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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 May 2008 (02.05.2008)

PCT

(10) International Publication Number
WO 2008/050136 A1

(51) International Patent Classification:
B60R 25/00 (2006.01)

(21) International Application Number:
PCT/GB2007/004085

(22) International Filing Date: 26 October 2007 (26.10.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0621340.9 26 October 2006 (26.10.2006) GB

(71) Applicant *(for all designated States except US)*: **AUTO-TXT LIMITED** [GB/GB]; Unit 33, Bilton Industrial Estate, Humber Avenue, Coventry CV3 1JL (GB).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **COLE, Stephen** [GB/GB]; Oak Tree View, Kinwarton, Alcester B49 6HB (GB). **COLE, Christopher** [GB/GB]; Millstream House, The Green, Cumbria LA18 5HL (GB). **SZCZYGIEL, Michael** [GB/GB]; Rosedale House, Rosedale Road, Richmond, Surrey TW9 2SZ (GB). **HALSTEAD, Andrew** [GB/GB]; Woodview, Mole Road, Sindlesham RG41 5DB (GB).

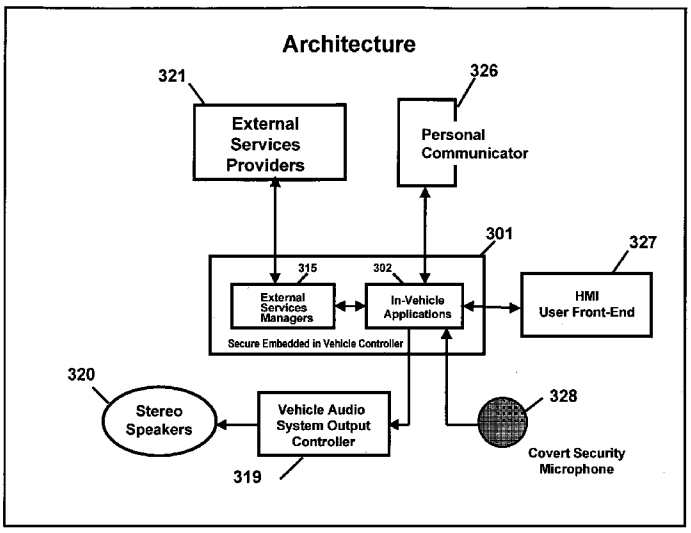
(74) Agent: **BUTLER, Michael, John**; Frank B. Dehn & Co., St Bride's House, 10 Salisbury Square, London EC4Y 8JD (GB).

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

(54) Title: IN-VEHICLE APPARATUS



(57) Abstract: An in- vehicle system (301), adapted to store information concerning vehicle usage, to store vehicle options for a driver of the vehicle, to transmit data to a remote location (321) and to receive data from the remote location (321) for provision to the driver of the vehicle. The system also being adapted to store permissions associated with an authorised driver of the vehicle, such permissions relating to the security of information that is transmitted from the vehicle by the system or received in the vehicle by the system. The system recognises a person as an authorised driver of a vehicle by interfacing with a mobile phone or other communications device of that person. If the vehicle is driven by a person who is not recognised as an authorised driver of the vehicle, the system transmits data to the remote location warning of a suspected unauthorised driver of the vehicle, and prevents access by the suspected unauthorised driver to secure information stored by the system or received from the remote location.

WO 2008/050136 A1

In-Vehicle Apparatus

The present invention relates to a method and apparatus for providing information to the driver of a vehicle. The invention relates principally but not exclusively to an apparatus for providing information to the driver of a motor vehicle such as an automobile or the like.

Information is provided to motor vehicle drivers from a variety of sources and in a variety of different ways. The most basic and conventional information provided to the driver relates to instantaneous vehicle information such as road speed, engine temperature, oil temperature and so forth. This information is presented on a dashboard display. Advances in automotive technology have expanded the basic information available to drivers to include more detailed vehicle information such as tyre pressures, cabin temperatures and also external temperatures, conditions and the like.

Location information is also now commonly available in cars in the form of satellite navigation systems which provide the driver with the coordinates of the car, directions to a chosen destination and points of interest and the like.

In addition to vehicle related information, other information and data services are also available to drivers and passengers alike. For example, many cars are now provided with built-in telephony systems allowing drivers to use mobile telephones 'hands-free' in accordance with laws prohibiting the use of telephones whilst driving. Modern communication methods also mean internet services and television can also now be provided to drivers and passengers in moving vehicles.

It will be recognised that the modern motor vehicle has now developed to the extent that the driver and passengers have access to a wide range of information and services in the vehicle which provide significant advantages for driver comfort and

enjoyment. The information available to drivers does however cause significant problems.

For example, the information provided to a driver is commonly presented in a number of different ways and from various interfaces. This can increase the time the driver needs to locate and assimilate particular information and this thereby results in an increase in the time during which the driver is not concentrating on the road.

Despite the benefits of the range of information available to drivers, the volume of information available can in fact be dangerous and can distract the driver from the fundamental task of safely operating the vehicle.

This particular problem has been recognised in the industry and systems have been developed such as the Integrated Driver Information System (IDIS) by Volvo in an attempt to solve the problem. The IDIS system assesses driver workload via data coming from the various electronic systems of the car and suppresses non-essential communications with the driver during periods of high workload, most notably incoming mobile phone calls. For example, the system may determine that it is raining using data received from the windscreen wiper sensors and that the vehicle is in an overtaking manoeuvre from data received from the road speed indicator and turn indicator. In the event that a mobile phone call is incoming, or an instructions from the Sat-Nav system is about to be issued, this would then be suppressed until this manoeuvre was complete and the driver was again in a safe condition to receive the information.

Although systems such as IDIS do improve driver safety they fail to address all of the problems associated with in-car information systems and, furthermore, fail to account for any variations in driver needs. Furthermore, the existing systems fail to offer secure control of the information received by the driver and/or information which the driver may communicate from the vehicle to other parties.

There is therefore a need for a system which overcomes the problems associated with the prior art and which is arranged to provide the driver with information safely, securely and in accordance with the driver's particular requirements.

Viewed from one aspect, the invention provides an in-vehicle system for use in a vehicle, the system being adapted to store information concerning vehicle usage, to store vehicle options for a driver of the vehicle, to transmit data to a remote location and to receive data from the remote location for provision to the driver of the vehicle, the system also being adapted to store permissions associated with an authorised driver of the vehicle, such permissions relating to the security of information that is transmitted from the vehicle by the system or received in the vehicle by the system, wherein the system is adapted to recognise a person as an authorised driver of a vehicle by interfacing with a mobile communications device of that person, and wherein if the vehicle is driven by a person who is not recognised as an authorised driver of the vehicle, the system is adapted to transmit data to the remote location warning of a suspected unauthorised driver of the vehicle, and to prevent access by the suspected unauthorised driver to secure information stored by the system or received from the remote location.

Preferably the system is adapted to transmit data using a secure data protocol and to receive data using a secure data protocol. Preferably, there is a provided a data synchronisation module that provides secure synchronisation of data stored by the system in the vehicle, with data stored on a database at the remote location. Preferably the system uses a security key that controls the permissions that have been set and are associated with the driver's details, the vehicle details, the identity of a system unit in the vehicle, and the driver's mobile communications device. Preferably, a security encryption algorithm is determined using a combination of in-vehicle system hardware, an identifier for a system unit in the vehicle, and host system identification.

The invention also extends to a system as set out above, installed in a vehicle, and to a method of use of such a system.

Viewed from another aspect there is provided a method of presenting information to the driver of a vehicle comprising the steps of determining the identify of a driver, retrieving data related to the identified driver indicating one or more driver specific parameters and displaying information to the driver in accordance with at least one of said parameters.

Viewed from another aspect there is provided an apparatus for use in a vehicle comprising a presentation unit arranged to present information to a driver and to receive an indication of the identity of a driver and data related to the identified driver indicating one or more driver specific parameters, e.g. Driver address Data Base, music file, seat position etc. wherein in use the presentation unit presents information to the driver in accordance with at least one of the driver specific parameters.

In accordance with an invention disclosed herein information can be presented in the vehicle based on parameters associated with and defined by the identified driver. The parameters can be pre-defined e.g. priority of events. by the driver and may relate to any aspect of information presented in the vehicle including the content of the information and/or the way in which the information is displayed or presented. The information content may for example include confidential or sensitive driver related information. e.g. unusual points of interest.

The presentation unit in effect provides a human machine interface (HMI) for use in a vehicle through which the driver can receive and control the information available in the vehicle according to personalised preferences and linked to the driver's identity. The presentation unit may be arranged to receive any relevant information the driver may need or request. For example, the presentation unit may be provided with satellite navigation capabilities and may be arranged to provide location and directional information to the driver. Additionally, the unit may be arranged to provide traffic information, audio entertainment information (music/radio), visual entertainment information (television), internet access, driver training or

instructional information, warning or advisory information (speed limits, speed camera and so forth) or other information.

The device may also be configured to receive information from the vehicle itself such as road speed, engine temperature or other information which the driver would normally receive from the dashboard. This may be received by, for example, a suitable interface with the vehicle electronics. This information may be processed by a suitable data processing means within or associated the unit to provide the driver with additional information such as indications of poor or dangerous driving style for example. This information may additionally be stored by the unit either locally or remotely for post journey analysis. Thus, the unit may be used for the provision of driver training wherein the information received and displayed by the unit may provide advice or driving tips to the driver.

The driver parameters may be determined in any suitable way. For example, the driver may pre-configure the way in which information is to be presented and may then 'save' these settings for future use. Data related to the selected parameters can then be stored and subsequently retrieved when the driver uses the vehicle. Where a plurality of drivers operate a particular vehicle, relevant data relating to the present driver can be retrieved and applied.

Alternatively, or additionally, the driver may select a particular pre-defined group of parameters to apply. For example the driver may select a group relating to suitable parameters for drivers with poor hearing or colour blindness. The presentation unit may then present information to the driver in accordance with parameters suitable for that group of drivers.

The data indicating the driver specific parameters may be stored or saved locally within the vehicle or within the presentation unit using a suitable data storage means or device. The data may alternatively be stored on a removable device such as a memory stick, disc or other mobile data storage device which the driver can conveniently carry. Data could for example be stored in the memory of a personal

digital assistant (PDA) or mobile telephone which the driver may carry. Data may then be retrieved using a suitable wireless or wired connection.

