(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 December 2004 (02.12.2004)

PCT

(10) International Publication Number
WO 2004/104733 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number:
PCT/US2004/014647

(22) International Filing Date: 10 May 2004 (10.05.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/441,880 20 May 2003 (20.05.2003) US

(71) Applicant and
(72) Inventor: **GOTFRIED, Bradley, L.** [AU/US]; 8949 SE Bridge Road, Hobe Sound, FL 33455 (US).

(74) Agent: **RODMAN, Steele, J., Jr.**; Akerman Senterfitt, P.O. Box 3188, West Palm Beach, FL 33402-3188 (US).

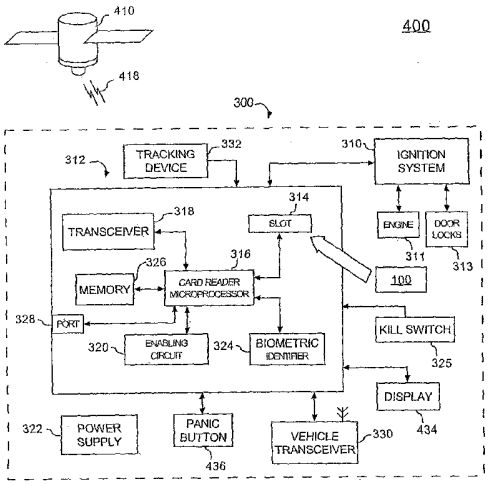
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: VEHICLE MONITORING SYSTEM



(57) Abstract: A vehicle monitoring system. The system includes an electronic access card in which the electronic access card stores information associated with a user of the electronic access card, a card reader for receiving the electronic access card and for reading the associated information and a vehicle transceiver coupled to the card reader. The vehicle transceiver transmits at least a portion of the associated information to at least one of a monitoring station and a portable unit. The monitoring station and the portable unit each include a computer for displaying the associated information. In one arrangement, the card reader and the vehicle transceiver can be mounted in a vehicle, and the vehicle transceiver can transmit the associated information from any vehicle having the card reader and the vehicle transceiver. In addition, the portable unit can be a law enforcement mobile unit.

WO 2004/104733 A2

VEHICLE MONITORING SYSTEM

CROSS REFERENCE TO RELATED APPLICATIONS

(Not Applicable)

STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

(Not Applicable)

BACKGROUND OF THE INVENTION

1. Technical Field

[0001] The present invention relates generally to monitoring systems and more particularly, to a monitoring system for tracking an operator of a vehicle.

2. Description of Related Art

[0002] Every year, large numbers of police officers are injured or even killed during traffic stops. Significantly, law enforcement personnel are normally unaware of the history of the individual operating a stopped vehicle. Moreover, the nature of the officer/driver interaction, because it is a simple traffic stop, causes many law enforcement personnel to let their guard down. Many times, however, an officer stops a driver who is wanted by the police or is involved in some type of illegal activity. Unfortunately, these types of individuals may perform violent acts to avoid being apprehended.

[0003] Several measures have been adopted in an effort to protect police officers. For example, if the police have acquired useful information about a particular person or vehicle, police dispatchers may broadcast such information to officers in the field. If a policemen were to encounter such a person or automobile, the officer may take any necessary precautions to protect himself or herself. Nevertheless, without the necessary information, there is no way to warn officers

about the possible dangers associated with certain drivers. Accordingly, there is a need for a system to overcome the deficiencies of the prior art without leading to complications or substantially increased costs.

SUMMARY OF THE INVENTION

[0004] The present invention concerns a vehicle monitoring system. The system includes an electronic access card in which the electronic access card stores information associated with a user of the electronic access card, a card reader for receiving the electronic access card and for reading the associated information and a vehicle transceiver coupled to the card reader. The vehicle transceiver transmits at least a portion of the associated information to at least one of a monitoring station and a portable unit. The monitoring station and the portable unit each include a computer for displaying the associated information. In one arrangement, the card reader and the vehicle transceiver are mounted in a vehicle, and the vehicle transceiver can transmit the associated information from any vehicle having the card reader and the vehicle transceiver. Further, the portable unit can be a law enforcement mobile unit.

[0005] In one aspect of the invention, the electronic access card can include a biometric identifier for identifying the user and can transmit an authorizing signal to the card reader when the user is biometrically identified. The card reader can read the associated information in response to the authorizing signal. As an example, the biometric identifier can generate digitized images of fingerprints.

[0006] In another arrangement, the electronic access card can include at least one electrical contact to permit the transfer of the associated information to the card reader. Moreover, the electronic access card can include a transceiver for transmitting the associated information to the card reader. The associated information stored on the electronic access card can include at least one of a name, an address, a driving history of the user, a criminal history of the user, insurance

coverage held by the user, vehicle registration and at least one digital photograph of the user.

[0007] The card reader can also include a tracking device, and the tracking device can receive navigational data. In yet another aspect of the invention, the vehicle transceiver can transmit the navigational data to at least one of the monitoring station and the portable unit in which the navigational data can be displayed on the computer. As an example, the vehicle transceiver can transmit the navigational data and the associated information to at least one of the monitoring station and the portable unit using at least one communications satellite or a wireless communications network. Additionally, the vehicle transceiver can transmit the navigational data and the associated information to at least one of the monitoring station and the portable unit in accordance with a predetermined interval.

[0008] In yet another arrangement, the system can further include an ignition system, and the card reader can include an enabling circuit for enabling the ignition system. When enabled, the ignition system can start an engine of a vehicle and can lock and unlock at least one door lock of the vehicle. The enabling circuit can also be used to disable the ignition system. In that case, a disabling signal can be transmitted to the vehicle transceiver from the monitoring station and forwarded to the card reader. The enabling circuit can disable the ignition system, and the ignition system can stop an engine of a vehicle in response to the receipt of the disabling signal by the card reader.

[0009] If the system includes an ignition system, the card reader, the vehicle transceiver and the ignition system can be mounted in a vehicle. The vehicle can further include a vehicle biometric identifier for identifying the user in which the vehicle biometric identifier can transmit an authorizing signal to the card reader when

the user is biometrically identified. The card reader can read the associated information in response to the authorizing signal. As an example, the vehicle biometric identifier can be positioned in the interior of the vehicle. Alternatively, the vehicle can include at least one door, and the vehicle biometric identifier is mounted on the door.

[0010] The system can also include at least one toll booth having at least one sensor and at least one gate for controlling the flow of traffic through the toll booth. The card reader, the vehicle transceiver and the ignition system can be mounted in a vehicle in which the vehicle transceiver can transmit to the sensor the associated information read from the electronic access card. For example, the associated information can include at least information about the user's account with a toll collection agency. In another arrangement, the electronic access card can include a transceiver for transmitting to the sensor the associated information stored on the electronic access card.

[0011] The system can also include a panic button. When the panic button is pressed, the vehicle transceiver can transmit a distress signal to at least one of the monitoring station and the portable unit. As an example, the distress signal can include at least an emergency message and the navigational data. Additionally, the system can also include a display coupled to the card reader for receiving at least a portion of the associated information from the card reader and for displaying the associated information when the user operates the vehicle. The display can be located on the vehicle and the displayed information can include at least a unique identifier assigned to the user of the electronic access card.

[0012] The present invention also concerns a method for monitoring a vehicle. The method includes the steps of providing an electronic access card, storing on the

electronic access card information associated with a user of the electronic access card, reading the associated information, transmitting at least a portion of the associated information from a vehicle transceiver to at least one of a monitoring station and a portable unit and displaying the associated information. In one arrangement, the portable unit can be a law enforcement mobile unit. Also, the associated information stored on the electronic access card can include at least one of a name, an address, a driving history of the user, a criminal history of the user, insurance coverage held by the user, vehicle registration and at least one digital photograph of the user. The method can also include the steps of biometrically identifying the user, transmitting an authorizing signal when the user is biometrically identified and reading the associated information in response to the authorizing signal.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] FIG. 1 illustrates an electronic access card in accordance with the inventive arrangements.

[0014] FIG. 2 illustrates a biometric identifier in accordance with the inventive arrangements.

[0015] FIG. 3 illustrates a vehicle in which access to the vehicle is controlled by the electronic access card of FIG. 1 in accordance with the inventive arrangements.

[0016] FIG. 4 illustrates a slot of a card reader positioned on an exterior of a vehicle in accordance with the inventive arrangements.

[0017] FIG. 5 illustrates a vehicle monitoring system in accordance with the inventive arrangements.

[0018] FIG. 6 illustrates a vehicle having a display for displaying license plate numbers in accordance with the inventive arrangements.

