(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 073 179 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
24.06.2009 Bulletin 2009/26

(51) Int Cl.:
G08B 13/14 *(2006.01)*

(21) Application number: **07024625.1**

(22) Date of filing: **19.12.2007**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC MT NL PL PT RO SE SI SK TR
Designated Extension States:
AL BA HR MK RS

(71) Applicant: **Harman Becker Automotive Systems GmbH**
76307 Karlsbad (DE)

(72) Inventors:
- **Wlotzka, Paul**
  72622 Nürtingen (DE)
- **Ohler, Jens**
  75249 Kieselbronn (DE)

(74) Representative: **Bertsch, Florian Oliver et al**
Kraus & Weisert
Patent- und Rechtsanwälte
Thomas-Wimmer-Ring 15
80539 München (DE)

Remarks:
Amended claims in accordance with Rule 137(2) EPC.

(54) Theft protection system and method of enabling an operating mode of an electronic device

(57) Theft protection system for an electronic device (101; 201) comprising
- an electronic device (101; 201) comprising
- a radio frequency identification unit (102; 202) emitting a radio frequency signal (105; 205) containing request information and
- a theft protection unit (103; 204) enabling an operating mode of the electronic device (101; 201) upon reception of a signal (110; 210) containing predetermined identification information, and

- at least one radio frequency identification transponder (107; 206), wherein, when the radio frequency identification unit (102; 202) receives said signal (110; 210) containing predetermined identification information, which is emitted by said radio frequency identification transponder (107; 206) in response to receiving the radio frequency signal (105; 205) containing request information, the theft protection unit (103; 204) enables the operating mode of the electronic device (101; 201).

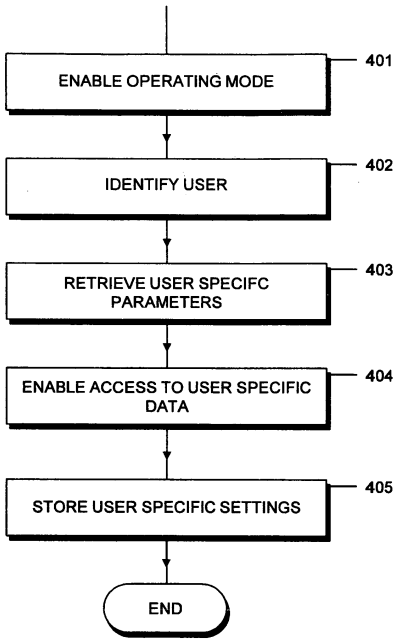


FIG. 4

EP 2 073 179 A1

Description

Field of the Invention

[0001] This invention relates to a theft protection system for an electronic device and to a method of enabling an operating mode of an electronic device, by which method a theft protection is achieved.

Background of the Invention

[0002] Modern electronic devices are an attractive target for thieves. Particular portable electronic devices, such as mobile phones or personal navigation devices (PND) are stolen frequently. Mobile navigation devices are becoming wide-spread and are often mounted in a detachable manner inside a vehicle. It is relatively simple for a thief to steel such a device from a vehicle, and cases of PND thievery are rapidly increasing. Accordingly, there is a need to provide a theft protection system for protecting these devices against theft.

[0003] Conventional theft protection systems use, for example, a code, such as a sequence of characters, which has to be entered when the electronic device is switched on. Yet this type of protection is rather uncomfortable, as the user has to remember the code and needs to enter the code every time at startup. Furthermore, if the owner of such a device wants to lend the device to another person, the person would have to remember the code. That way, the code may also become known to other people not intended to use the device. Furthermore, the code may be learned by people skilled in code decryption. The protection offered by such codes is thus limited.

[0004] A further conventional theft protection system for vehicle-mounted electronic devices is known in the art. In this system, a face plate of the electronic device usually comprising input or display means is detached from the electronic device in order to prevent operation of the device in case the device is stolen. A user of the device has to detach the face plate and carry the face plate when parking the vehicle for an effective theft protection, yet this is very uncomfortable. First, the user often forgets to detach the face plate, and second, carrying the face plate around is very inconvenient. Thus, users often store the face plate in another place inside the vehicle, such as inside the glove box. Accordingly, an effective theft protection is prevented. Furthermore, detaching a face plate of a portable device is not feasible, as the user of the portable device may carry the device itself instead of carrying a face plate of the device.

[0005] Furthermore, theft protection systems for electronic devices which are being sold in a store are known in the art. For protecting electronic devices sold in a store against theft, a radio frequency identification (RFID) tag is attached to the electronic device. At the store exit a radio frequency identification reader (RFID reader) is provided which can read the RFID tag. When a customer pays for the electronic device, the RFID tag is deactivated by the reader, and no alarm is triggered. If a customer does not pay for the electronic device before leaving the store, the RFID reader reads out the RFID tag, determines that the device is being stolen, and sets off the alarm. Although this system is useful for stores, it does not provide any theft protection for the electronic device once the person buying the electronic device has left the store.

Summary of the Invention

[0006] Accordingly, a need exists to provide a system and a method for protecting an electronic device from theft, which are easy to use by a user of the electronic device and which provide a good protection.

[0007] This need is met by the system and the method of the independent claims. The dependent claims describe preferred embodiments of the invention.

[0008] According to a first aspect of the invention, a theft protection system for an electronic device is provided, comprising an electronic device comprising a radio frequency identification unit emitting a radio frequency signal containing request information and a theft protection unit enabling an operating mode of the electronic device upon reception of a signal containing predetermined identification information. Furthermore, the theft protection system comprises at least one radio frequency identification transponder, wherein, when the radio frequency identification unit receives said signal containing predetermined identification information, which is emitted by said radio frequency identification transponder in response to receiving the radio frequency signal containing request information, the theft protection unit enables the operating mode of the electronic device. The radio frequency identification unit may be in the form of an RFID reader capable of sending and receiving radio frequency signals. For example at startup of the mobile navigation device, the RFID unit transmits a radio frequency (RF) signal containing request information. Request information refers in general to information that prompts the transponder to transmit a signal containing identification information. As such, the RF signal containing request information may be a simple RF signal of a predetermined frequency, or a predetermined modulation, or it may be an RF signal comprising instructions, e.g. in the form of a modulation, said instructions being demodulated and interpreted by the transponder. The transponder is formed so that in response to receiving the RF signal from the RFID unit it emits a signal comprising identification information.

[0009] There are several ways a transponder can transmit a signal comprising identification information to the RFID unit. The RFID unit as well as the transponder may comprise coils and thus form some kind of air-coupled transformator, wherein the transponder modulates the current in its coil which is detected by the RFID unit. Further techniques that may be used to generate the sig-

nal comprising identification information are backscattering, which is particularly useful in the far field of the field emitted by the RFID unit, or load modulation, which is particularly useful in the near field. The RFID transponder may also actively emit a signal comprising identification information, e.g. in the radio frequency range. If the RFID unit receives a radio frequency signal comprising predetermined identification information, the theft protection unit enables the operating mode of the electronic device. Predetermined identification information may for example be an identification number of a transponder associated with the electronic device. A predetermined identification information may be configured during device manufacture or at an initiation step before or after the device was sold. The operating mode enabled by the theft protection unit is preferably a mode in which the full functionality of the electronic device can be accessed by the user. If said operating mode is not enabled, the electronic device is preferably not of any use to a user. The theft protection unit may be provided in form of software code portions which enable the operating mode, yet it may also be provided in the form of hardware, which e.g. provides power to certain components of the electronic device in the operating mode. As a result, without the RFID transponder being within a range to transmit said signal comprising predetermined identification information to the RFID unit, the electronic device is not of any use. For a thief who is not in possession of the RFID transponder, it is thus not attractive to steel the electronic device. On the other hand, a user of the electronic device being in possession of said RFID transponder may simply enable said operating mode by bringing said RFID transponder within a range in which the RFID unit can receive the signal comprising identification information. The RFID transponder may simply be carried on a key ring by the user, as a result of which a vehicle-mounted electronic device will for example be theft-protected as soon as the user leaves the vehicle, and said operating mode will always be enabled as soon as the user enters the vehicle. Thus, a theft protection system for an electronic device is provided which is easy to use and offers a high level of protection. Furthermore, multiple RFID transponders may be provided to predetermined persons whom access is to be given to the electronic device.