The presentation unit may be provided with a suitable internal data storage device containing data relating to particular authorised drivers of the vehicle. The driver can be identified and the relevant data retrieved from the device and then used to present the information in accordance with the driver's 'profile'. Alternatively, the data may be retrieved from a data storage device remote from the vehicle. This may be retrieved by any suitable means of communication with a central processing/data centre or the like where details relating to one or more driver are stored.

The presentation unit may be any suitable unit arranged to communicate information to the driver. Preferably, the unit comprises a visual display means, an audio output means, a user interface and suitable associated control apparatus. As stated above, the unit may also comprise a data storage device, data processing means and interface for communication with a central processing/data centre and/or mobile telephone or PDA.

The unit itself may be stand-alone or may alternatively be integrated into the vehicle dashboard.

Alternatively, the components may be wholly or partially distributed throughout the vehicle. For example, the display means may be located on or near the dashboard in front of the driver with the control apparatus being located in another part of the vehicle. This advantageously reduces the space consumed by the device within the vehicle cabin. In such a distributed arrangement the display device, audio output means and user interface may be separate devices arranged to communicate with the control apparatus using a suitable wired or wireless connection or connections.

The display means may be any suitable device capable of being employed in a vehicle. The display may for example be a liquid crystal display (LCD) or the like. Alternatively the display means may be a projector arranged to project information

on to the inside of the windscreen in an 'head up display' type arrangement.

The audio output device may be any suitable audio transducer arranged to communicate audio information to the driver. Alternatively, or additionally, the unit may be configured so as to utilise the in-car audio equipment to provide audio information to the driver.

The unit is also preferably arranged to communicate with a driver's mobile telephone or PDA. Communication with the mobile phone or PDA may be for telephony services, data retrieval or for identifying the driver. The unit may be arranged to communicate with a mobile telephone or PDA by hard wired connection or by wireless protocol such as Bluetooth or the like. Preferably the unit is arranged to control the mobile phone so as to allow the driver to operate the phone via the presentation unit. Alternatively, or additionally, the unit may be provided with a suitable interface for receiving a mobile phone SIM card and may in such and arrangement itself be provided with mobile phone functionality. Thus, the driver is able to make and receive telephone calls and/or make use of other phone related services via the presentation unit. The unit preferably configured to allow the driver to access phone stored information such as a telephone directory, calendar and so forth.

The unit may additionally be provided with a suitable microphone or interface to allow voice control (using suitable software) and the use of telephony services via the presentation unit. Thus, the driver can make and receive calls via the presentation unit and may also control the unit using voice commands.

The driver may control the presentation unit using any suitable interface conveniently located within the vehicle for the driver to use. The interface may for example be in the form of a touch screen visual display means, keypad or other tactile interface. The interface may alternatively or additionally use voice control. The interface is preferably arranged to allow the driver to control the functionality of the presentation unit in use but may additionally be used to identify the driver. For

example, the driver may be identified by entering a numerical code or PIN number into the interface.

The use of a numerical code or the like provides a basic means to identify the driver. However, from a security and convenience perspective this has significant drawbacks since the driver is required to remember his or her identity code and must manually enter the code before the presentation unit can be activated and before the driver can access their information.

As discussed above, the content of information available to an identified driver may include confidential or sensitive information i.e. information which is only intended for the identified driver. This may include access to on-line information, insurance information or information relating to law enforcement. As an example, a driver may have a speeding conviction and may be required by law to adhere to particular speed limits. The presentation unit may be arranged, by means of the driver's parameters, to display the driver's speed and any local speed limit. In this example the unit may further be arranged to record data relating to the driver's speed for post journey analysis by the driver or by law enforcers. It will therefore be appreciated that in these and other instances it is essential that the driver of the vehicle is securely recognised and identified.

Preferably, the driver is identified passively by means of a device associated with the driver and more preferably by means of a device which the driver normally carries. This advantageously provides a means to securely identify the driver since the driver must be identified by having a particular device in their possession whilst in the vehicle.

To overcome the problems identified with using a personal identity code (PIN) or the like, the device used to identify the driver is preferably an integral part of the driver's day to day lifestyle. Preferably, the driver is identified by communication between the presentation unit and the driver's mobile telephone or personal digital assistant (PDA). These devices are referred to hereinafter as 'Personal

Communicators' or driver identifiers. The Personal Communicators or driver identifiers may be any item that can be embedded with suitable electronics which can be used for determining the driver's identity. These may for example include personal accessories such as time pieces and grooming aids, electronic notepads, headgear visors, the frames of eye glasses, fashion accessories, articles of clothing, keys and key rings/attachments or even surgical implants. These items may be tagged with radio frequency identifiers (RFIDs) which may be read by the presentation unit to securely identify the driver. Thus, the driver can be automatically and passively recognised without the need for a PIN code or other manual identification means.

The presentation unit may be configured to operate in the absence of a confirmed driver identity with limited functionality. In such a situation the unit would not apply a driver's predetermined parameters or allow access to any information content identified to the unit as confidential or sensitive to an authorised driver.

In an arrangement where a PDA or mobile telephone is used to identify the driver, the presentation unit and the device may be paired, for example by Bluetooth, such that the presentation unit is only activated when in communication with the device or when communication between the devices has identified the driver. This provides a further level of security to the unit and prevents unauthorised access to the driver's parameters and information content which should only be available to a securely identified driver.

Viewed from another aspect there is provided an in-car apparatus comprising a visual display unit, a user interface and an associated control unit, the control unit being arranged to receive an indication of the identity of a driver by means of a driver identifier and to receive data indicating the information and/or services for which the driver is authorised to receive and/or use; the apparatus further being provided with access to information and/or services, wherein the unit is arranged in use to permit or deny access to information and/or services based on the driver's identity.

The term information and/or services is not intended to be limited to information or services which may be received by the vehicle but may also extend to telephony services or other services with which the driver may communicate with external parties. Thus, the in-car apparatus manages communication to and from the vehicle as well as the information and services which are made available to the identified driver.

Viewed from another aspect an invention disclosed herein provides an apparatus for controlling communication both to and from a vehicle. Thus, viewed from yet another aspect there is provided a communication device for use in a motor vehicle comprising (a) a communication interface arranged to transmit and receive information and/or services to and/or from one or more external source(s); (b) a user interface arranged to communicate information and/or services to and/or from a user; and (c) means to determine a user's (e.g. driver's) identity and information and/or services said user is authorised to access; wherein the device is arranged to permit access to the information and/or services in accordance with the information and/or services the user is authorised to access or use.

Viewed from a still further aspect of an invention disclosed herein there is provided an in-car system for selectively displaying information to a driver from a plurality of sources, the system comprising a display apparatus including a display unit and a control module and a plurality of information sources which can be displayed on the display unit by means of the control module, there being stored data indicating which information sources can be displayed to particular drivers; and the system further comprising means to identify a driver and wherein in use the system communicates information to the driver in accordance with the stored data indicating which information sources can be displayed to the identified driver.

The presentation unit or apparatus may also be arranged to monitor vehicle operations and/or geographical locations and store data indicating journeys travelled and data relating to the journey. The unit may also be arranged to compare the

monitored or recorded data against pre-determined driver parameters and to issue control or warning indications if the monitored or recorded data does not match, or falls outside, of on or more pre-determined driver parameters. For example, the driver parameters may comprise data indicating accepted routes or times/dates of travel. The unit may receive this information, after driver recognition, and compare this against a current or recent journey. If the journey falls outside of the parameters the driver or remote control centre may be alerted. This could for example indicate a stolen vehicle or an unauthorised journey. The presentation unit can therefore act as a security system which can be configured to monitor the vehicle.

In another instance the owner of a vehicle may become aware that a vehicle has been stolen and may alert a control centre or the police. The control centre may then in turn communicate with the presentation unit causing the unit to monitor the journey and/or communicate data relating to the journey back to the control centre or directly to the police. In such an arrangement the unit would be provided with means to communicate with the control centre and with means to receive control signals to enter a 'stealth mode'. In effect the vehicle enters a mode in which the journey is tracked without the unauthorised driver being advised.

The unit may additionally or alternatively automatically determine that a vehicle has been stolen by means of a break or discontinuity in contact with the vehicle. The unit and vehicle may be provided with means to indicate if the unit has been removed from the vehicle, such as for example by tagging the car with an RFID tag or the like. In the event that the unit and tag are no longer in communication the unit may be configured to issue a warning indicator to a control centre or other party indicating that it is no longer located in a vehicle. This can therefore deter a thief from stealing the unit itself and/or the vehicle.

The driver defined parameters may also extend to historical data relating to the way in which the particular driver operates the car. This data may be provided by the driver, such as a maximum road speed, or it may be determined by the unit itself by recording and storing data for an identified driver over a period of time such as

braking, acceleration, steering wheel movement etc.. The data can then be compared by the unit against the relevant instantaneous journey information using a suitable data processor. The comparison can then be used to determine if the vehicle has been stolen or is being operated outside of the pre-defined parameters. As stated above, the parameters may be defined by the driver or may be defined in accordance with a court order or insurance company request. Thus, the unit can monitor breaches of the parameters relating to the identified driver and may communicate these breaches to third parties.

Viewed from another aspect there is provided a method of monitoring a vehicle comprising the steps of (a) receiving an indication of the identity of the driver of a vehicle; (b) receiving data relating to the identified driver; (c) receiving vehicle operating data over the course of one or more journey(s); and (d) comparing the vehicle operating data and driver data.

The data may be compared in real time or may be compared or processed as part of a post journey analysis. The driver data may include information relating to normal journeys or normal driving style for example and may then be compared with received vehicle operating data. The comparison can be used to determine for example if the vehicle is being operated by an unauthorised driver (which could be a theft or just a case of an innocent oversight by a family member or domestic servant.

It will be recognised that features of the aspects, embodiments and examples of inventions disclosed herein can be used in isolation or in any suitable and convenient combination. The novel and inventive features of the inventions described herein can be conveniently applied to a range of in-car or in-vehicle devices and, thus aspects of inventions disclosed herein extend to a driver training apparatus, a vehicle tracking apparatus and an in-car satellite navigation system.

Aspects of inventions disclosed herein allow for the integration of a plurality of separate in-car systems into a single device. The integration allows for the convenient management of driver information services, driver communication

services and vehicle security services through a common portal. Furthermore, the invention allows the driver's identity to act as the secure means to activate individual driver profiles that define how and when information is to be presented to the driver to enable communication and navigation..