[0019] FIG. 7 illustrates a toll collection system in accordance with the inventive arrangements.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0020] Referring to FIG. 1, an electronic access card 100 is shown. The card 100 can be used to permit a user to access, for example, a secure area, a financial account, sensitive information or a mechanized vehicle such as an automobile. The user is not necessarily limited to being the owner of the card 100, as any authorized individual may be permitted to use the card 100. In addition, the card 100 can store useful information associated with the user(s) of the card 100, examples of which will be described later. For convenience, the card 100 can be roughly the size of a conventional credit card. It must be noted, however, that the card 100 can be any other suitable size.

[0021] The card 100 can include a microprocessor 110, a biometric identifier 112, one or more electrical contacts 114, a memory 116, a transceiver 118 and a power supply 120. The card 100 can also include one or more magnetic strips 122 for storing information in a manner similar to that employed by conventional credit cards. Control and data interfaces can also be provided for permitting the microprocessor 110 to access or to control the operation of the biometric identifier 112, the electrical contacts 114, the memory 116 and the transceiver 118. The microprocessor 110 can also be provided with suitable software or firmware for the conventional operations performed by the microprocessor 110. Further, the microprocessor 110 can be provided with program routines in accordance with the inventive arrangements.

[0022] The biometric identifier 112 can measure any suitable biometric characteristic of a person in possession of the card 100, can convert this measurement into a digital signal and can transfer the signal to the microprocessor 110. For example, the biometric identifier 112 can be designed to perform fingerprint

scans, voice analyses and retinal or iris scans. Those of ordinary skill in the art, however, will appreciate that the invention is not limited to these examples, as the biometric identifier 112 can measure other biometric characteristics. The biometric identifier 112 will be described in detail later.

[0023] The electrical contacts 114 can be used to create a signal path from external components to the microprocessor 110, which can facilitate the transfer of virtually any type of data between the microprocessor 110 and such components. As an example, the card 100 may be inserted in a card reader having its own biometric identifier (not shown). In this case, the user of the card 100 can provide a biometric sample to the biometric identifier of the card reader, and the card reader can generate a signal to be transferred through the electrical contacts 114 to the microprocessor 110. Based on the type of signal generated, the microprocessor 110 can determine whether the user is authorized to use the card 100. Also, authorized biometric samples may be transferred from an external component to the memory 116 through the electrical contacts 114. It is understood, however, that the invention is not limited to the above examples, as other types of data can be transferred to the microprocessor 110 through the electrical contacts 114.

[0024] The memory 116 can be any suitable memory capable of storing digitized biometric samples previously measured by the biometric identifier 112 as well as other types of information concerning the owner of the card 100. For example, the memory 116 can be used to store digitized images of fingerprints, digitized samples of a person's voice or digitized images of a person's retina or iris. In addition, examples of information pertinent to the user of the card 100 that can be stored in the memory 116 include name, address, social security number, account information, driver license number, driving record, criminal history (if any), insurance

coverage and vehicle registration. One or more digital photographs of the user of the card 100 may also be stored in the memory 116. Those of ordinary skill in the art, however, will appreciate that the memory 116 can store other suitable types of data. Also, the magnetic strip 122 can store at least a portion of the data stored in the memory 116 to permit the card 100 to be used with conventional card readers.

[0025] The memory can be programmable read only memory (PROM), erasable programmable read only memory (EPROM), electrically erasable programmable read only memory (EEPROM) or flash memory. Of course, other types of memory may be used with the invention. In one arrangement, the memory 116 can be interchangeable or replaceable so that chips containing pre-stored data may be used. Alternatively, if the memory 116 is programmable or erasable, the memory 116 can be updated or reprogrammed through the electrical contacts 114 and the microprocessor 110.

[0026] The transceiver 118 can transmit and receive radio frequency (RF) signals, process these signals and forward them to the microprocessor 110 when RF signals are received by the transceiver 118 or forward them to an external receiver or transceiver when RF signals are transmitted from the transceiver 118. Any suitable standard can be used to transmit the RF signals. For purposes of the invention, the term radio frequency can include any electromagnetic wave capable of being wirelessly propagated through a suitable medium. The transceiver 118 enables the card 100 to wirelessly receive and transmit data that can be transmitted to or from the card 100 through the electrical contacts 114. For example, if the memory 116 is programmable or erasable, data can be transmitted from an external transmitter (not shown) and can be received by the transceiver 118, which can forward the data to the microprocessor 110. The microprocessor 110 can then

transmit the data to the memory 116. Moreover, the transceiver 118 can receive authorizing signals from an external biometric identifier (not shown) if the user has provided a biometric sample to the external biometric identifier. Thus, if the user is an authorized user, such a status can be wirelessly forwarded to the microprocessor 110 through the transceiver 118.

[0027] The power supply 120 can provide power to one or more of the components of the card 100. For example, the power supply 120 can provide power to the microprocessor 110, the biometric identifier 112 and the transceiver 118. In another arrangement, the card 100 can receive power from an external source through the electrical contacts 114. These embodiments are not mutually exclusive, as the card 100 can include its own power supply 120 and can also receive power through the electrical contacts 114. As an example, the power supply 120 can be one or more batteries, and the batteries can be interchangeable or replaceable.

[0028] In operation, a user can provide a biometric sample to the biometric identifier 112. The biometric identifier 112 can measure the biometric sample and can convert this measurement into a digital signal. The biometric identifier 112 transmits the digital signal to the microprocessor 110, which then can compare the digitized sample with biometric samples stored in the memory 116. If there is a match, the microprocessor 110 can transmit an authorizing signal to an external reader (not shown) through the electrical contacts 114 or the transceiver 118. In addition to the authorizing signal, the microprocessor 110 can forward relevant information about the user to the external reader through the electrical contacts 114 or the transceiver 118. The external reader can transmit data to the microprocessor 110 (and on to the memory 116 if desired) through the electrical contacts 114 and/or the transceiver 118.

[0029] Referring to FIG. 2, an example of a biometric identifier 112 in accordance with the inventive arrangements is shown. In this example, the biometric identifier 112 can generate digitized images of fingerprints and forward these digital signals to the microprocessor 110. The biometric identifier 112 can include a platen 210, a light source 212, a fingerprint scanner 214 and a pressure switch 216.

[0030] The light source 212 can direct light towards the platen 210 and can be, for example, a light emitting diode. The platen 210 can also be transparent to the wavelength of the emitted light and can contain the pressure switch 216, which can be electrically coupled to the microprocessor 110. The pressure switch 216 can detect when a user has placed his or her finger on the platen 210 and can signal the microprocessor 110. In addition, the microprocessor 110 can control the operation of the light source 212 and the fingerprint scanner 214. The fingerprint scanner 214 can be any biometric device capable of scanning fingerprint images and converting these images into digitized images.

[0031] A user can place his or her finger on the platen 210, and the pressure switch 216 can detect this contact and can signal the microprocessor 110. The microprocessor 110 can signal the fingerprint scanner 214 and the light source 212, which can emit the light needed to create a scanned image of the user's fingerprint. The light can pass through the platen 210 and can strike the user's finger, which can cause the light to be reflected to the fingerprint scanner 214.

[0032] From the reflected light, the fingerprint scanner 214 can generate a scanned image of the user's fingerprint and can convert the image into a digital signal. The fingerprint scanner 214 can forward this signal to the microprocessor 110, which can compare the digitized image with authorized images that are stored in the memory 116. If there is a match, the microprocessor 110 can transmit an

authorizing signal through the electrical contacts 114 (see FIG. 1) or the transceiver 118 (also see FIG. 1).

[0033] Authorized fingerprint images can be loaded into the memory 116 at any time. For example, the owner of the card 100 and any other authorized users can have digitized images of their fingerprints generated by an external scanner and transferred to the memory 116 through the electrical contacts 114 or the transceiver 118. This process can occur when the card 100 is first activated or at any time following its activation. In addition, the owner of the card 100 can have previously authorized fingerprint images removed from the memory 116 by an external card reader containing suitable software and circuitry.

[0034] In another arrangement, the microprocessor 110 can include a clock that measures the amount of time that has passed since the confirmation of an authorized fingerprint. Additionally, the microprocessor 110 can be programmed to disable the card 100 after a predetermined time interval following this confirmation to limit the possibility of unauthorized use of the card 100. For example, once the microprocessor 110 verifies that a user that has had his or her fingerprint scanned is permitted to use the card 100, the microprocessor 110 can disable the card 100 one minute later. The microprocessor 110 can disable the card 100 through a variety of ways, including by blocking the transfer of data to and from the card 100.

[0035] Of course, the card 100 can be re-activated once it is disabled if the authorized user provides another fingerprint sample. The microprocessor 110 can also be programmed to initiate another scanning and comparison process just prior to the exhaustion of the predetermined time interval. As a result, the authorized user may continuously keep his or her finger on the platen 210 to override the disabling feature. As will be explained later, a signal can be transmitted to the microprocessor

110 from an external component that can override this disabling feature. It is understood that the predetermined time interval can be any suitable length of time. Moreover, other suitable measures to prevent illegal use of the card following initial authorization may be employed.