[0010] The electronic device may be a mobile electronic device, or it may be a built-in or stationary electronic device. Examples of mobile electronic devices are a mobile phone, a portable music player, a digital or analog camera or the like. Examples of built-in or stationary electronic devices are a car stereo system or a navigation system mounted to the dashboard of a vehicle, or a home stereo system, an entertainment system, a television, a computer system or the like. Preferably, the electronic device is a mobile navigation device.

[0011] According to a further aspect of the invention, the at least one radio frequency identification transponder comprises a transponder which is powered by receiving a radio frequency signal from said radio frequency identification unit. For this purpose, the radio frequency signal containing request information emitted by the RFID unit may be used. Such a RF signal-powered transponder has the advantage that it requires no battery, and thus has a prolonged lifetime. Furthermore, this kind of transponder is very compact, so that it can be mounted in a variety of places and be integrated into very small components. Preferably, the at least one radio frequency identification transponder comprises a power antenna and a condenser. A power antenna is a regular antenna which is formed so as to retrieve power from a radio frequency signal. The power retrieved by the antenna may then be stored in the condenser, and said power may then be used to power the radio frequency identification transponder. Powering a RFID transponder using a radio frequency signal is known in the art and will thus not be discussed in more detail here.

[0012] According to another aspect of the invention, the at least one radio frequency identification transponder comprises a battery-powered transponder. The advantage of a battery-powered transponder is that it can emit a signal comprising identification information even if it receives only a relatively weak radio frequency signal containing request information. Accordingly, the range of the battery-powered transponder is increased. Furthermore, battery-powered transponders can be more reliable than passive, RF signal-powered transponders. As an example, the theft protection system may comprise a passive transponder, i.e. a transponder which is powered by receiving the radio frequency signal, and an active transponder, i.e. a battery-powered transponder. Providing different types of transponders has the advantage that for a particular application the appropriate transponder can be provided. The at least one radio frequency identification transponder may for example comprise a transponder being mounted inside a vehicle. Such a transponder may be mounted rather close to a position in which the electronic device is mounted, and accordingly, the transponder may be a passive transponder as it does not require a large range. The transponder may be integrally connected to a component of the dashboard, so that it may not be easily removed. This has the advantage that as soon as, e.g. a mobile navigation device is put into its mounting position inside the vehicle, the theft protection unit will enable the operating mode, as a result of which a person may use the full functionality of the mobile navigation device. Yet if the device is removed from the vehicle, e.g. by a thief, the operating mode will no longer be enabled as the transponder remains inside the vehicle. As the device is thus rendered useless, an effective theft protection is provided. It is also an advantage to use a passive transponder for being mounted inside the vehicle, as this kind of transponder does not comprise a battery which may have to be changed after some time, nor does it require any other power connection. The RFID transponder may be provided together with the electronic device, and may then be mounted inside the vehicle, yet it may also be directly provided

with the vehicle. The transponder may then be programmed to transmit the appropriate predetermined identification information or the PND may enter the identification number of the transponder into a list of authorized transponders. RFID transponders that are able to store information are known in the art and will not be discussed in greater detail here.

[0013] According to another aspect of the invention, the at least one radio frequency identification transponder comprises a mobile transponder being formed so as to be carried on a key ring. Such a transponder may have the form of a small tag, yet it may also be integrated in a key, such as the car key. This has the advantage that the user may attach such a transponder to his key ring, and may thus always carry the transponder with him, whereby said protection of the electronic device is ensured. As soon as the user in possession of such a transponder carries e.g. a mobile electronic device with him, the operating mode is enabled. If the user leaves the mobile electronic device at some place, the operating mode will not be enabled as the transponder will not be within range. Thus, the device is theft-protected. The mobile transponder may be a battery-powered transponder, which has the advantage that the range is included. Also changing a battery on a mobile transponder is in general a simple task. Yet a passive mobile transponder is also advantageous, as it is very small and compact. Preferably, a transponder is provided inside a vehicle, and one or more additional mobile transponders are provided. The mobile electronic device will thus be fully operational when carried by a legitimate user possessing a mobile transponder and when mounted inside the vehicle.

[0014] According to an embodiment of the invention, the theft protection unit is formed so as to not enable or to disable said operating mode if no signal comprising the predetermined identification information is received by the radio frequency identification unit at a startup of an electronic device or a predetermined amount of time after startup, respectively. The operating mode will thus not be enabled if no transponder is within range at startup. Also, after the electronic device has been running for a predetermined amount of time, it may want to confirm that the transponder is still within range. Otherwise, a person could steel the electronic device while the device is running and may then use the device as long as it is not shut down. It is thus advantageous to check periodically whether an appropriate transponder is within range. The RFID unit may for example send out and RF signal containing request information 10, 20 and 30 minutes after the electronic device was started up. If no signal comprising the predetermined identification information is received in response, the theft protection unit will disable said operating mode, rendering the electronic device essentially inoperable.

[0015] According to another embodiment, the theft protection system furthermore comprises an indicator being at least periodically activated while said operating mode is not enabled. The indicator is generally used to make potential thieves aware of the fact that the mobile navigation device is theft-protected. A mobile navigation device may for example be provided with a light-emitting diode which periodically lights up when the mobile navigation device is switched off indicating that the navigation device is theft-protected and an appropriate transponder is required to enable the operating mode. Other means, such as illumination means already provided on the mobile navigation device, may be used as an indicator. A display of the navigation device may also be used as an indicator. Such an indicator has the advantage that a potential thief will not try to steel the mobile navigation device, as he will note that he will not be able to operate the device.

[0016] The potential thief will thus not be tempted to break into a vehicle, whereby damages to the vehicle are prevented and other inconveniences, such as having to deal with the police or insurance, or having to bring the vehicle to a mechanic shop for repair, are avoided. It is also prevented that a potential thief takes other items located inside the vehicle with him, if the thief is prevented from breaking into the vehicle in the first place. With such a theft protection system, the owner of the electronic device can leave the navigation device inside the vehicle without having the fear that it will be stolen. It is very convenient to not have to carry the electronic device, or a mobile face plate of a built-in electronic device or the like.

[0017] According to another embodiment, the theft protection unit is formed so as to enable said operating mode in response to a predetermined character sequence being entered by means of an input unit. The character sequence may for example be a multi digit code, e.g. four digit code, which can be entered by the user of the electronic device in order to enable the operating mode. This way of enabling the operating mode is provided for situations in which the owner of the electronic device does not carry the appropriate RFID transponder. This is particular advantageous in situations where the user of e.g. a navigation device has lost the transponder, yet still relies on using the navigation device. Although entering a character sequence for enabling the operating mode is less convenient, it is still advantageous to provide this optional feature, particularly in the above-described situations.