Viewed from one general aspect, the invention can be considered as providing the delivery of personalised content to the driver through an HMI (Human Machine Interface) where content is initially gathered from a range of predetermined sources both on-board and off-board the vehicle. The customisation of the content is determined by Automatic Driver Recognition based on what the driver has subscribed to or has access to. After this content is identified and accessed it is assembled and composed for delivery through a single HMI to the driver. Viewed from this aspect, the invention adds value to content through this process of customisation.

It will further be recognised that aspects of inventions extend to methods of operating the various aspects described herein.

A preferred embodiment of the invention is designed to provide the owner/driver of an automobile an information system which allows him/her to set permissions relating to the security of information that is private and confidential to them (private or business), that is of use to them while they are using their automobile and also that that is generated by the use of their automobile.

The system of the preferred embodiment will also allow the owner/driver to configure permissions related to what will be transmitted to the automobile from a central database and how information generated by the automotive is presented back to the off board systems. The configuration of information and permissions is carried out via a secure internet service that is personal to the driver/owner of the vehicle, and covers the following areas of information.

Personal contact information for navigation and communication while in the vehicle

Journey data, including mileage, speed, trip log, locations travelled to whilst the vehicle is in use

Point of interest data for business usage and also private usage while in the vehicle

Alert data including security events, vehicle movement without permission, speeding and so forth.

In the preferred embodiment, the key to unlock this information being presented to the driver inside the vehicle, and also what is allowed to be sent from the vehicle to off board systems, is the owner/driver's mobile phone. If the phone is not present the vehicle can be set up to transmit unauthorized usage data, whereas if the phone is present, the data can be set accordingly.

Key technical features that have been developed which make the preferred embodiment viable in implementation terms include:

A secure data protocol - a proprietary protocol that secures information between the secure web database and the vehicle module and database. This is designed to operate over multiple network systems, including GSM, GPRS and Wifi. A security encryption algorithm is determined using a combination of the vehicle hardware of the system unit installed in the vehicle, the unit identification and the host system identification. This security is designed to protect against unauthorized data copy, replay and manipulation.

Automated data synchronization - a proprietary distributed software application that secures the synchronization of data between the vehicle database and the web database. This covers download data and upload data. This is based on a security key that controls the permissions that have been set and are associated with the driver's details, the vehicle details, the vehicle

module and the driver's mobile phone. The application ensures that all these resources are synchronized to the latest event (normally a vehicle movement or journey) and that the data is being communicated in conformance with the driver's permission levels.

Automated driver authentication - this is a proprietary application that controls the release of secure data (to the in vehicle touch screen as well as off board database) to a driver of a vehicle dependent on the identity of their mobile phone, or other mobile communications device.

Embodiments of aspects of the invention will now be described by way of example only, and with reference to the accompanying Figures in which :

Figure 1 shows two levels of vehicle security encompassed by the invention, (1) Stolen Vehicle Tracking and Recovery based on UK ABI (Association of British Insurers) Category 5 or equivalent standards; and (2) Stealth Security add-ons to enhance the coverage of the insurance industry standard Category 5 or equivalent;

Figure 2 shows two types of Stealth Security (1) where the vehicle is reported as stolen and tracking is initiated (unbeknown to the thief); and (2) Suspicious Journey detection by the in-car security system which alerts Tripwire function to generate an urgent message to the driver's HMI Front End. The driver's response determines whether the Tripwire stands down or alerts the Security Services Provider;

Figure 3 shows the architecture of invention indicating the key components and their interrelationship;

Figure 4 shows a schematic of the vehicle security system whilst in the vehicle is in the Parked/In-Service State;

Figure 5 shows a schematic of the in-vehicle system when the vehicle is in the

Vehicle Ready to Use State;

Figure 6 shows a schematics of the Driver Applications system components in the Vehicle in Use State;

Figure 7 shows the components involved in the Stealth Security, Vehicle Theft Reported scenario; and

Figure 8 shows the components involved in the Stealth Security, Suspicious Journey Detected scenario.

The main components of a preferred embodiment of the invention are described as follows. The figures are described in detail subsequently.

The main components of the preferred embodiment are :

(1) a Secure Embedded in-Vehicle Controller (SEiVC) that manages systems functions related to applications and communications contained within the scope of this invention,;

(2) External Services Managers within the SEiVC controlling communications between in-vehicle applications and external service providers;

(3) A Vehicle Driver Applications Manager controlling voice communications and information (data related) applications;

(4) A Vehicle Security Applications Manager controlling in-vehicle aspects of security;

(5) A Human Machine Interface (HMI), a user front-end for visual information presentation to the vehicle driver and touch screen input;

(6) Personal Communicator used by the driver for voice communications and driver identification to the Vehicle Security Applications Manager (VSAM);

(7) Audio Output Controller providing audio output capability through a vehicle's audio system speakers; and

(8) Covert Security Microphone for eavesdropping on post-theft in-vehicle conversations.

The HMI User Front End consists of a simple output medium with limited input capability that is driven by a remote HMI controller managed by the SEiVC. Thus, from a hardware standpoint, the HMI architecture consists of (a) an HMI user front end located at the selected point of installation. This is point of interaction for the user (Driver) and thus is intended to reside in a location that is highly accessible; and (b) a remote HMI controller positioned out of sight of the driver. The HMI controller may be physically within the SEiVC, or physically separate. Interfacing components reside at both HMI User Front-End and controller ends for wireless or by-wire data transfer.

In use the Driver Applications Manager launches the HMI Front End via the HMI Controller. Through touch screen inputs on the HMI Front End the driver can activate specific applications. Outputs generated by these applications are streamed back to the HMI Front End via the HMI Controller. The Applications supported by the applications manager include the personalised driver data information services, personalised driver voice communication services and also vehicle security.

These applications are described in more detail as follows :

Personalised driver data information services : Data information services will include, amongst others a 'points of interest' database. Upon recognition of the driver's identify the points of interest for that driver will be loaded into working

memory. For example, a disabled driver would be interested in facilities for the disabled along his/her planned route or in the immediate vicinity of the current vehicle location. Another driver may be most interested in parking facilities. Such preferences for each driver are loaded into memory according to recognised driver identity.

Personalised driver communication : The preferred embodiment of the invention enabled hands free calling functionality incorporating an external microphone and vehicle speakers allowing the driver to (1) make calls and answer calls (2) Store/view/delete contacts in a globally available database, (3) specify preferences for how the contact list is to be presented (4) access and display each unique list of driver contacts according to recognised driver identity

Vehicle Security : When the vehicle is not in use (i.e. ignition off) and in a parked condition, the Vehicle Security Applications Manager (VSAM) is in a SET Mode (described in more detail below). After recognition of an authorised Personal Communicator, the VSAM UNSETS when the ignition is turned on.

In use, the system is activated as follows. Upon the VSAM switching to the UNSET mode the Driver Applications Manager (for launching specific information and communications services) is activated/booted in system memory of the SEiVC. After system boot-up, the Driver Application Manager presents the user (i.e. vehicle driver) with a menu to launch individual applications including but not limited to (1) personalised driver information services (2) personalised driver communications services (3) integrated data management facilities supporting (1) and (2).

Once activated the Driver Application Manager allows the driver to access personal data from the data storage unit in the device and/or data from the personal communicator. This data is held in databases with the respective devices which are unique to the individual driver profiles. Multi-driver profiling extends across the system to enable multiple individual driver profiles (i.e. driver 1, driver 2 etc.) to be created.

The system not only extend to secure access to information but also provides improved security for the vehicle itself. Specifically the preferred embodiment of the invention addresses two vehicle theft scenarios :

(1) the theft of the vehicle through acquisition of the means to start the vehicle; and

(2) the theft of the means of both starting the vehicle and identifying the authorised driver.

In Scenario 1, the In-vehicle Security System uses the detection of unauthorised movements of the vehicle to alert an external security services provider track the movements of the vehicle and initiate procedures to confirm the identify of the driver.

For modern vehicles the means to start the vehicle is almost always a set of keys. When the vehicle is in a parked condition the VSAM is in a SET mode. Without recognising an authorised Personal Communicator the VSAM will not UNSET even though the car may be driven. The movement of the car in SET mode after a few seconds will trigger an audio reminder to the driver to turn on their Personal Communicator. If the vehicle continues with the VSAM in the SET mode beyond a defined perimeter commonly known as a geo fence the VSAM alerts the external Security Services Provider to initiate procedures to track the vehicle and contract its owner. The VSAM will only switch from the SET to the UNSET mode when the presence of an authorised Personal Communicator is detected. Once the VSAM is UNSET the Driver Applications Manager is automatically launched and updates to the Contacts Database and Driver profiles are downloaded from the Personal Communicator. In order meet UK police requirements systems designed to deter key targeted theft the VSAM must comply with the Association of British Insurers Category 5 standard for Stolen Vehicle Tracking and Recovery. This invention fully integrates the Category 5 compliant VSAM. See Table 1.

TABLE 1

Category 5 Standard Key Theft	Driver	Vehicle				SSP	Police
	Personal Device	ADR	GPS	Stealth Security			
			Geofencing	Tripwire	HMI		
Authorised Driver Recognition	Not Present	Not OK					
Unauthorised Vehicle Movement			Detected				
Suspicious Journey							
Vehicle Owner Reports Theft							
Vehicle Tracking						Activated	
Contact Owner -Theft Confirmed						Informed	Alerted
Vehicle Immobilisation						Executed	Authorised
Vehicle Recovery							Executed

In scenario 2, there are two further distinctions: (a) the owner of the vehicle reports the theft to the police and security services provider, (b) a journey analyser detects a suspicious journey and requests the driver to respond to an urgent message thereby establishing whether the vehicle is being operated by an authorised driver.

In scenario (b) the driver's personal communicator (or other identifier) may have been stolen. Thus, when the thief enters the vehicle the system identifies what it considers to be an authorised driver and UNSETS the VSAM. Once UNSET, the personalised driver information and communications applications are available for use by the thief (posing as the authorised driver) as well as the actual authorised driver(s) of the vehicle. As far as the VSAM is concerned everything is OK. To address this problem the preferred embodiment of the invention incorporates a Stealth Security Function for dealing with two situations (a) Owner Reports Vehicle Stolen (b) Suspicious Journey Detected.