[0036] Although one example of a biometric identifier 112 has been presented, it is important to note that the invention is in no way limited to this particular system. Those of ordinary skill in the art will appreciate that other systems suitable for measuring biometric characteristics can be used. For example, the biometric identifier 112 can be designed to perform iris or retinal scans. In fact, the invention does not require the use of biometric identifier 112, as the card 100 of FIG. 1 can operate without such a device.

[0037] The card 100 can be used to allow its owner or other authorized users access to a wide variety of things. An example of how the card can provide access to a vehicle is shown in FIG. 3. The vehicle can be any mechanized form of transportation, such as automobiles, locomotives, airplanes or ships. The vehicle can also be a form of transportation in which the primary force of locomotion is provided by a human, such as a bicycle. The card 100 can provide access to an ignition system of a vehicle or some other critical component of operation.

[0038] In this example, the card 100 can provide a user with access to an ignition system 310 of a vehicle 300. The vehicle 300 can include a card reader 312, which can be electrically coupled to the ignition system 310. As an example, the card reader 312 can be mounted inside a passenger compartment (not shown) of the vehicle 300, preferably within a comfortable reaching distance of the steering means of the vehicle 300. It is understood, however, that the card reader 312 can be positioned at any other suitable location in or on the vehicle 300. The ignition

system 310 can start an engine 311 of the vehicle 300 and can include circuitry to unlock or lock one or more door locks 313 of the vehicle 300. As will be described below, the card reader 312 can transmit a signal to the ignition system 310 to allow a driver to start the vehicle 300 or unlock one or more of its doors.

[0039] Referring to FIGS. 1 and 3, the card reader 312 can include a slot 314 for receiving the card 100, a card reader microprocessor 316, a transceiver 318 and an enabling circuit 320 for selectively enabling or disabling the ignition system 310. The card reader 312 can receive power from a power supply 322. In one arrangement, the power supply 322 can be associated with the vehicle 300. For example, the power supply 322 can be an automobile battery; however, other suitable power supplies can be used to power the card reader 312.

[0040] The slot 314 can include electrical contacts (not shown), which can be used (along with the electrical contacts 114 of the card 100) to complete a circuit path (not shown) between the card reader microprocessor 316 and the microprocessor 110 of the card 100 when the card 100 has been inserted in the slot 314. This path can be used for the transmission of data between these components. In addition, the circuit path can be used to provide power from the power supply 322 to one or more of the components of the card 100. In another arrangement, the transceiver 318 of the card reader 312 can wirelessly transmit data to or receive data from the transceiver 118 of the card 100 or any other suitable transceiver or transmitter.

[0041] As an example, when the user of the card 100 is biometrically identified by the card 100, the user can insert the card 100 into the slot 314 of the card reader 312. The microprocessor 110 of the card 100 can signal the card reader microprocessor 316 – through the electrical contacts 114 - that the card 100 has

been enabled by an authorized user. In response, the card reader microprocessor 316 can signal the enabling circuit 320, which in turn can enable the ignition system 310 for starting the engine 311. As another example, when the user of the card 100 is identified, the microprocessor 110 of the card 100 can signal the card reader microprocessor 316 through the transceiver 118 of the card 100 and the transceiver 318 of the card reader 312. Further, the card reader microprocessor 316 can signal the enabling circuit 320 to enable the ignition system 310 for starting the engine 311 or unlocking one or more of the door locks 313 of the vehicle 300.

[0042] In either arrangement, the card reader microprocessor 316 can transmit a signal (through the electrical contacts 114 or the transceiver 318 and the transceiver 118) back to the microprocessor 110 informing the microprocessor 110, for example, that the engine of the vehicle 300 has been started. The microprocessor 110 can then override the disabling feature associated with the biometric identification of the user. This way, the user is not required to continuously provide a biometric sample to keep the ignition system 310 enabled and, hence, the engine 311 running.

[0043] Although FIG. 3 illustrates the slot 314 as being integrated with the card reader 312, the invention is not so limited. For example, referring to FIG. 4, the slot 314 can be positioned on one or more doors 402 of the vehicle 300. The slot 314 can also be positioned on a trunk 404 of the vehicle 300.

[0044] Referring back to FIG. 3, if the card 100 does not include its own power source, the user can insert the card 100 into the slot 314, and as noted earlier, power can be transferred from the power supply 322 to the components of the card 100. At this point, the biometric identifier 112 can perform the biometric measurement and the microprocessor 110 can execute the comparison step. In

accordance with the above discussion, if the user is an authorized user, the microprocessor 110 of the card 100 can then send an authorization signal to the card reader microprocessor 316 through the circuit path created by the insertion of the card 100 in the slot 314. Alternatively, the microprocessor 110 can signal the card reader microprocessor 316 through the transceiver 118 of the card 100 and the transceiver 318 of the card reader 312.

[0045] In another embodiment, the card reader 312 can include a biometric identifier 324, which can be used in place of the biometric identifier 112 on the card 100. Similar to the biometric identifier 112 on the card 100, the biometric identifier 324 can perform a biometric measurement, convert the measurement into a digital signal and transmit the signal to the card reader microprocessor 316. The card reader 312 can also include a memory 326 for storing authorized biometric samples for comparison with biometric measurements that the biometric identifier 324 performs. The overall operation of the biometric identifier 324 and the processes used to confirm the identity of a user are similar to the operation described in relation to FIGS. 1 and 2, and as such, no further description is warranted. The biometric identifier 324 can be constructed to perform fingerprint, iris or retinal scans or voice analysis, although the biometric identifier 324 is not limited to receiving these particular types of biometric measurements. As another example and referring back to FIG. 4, a biometric identifier 324 may also be mounted on one or more doors 402 or the trunk 404 of the vehicle 300.

[0046] Continuing with FIG. 3, the card reader 312 can also include a port 328. The port 328 can be used to transfer data between the card reader 312 and an external component. For example, authorized biometric samples that have been digitized can be transferred through the port 328 to the memory 326. Those of

ordinary skill in the art will appreciate that the invention is not limited to this example, as any other suitable type of data can be transferred to the card reader 312 through the port 328. In addition, the biometric identifier 324 can be used to generate authorized biometric measurements for storage in the memory 326. These digitized measurements can be compared with subsequently measured samples to confirm that the provided sample is from an authorized user.

[0047] After the engine 311 has been started, there are several ways to shut it off. For example, the user can merely remove the card 100 from the slot 314, and the card reader microprocessor 316 can signal the enabling circuit 320. The enabling circuit 320 can then disable the ignition system 310, which can cause the engine 311 to stop. Alternatively, the vehicle 300 can include a kill switch 325 for stopping the engine 311. Specifically, the user can depress the kill switch 325, which can signal the card reader microprocessor 316. Like the example above, the card reader microprocessor 316 can signal the enabling circuit 320 to disable the ignition system 310 and, hence, the engine 311. The kill switch 325 may be particularly useful, for example, if the authorization signal from the card 100 was wirelessly transmitted, i.e., the card 100 was never inserted in the slot 314.

[0048] Although the card 100 has been illustrated as providing access to a vehicle, particularly one with an engine, it must be noted that the invention is not limited in this regard. For example, the card 100 can be used to provide access to non-mechanized vehicles. In addition, the card 100 can be used to provide access to other forms of machinery. Specifically, the card 100 can provide access to automatic teller machines, entrances to buildings or residences, safes or safety deposit boxes, computers or any other device that may warrant restriction to its access by the general public.

[0049] Referring to FIG. 5, the vehicle 300 can be part of a vehicle monitoring system 400. In this arrangement, the vehicle 300 can also include a vehicle transceiver 330 and a tracking device 332. The system 400 can include one or more tracking satellites 410, one or more communications satellites 412, a wireless communications network 414 and one or more monitoring stations 416. The monitoring station 416 can include a transceiver 417 and one or more computers 419. In addition, the tracking device 332 can receive navigational data from the tracking satellites 410 and can forward this data to the card reader microprocessor 316. In one arrangement, the tracking device 332 of the vehicle 300 can be a global positioning system (GPS) receiver and the tracking satellites 410 can be GPS satellites. Further, the navigational data can include GPS coordinates such as a latitude coordinate, a longitude coordinate and an altitude coordinate. The tracking satellites 410 can communicate with the tracking device 332 over a satellite communications link 418, which can be any link suitable for broadcasting RF signals from the tracking satellites 410 to the tracking device 332.

[0050] The vehicle transceiver 330 can transmit data to or receive data from the transceiver 417 of the monitoring station 416. In one arrangement, data can be transmitted between the vehicle transceiver 330 and the transceiver 417 of the monitoring station 416 over a communications link 420 facilitated by the communications satellite 412. The communications link 420 can be any communications link suitable for broadcasting RF signals between the vehicle transceiver 330, the communications satellite 412 and the transceiver 417 of the monitoring station 416. Alternatively, data can be transmitted between the vehicle transceiver 330 and the transceiver 417 of the monitoring station 416 over a communications link 422 and the wireless communications network 414.