[0018] According to a further aspect of the invention, each transponder comprises an identification number, said identification number being transmitted as part of the identification information. The identification number may be stored in the transponder in a permanent or non-permanent memory, such as an EPROM, an EEPROM, a Flash PROM, or a flash memory. The transponder may for example comprise circuitry on a microchip which reads out the identification number and transmits the identification number with the emitted signal. The identification number may be assigned to the transponder during the production process of the transponder, yet it may also be assigned at a later stage. For example if a trans-

ponder is lost, a new transponder may be acquired by the owner of the electronic device, and said transponder may then be initialized by assigning a new identification number associated with said electronic device to said transponder.

[0019] According to an embodiment the identification information identifies a user of the electronic device, wherein the electronic device is formed so as to operate in said operating mode taking into account data relating to the identified user. Each user of the electronic device may for example possess a transponder with an individual identification number associated with said user. Said identification number can then be transmitted as part of the identification information, and the navigation device can thus determine which user is enabling the operating mode. In one embodiment, the electronic device is formed so that it retrieves user-specific operating parameters in response to the radio frequency identification unit receiving a radio frequency signal containing predetermined identification information. A user may for example define particular parameters of e.g. a mobile navigation device, such as a language setting, a color setting, or other preferred settings or parameters relating to navigation, such as home position, last destination or route options, and these parameters may then be retrieved when the user is identified using the predetermined identification information received by the RFID reader. The operation of the mobile navigation device can thus be personalized. This has the advantage that in the case where multiple users use the mobile navigation device, a user does not have to adjust the settings every time another user has used the device. Simply by carrying the transponder the mobile navigation device will obtain the information of which person is using the device, and it can adjust its settings accordingly by using the retrieved user-specific operating parameters.

[0020] According to another embodiment, the electronic device is formed so that it grants access to user-specific data in response to the radio frequency identification unit receiving a radio frequency signal containing predetermined identification information. The electronic device may for example comprise storage means such as a flash memory or a hard drive on which a user can save data, such as route data, pictures, music files, and the like. When multiple users use the electronic device, a user may not wish to grant other users access to their data. It is thus an advantage if the electronic device identifies the user by means of the received identification information and then grants access to data belonging to said user. The device may then block access to the data of other users.

[0021] In the case where multiple transponders are within range of the RFID unit of the electronic device, the mobile navigation device may enable a default operating mode. Using an input means, e.g. a soft key, a user may then select to access a particular user profile, e.g. in the form of user-specific parameters, as well as user-specific data. In this case the user-specific data may furthermore be password-protected, e.g. by means of a numerical code.

[0022] Furthermore, additional theft-protection means may be provided, such as a detachable face plate or a coded detachable face plate, or the like. Furthermore, the electronic device may comprise a mobile communication unit which is formed so as to enable a tracking of the mobile navigation device. The mobile communication unit may be formed so as to enable a mobile communication functionality of the electronic device, e.g. via a mobile telephony network. Signals sent to the mobile telephony network by the mobile communication unit may then be used for tracking the electronic device. It may for example be detected by multiple unsuccessful tries to operate the electronic device that the electronic device was stolen. As a result, the electronic device may establish a connection to the mobile telephony network to enable a tracking of the device. Systems for tracking devices using mobile communication signals are known in the art and will not be described in more detail here. Providing such a system has the advantage that it may be possible to retrieve the device once the device was stolen. Such a tracking is particularly advantageous for mobile electronic devices, e.g. a mobile navigation device, or for electronic devices mounted inside a vehicle, as the device may be tracked when removed from the vehicle or when stolen together with the vehicle.

[0023] Furthermore, a method is provided of enabling an operating mode of an electronic device, comprising the steps of emitting a radio frequency signal containing request information by a radio frequency identification unit provided in the electronic device, receiving, at a transponder, said radio frequency signal containing request information and transmitting back to the radio frequency identification unit a signal containing predetermined identification information, wherein, when said signal containing predetermined identification information is received by the radio frequency identification unit, a theft protection unit provided in the electronic device enables the operating mode of the mobile navigation device. The transponder may for example be an active or a passive RFID transponder, transmitting the identification information in response to receiving the signal containing request information. Preferably, by enabling the operating mode, full functionality of the electronic device is provided. Enabling the operating mode in such a way has the advantage that the electronic device is protected from theft as it will not enter said operating mode if no transponder is within a range over which it can transmit the signal containing the predetermined identification information to the RFID unit. As in general only a legitimate user possesses an appropriate transponder, or a transponder may only be located in places in which the electronic device is to be used, an unauthorized person will not be able to enable the operating mode of the mobile navigation device and thus to use the device. Preferably, the method further comprises the steps of identifying a user of said electronic device by means of said identifi-

cation information and of operating said navigation device in said operating mode taking into account data relating to the identified user. The data relating to the identified user may comprise operating parameters of the electronic device, such as personal settings and the like, and it may comprise access information, e.g. information about which data or which data files may be accessed by the identified user. Enabling an operating mode this way has the advantage that multiple users can use the electronic device each with their own device settings and data files. The transponder may be mounted inside the vehicle or may be formed so as to be carried on a key ring. Preferably, a plurality of transponders is provided, e.g. a transponder being mounted inside a vehicle, and one or more transponders for being carried on a key ring. It is thus ensured that plural users are able to use the electronic device.

[0024] Furthermore, the method of enabling an operating mode of an electronic device may comprise any of the steps described above with reference to the theft protection system.

[0025] In particular in view of the increasing rate of theft of e.g. mobile navigation devices, the above-described system and method and their embodiments provide a number of advantages. In particular, a stolen electronic device is rendered useless to a thief, and basing the described method and system on RFID technology is cost-efficient.

[0026] Further details and advantages of the invention will be become apparent from the following detailed description of the preferred embodiments with reference to the figures.

Brief Description of the Drawings

[0027]

Fig. 1 shows a schematic drawing of an embodiment of a theft protection system for a mobile navigation device according to the present invention.

Fig. 2 shows a schematic drawing of another embodiment of a theft protection system for a mobile navigation device according to the present invention.

Fig. 3 shows a flow diagram of an embodiment of a method of enabling an operating mode of a mobile navigation device.

Fig. 4 shows a flow diagram of an alternate embodiment of a method of enabling an operating mode of a mobile navigation device.

[0028] For explanatory purposes only, the following detailed descriptions are based on a mobile navigation device. Yet it will be appreciated by a person skilled in the art that the theft protection system and the method of the present invention may be used in conjunction with any other electronic device, such as a personal data assistant, a mobile phone or a car stereo system.

[0029] Fig. 1 shows a schematic drawing of a theft protection system 100 for a mobile navigation device 101. The mobile navigation device 101 comprises a radio frequency identification unit 102 and a theft protection unit 103. In this embodiment, the mobile navigation device is a personal navigation device (PND), and the RFID unit 102 is comprise in the theft protection unit 103. When the PND 101 is turned on by a user, the theft protection unit 103 prompts the RFID unit 102 to emit a radio frequency signal containing request information via antenna 104. The emitted radio frequency signal is depicted by arrow 105. Using antenna 106, a radio frequency identification transponder 107 receives the radio frequency signal. The RFID transponder 107 may be an active, semi-active or passive transponder, and may operate on power derived from the radio frequency signal 105 and stored in a condenser, or from power derived from a battery, or a combination thereof. The antenna 106 may take a range of shapes, such as a coil shape or the shape of printed circuit tracks, and it will depend on the particular application, e.g. the frequency of the RF signal which shape the antenna 106 will have. The RFID transponder 107 comprises a transceiver 108 and an ID memory 109. The ID memory 109 may store an identification number that is representative of the transponder 107. The ID memory may be in the form of a read-only-memory with a set identification number stored, yet the transponder 107 may also comprise a writable permanent memory unit, e.g. an electrically erasable programmable read-only-memory (EEPROM) or an ferro-electric random access memory (FRAM), yet it may also comprise a volatile memory, such as a static random access memory (SRAM). A writable memory may be used to store additional information in the RFID transponder 107. The transceiver 108 reads the identification number of the transponder and transmits it by means of antenna 106. Depending on the type of transponder used, several modes of transmission are possible. The transponder 107 may for example modulate the electromagnetic field emitted by the RFID unit 102 via antenna 104, which is then detected by antenna 104 and the RFID unit 102. The electromagnetic field emitted by antenna 104 may for example be manipulated by using backscattering or load modulation. As said before, backscattering is generally used in the far field, whereas load modulation is used in the near field. Modulation may for example occur by inductive coupling using antenna 106. Effectively, this corresponds to a radio frequency signal emitted by antenna 106, wherein the radio frequency signal is modulated in such a way that identification information is transmitted. The identification information comprises the identification number of the transponder 107 stored in the ID memory 109. The signal 110 is received by the antenna 104 and demodulated in the RFID unit 102. Several ways of modulating the radio frequency signal are known in the art, such as amplitude shift keying, frequency shift