In cases where the owner reports that a vehicle has been stolen the external security systems provider remotely activates tracking whilst allowing seemingly 'normal' functionality to the driver (i.e. the thief). Unknown to the thief the vehicle is being tracked by the external security systems provider with a view to initiating vehicle recovery procedures. During the time the vehicle is being driven in this state the

personalised information and communication services are available to the thief creating the impression that everything is OK. See Table 2

TABLE 2

Stealth Security 1 - Key & Personal Communicator Theft - Owner Reported	Driver	Vehicle				SSP	Police
	Personal Device	ADR	GPS	Stealth Security			
			Geofencing	Tripwire	HMI		
Authorised Driver Recognition	Present	OK					
Unauthorised Vehicle Movement			OK				
Suspicious Journey							
Vehicle Owner Reports Theft						Informed	Alerted
Vehicle Tracking / Covert Microphone					Normal	Activated	Informed
Vehicle Immobilisation						Executed	Authorised
Vehicle Recovery							Executed

Where both the means of starting the vehicle and identifying the authorised driver have been illegally acquired the vehicle is likely to be driven some distance to an area never visited by the authorised driver. Several hours may elapse before the owner is aware that the vehicle has been stolen. During this period the Journey Analyser function identifies instances of journeys that are out of character to the statistically determined profile of journeys taken by authorised drivers over an extended period of time (typically measured in months). This is augmented by "geo Red Flag" areas specified by the owner. For example the owner could specify that the vehicle never leaves the UK except in the month of August, or would never be driving in London docklands. The profile of actual journeys is determined by journey profiling algorithms resident in the memory of the Secure Embedded in-Vehicle Computer. Journey profiles include but are not limited to geographic attributes of journey trajectories in the national road system based on vehicle location by Ordnance Survey coordinates and/ or Post Codes, time of day and basic performance attributes such as speed, braking and de-acceleration profiles along routes taken. A Tripwire function is activated when it receives an alert from the

Journey Analyser that a suspicious out of character journey has been detected with regard to the attributes cited above. Once alerted, the Tripwire function confirms the identity of the driver by posting a short message on the HMI Front End requested the driver to enter a code known only to the authorised driver such as pin number. Another gambit might be to display an urgent message to the driver to call a designated telephone number, or to automatically initiate a call to a security officer at the external Security Service Provider (SSP). After three Tripwire requests failure of the driver to respond with the correct code or call the number automatically triggers an alert from the VSAM to the external Security Services Provider which would commence tracking the vehicle and attempt to contact the vehicle owner at other than their registered mobile phone (now assumed to be in possession of the thief). Journey Analyser and Tripwire provide security cover in the interim period from the time of the theft of the vehicle key and Personal Communicator to the time when the owner reports the theft to the police. In some cases this period could be several hours. Table 3 shows the case where the driver doesn't respond or responds incorrectly.

TABLE 3

Stealth Security 2 Suspicious Journey - Driver ID In Doubt	**Driver**	**Vehicle**				**SSP**	**Police**
	Personal Device	**ADR**	**GPS**	**Stealth Security**			
			Geofencing	**Tripwire**	**HMI**		
Authorised Driver Recognition	Present	OK					
Unauthorised Vehicle Movement			OK				
Suspicious Journey				Detected>	Request ID Not OK	Alerted	
Vehicle Tracking / Covert Microphone					Normal	Activated	Informed
Vehicle Owner Confirms Theft						Informed	Alerted
Vehicle Immobilisation						Executed	Authorised
Vehicle Recovery							Executed

Table 4 shows the case where the driver responds correctly and the Trip wire system stands down.

TABLE 4

Stealth Security 2 Suspicious Journey - Driver ID OK	Driver	Vehicle				SSP	Police
	Personal Device	ADR	GPS	Stealth Security			
			Geofencing	Tripwire	HMI		
Authorised Driver Recognition	Present	OK					
Unauthorised Vehicle Movement			OK				
Suspicious Journey				Detected> Stand Down	Request ID <OK		
Vehicle Tracking / Covert Microphone							
Vehicle Owner Confirms Theft							
Vehicle Immobilisation							
Vehicle Recovery							

Turning to the Figures, the detailed operation of an embodiment of the invention will now be described.

Table 5 sets out the nomenclature used in Figures 3 to 8 :

Domain	Component	SubComponent	Item	SubItem	Fig 3	Fig 4	Fig 5	Fig 6	Fig 7	Fig 8
	SEiVC				301	401	501	601	701	801
		InVehicle Applications			302					
		In-Vehicle Security Apps Mgr				403	503		703	803
			Auth. User			404				
			SET Mode			405				
			UNSET Mode			406	506			
			Geo Fence			407				
			Stealth Security				508			
				Confirmed Theft					709	
				Suspicious Driver						810
		Driver Services App Mgr					511	611	711	811
			Voice Comms				512	612	712	812
			Info Apps				513	613	713	
			Contacts DB				514	614	714	
			Driver Profiles				514A	614A	714A	
		External Services Mgr			315	415	515	615	715	815
			Security			416	516		716	816
			Voice Comms					617		817
			Info Services					618		818
	Audio Output Controller				319					819
	Stero Speakers				320					
Off-Board Services (Ref X02)					321					
	Comms Network Provider					422	522	622	722	822
	Secure Service Centre					423	523	623	723	823
	Information Services							624		824
Driver (Ref X03)										
	Personal Communicator				326	426	526	626	726	826
	HMI User Front End				327		527	627	727	827
	Covert Security Microphone				328				728	828

TABLE 5

In Figure 3 the Secure Embedded in Vehicle Controller (SEiVC) 301 is the device through which all external communications and information services 321 are directed to and from the vehicle. Within the SeiVC External Services Managers 315 act as secure communication gateways to handle communications between in-vehicle applications 302 and external services providers 321. In the first embodiment of this invention the SEiVC manages and integrates three applications (1) In-Vehicle Security (2) Hands Free Calling (Communications Services) (3) SATNAV (Information Services). The SEiVC acts as the portal through which the driver's mobile phone 326 is linked to the GSM wireless network services provider and navigation related information such as traffic advisories are presented to the driver's touch screen (HMI User Front End) 327. Driver information such navigation turn by turn instructions can be formatted for voice output through the vehicle audio system 319, 320. A Covert Security Microphone 328 can be remotely activated to eavesdrop on conversations in the vehicle when it is confirmed as stolen.

In-Vehicle Security – The VSAM detects two basic types of theft (1) the theft of the vehicle keys (2) the theft of the vehicle key and the device used to identify the driver. The Association of British Insurers Category 5 Standard covers the detection of vehicle theft through the theft of the vehicle key and the means for tracking and recovering a stolen vehicle:

Figure 4 shows the components of Key Theft Security Detection as the vehicle is in a parked or in-service state (1) User Authentication 404 (2) SET Mode 405, (3) UNSET Mode 406, (4) Geo-Fence Alarm 407. 'Parked' means the vehicle ignition is off and the vehicle is stationary. 'In-service' means that the vehicle can be started and driven without driver authorisation within a prescribed perimeter area defined by a radial distance. This perimeter is known as a geo-fence to vehicle security practitioners. This in-service distance allowance enables casual drivers such as valet parking attendants, service technicians or family members to drive short distances without having to possess the authorised driver's registered mobile phone. The GPS co-ordinates of the vehicle are continuously monitored by the SEiVC when the

vehicle is in a stationary parked state. When these co-ordinates change to the extent that the vehicle has crossed the geo-fence perimeter from its last known stationary position without an authorised driver's mobile phone being detected a geo-fence alarm 407 is raised. Movement can be through the act of driving the car or through the act of towing or transporting the car.

The default modality when the vehicle is parked with the ignition off is SET 405. The Secure Embedded Process Controller 401 stores the GPS position of the vehicle when parked. Whilst in the SET mode the Secure Embedded Process Controller can recognise and pair up with a registered mobile phone 426 within a physical proximity of several meters. A registered mobile phone number is related to an identified driver authorised to operate the vehicle. If a registered mobile phone 426 is detected the modality of the VSAM 403 changes to UNSET 406 signifying authentication of the driver. Any movement of the vehicle (detected by GPS co-ordinates outside of the geo-fence perimeter) whilst in the SET condition is indicative of a potential unauthorised user. This will activate a Geo-Fence Alarm 407 causing the VSAM 403 to alert the Security Services Provider (SSP) 423. The SSP will initiate vehicle tracking and attempt to contact the owner to confirm the vehicle status.

In Figure 5 the UNSET mode 506 initiates the Stealth Security mode 508. Stealth Security provides an additional level of security to cover cases where there the authorised driver's mobile phone 526 has been stolen or misappropriated. UNSET mode also initiates the Driver Applications Manager 511 which downloads new entries in the contact phone book and driver profiles stored in the mobile phone 526 and updates the contacts database 514 and driver profiles 514A. The Driver Applications Manager also activates the driver's touch screen display 527 and presents a menu for launching specific driver applications: (1) hands-free calling or (2) SATNAV. The External Vehicle Security Services Manager 516 remains enabled to handle any Stealth Security incidents that require communications with the Security Services Provider 523.

In Figure 6 the vehicle driver launches specific applications (1) hands-free calling (Voice Communications 612, (2) SatNav (Information Applications) 613 from the touch screen 627. The Contacts Database 614 and Driver Profiles 614A are available to support applications as needed when they are launched. Each application in turn initiates the required External Services Manager (Communication Gateways) 617, 618 to link the application to the required external service which always requires connection to the Wireless Network Service Provider 622. In the case of mobile phone hands- free calling it may also require communication with the Security Services Provider 623. In the case of SatNav it requires communication with the provider of traffic advisories and navigation data 624.

Making Calls – A "Make Call" icon is displayed on the touch screen display 627. Touching this icon will allow the driver to key in a phone number or make a further selection to retrieve a list of names and numbers from the contacts database 614. Once a number is keyed in or selected from the list displayed on the touch screen 627 control is passed from the Voice Communications Application 612 to the hands-free kit of the mobile phone.626 to establish the connection to Wireless Network Service Provider 622 via External Voice Communications Services Manager 617.