[0051] As is known in the art, the wireless communications network 414 can include, for example, wireless repeaters, base station units and switches for facilitating communications between a wireless unit and the public switched telephone network (PSTN) or another wireless unit. Thus, in addition to supporting any suitable type of RF communications, the communications link 422 may also include portions of a hard-wired communications connection, as shown in FIG. 5. The transceiver 417 of the monitoring station 416 can receive any hard-wired connections in addition to wireless signals. For purposes of the invention, when referring to any transmissions between the vehicle transceiver 330 and the transceiver 417 of the monitoring station 416, it is assumed that such a transmission can be sent over the communications link 420 or the communications link 422 unless otherwise noted.

[0052] Virtually any type of data can be transmitted between the vehicle 300 and the monitoring station 416. For example, the card reader microprocessor 316 can forward the navigational data that it receives to the vehicle transceiver 330, which can then transmit such data to the transceiver 417 of the monitoring station 416. As another example, the card reader microprocessor 316 can forward information that is stored on the card 100 to the vehicle transceiver 330 for transmission to the transceiver 417.

[0053] Any data received by the transceiver 417 of the monitoring station 416 can be displayed on the computer 419. Accordingly, operators at the monitoring station 416 can have access to the whereabouts of a particular vehicle 300 and any relevant information associated with the user of the card 100 that is stored on the card 100. For example, the name, address, age, driver license number, license plate number, driving history, criminal history, vehicle registration and insurance coverage

of the user in addition to the location of the vehicle 300 can be displayed on the computer 419 of the monitoring station 416. One or more digital photographs of the user may also be displayed on the computer 419. It is understood, however, that other suitable types of information can be stored on the card 100 and eventually displayed on the computer 419.

[0054] In another embodiment, information concerning the user of the card 100 can be transmitted from the computer 419 through the transceiver 417 of the monitoring station 416 to the vehicle transceiver 330 and the card reader microprocessor 316. The card reader microprocessor 316 can then transfer this information to the card 100 through any of the techniques discussed in relation to FIG. 3. As an example, if the user of the card 100 has received a traffic citation, the driving history of the user of the card 100 can be updated at computer 419 of the monitoring station 416, and this update can be forwarded to the card reader microprocessor 316 and eventually the card 100.

[0055] A disabling signal can also be transmitted from the monitoring station 416 to the vehicle 300. Specifically, the computer 419 can generate the disabling signal, and the signal can be transmitted to the card reader microprocessor 316 through the transceiver 417 of the monitoring station 416 and the vehicle transceiver 330. In response, the card reader microprocessor 316 can signal the enabling circuit 320, which can then disable the ignition system 310 or any other component of the vehicle vital to its operation. Disabling the ignition system 310 can stop the engine 311 of the vehicle 300. Such a feature can be useful, for example, if the vehicle 300 has been stolen or if the owner of the vehicle 300 is wanted by a law enforcement agency.

[0056] Other signals may be forwarded from the monitoring station 416 to the vehicle 300 as well. For example, if the system 400 uses GPS technology to determine the location of the vehicle 300, the system 400 can employ differential GPS to produce more accurate readings. As is known in the art, differential GPS technology relies on a stationary GPS receiver with known GPS coordinates for correcting errors in the transmissions from GPS satellites to other stationary or mobile targets containing GPS tracking devices. As an example, a differential tracking device 424 can be built into the monitoring station 416 and can receive signals from the tracking satellites 410 over the satellite communications link 418.

[0057] The differential tracking device 424, because its GPS coordinates have previously been accurately measured, can generate an error correction factor that can be used to error correct the transmissions from the tracking satellites 410. The error correction factor can be transmitted from the transceiver 417 of the monitoring station 416 to the vehicle transceiver 330 and the card reader microprocessor 316. The card reader microprocessor 316 can use this error correction factor to produce a more accurate reading of the GPS coordinates of the vehicle 300.

[0058] It is understood, however, that the differential tracking device 424 is not limited to being positioned at the monitoring station 416, as any number of differential tracking devices 424 can be placed at other suitable locations. Moreover, the system 400 can be designed to rely on pre-existing differential tracking devices 424 constructed by, for example, a governmental agency. Nevertheless, the use of differential GPS is not a requirement of the invention; in fact, it must be stressed that the invention is not limited to tracking a vehicle 300 through the use of GPS technology, as any other technique for locating the vehicle 300 can be practiced with the invention.

[0059] Enabling signals for starting the ignition system 310 can also be transmitted from the monitoring station 416 to the vehicle 300. In particular, once the user has been biometrically identified, the card reader microprocessor 316 can generate an authorizing signal, which can be transmitted to the computer 419 of the monitoring station 416 through the vehicle transceiver 330 and the transceiver 417. In response, the computer 419 can produce an enabling signal, which can be transmitted from the transceiver 417 to the vehicle transceiver 330 and, in turn, the card reader microprocessor 316. The card reader microprocessor 316 can signal the enabling circuit to activate the ignition system 310 to start the engine 311 or unlock one or more of the door locks 311 of the vehicle 300.

[0060] The transmission of an enabling signal from the monitoring station 416 to the vehicle 300 may also be performed if the user of the card 100 has misplaced the card 100, if the card 100 has been stolen or if the user has accidentally locked the card 100 in the vehicle 300. Specifically, the user can be provided with a telephone number or Web site address for contacting the monitoring station 416 and a password unique to the user. If necessary, the user can contact the monitoring station 416 and can provide his or her password. The password can be given to a live person or can be received by an answering system 426 at the monitoring station 416. The answering system 426 can include suitable voice recognition software to permit the user to speak his or her password or can include circuitry for receiving tones from a touch-tone telephone. The answering system 426 can also include suitable software and circuitry for receiving the password over the Internet or some other communications network.

[0061] The live person or the answering system 426 can enter the received password into the computer 419, which can generate an enabling signal. In

accordance with the above discussion, the enabling signal can be forwarded to the card reader microprocessor 316, which can signal the enabling circuit 320 to cause the ignition system 310 to start the engine 311 of the vehicle 300 or to unlock one or more of the door locks 313 of the vehicle 300. Although unique to the user of the card 100, the user may choose to share his or her password with friends or family to allow such persons access to the vehicle 300.

[0062] Signals can also be transmitted between the vehicle 300 and a portable unit 428 in lieu of or in addition to the monitoring station 416. As an example, the portable unit 428 can be a police cruiser or any other law enforcement mobile unit. It is understood, however, the portable unit 428 can be associated with other types of agencies. The portable unit 428 can include a computer 430 and a transceiver 432 to facilitate the transmission of signals between the portable unit 428 and the vehicle 300. As a result, all or at least a portion of the features associated with the monitoring station 416 can be performed by the portable unit 428.

[0063] For example, if the vehicle 300 is within the range of the transceiver 432 of the portable unit 428, information associated with the user of the card 100 can be transmitted from the vehicle transceiver 330 to the transceiver 432. The received data can then be displayed on the computer 430 of the portable unit 428. Thus, if the vehicle 300 is stopped by the portable unit 428, the operator of the portable unit 428, which may be a law enforcement officer, can have access to the driving history or criminal history of the operator of the vehicle 300, i.e., the user of the card 100. The operator of the portable unit 428, informed of potentially troubling history concerning the operator of the vehicle 300, can take whatever precautionary steps that are warranted.

[0064] In one arrangement, the information being transmitted from the vehicle 300 can be transmitted in accordance with a predetermined interval. For example, the card reader microprocessor 316 can instruct the vehicle transceiver 330 to broadcast the information that it receives from the card reader microprocessor 316 (e.g., driver information, GPS coordinates) every few seconds or minutes. For longer time intervals, less power is consumed from the power supply 322, which may become an issue if the engine 311 of the vehicle 300 is off. Accordingly, the card reader microprocessor 316 can monitor the power supply 322 and can adjust the time between transmissions to preserve power.

[0065] During the time interval, the card reader microprocessor 316 may enter a passive stage in which only the most vital functions are performed. Once the time interval is over, the card reader microprocessor 316 can enter an active stage. In the active stage, the card reader microprocessor 316 can receive information from the tracking device 332 and can update, if necessary, any information concerning the user of the card 100. The card reader microprocessor 316 can then instruct the vehicle transceiver 330 to transmit the updated data to the monitoring station 416 or the portable unit 428. Once the data is transmitted, the card reader microprocessor 316 may reenter the passive stage, and another time interval may begin. This feature can increase the efficiency of the card reader 312 by lowering its power consumption.

[0066] In another arrangement, an activation signal can be transmitted from the transceiver 417 of the monitoring station 416 or the transceiver 432 of the portable unit 428 to the vehicle transceiver 330 and to the card reader microprocessor 316. The card reader microprocessor 316 can enter the active stage and can perform whatever tasks that are typically performed during the active stage.