keying or phase shift keying, and any of these methods may be used. Further transmission methods, such as encoding and anti-collision methods may be used in transmitting signals between the RFID unit 102 and the transponder 107. The RF signals may be in the ultra-high frequency (UHF) range, e.g. between 300 kHz and 3 GHz, yet they may also be in the long wave (LW), medium wave (MW) or short wave (SW) frequency range. The theft protection unit 103 may for example prompt the RFID unit 102 to continuously emit an RF signal until a signal comprising identification information is received or until a predetermined amount of time has passed. A continuous emission of an RF signal has the advantage that a passive RFID transponder can be supplied with power.

[0030] After receiving the signal 110 and extracting the identification information from the signal, the theft protection unit 103 determines whether the identification information originates from an authorized transponder. An authorized transponder is for example a transponder associated with the mobile navigation device 101, e.g. a transponder delivered together with the mobile navigation device or a transponder set up to grant access to the mobile navigation device. The theft protection unit 103 may have a number of identification numbers stored, for which access will be granted to the mobile navigation device. If a comparison between these numbers and the identification number transmitted by the RFID transponder 107 brings up a match, the theft protection unit 103 will enable an operating mode of the navigation device. In said operating mode, a user may be able to access the full functionality of the mobile navigation device 101. The theft protection unit 103 may be part of a software program running at the startup of the mobile navigation device 101, said software program being able to control the RFID unit 102 and being formed so as to grant access to said operating mode if a valid identification number is received. As such, said software program may run on a microprocessor comprised in the mobile navigation device 101. On the other hand, the theft protection unit 103 may also be realized in form of hardware, which for example controls the RFID unit 102 and enables a startup of the mobile navigation device 101 in said operating mode.

[0031] In case no signal comprising the predetermined identification information is received by the RFID unit 102, the theft protection unit 103 will not enable said operating mode, yet it may continue to prompt the RFID unit 102 to keep sending out radio frequency signals 105 for a predetermined amount of time. After said predetermined amount of time, the theft protection unit 103 may power down the mobile navigation device 101, or it may issue a warning in audible or visible form. That way, a user of the mobile navigation device 101 will be notified that he has to bring an authorized transponder within range to be able to use the device 101.

[0032] The mobile navigation device 101 may be formed so as to be detachably fixed to a windscreen of a vehicle or dashboard mounted inside a vehicle. The RFID transponder 107 may have the form of a foil tag which is attached to a component inside a vehicle. Preferably, the transponder is attached to said component in a hidden or a hard to access position. As soon as the mobile navigation device 101 is placed in its mount inside the vehicle, it will be able to receive signals 110 comprising identification information from said transponder once the mobile navigation device is switched on. As the signal transmission and checking of the identification number is performed automatically, a user does not have to perform any additional steps when he wants to use the device 101. When the device 101 is removed from the vehicle, e.g. by an unauthorized person, the RFID unit 102 will no longer be able to receive a signal 110 from the RFID transponder 107, and accordingly, the mobile navigation device will not enter its operating mode. As the unauthorized person will in general not be able to retrieve the RFID transponder from the vehicle, the mobile navigation device 101 will be rendered useless to the unauthorized person and will thus be effectively theft-protected. The described embodiment thus provides an easy to use and effective theft protection of the mobile navigation device 101.

[0033] Fig. 2 shows a schematic drawing of another embodiment of the present invention. The theft protection system 200 comprises a mobile navigation device 201 with an RFID unit 202 connected to an antenna 203 and a theft protection unit 204. Again, the theft protection unit 204 prompts the RFID unit 202 to emit a radio frequency signal 205 which is received by a RFID tag 206, which comprises an antenna 207 in form of a coil and a microchip 208. The RFID tag 206 is formed so as to be carried on a key ring, meaning it is compact and comprises a means 209 for attachment to a key ring. The RFID tag 206 may further comprise a condenser or a battery (both not shown). The microchip 208 comprises a memory, e.g. permanent erasable or non-erasable, as well as a transceiver and processing means for processing, storing and retrieving information. In response to receiving the radio frequency signal 205, the tag 206 emits a signal 210 comprising identification information. In case of an active tag 206 comprising a battery, the range over which the signal 210 can be transmitted to the RFID unit 202 is extended, and the tag 206 may be carried in a person's pocket while still being able to transmit the signal 210 to a mobile navigation device 201 being held in the person's hand or located within a few meters of the person. As described above, with the reception of the signal 210 comprising predetermined identification information, i.e. identification information from an authorized RFID tag, by the RFID unit 202, the theft protection unit 204 will enable the operating mode of the mobile navigation device 201. As this occurs automatically, a user may thus enter the operating mode of the mobile navigation device 201 without any additional steps by simply carrying the RFID tag 206 in his pocket. If the device 201 gets stolen, e.g. out of the vehicle or out of the user's backpack, the thief will generally not be in possession of the RFID tag

206, and accordingly, the device 201 will be rendered useless to the thief.

[0034] The mobile navigation device 201 furthermore comprises a processing unit 211, an indicator 212, a memory 213 and an input unit 214. While the device 201 is switched off, components of the theft protection unit 204 may still be active and prompt the indicator 212 to display a warning that the device 201 is theft protected. The indicator 212 can have the form of a light-emitting diode, which may periodically light up, yet it may also use existing display means, for example lighting means provided on the mobile navigation device 201 or a display of the mobile navigation device 201 to display the warning. The display may for example show a text line such as "theft-protected" or "code" to indicate that stealing the device will not be crowned with success, as the device will be rendered useless. When the mobile navigation device 201 is switched on, the indicator 212 may display the warning as long as the operating mode was not entered. The indicator 212 may also issue a more explicit warning in this case, as it can be assumed that the mobile navigation device 201 was stolen when it is activated without the presence of an authorized tag. The indicator 212 may for example sound an alarm or may display a more visual warning. Providing an indicator 212 is particularly advantageous, as it can prevent a theft of the mobile navigation device in the first place. The mobile navigation device 201 may further comprise a mobile communication unit (not shown) which builds up a connection to a server when it is detected that the device was stolen, e.g. via a mobile telephony network. A tracking of the mobile navigation device 201 may then be enabled, e.g. by using signals of the mobile communication unit.