Receiving Calls – Calls are received from the Wireless Network Service Provider 622 by the Mobile Phone Hands Free Calling (Voice Communications) Application 612. During periods of high driver workload known to the Secure Embedded in-Vehicle controller 601 calls are not answered but the caller number and time are recorded for display to the driver when the driving workload is acceptable for making return calls. When driving workload is back to normal a list of missed calls is displayed on the touch screen 627. With each touch selection made by the driver any recorded messages are automatically retrieved and played to the driver via the mobile phone hands free kit. Associated with the display of each missed call is a touch screen soft select for making a return call. The driver also can manually invoke the holding back of received calls by making the appropriate selection on the touch screen 627. Upon unsetting this command via the touch screen a list of

missed calls is displayed and any recorded messages are automatically retrieved. The call-back procedure is as just described in 'Making Calls' above. Where there is no blocking of incoming calls when a call is received by the Mobile Phone Hands Free Calling (Voice Communications) Application 612 an incoming call icon flashes on the touch screen together with an optional audio alert via the vehicle loudspeaker system. By soft selecting an Accept Call prompt through the touch screen or voice activation device control is passed to the hands free kit of the mobile phone 626 to enable the caller to talk with the driver.

Figure 6 shows the functional components for supporting SatNav. All communications between the in-vehicle navigation system and the external SatNav information services provider are mediated by the SATNAV (Information Services) application 613.

The touch screen modalities supported by the SatNav (Information Services) Application 613 include but are not limited to: (1) Specifying the journey destination. (2) display of maps and current vehicle position on the maps, (3) navigation preferred routing and turn by turn instructions, (4) points of interest at and near the current location of the vehicle, in particular those points associated with speed (cameras and posted limits) and (5) traffic advisories. Navigation instructions, points of interest and traffic advisories can also be presented to the driver in an audio manner through the vehicle's audio speaker system.

The journey destination can be specified by the driver in two ways using the touch screen display 627 (1) entry of destination address details via the use of a soft alphanumeric key pad displayed on the touch screen (2) soft selecting from a displayed scroll list of contact names. In the latter case the address details are retrieved from the contacts database 614. In both cases the address details are transferred to the SatNav navigation preferred routing and map display functions.

Those familiar with the art will recognise that this invention integrates functionality representing advanced state of the art capabilities for vehicle navigation systems

The navigation system will provide driver comprehension features including but not limited to 3D map displays, distance to turn indicators, scrolling map , turn arrow to highlight the way ahead, intelligent re-routing for missed turns, speed camera database.

The navigation system will provide adjustable trip calculation and user profiles to avoid or favour specific road types

Points of Interest – The navigation system provides millions of points of interest such as petrol stations, car parks, cinemas and hospitals. Each driver can prioritise which points of interest are of importance and which type should be displayed as a default on journeys.

Traffic Advisories – The navigation system will support but not be limited to TMC and GPRS traffic information.

Stealth Security – Figure 1 shows the two types of vehicle theft security, Type 1(Category 5) covering vehicle key theft and Type 2 (Stealth Security) covering reported theft or theft of both the vehicle key and the mobile phone identifying an authorised driver of the vehicle. In order to be recognised by the UK police forces, systems for dealing with vehicle key theft require compliance with the Category 5 standard of the Association of British Insurers. This invention describes an added Stealth Security component to cover situation where both the vehicle key and the authorised driver's mobile phone are stolen or misappropriated. Figure 2 shows two types of Stealth Security. The first is the Stolen Vehicle Reported variant where after the reported theft of the vehicle the foreground driver information and communication service applications continue as normal with vehicle tracking running surreptitiously in the background unbeknown to the thief. The second is the Suspicious Journey Detected variant where out of the ordinary suspicious journeys are detected by a journey analyser. Once a suspicious journey is detected, control is passed to a Tripwire function that confirms the identity of the driver by prompting

the driver to reply to an urgent message. Whilst an authorised driver would have no problem in responding to such infrequent messages, a thief would not be privy to the information (such as a PIN) needed remove suspicion.

Figure 7 shows the case of an authorised driver's mobile phone 726 that is stolen along with the keys and the vehicle owner upon recognition that the vehicle was missing and presumed stolen would report the theft using another phone. In order to obtain police response the theft must be reported to the police. In addition the owner would also contact the Security Services Provider 723 that would put Stealth Security 709 into tracking mode and begin tracking of the vehicle's movements via GPS. In addition once in tracking mode Stealth Security 709 would activate the covert security microphone 728. This enables the in-car conversations of the thief with colleagues either in person or via mobile phone to be monitored by the Security Services Provider 723 and the police. This helps pinpoint the intended destination and provides valuable collateral information to enable recovery of the stolen vehicle. Driver mobile phone hand-free calling (Voice Communication) applications 712 and SatTNav (Information Applications) 713 would continue to operate as normal.

In Figure 8 an authorised driver's mobile phone 826 is stolen along with the keys. Stealth Security has a means of detecting the theft before the owner is aware of it. This allows the Security Services Provider to be alerted BEFORE receiving a call from the owner. At the time Stealth Security is activated by the UNSET mode 506 (Figure 5) the Journey Analyser 810.1 of the Suspicious Journey Detection (SJD) component 810 (Figure 8) is placed on standby. Once the journey commences the Journey Analyser identifies journey attributes that differ markedly from the authorised driver's normal profile of journeys and the driver's expressed "Red Flag" restrictions on the use of the vehicle. Where a suspicious journey is detected the Tripwire 810.2 function is alerted which issues a prompt to the driver to respond to a message displayed on the touch screen 827 or issued via the vehicle audio system 819. The Tripwire then issues a command to the Driver Services Applications Manager 811 to display an urgent message to the touch screen 827. The prompt can also be voice annunciated through the Vehicle Audio System 819. The reply to the

prompt can be the entry of code into the touch screen, or the selection of a displayed call back urgently telephone number. Alternatively the Tripwire can trigger that a call be automatically made to the Security Service Centre. Call back can be executed by simply soft selecting the telephone number displayed on the touch screen 827. Where the driver response (an entered PIN number or spoken PIN number to an operator at the SSP 823) validates the fact that the driver is the authorised driver, the Tripwire "stands down". Where the response is incorrect or there is no response after 3 requests, the Tripwire 810.2 alerts Stealth Security SJD 810 to switch to tracking mode and alert the Security Services Provider 823 to begin tracking the vehicle's movements. In addition once in tracking mode Stealth Security Suspicious Journey Detection 810 activates the Covert Security Microphone 828. This enables the in-car conversations of the thief with colleagues either in person or via mobile phone to be monitored by the Secure Services Centre and the police. This helps pinpoint the intended destination and provides valuable collateral information to enable recovery of the stolen vehicle.

The following terms and acronyms are used throughout the detailed description of the preferred embodiments of the invention :

Personal Communicator: In the first embodiment of the invention this is a mobile phone or PDA with mobile phone capabilities

HMI User Front End – In the first embodiment of the invention this refers to a widescreen display with touch screen overlay.

HMI Controller – In the first embodiment of the invention this refers to a touch screen display controller.

Communications Services Application: In the first embodiment of the invention this refers to hands free calling using short range wireless communications link.

Information Services Application: In the first embodiment of this invention this

refers to SatNav with traffic advisories and points of interest including but not limited to local speed limits in the current location of the vehicle.

Secure Embedded in Vehicle Controller – In the first embodiment of the invention this refers to [Outline Spec of Auto-txt V9 in generic terms]

Audio Interface Controller: In the first embodiment of the invention this refers to a controller for audio output to the vehicle radio speakers.

Mobile Phonebook: In the first embodiment of the invention this refers to the list of names, telephone numbers and other contact details stored in the memory of a mobile phone.

Contact Database: In the first embodiment of the invention this refers to the contact details extracted from the mobile phonebook of the authorised driver and loaded into a database resident on the Secure Embedded in Vehicle Controller

Driver Profiles – refers the individual preferences of authorised drivers as to how they want to interact with their individual driver applications. Preferences includes but is not limited to, visual audio presentation style, application features/functions/options to be enabled or suppressed and so forth.

Security Services Provider; The first embodiment of the invention this is a Secure Operating Centre as defined by the Association of British Insurers Category 5 standard for After Theft Systems for Vehicle Recovery.

Stealth Security Mode; In the first embodiment of the invention this allows seemingly 'normal' applications (SatNav and Hands Free Calling) functionality to an unauthorised driver. However in this state the vehicle can be (unknowingly to the unauthorised driver) tracked by the Secure Operating Centre

Set Mode – In the first embodiment of the invention this refers to the state of the

Vehicle Security Applications Manager (VSAM) when the vehicle is in a parked condition with the ignition switched off

Unset Mode – In the first embodiment of the invention this refers to the state of the VSAM after an authorised mobile phone has been recognised

User Authentication - The function whereby using wireless communications the VSAM pairs up with a Personal Communicator in the near proximity and verifies that the unique identifier of the Personal Communicator (in the first embodiment of this invention, a mobile phone number) is registered to an authorised driver of the vehicle.

Category 5 Standard – The standard for Stolen Vehicle Tracking and Recovery of the Association of British Insurers.

Automotive Aftermarket – Referring to the market for automotive equipment installed on used vehicles or new vehicles at franchised dealers.

CLAIMS

1. An in-vehicle system for use in a vehicle, the system being adapted to store information concerning vehicle usage, to store vehicle options for a driver of the vehicle, to transmit data to a remote location and to receive data from a remote location for provision to the driver of the vehicle, the system also being adapted to store permissions associated with an authorised driver of the vehicle, such permissions relating to the security of information that is transmitted from the vehicle by the system or received in the vehicle by the system, wherein the system is adapted to recognise a person as an authorised driver of a vehicle by interfacing with a mobile communications device of that person, and wherein if the vehicle is driven by a person who is not recognised as an authorised driver of the vehicle, the system is adapted to transmit data to a remote location warning of a suspected unauthorised driver of the vehicle, and to prevent access by the suspected unauthorised driver to secure information stored by the system or received from the remote location.

2. A system as claimed in claim 1, wherein the system is adapted to transmit data using a secure data protocol and to receive data using a secure data protocol.

3. A system as claimed in claim 1 or 2, wherein there is a provided a data synchronisation module that provides secure synchronisation of data stored by the system in the vehicle, with data stored on a database at a remote location.

4. A system as claimed in claim 1, 2 or 3, wherein the system uses a security key that controls the permissions that have been set and are associated with the driver's details, the vehicle details, the identity of a system unit in the vehicle, and the driver's mobile communications device.