As a result, operators in the monitoring station 416 or the portable unit 428 may instantaneously access information about the vehicle 300 and the user of the card 100.

[0067] In another embodiment of the invention, each user of the card 100 can be assigned one or more unique identifiers. The assigned identifiers can be unique in that each identifier will be given to only one user. For purposes of the invention, the term "unique identifier" can include any suitable sequence of characters, such as alphanumeric characters, used to identify a particular person or a registration out of a pool of other individuals or registrations. As an example, the unique identifier can be a license plate number, a driver license number or an insurance account number. A government agency or any other authorized entity can assign the unique identifiers, and the identifiers can be permanent such that each assignee may keep the assigned identifier throughout his or her lifetime or for the duration of the function with which the identifier is associated. For example, if the unique identifier is a license plate number, the assignee may keep the assigned license plate number for his or her driving history.

[0068] Referring to FIG. 1, each individual using the card 100 may have his or her unique identifier transferred to the card 100 from an external system to the microprocessor 110 through the transceiver 118 or the electrical contacts 114. The microprocessor 110 can then transfer to the memory 116 for storage any number of the unique identifiers. Referring to FIGS. 1 and 5, when the user of the card 100 is biometrically identified and the card 100 is inserted in the slot 314 of the card reader 312, the card reader microprocessor 316 can access this particular user's assigned identifier through the electrical contacts 114. Alternatively, the identifier can be

transferred to the card reader microprocessor 316 through the transceiver 118 of the card 100 and the transceiver 318 of the card reader 312.

[0069] In addition, the unique identifier can be transmitted to the computer 419 of the monitoring station 416 or the computer 430 of the portable unit 428 in accordance with the above discussion. Thus, the user's unique identifier can be displayed at the computer 419 or the computer 430 with other information concerning the user.

[0070] Referring to FIG. 5 only, the user's unique identifier can also be displayed on the vehicle 300. For example, the vehicle 300 can include a display 434 for displaying the identifier of the user of the card 100. In one arrangement, the display 434 can be a liquid crystal display having a backlit display. Such a display 434 can increase the visibility of the identifier. Those of ordinary skill in the art, however, will appreciate that other suitable display units can be used with the invention. In fact, the display 434 is not limited to a purely electronic display, as electro-mechanical or simply mechanical displays can be used as well.

[0071] The card reader microprocessor 316 can forward to the display 434 the identifier that has been assigned to the user of the card 100 that has been biometrically identified. The display 434 can then display the user's identifier. This feature of the card 100 is applicable to any vehicle 300 having a card reader 312 and a display 434. As such, the user's unique identifier can be transferrable such that it can be displayed on any vehicle 300 that he or she operates and that is equipped with these components.

[0072] The display 434 can be positioned at any suitable location on the vehicle 300. In one arrangement, the display 434 can be mounted on the rear of the vehicle 300, just below the bumper. This configuration is illustrated in FIG. 6.

Notably, many states require conventional license plates to be mounted on a motorized vehicle in this area.

[0073] Referring back to FIG. 5, the vehicle 300 can include one or more panic buttons 436. In one arrangement, the panic button 436 may be positioned near the driver's seat of the vehicle 300 for easy access by the user of the card 100 if the user is driving the vehicle 300. Of course, the panic button 436 may be positioned at any other suitable location inside or even outside the vehicle 300. When the panic button 436 is pushed, a signal can be forwarded to the card reader microprocessor 316 of the card reader 312. The card reader microprocessor 316 can then instruct the vehicle transceiver 330 to transmit a distress signal to either the transceiver 417 of the monitoring station 416 or the transceiver 432 of the portable unit 428 or both. The navigational data of the vehicle 300 and any relevant information associated with the user of the card 100 may also be transmitted to the monitoring station 416 and/or the portable unit 428 in addition to the distress signal.

[0074] The distress signal received by the monitoring station 416 or the portable unit 428 may contain an emergency message such as "Send Help Immediately," which can be displayed at the computer 430 of the portable unit 428 or the computer 419 of the monitoring station 416. The card reader microprocessor 316 may be programmed with the emergency message prior to the activation of the overall system 400.

[0075] Referring to FIG. 7, a toll collection system 600 in accordance with the inventive arrangements is shown. The toll collection system 600 can include a computer 610, a communications network 612 such as the Internet, a toll collection agency 614, at least one toll booth 616 and at least one vehicle 300 as described in relation to FIG. 5. The toll booth 616 can include one or more sensors 618 and one

or more gates 620 for selectively permitting the passage of traffic. In this arrangement, the vehicle 300, in combination with the card 100, can be used to automatically pay tolls associated with the passage of, for example, certain highways, bridges or ferries.

[0076] Specifically, the card 100 can be programmed with account information associated with the user of the card 100. Referring to FIGS. 1 and 5, the account information can be stored in the memory 116 and can be eventually transferred to the card reader microprocessor 316. The transfer of information to the card 100 has been previously illustrated, and a detailed discussion is not warranted. Referring back to FIG. 7, the user of the card 100 can then make a payment with the toll collection agency 614. As an example, the user can make an electronic payment over the communications network 612 to the toll collection agency 614 using the computer 610. The user of the card 100 is credited with this payment, and the information is forwarded to a database (not shown) at the toll booth 616. The sensor 618 contains suitable software and circuitry for accessing this database.

[0077] When the vehicle 300 approaches the toll booth 616, the sensor 618 can transmit an activation signal to the vehicle transceiver 330. The vehicle transceiver 330 can pass the activation signal to the card reader microprocessor 316. Subsequently, the card reader microprocessor 316 can forward to the vehicle transceiver 330 the account information associated with the user of the card 100 who has previously been biometrically identified. The vehicle transceiver 330 can transmit the account information to the sensor 618, which automatically checks the database to determine whether the account is in good standing. If the account has an acceptable credit, the sensor 618 signals the gate 620 to permit the vehicle to pass.

[0078] In another embodiment, the card reader microprocessor 316 can instruct the vehicle transceiver 330 to transmit the account information in accordance with a predetermined interval, similar to the process described above with respect to the transmissions to the monitoring station 416 and the portable unit 428. If so, the activation signal transmitted from the sensor 618 may not be necessary for operation of the system 600.

[0079] Also, the transceiver 318 on the card 100 can receive the activation signal from the sensor 618 and can transmit the account information associated with the user of the card 100 back to the sensor 618. This feature permits the vehicle 300 to pass through the toll booth 616 even if the vehicle 300 is not equipped with a vehicle transceiver 330. Although the present invention has been described in conjunction with the embodiments disclosed herein, it should be understood that the foregoing description is intended to illustrate and not limit the scope of the invention as defined by the claims.

CLAIMS

What is claimed is:

1. A vehicle monitoring system, comprising:

an electronic access card, wherein said electronic access card stores information associated with a user of said electronic access card;

a card reader for receiving said electronic access card and for reading said associated information; and

a vehicle transceiver coupled to said card reader, wherein said vehicle transceiver transmits at least a portion of said associated information to at least one of a monitoring station and a portable unit;

wherein said monitoring station and said portable unit each include a computer for displaying said associated information.

2. The system according to claim 1, wherein said card reader and said vehicle transceiver are mounted in a vehicle;

wherein said vehicle transceiver transmits said associated information from any vehicle having said card reader and said vehicle transceiver.

3. The system according to claim 1, wherein said portable unit is a law enforcement mobile unit.

4. The system according to claim 1, wherein said electronic access card includes a biometric identifier for identifying the user and transmits an authorizing signal to said card reader when the user is biometrically identified;

wherein said card reader reads said associated information in response to said authorizing signal.

5. The system according to claim 4, wherein said biometric identifier generates digitized images of fingerprints.

6. The system according to claim 1, wherein said electronic access card includes at least one electrical contact to permit the transfer of said associated information to said card reader.

7. The system according to claim 1, wherein said electronic access card includes a transceiver for transmitting said associated information to said card reader.

8. The system according to claim 1, wherein said associated information stored on said electronic access card includes at least one of a name, an address, a driving history of the user, a criminal history of the user, insurance coverage held by the user, vehicle registration and at least one digital photograph of the user.

9. The system according to claim 1, wherein said card reader includes a tracking device and said tracking device receives navigational data.

10. The system according to claim 9, wherein said vehicle transceiver transmits said navigational data to at least one of said monitoring station and said portable unit;

wherein said navigational data is displayed on said computer.

11. The system according to claim 10, wherein said vehicle transceiver transmits said navigational data and said associated information to at least one of said monitoring station and said portable unit using at least one communications satellite.

12. The system according to claim 10, wherein said vehicle transceiver transmits said navigational data and said associated information to at least one of said monitoring station and said portable unit using a wireless communications network.

13. The system according to claim 10, wherein said vehicle transceiver transmits said navigational data and said associated information to at least one of said monitoring station and said portable unit in accordance with a predetermined interval.