[0035] The input unit 214 may be provided to enter information when operating the mobile navigation device 201. Yet for the case where the owner or an authorized person of the mobile navigation device has misplaced or forgotten their authorizing RFID tag, an additional way of entering the operating mode of the device is provided in the embodiment of Fig. 2. After no signal 110 comprising identification information is received by the RFID unit 202 for a predetermined amount of time, the user of the device 201 may be prompted to enter a code. The user may then enter the code, e.g. in form of alphanumerical characters, by means of the input unit 214. The theft protection unit 204 then checks whether the entered code is a predetermined access code for the mobile navigation device 201, and if so, it will enable the operating mode. Although entering a code manually is less convenient for a user, it still provides a backup in case a transponder or RFID tag is lost or not available. Particularly in mobile use, e.g. when hiking, rendering the mobile navigation device useless by losing an RFID tag would be disastrous. It is thus advantageous to provide this additional way of entering the operating mode.

[0036] For navigational functionality, the mobile navigation device 201 runs software programs on a processing unit 211. Different applications, such as music players or picture viewers may also be run on the processing unit 211. For these applications, the processing unit 211 accesses a memory 213, which may comprise user-specific information, such as parameters used when running the applications, as well as user files, e.g. data files comprising route or track information, music or pictures and the like. Generally, different users of the mobile navigation device 201 prefer different settings for running the device and the applications, such as language, font size, brightness of the display and similar settings. Preferably, each user of the mobile navigation device 201 has his own RFID tag 206 with an individual identification number, and by receiving said identification number by means of the RFID unit 202, the user currently using the mobile navigation device can be identified. The identification number may be provided to the processing unit 211 by the theft protection unit 204, or the processing unit 211 may directly access the RFID unit 202 to obtain the identification number. After identifying the current user of the mobile navigation device, the processing unit 211 can retrieve user-specific settings from the memory 213. Additionally or alternatively, it may also grant access to data files stored in the memory 213 and belonging to the current user. As these steps may be automatically performed at startup of the device 201, the device operates with the settings preferred by the current user without the user needing to perform any additional steps. Furthermore, the user can access his data files without having access to data files of other users. The memory 213 may comprise a hard drive or a flash memory or the like, and the user-specific parameters and data files may be stored on the same memory or in different memories.

[0037] It should be clear that the mobile navigation devices 101 and 201 may comprise further components that are common to mobile navigation devices, yet these components are not shown in Figs. 1 and 2 for clarity. In particular, they may comprise a GPS antenna, a navigational unit, a display, further input means, loudspeakers and the like.

[0038] Fig. 3 is a flow diagram of an embodiment of a method for enabling an operating mode of a mobile navigation device. In step 301, a person turns on the mobile navigation device. In the next step 302, an RFID reader comprised in the mobile navigation device emits an RF signal, preferably continuously. A person authorized to use the mobile navigation device will generally be in the possession of an appropriate transponder. In step 303, the transponder receives the RF signal emitted by the RFID reader. To receive the signal, the transponder has to be within a predetermined range. In response to receiving the RF signal, the transponder emits in step 304 an RF signal comprising identification information. The transponder may achieve this by modulating and back-reflecting the RF signal emitted by the RFID reader, or any other suitable way known to a person skilled in the art. The RF signal comprising the identification information is then received at the RFID reader in step 305. If

the transponder is out of range to receive the RF signal emitted by the RFID reader or to transmit the identification information to the RFID reader, the RFID reader may continue sending out an RF signal as in step 302, and a warning may be issued or the mobile navigation device may be shut down after a predetermined amount of time. In step 306, a theft protection unit checks the identification information received. In the case where the identification information is an identification number, the theft protection unit may compare this number to a list of identification numbers of transponders authorized to grant access to the mobile navigation device. It is checked in step 307 whether the identification information received is predetermined identification information, e.g. a number on said list. If that is the case, the operating mode of the mobile navigation device is enabled in step 308. If the identification information is not predetermined identification information, the transponder is not authorized to enable the operating mode, and accordingly, the RFID reader will continue to emit RF signals in step 302. This procedure may be continued until predetermined identification information is received or until a predetermined amount of time has passed, after which the mobile navigation device may again be deactivated or a warning may be issued. Using this method, the mobile navigation device is effectively protected against theft, as the operating mode is only enabled if the predetermined identification information is received, which is generally only the case if an authorized transponder is within range of the radio frequency identification reader.

[0039] Fig. 4 shows part of a flow diagram of another embodiment of a method of enabling an operating mode in a mobile navigational device. Step 401 can be executed after step 307 of Fig. 3, i.e. after it has been determined that the identification information received is predetermined identification information. The operating mode of the mobile navigation device is enabled in step 401, in which full functionality of the mobile navigation device is provided to a user. In step 402, the current user of the mobile navigation device is identified. This can be easily achieved if each user of the mobile navigation device possesses their own transponder comprising individual identification information, which is transmitted. In a next step 403 parameters specific to the current user are retrieved. As said before, these may be particular configuration parameters of the mobile navigation device or of an application running on said device. Parameters may also relate to the navigational functionality of the mobile navigation device and may as such comprise route or track information, location information and the like. Furthermore, access is enabled to data specific to the current user in step 404. Besides data files, such as music or image files, access may also be granted to address data of a personal address book and similar data relating to a particular user. Steps 403 and 404 can also comprise granting a particular user only limited access to the mobile navigation device, for example access to only particular applications. A mobile phone functionality of the mobile navigation device may for example be blocked for particular users.

[0040] While using the mobile navigation device, the user may make changes to the settings. He may thus store these user-specific settings in step 405, e.g. in form of a user profile comprising user-specific parameters. This profile may then be retrieved next time said user turns on the mobile navigation device and identifies himself using his RFID transponder. As can be seen, the above-described embodiment both provides an effective theft protection as well as a very convenient personalization of the mobile navigation device.

[0041] In some cases, more than one user possessing an authorized RFID transponder may be within range of the RFID reader of the mobile navigation device. The mobile navigation device may then start up in a default mode, meaning it does not load user-specific parameters, or it may provide the possibility of choosing which set of user-specific parameters to load at the start-up. The mobile navigation device may also comprise a button, e.g. a soft key, using which the current user can be easily selected. Furthermore, several anti-collision methods are known in the art for dealing with the case where multiple RFID transponders are within range of an RFID reader. These may be used with the above-described invention. The user, who is e.g. selected by pressing a soft key, may then have to enter a personal identification number code, e.g. a multi character code, in order to access the user-specific parameter and/or the user-specific data files.

[0042] As can be seen from the above description, the method and system of the present invention provide effective means to protect a mobile navigation device from theft. Furthermore, the system is very cost-efficient and can be easily integrated into a mobile navigation device. Furthermore, the system is very user-friendly, as the user has only to carry the transponder, which is generally very small and light-weight.

Claims

1. Theft protection system for an electronic device (101; 201) comprising

   - an electronic device (101; 201) comprising

     - a radio frequency identification unit (102; 202) emitting a radio frequency signal (105; 205) containing request information and
     - a theft protection unit (103; 204) enabling an operating mode of the electronic device (101; 201) upon reception of a signal (110; 210) containing predetermined identification information,

   and
   - at least one radio frequency identification trans-

ponder (107; 206),

wherein, when the radio frequency identification unit (102; 202) receives said signal (110; 210) containing predetermined identification information, which is emitted by said radio frequency identification transponder (107; 206) in response to receiving the radio frequency signal (105; 205) containing request information, the theft protection unit (103; 204) enables the operating mode of the electronic device (101; 201).

2. Theft protection system according to claim 1, **characterized in that** the at least one radio frequency identification transponder (107; 206) comprises a transponder which is powered by receiving a radio frequency signal from said radio frequency identification unit (102; 202).

3. Theft protection system according to claim 1 or 2, **characterized in that** the at least one radio frequency identification transponder (107; 206) comprises a power antenna (106; 207) and a condenser.

