequency range from 3.1 to 10.6 GHz.

For example, second device 102 (e.g., a smartphone) may periodically broadcast (e.g., send) a first UWB signal. Responsive to vehicle 106 receiving the first UWB signal, vehicle 106 may send a second UWB signal to second device 102. The second UWB signal may include one or more packets that include the time that vehicle 106 received the first UWB signal and the time that vehicle 106 sent the second UWB signal. Second device 102 may determine, based on the send time and receive time of the first UWB signal and the send time and receive time of the second UWB signal to determine the distance between second device 102 and vehicle 106. Vehicle 106 may similarly determine distance. Responsive to second device 102 and/or vehicle 106 determining that the distance between second device 102 and vehicle 106 is equal to or less than a threshold distance, second digital key application 112 may send the request including the identifying information for vehicle 106 to computing system 104.

Responsive to receiving the request from second device 102, computing system 104 may authenticate second device 102. For example, computing system 104 may encrypt a transmission including credentials for accessing the second digital key using a public key (e.g., a key that is available to the public) associated with second device 102. Due to public-key cryptography techniques, the transmission may only be decrypted using a private key (e.g., a key that is only available to a specific computing device) associated with the second device 102. As a result, only

second device 102 should be able to decrypt the transmission including the credentials for accessing the second digital key.

Responsive to decrypting the encrypted transmission including the credentials from computing system 104, second digital key application 112 may use the credentials to obtain the second digital key for vehicle 106. Second digital key application 112 may store the second digital key in a second digital key repository 114. The user of second device 102 may then use the second digital key to operate vehicle 106. In some examples, vehicle 106 may receive information from computing system 102 about restrictions on the usage of the second digital key. For example, vehicle 106 may receive geographic, performance, and time restrictions from computing system 102 and prevent the user of second device 102 from performing any action in conflict with the geographic, performance, and time restrictions (e.g., driving outside of a specific geographic area, performing unauthorized operations, driving after the passage of a predetermined duration of time, etc.).

The second digital key may be configured to expire in response to satisfaction of a condition. For example, the second digital key may expire after a predetermined amount of time, based on the vehicle state (e.g., shutting off of vehicle 106), a transmission from computing system 104, etc. For example, the user of second device 102 may provide a user input to second digital key application 112 indicating that the user has finished operating vehicle 106. In turn, second digital key application 112 may cause the second digital key to expire. In any case, once expired, the second digital key may not be used to operate vehicle 106. If the user of second device 102 needs to operate vehicle 106 again, the user of second device 102 may request another digital key using the procedure described above.

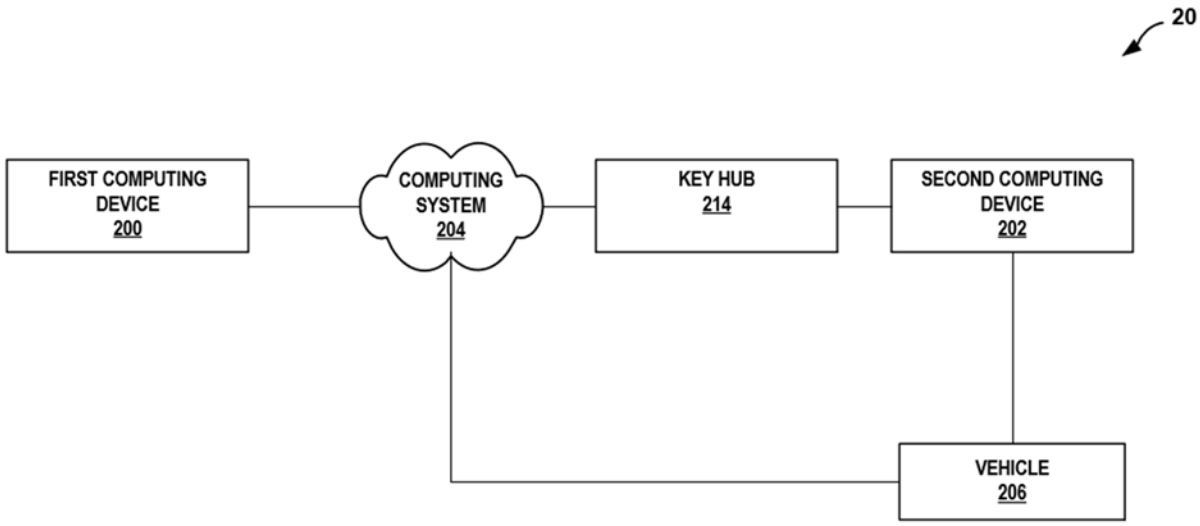

FIG. 2

FIG. 2 is a conceptual diagram illustrating system 20. System 20 may be substantially similar to system 10 of FIG. 1 except for any differences described here. As shown in FIG. 2, system 20 includes a first computing device 200 ("first device 200"), a second computing device 202 ("second device 202"), a computing system 204, a vehicle 206, and a key hub 214.

In some examples, a third party, such as a parking service, may provide a service to multiple clients. Consequently, the third party may need to manage multiple digital keys for operating multiple vehicles. In accordance with techniques of this disclosure, system 20 may include a key hub 214 that functions as a secure repository for digital keys. Key hub 214, which may have a pre-negotiated certification with multiple vehicle manufacturers, may communicate with computing system 204 to obtain a corresponding second digital key for each vehicle requiring service. Key hub 214 may store the second digital keys and transmit a specific second digital key in response to a request from second device 202 (e.g., via second digital key application 112). All communications may be encrypted as described above to ensure safety.

It is noted that the techniques of this disclosure may be combined with any other suitable technique or combination of techniques. As one example, the techniques of this disclosure may be combined with the techniques described in U.S. Patent Application Publication No. 2021/0394637A1. In another example, the techniques of this disclosure may be combined with the techniques described in U.S. Patent Application Publication No. 2020/0086828A1. In yet another example, the techniques of this disclosure may be combined with the techniques described in U.S. Patent Application Publication No. 2021/0402989A1. In yet another example, the techniques of this disclosure may be combined with the techniques described in Autowatch UK Ltd., Ghost - Service / valet mode, June 10, 2022, https://autowatch.co.uk/ghost-service-valet.