14. The system according to claim 1, further comprising an ignition system;

wherein said card reader includes an enabling circuit for enabling said ignition system.

15. The system according to claim 14, wherein said ignition system, when enabled, starts an engine of a vehicle and locks and unlocks at least one door lock of the vehicle.

16. The system according to claim 1, further comprising an ignition system;

wherein said card reader further includes an enabling circuit for disabling said ignition system;

wherein a disabling signal is transmitted to said vehicle transceiver from said monitoring station and forwarded to said card reader;

wherein said enabling circuit disables said ignition system and said ignition system stops an engine of a vehicle in response to the receipt of said disabling signal by said card reader.

17. The system according to claim 1, further comprising an ignition system;

wherein said card reader, said vehicle transceiver and said ignition system are mounted in a vehicle;

wherein the vehicle further includes a vehicle biometric identifier for identifying the user;

wherein said vehicle biometric identifier transmits an authorizing signal to said card reader when the user is biometrically identified;

wherein said card reader reads said associated information in response to said authorizing signal.

18. The system according to claim 17, wherein said vehicle biometric identifier is positioned in the interior of the vehicle.

19. The system according to claim 17, wherein the vehicle further includes at least one door and said vehicle biometric identifier is mounted on said door.

20. The system according to claim 1, further comprising an ignition system and at least one toll booth having at least one sensor and at least one gate for controlling the flow of traffic through said toll booth;

wherein said card reader, said vehicle transceiver and said ignition system are mounted in a vehicle;

wherein said vehicle transceiver transmits to said sensor said associated information read from said electronic access card;

wherein said associated information includes at least information about the user's account with a toll collection agency.

21. The system according to claim 1, further comprising an ignition system and at least one toll booth having at least one sensor and at least one gate for controlling the flow of traffic through said toll booth;

wherein said card reader and said ignition system are mounted in a vehicle;

wherein said electronic access card further includes a transceiver for transmitting to said sensor said associated information stored on said electronic access card;

wherein said associated information includes at least information about the user's account with a toll collection agency.

22. The system according to claim 10, further comprising a panic button;

wherein when said panic button is pressed, said vehicle transceiver transmits a distress signal to at least one of said monitoring station and said portable unit.

23. The system according to claim 22, wherein said distress signal includes at least an emergency message and said navigational data.

24. The system according to claim 1, further comprising a display coupled to said card reader for receiving at least a portion of said associated information from said card reader and for displaying said portion of associated information when the user operates the vehicle;

wherein said display is located on the vehicle and said displayed information includes at least a unique identifier assigned to the user of said electronic access card.

25. A method for monitoring a vehicle, comprising the steps of:

providing an electronic access card;

storing on the electronic access card information associated with a user of the electronic access card;

reading the associated information;

transmitting at least a portion of the associated information from a vehicle transceiver to at least one of a monitoring station and a portable unit; and

displaying the associated information.

26. The method according to claim 25, wherein the portable unit is a law enforcement mobile unit.

27. The method according to claim 25, wherein the associated information stored on the electronic access card includes at least one of a name, an address, a driving history of the user, a criminal history of the user, insurance coverage held by the user, vehicle registration and at least one digital photograph of the user.

28. The method according to claim 25, further comprising the steps of:

biometrically identifying the user;

transmitting an authorizing signal when the user is biometrically identified; and

reading the associated information in response to the authorizing signal.