4. Theft protection system according to any of the preceding claims,
characterized in that the at least one radio frequency identification transponder (107; 206) comprises a battery powered transponder.

5. Theft protection system according to any of the preceding claims,
characterized in that the at least one radio frequency identification transponder (107; 206) comprises a transponder being mounted inside a vehicle.

6. Theft protection system according to any of the preceding claims,
characterized in that the at least one radio frequency identification transponder (107; 206) comprises a mobile transponder (206) being formed so as to be carried on a key ring.

7. Theft protection system according to any of the preceding claims,
characterized in that the identification information identifies a user of the electronic device (101; 201), wherein the electronic device (101; 201) is formed so as to operate in said operating mode taking into account data relating to the identified user.

8. Theft protection system according to any of the preceding claims,
characterized in that the electronic device (101; 201) is formed so that it retrieves user specific operating parameters in response to the radio frequency identification unit (102; 202) receiving a radio frequency signal (110; 210) containing predetermined identification information.

9. Theft protection system according to any of the preceding claims,
characterized in that the electronic device (101; 201) is formed so that it grants access to user specific data in response to the radio frequency identification unit (102; 202) receiving a radio frequency signal (110; 210) containing predetermined identification information.

10. Theft protection system according to any of the preceding claims,
characterized in that each transponder (107; 206) comprises an identification number, said identification number being transmitted as part of the identification information.

11. Theft protection system according to any of the preceding claims,
characterized in that the theft protection unit (103; 204) is formed so as to not enable or disable said operating mode if no signal comprising the predetermined identification information is received by the radio frequency identification unit (102; 202) at a start-up of the navigation device (101; 201) or a predetermined amount of time after start-up, respectively.

12. Theft protection system according to any of the preceding claims,
characterized by further comprising an indicator (212) being at least periodically activated while said operating mode is not enabled.

13. Theft protection system according to any of the preceding claims,
characterized in that the theft protection unit (103; 204) is formed so as to enable said operating mode in response to a predetermined character sequence being entered by means of an input unit (214).

14. Theft protection system according to any of the preceding claims,
characterized by further comprising a mobile communication unit which is formed so as to enable a tracking of the electronic device.

15. Theft protection system according to any of the preceding claims,
characterized in that the electronic device is a mobile navigation device.

16. Method of enabling an operating mode of an electronic device (101; 201), comprising the following steps:

- emitting a radio frequency signal (105; 205)

containing request information by a radio frequency identification unit (102; 202) provided in the electronic device (101; 201),
- receiving, at a transponder (107; 206), said radio frequency signal (105; 205) containing request information and transmitting back to the radio frequency identification unit (102; 202) a signal (110; 210) containing predetermined identification information,
- wherein, when said signal (110; 210) containing predetermined identification information is received by the radio frequency identification unit (102; 202), a theft protection unit (103; 204) provided in the electronic device (101; 201) enables the operating mode of the electronic device (101; 201).

17. Method according to claim 16, **characterized by** further comprising the steps of identifying a user of said electronic device (101; 201) by means of said identification information and operating said mobile electronic (101; 201) in said operating mode taking into account data relating to the identified user.

18. Method according to claim 16 or 17, **characterized in that** said transponder (107; 206) is mounted inside a vehicle or formed so as to be carried on a key ring.

Amended claims in accordance with Rule 137(2) EPC.

1. Theft protection system for an electronic device (101; 201) comprising

- an electronic device (101; 201) comprising

  - a radio frequency identification unit (102; 202) emitting a radio frequency signal (105; 205) containing request information and
  - a theft protection unit (103; 204) enabling an operating mode of the electronic device (101; 201) upon reception of a signal (110; 210) containing predetermined identification information,

and
- at least one radio frequency identification transponder (107; 206),

wherein, when the radio frequency identification unit (102; 202) receives said signal (110; 210) containing predetermined identification information, which is emitted by said radio frequency identification transponder (107; 206) in response to receiving the radio frequency signal (105; 205) containing request information, the theft protection unit (103; 204) enables the operating mode of the electronic device (101; 201),
characterized in that
the at least one radio frequency identification transponder (107; 206) comprises a transponder being mounted inside a vehicle.

2. Theft protection system according to claim 1, **characterized in that** the at least one radio frequency identification transponder (107; 206) comprises a transponder which is powered by receiving a radio frequency signal from said radio frequency identification unit (102; 202).

3. Theft protection system according to claim 1 or 2, **characterized in that** the at least one radio frequency identification transponder (107; 206) comprises a power antenna (106; 207) and a condenser.

4. Theft protection system according to any of the preceding claims, **characterized in that** the at least one radio frequency identification transponder (107; 206) comprises a battery powered transponder.

5. Theft protection system according to any of the preceding claims, **characterized in that** the at least one radio frequency identification transponder (107; 206) comprises a mobile transponder (206) being formed so as to be carried on a key ring.

6. Theft protection system according to any of the preceding claims, **characterized in that** the identification information identifies a user of the electronic device (101; 201), wherein the electronic device (101; 201) is formed so as to operate in said operating mode taking into account data relating to the identified user.

7. Theft protection system according to any of the preceding claims, **characterized in that** the electronic device (101; 201) is formed so that it retrieves user specific operating parameters in response to the radio frequency identification unit (102; 202) receiving a radio frequency signal (110; 210) containing predetermined identification information.

8. Theft protection system according to any of the preceding claims, **characterized in that** the electronic device (101; 201) is formed so that it grants access to user specific data in response to the radio frequency identification unit (102; 202) receiving a radio frequency signal (110; 210) containing predetermined identification information.

9. Theft protection system according to any of the preceding claims, **characterized in that** each transponder (107; 206) comprises an identification number, said identification number being transmitted as part of the identification information.

10. Theft protection system according to any of the preceding claims, **characterized in that** the theft protection unit (103; 204) is formed so as to not enable or disable said operating mode if no signal comprising the predetermined identification information is received by the radio frequency identification unit (102; 202) at a start-up of the navigation device (101; 201) or a predetermined amount of time after start-up, respectively.

11. Theft protection system according to any of the preceding claims, **characterized by** further comprising an indicator (212) being at least periodically activated while said operating mode is not enabled.

12. Theft protection system according to any of the preceding claims, **characterized in that** the theft protection unit (103; 204) is formed so as to enable said operating mode in response to a predetermined character sequence being entered by means of an input unit (214).

13. Theft protection system according to any of the preceding claims, **characterized by** further comprising a mobile communication unit which is formed so as to enable a tracking of the electronic device.

14. Theft protection system according to any of the preceding claims, **characterized in that** the electronic device is a mobile navigation device.

15. Method of enabling an operating mode of an electronic device (101; 201), comprising the following steps:

- emitting a radio frequency signal (105; 205) containing request information by a radio frequency identification unit (102; 202) provided in the electronic device (101; 201),
- receiving, at a transponder (107; 206), said radio frequency signal (105; 205) containing request information and transmitting back to the radio frequency identification unit (102; 202) a signal (110; 210) containing predetermined identification information,
- wherein, when said signal (110; 210) containing predetermined identification information is received by the radio frequency identification unit (102; 202), a theft protection unit (103; 204) provided in the electronic device (101; 201) enables the operating mode of the electronic device (101; 201),

characterized in that
said transponder (107; 206) is mounted inside a vehicle.

16. Method according to claim 15, **characterized by** further comprising the steps of identifying a user of said electronic device (101; 201) by means of said identification information and operating said mobile electronic (101; 201) in said operating mode taking into account data relating to the identified user.