5. A system as claimed in any preceding claim, wherein a security encryption algorithm is determined using a combination of in-vehicle system hardware, an identifier for a system unit in the vehicle, and host system identification.

6. A system as claimed in any preceding claim, including a covert microphone for detecting speech inside the vehicle for transmission to a remote location.

7. A system as claimed in any preceding claim, adapted to provide audio output through the vehicle's audio system.

8. A system as claimed in any preceding claim, comprising an in-vehicle controller which is provides in vehicle applications and external service managers for controlling links to external service providers at remote locations.

9. A system as claimed in any of claims 1 to 8, installed in a vehicle.

10. A method of controlling the storing of data, transmission of data and receipt of data concerning operation of a vehicle and / or the provision of information to the driver of the vehicle, using a system as claimed in any of claims 1 to 8.

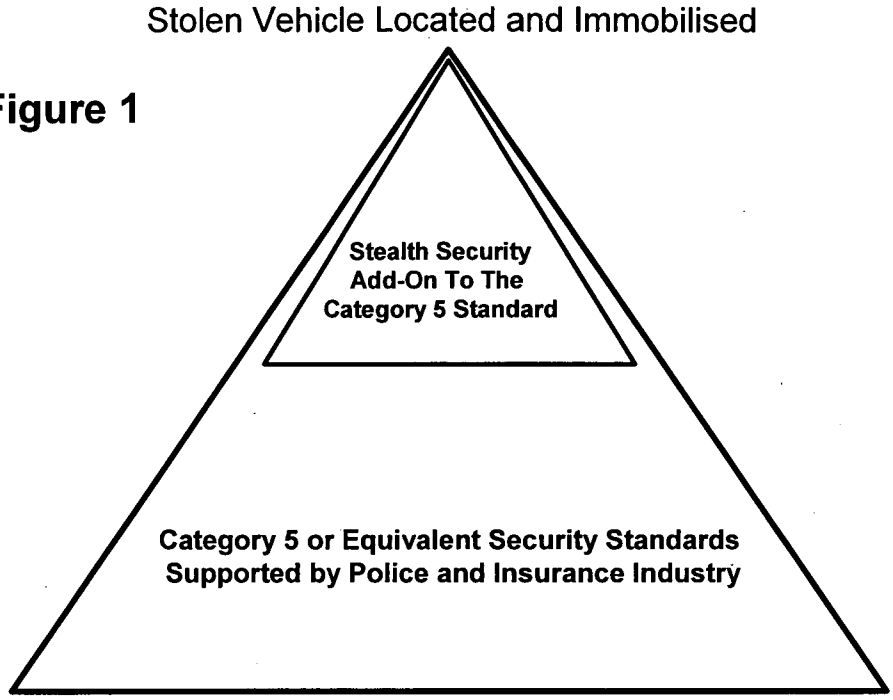
11. A method of presenting information to the driver of a vehicle comprising the steps of determining the identify of a driver, retrieving data related to the identified driver indicating one or more driver specific parameters and displaying information to the driver in accordance with at least one of said parameters.

12. A device for use in a motor vehicle comprising (a) a communication interface arranged to transmit and receive information and/or services to and/or from one or more external source(s); (b) a user interface arranged to communicate information and/or services to and/or from a driver; and (c) means to determine a driver's identity and information and/or services said user is authorised to access; wherein the device is arranged to permit access to the information and/or services in accordance with the information and/or services the user is authorised to access or use.

13. An in-car system for selectively displaying information to a driver from a

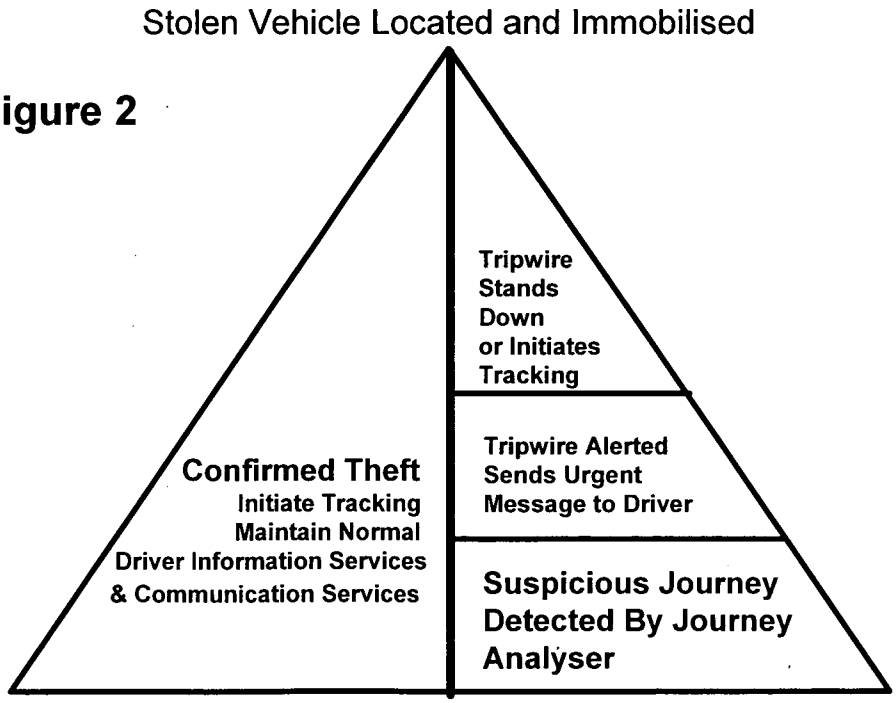
plurality of sources, the system comprising a display apparatus including a display unit and a control module and a plurality of information sources which can be displayed on the display unit by means of the control module, there being stored data indicating which information sources can be displayed to particular drivers; and the system further comprising means to identify a driver and wherein in use the system communicates information to the driver in accordance with the stored data indicating which information sources can be displayed to the identified driver.