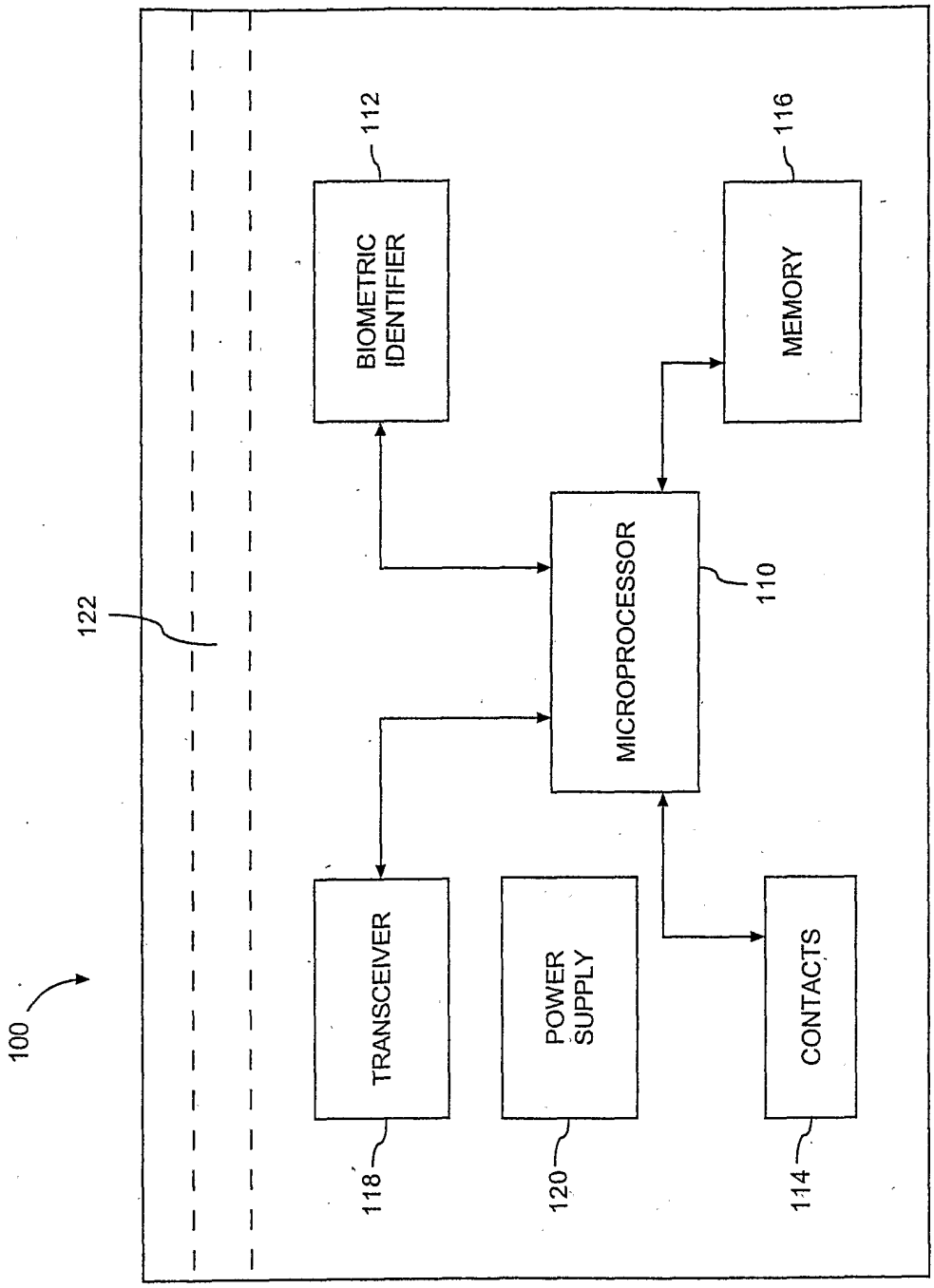

100
122
BIOMETRIC IDENTIFIER
112
MEMORY
116
MICROPROCESSOR
110
TRANSCEIVER
118
POWER SUPPLY
120
CONTACTS
114

FIG. 1

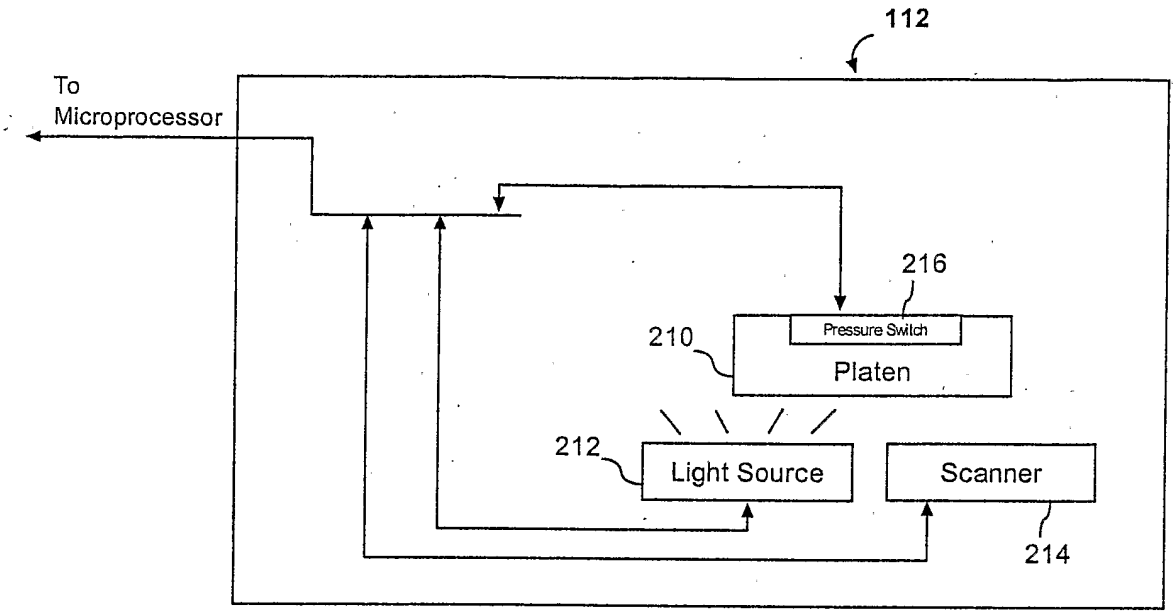

112
To
Microprocessor
216
Pressure Switch
210
Platen
212
Light Source
Scanner
214

FIG. 2

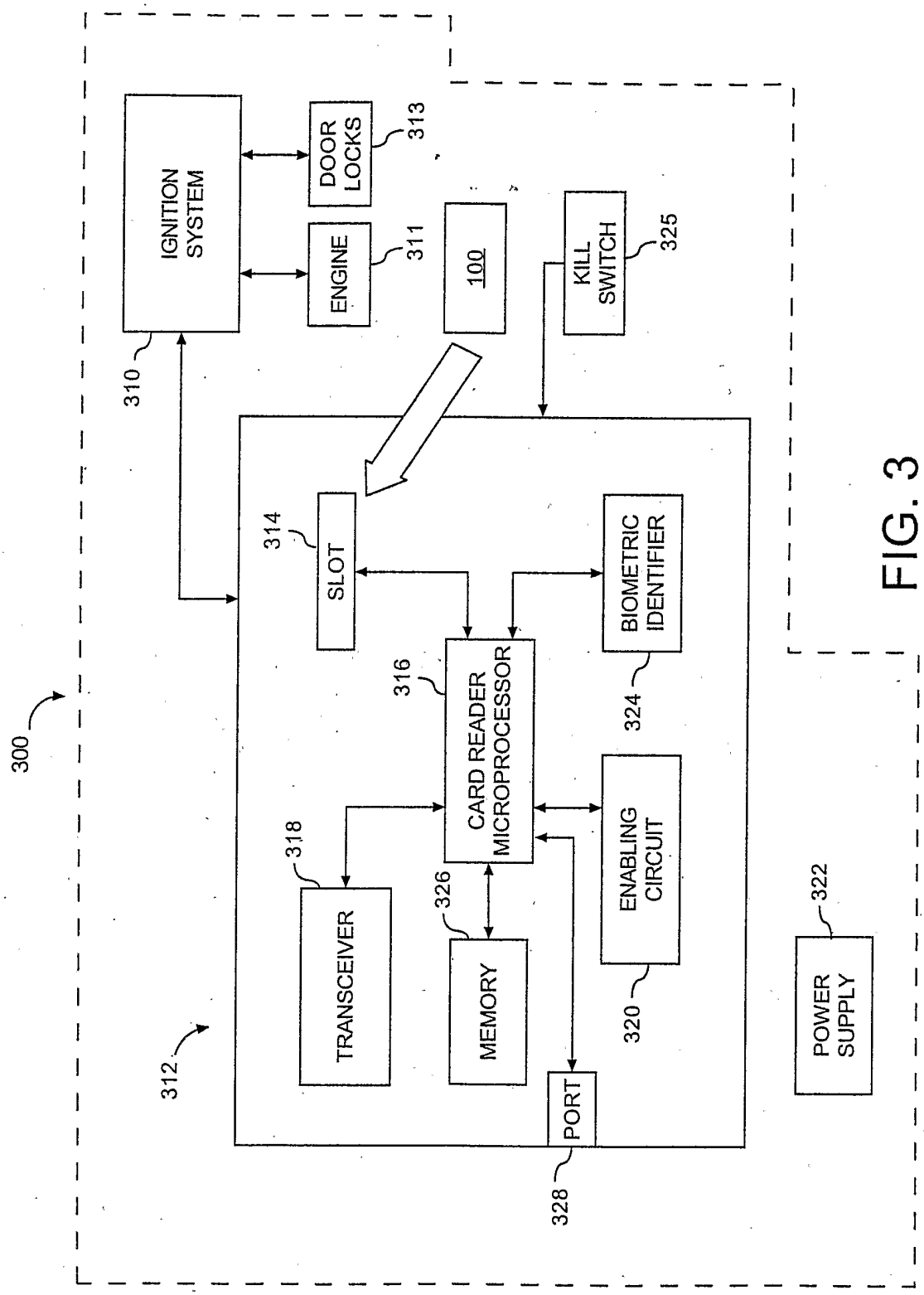

300
IGNITION SYSTEM
310
DOOR LOCKS
313
ENGINE
311
100
KILL SWITCH
325
312
SLOT
314
BIOMETRIC IDENTIFIER
324
CARD READER MICROPROCESSOR
316
TRANSCEIVER
318
MEMORY
326
ENABLING CIRCUIT
320
PORT
328
POWER SUPPLY
322