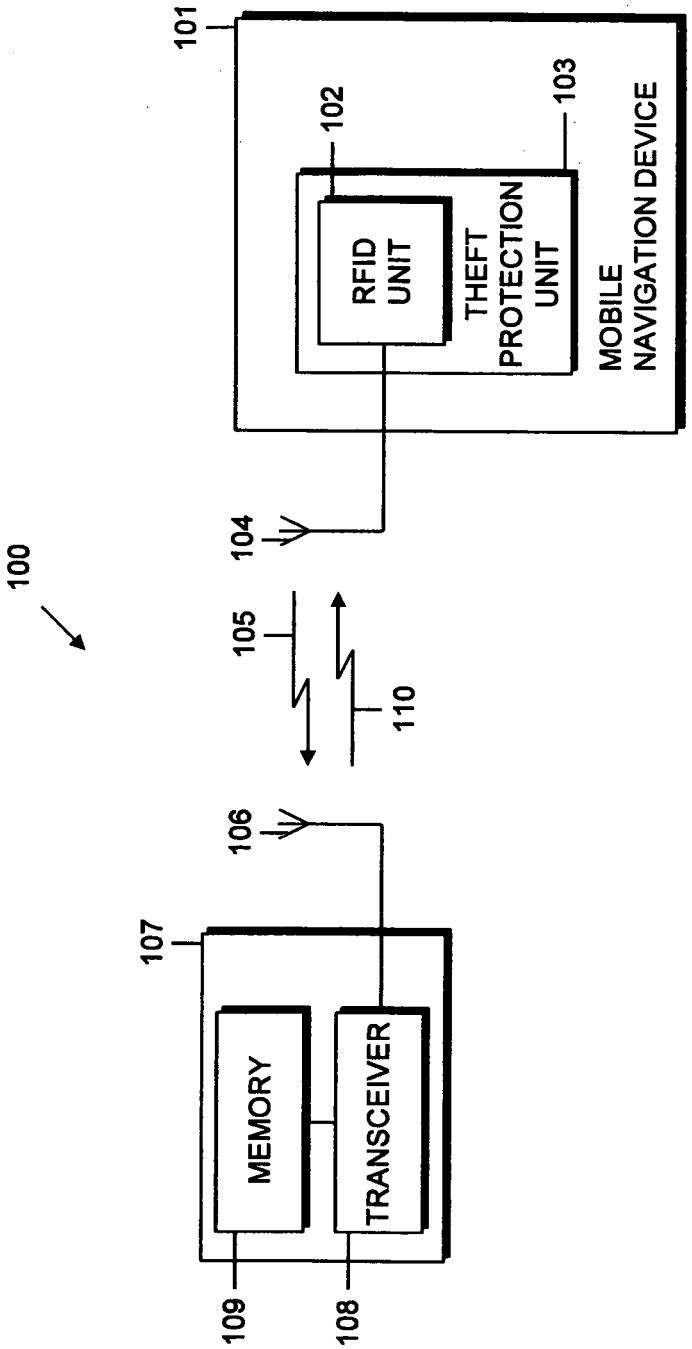
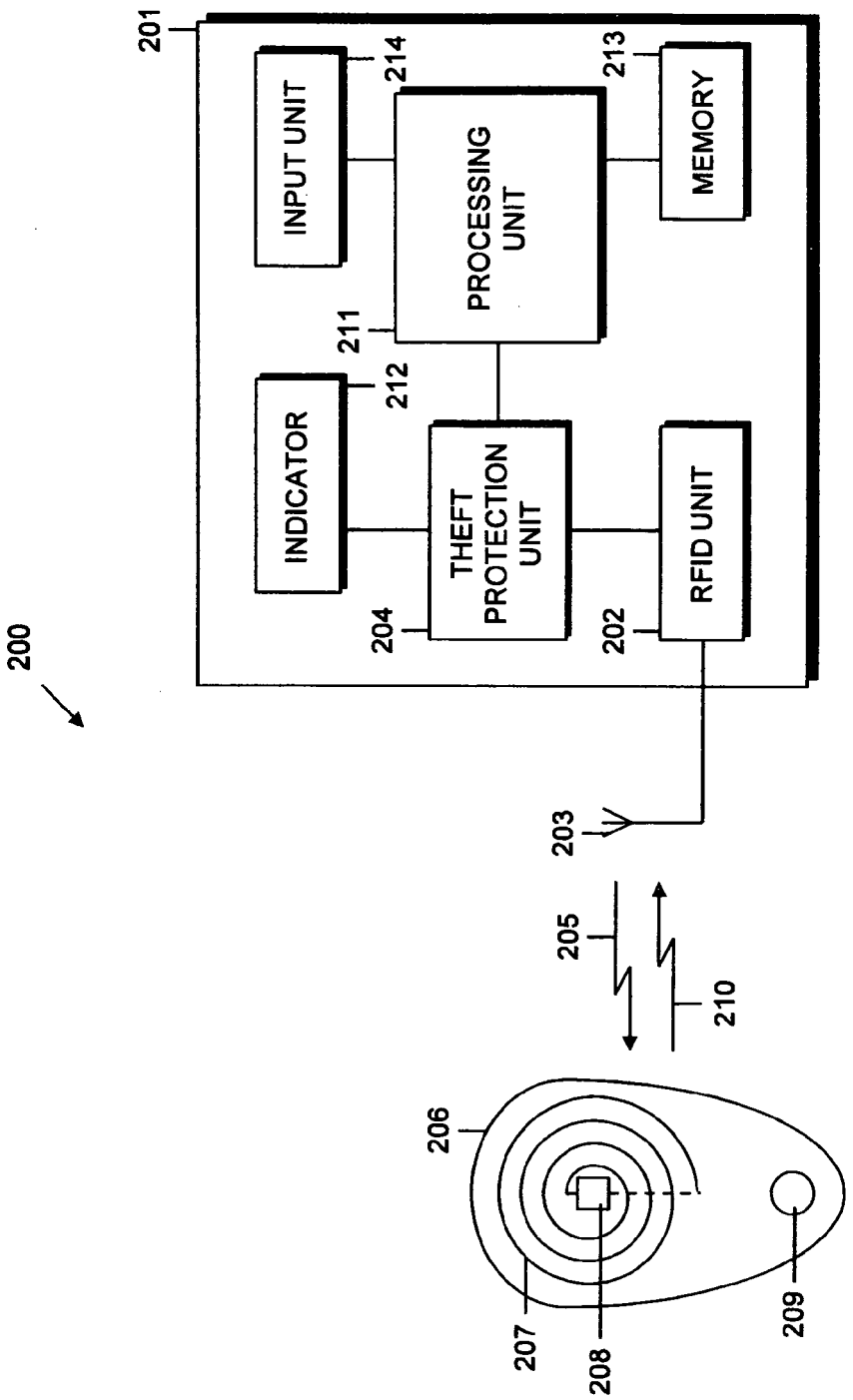

100
101
102
103
RFID UNIT
THEFT PROTECTION UNIT
MOBILE NAVIGATION DEVICE
104
105
110
106
107
MEMORY
TRANSCEIVER
109
108

FIG. 1

FIG. 2


200
201
INPUT UNIT
214
PROCESSING UNIT
213
MEMORY
211
INDICATOR
212
THEFT PROTECTION UNIT
RFID UNIT
204
202
203
205
210
206
207
208
209