Figure 1



Vehicle Security Pyramid

Figure 2



Stealth Security Pyramid

Figure 3

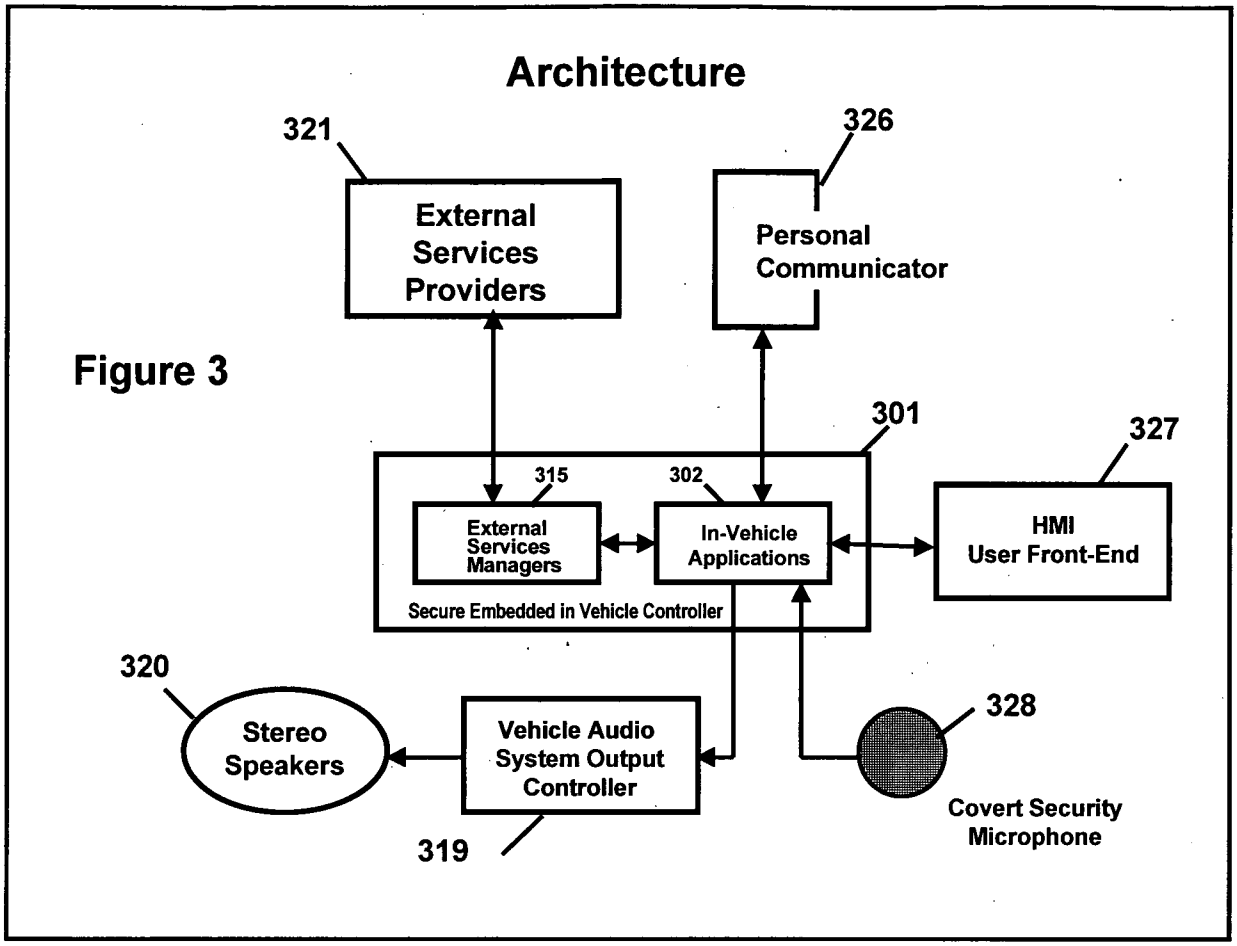


Figure 4
Key Theft Detection Security
Vehicle in Parked /In-Service State

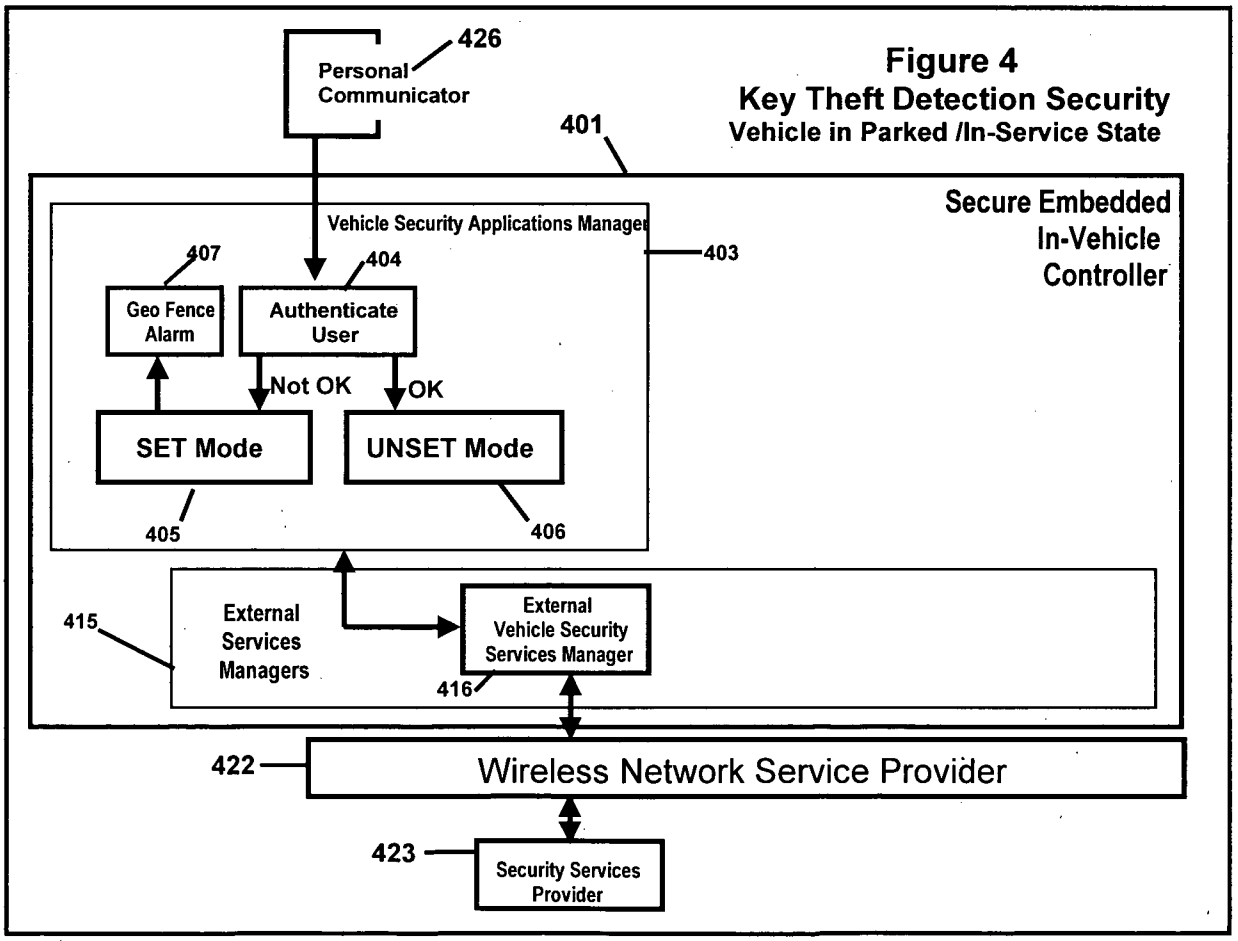


Figure 5
Vehicle in Readiness For Use State

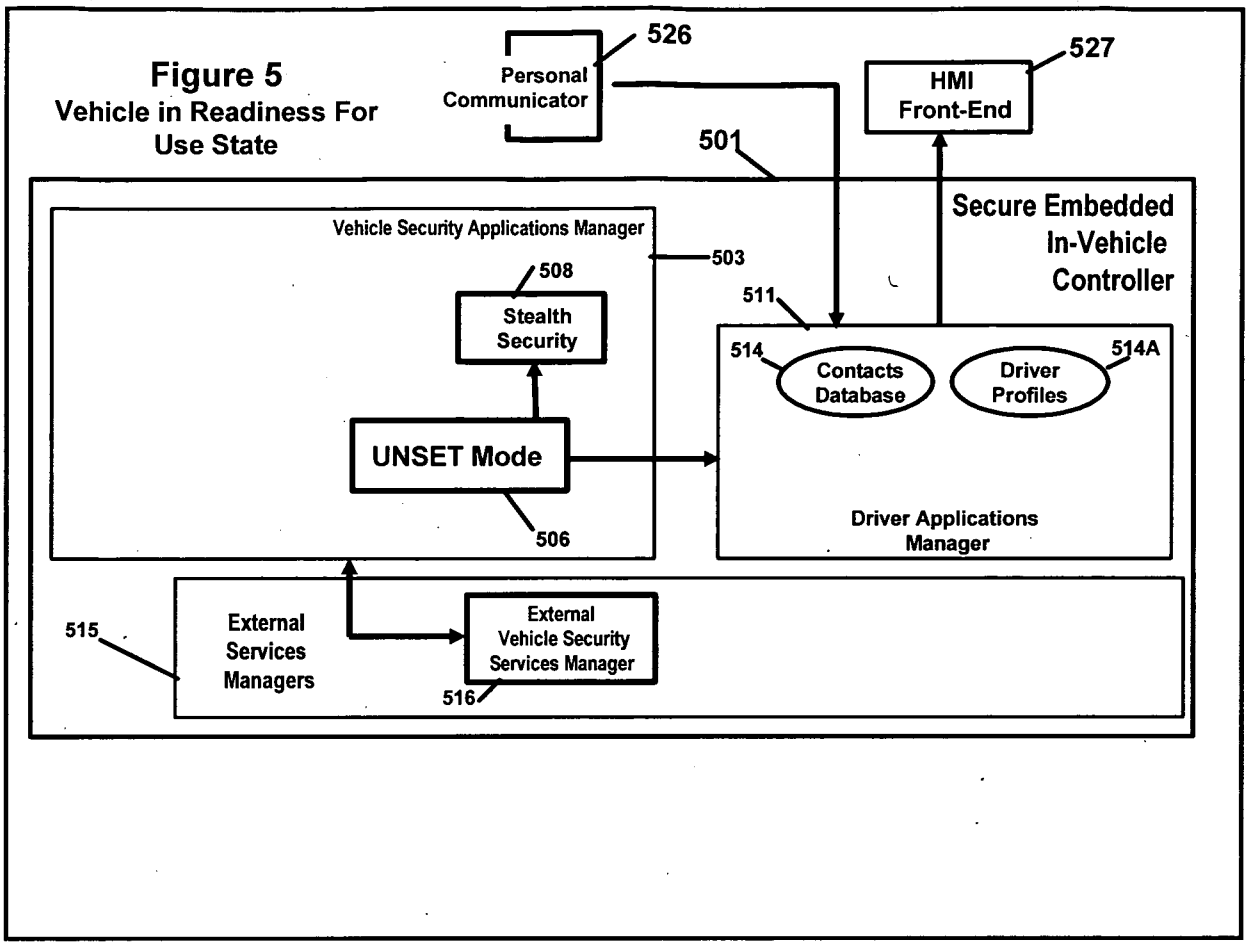
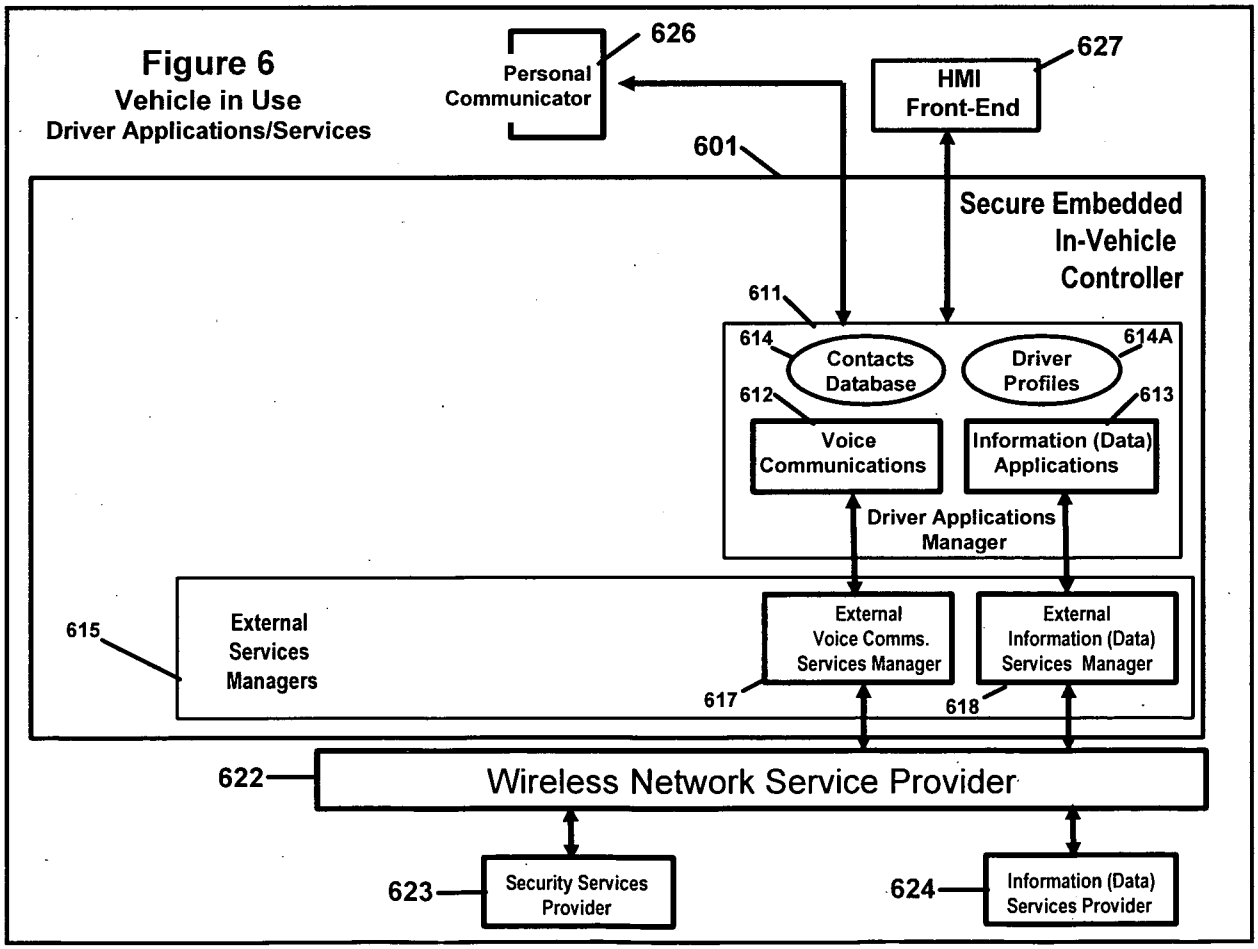