FIG. 3

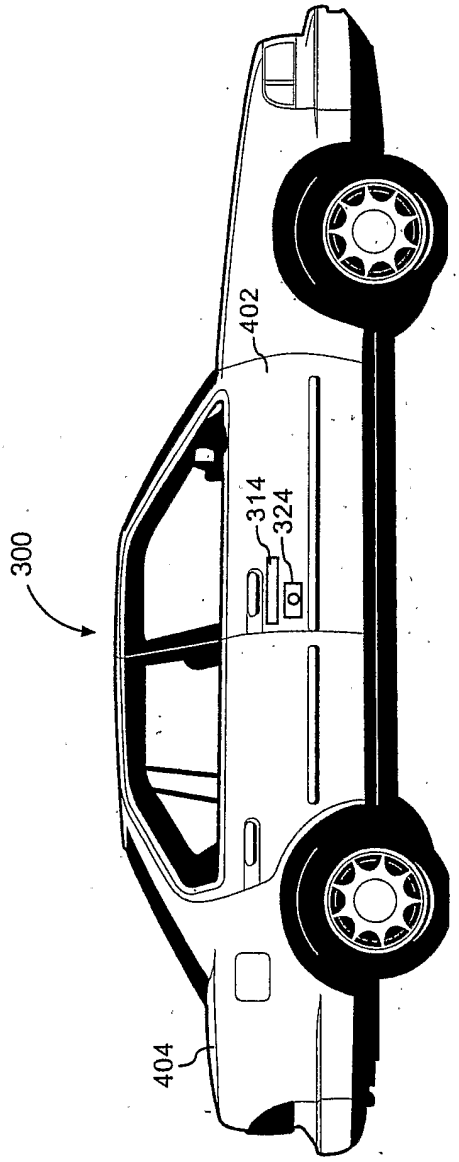


FIG. 4

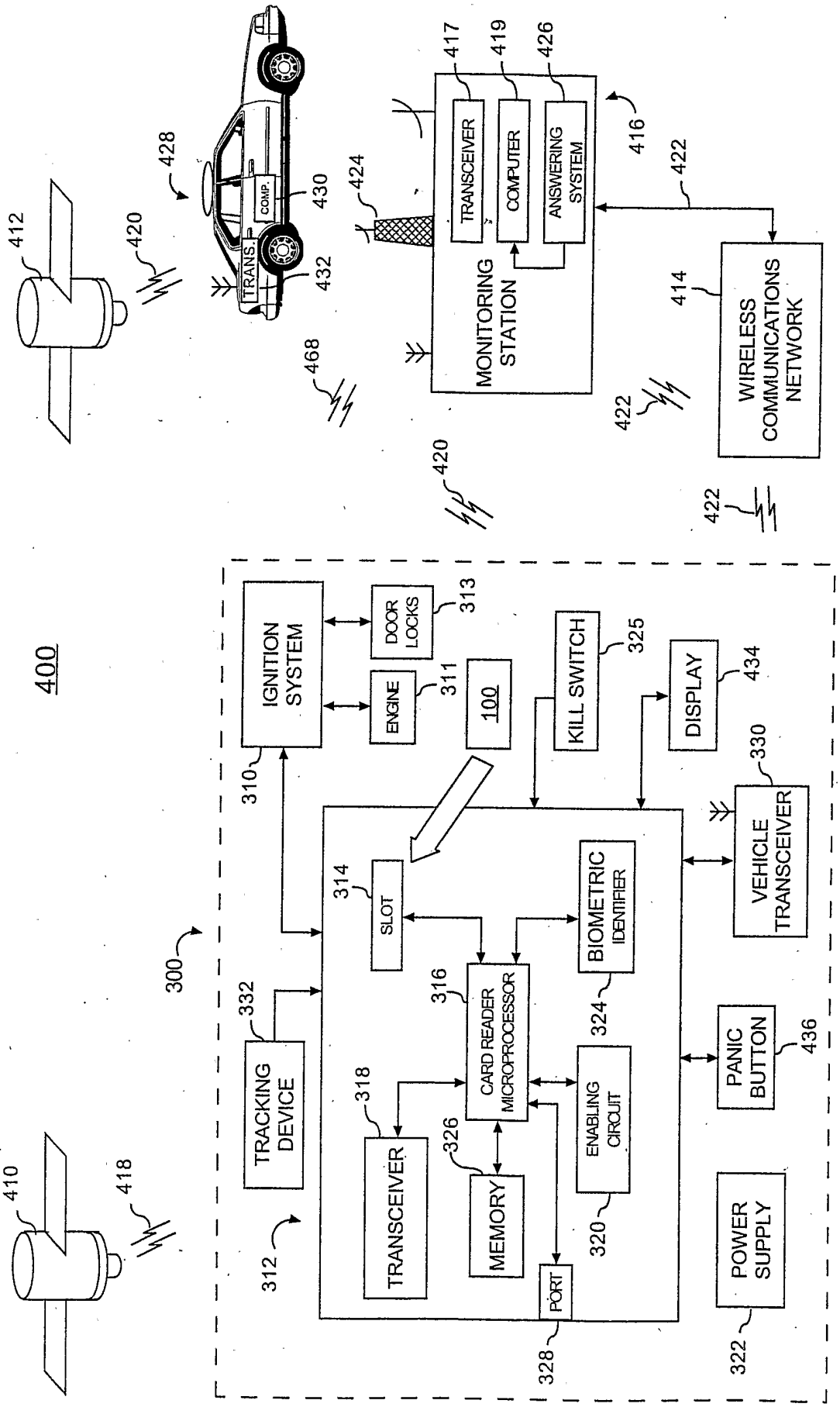

400
300
IGNITION SYSTEM
310
DOOR LOCKS
313
ENGINE
311
100
KILL SWITCH
325
DISPLAY
434
VEHICLE TRANSCEIVER
330
SLOT
314
BIOMETRIC IDENTIFIER
CARD READER MICROPROCESSOR
316
TRACKING DEVICE
332
TRANSCEIVER
318
MEMORY
326
ENABLING CIRCUIT
324
320
PANIC BUTTON
436
POWER SUPPLY
322
PORT
328
312
410
418
412
420
428
TRANS.
COMP.
430
432
468
424
TRANSCEIVER
COMPUTER
ANSWERING SYSTEM
417
419
426
416
MONITORING STATION
422
414
WIRELESS COMMUNICATIONS NETWORK
420
422

FIG. 5

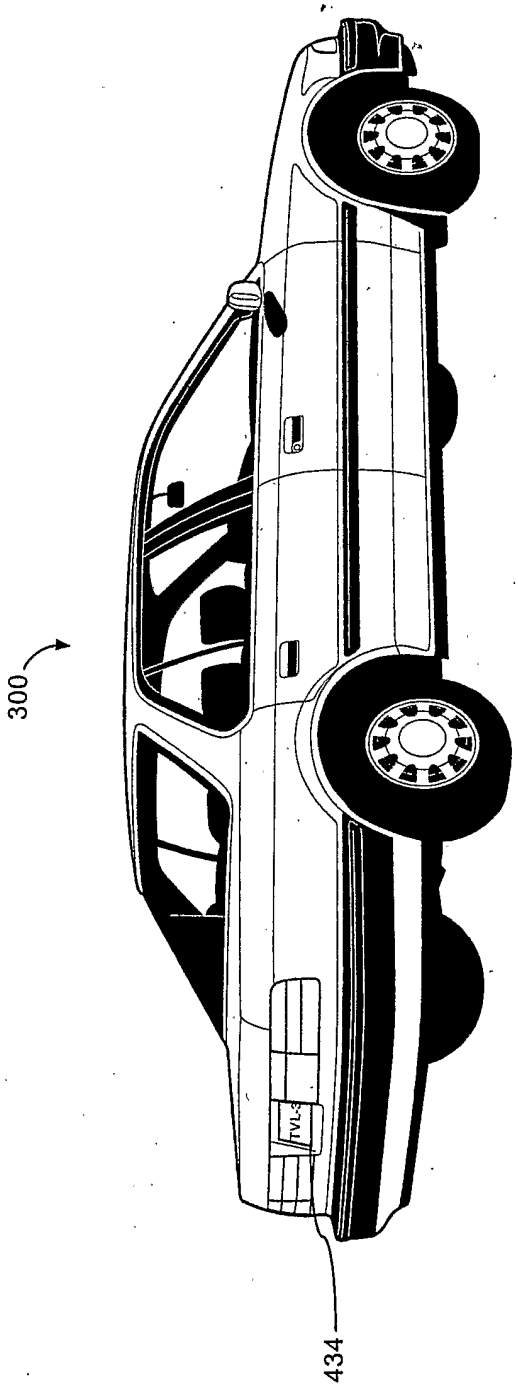


FIG. 6

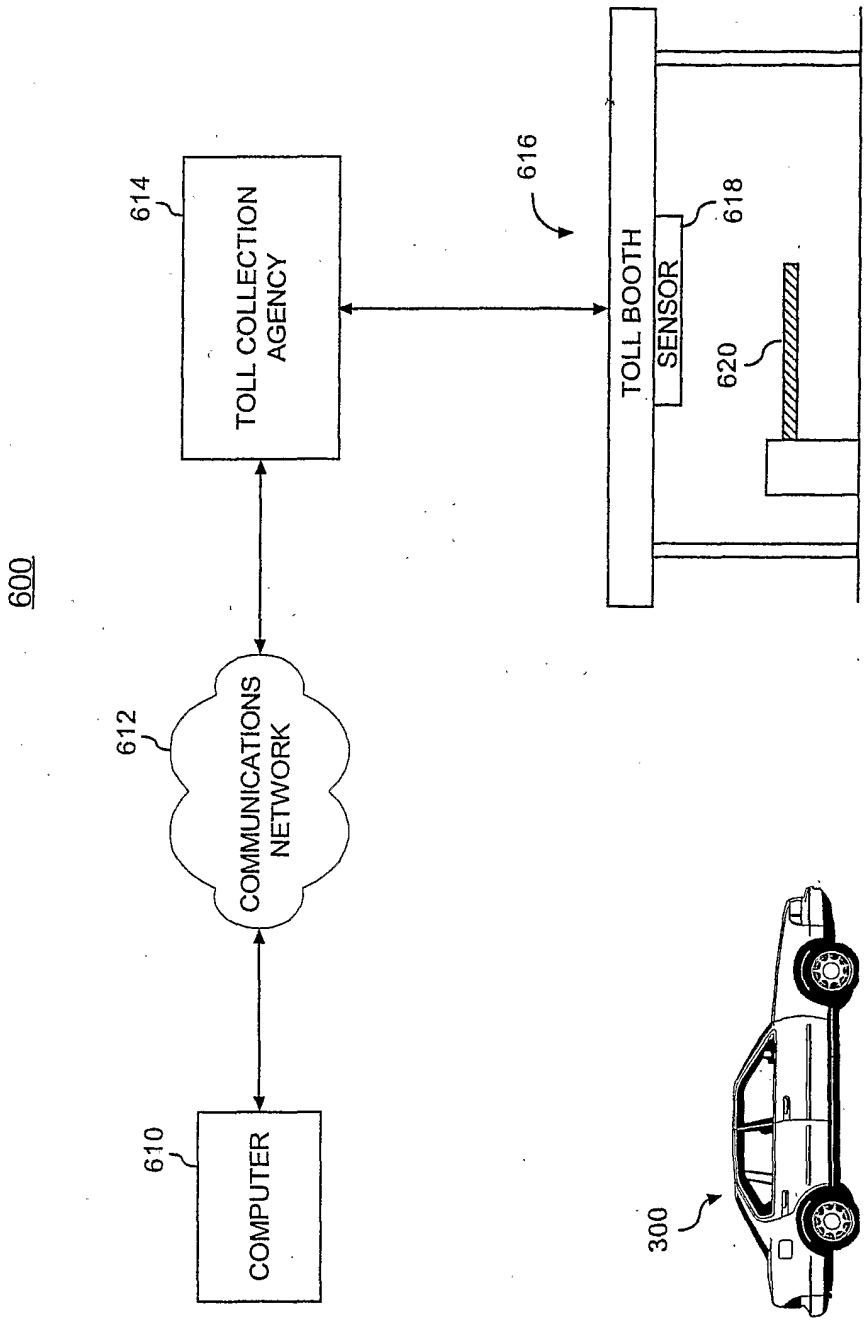

600
614
TOLL COLLECTION AGENCY
616
618
TOLL BOOTH
SENSOR
620
612
COMMUNICATIONS NETWORK
610
COMPUTER
300

FIG. 7