Figure 6
Vehicle in Use
Driver Applications/Services



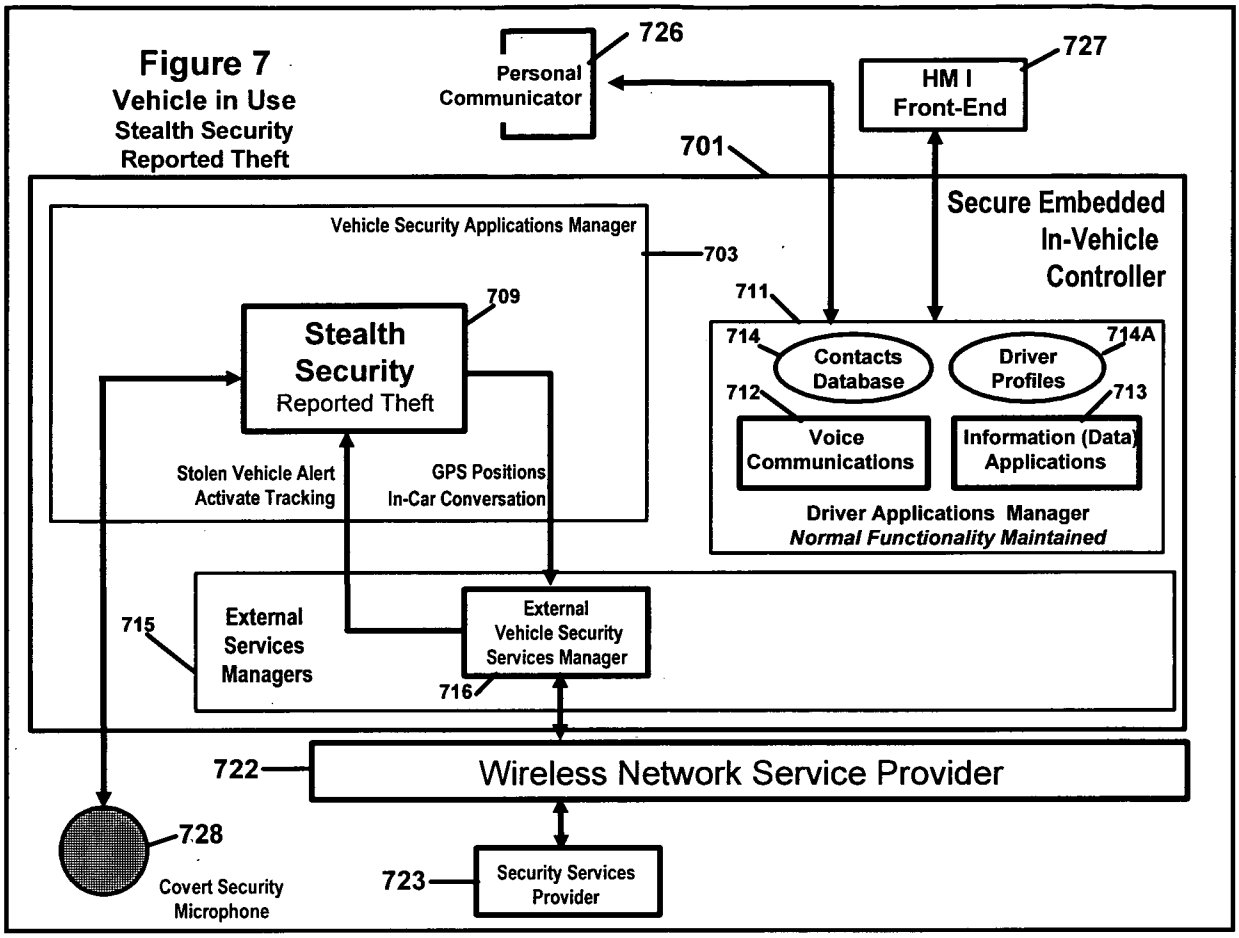


Figure 7
Vehicle in Use
Stealth Security
Reported Theft
Personal Communicator
726
HM I Front-End
727
701
Secure Embedded In-Vehicle Controller
Vehicle Security Applications Manager
703
709
Stealth Security Reported Theft
711
714
Contacts Database
714A
Driver Profiles
712
713
Voice Communications
Information (Data) Applications
Driver Applications Manager
Normal Functionality Maintained
Stolen Vehicle Alert
Activate Tracking
GPS Positions
In-Car Conversation
715
External Services Managers
External Vehicle Security Services Manager
716
722
Wireless Network Service Provider
728
Covert Security Microphone
723
Security Services Provider

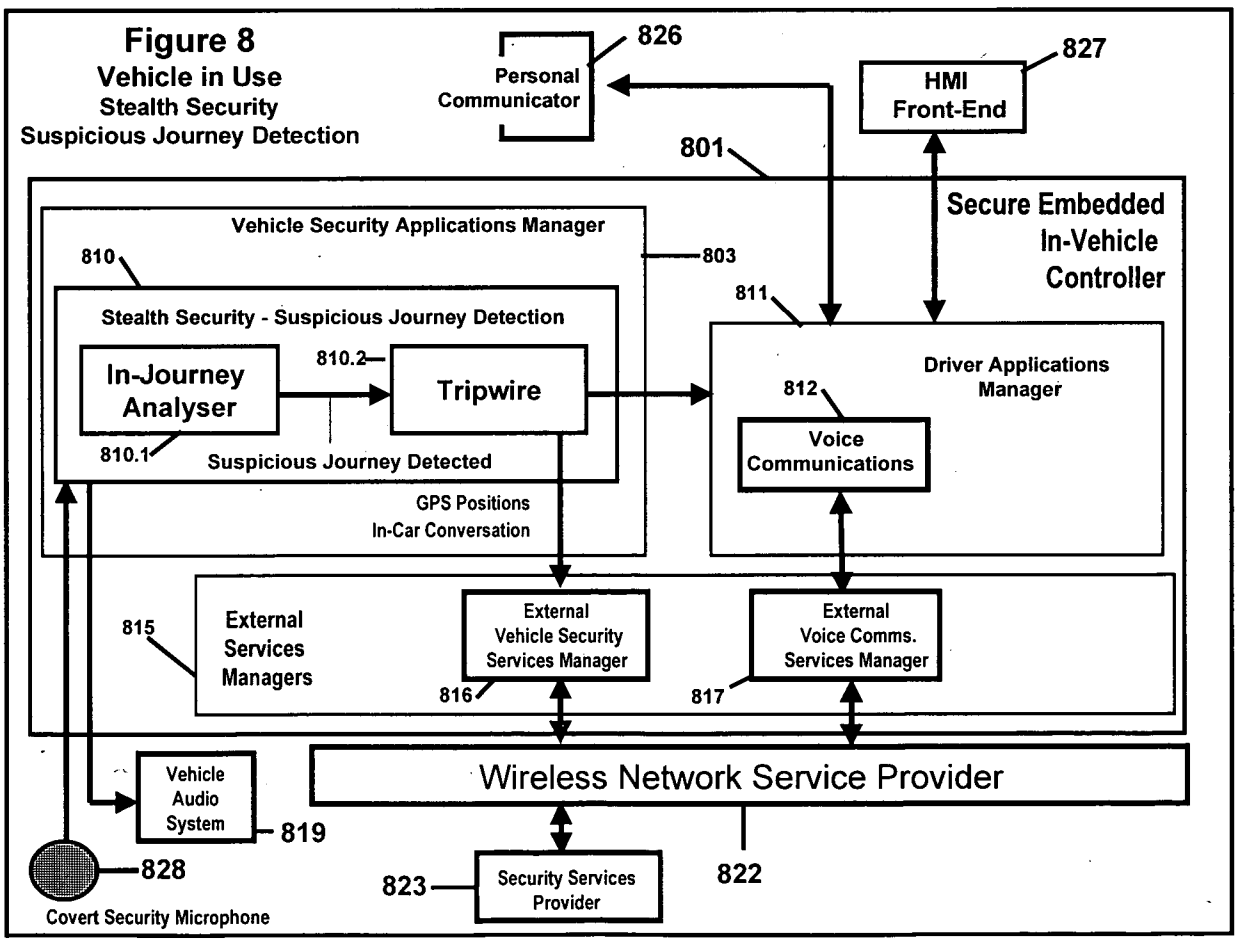


Figure 8
Vehicle in Use
Stealth Security
Suspicious Journey Detection
Personal Communicator
826
HMI Front-End
827
801
Secure Embedded In-Vehicle Controller
Vehicle Security Applications Manager
803
810
Stealth Security - Suspicious Journey Detection
811
In-Journey Analyser
810.2
Tripwire
Driver Applications Manager
812
Voice Communications
810.1
Suspicious Journey Detected
GPS Positions
In-Car Conversation
815
External Services Managers
External Vehicle Security Services Manager
816
External Voice Comms. Services Manager
817
Vehicle Audio System
819
Wireless Network Service Provider
828
Covert Security Microphone
823
Security Services Provider
822

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2007/004085

A. CLASSIFICATION OF SUBJECT MATTER
INV. B60R25/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
B60R

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	US 6 198 996 B1 (BERSTIS VIKTORS [US]) 6 March 2001 (2001-03-06) column 2, line 49 - column 22, line 12; figures	1,6-13 2-5
Y	EP 1 439 100 A (MATSUSHITA ELECTRIC IND CO LTD [JP]) 21 July 2004 (2004-07-21) paragraph [0075]; figures	2-5

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 January 2008	30/01/2008

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	David, Pascal

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/GB2007/004085

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6198996 B1	06-03-2001	JP 2000219092 A	08-08-2000
EP 1439100 A	21-07-2004	CN 1522903 A	25-08-2004
		DE 602004001881 T2	18-01-2007
		KR 20040066723 A	27-07-2004
		US 2004145447 A1	29-07-2004