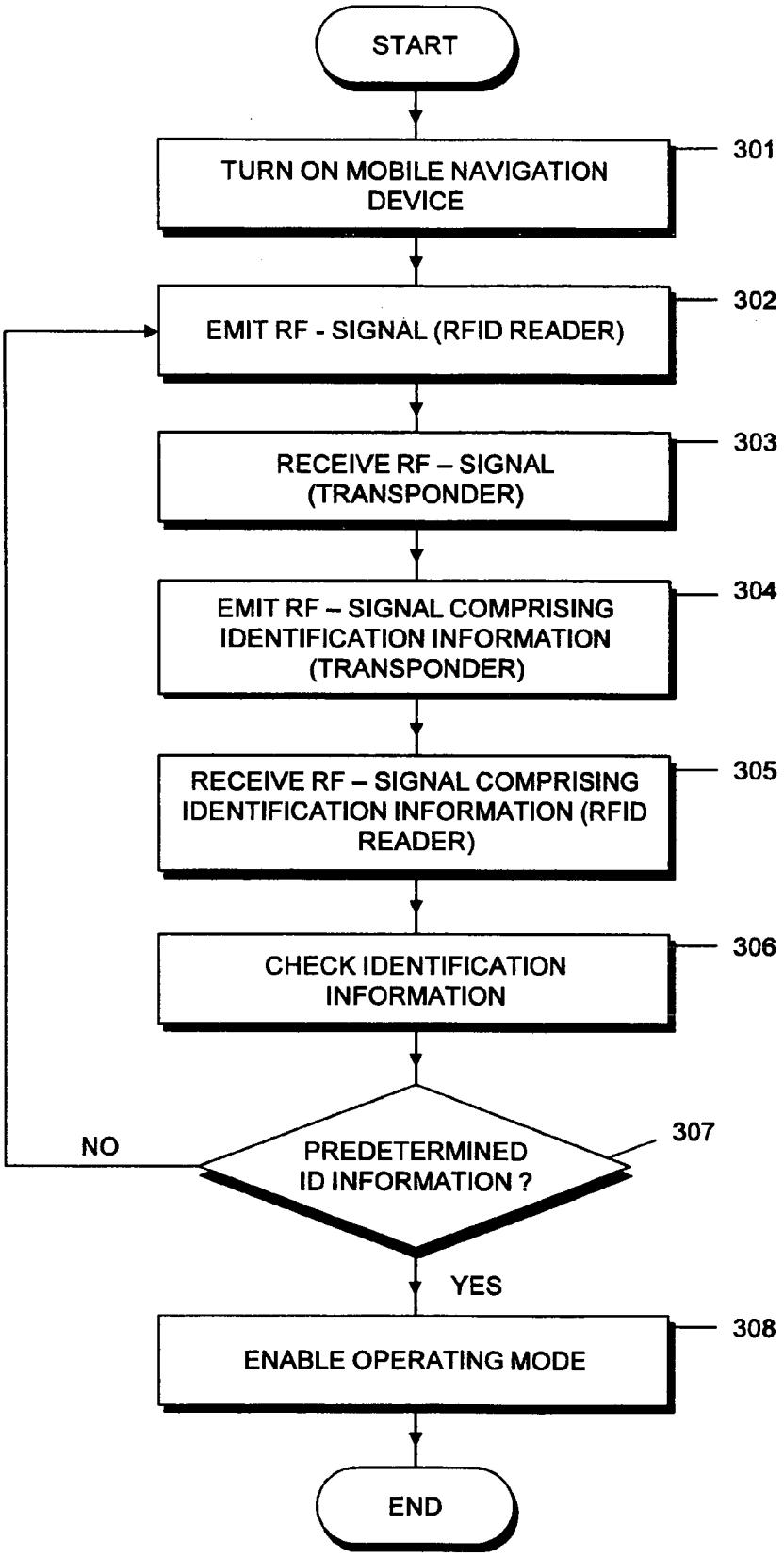

START
TURN ON MOBILE NAVIGATION DEVICE
301
EMIT RF - SIGNAL (RFID READER)
302
RECEIVE RF – SIGNAL (TRANSPONDER)
303
EMIT RF – SIGNAL COMPRISING IDENTIFICATION INFORMATION (TRANSPONDER)
304
RECEIVE RF – SIGNAL COMPRISING IDENTIFICATION INFORMATION (RFID READER)
305
CHECK IDENTIFICATION INFORMATION
306
PREDETERMINED ID INFORMATION ?
307
NO
YES
ENABLE OPERATING MODE
308
END

FIG. 3

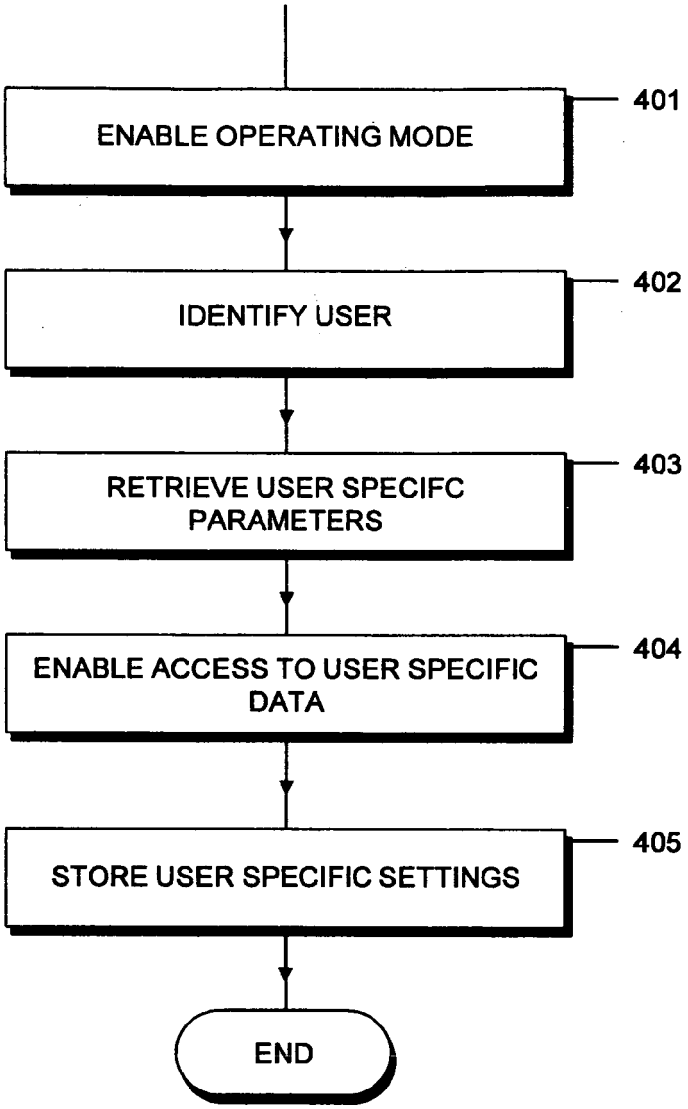

ENABLE OPERATING MODE
401
IDENTIFY USER
402
RETRIEVE USER SPECIFC PARAMETERS
403
ENABLE ACCESS TO USER SPECIFIC DATA
404
STORE USER SPECIFIC SETTINGS
405
END

FIG. 4

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 07 02 4625

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	EP 1 164 555 A (NOKIA MOBILE PHONES LTD [FI] NOKIA CORP [FI]) 19 December 2001 (2001-12-19) * paragraph [0016] - paragraph [0055] *	1-18	INV. G08B13/14
X	WO 2004/112363 A (PHILIPS INTELLECTUAL PROPERTY [DE]; KONINKL PHILIPS ELECTRONICS NV [NL) 23 December 2004 (2004-12-23) * page 3, line 14 - page 8, line 18 *	1-18	
X	DE 201 12 099 U1 (MAYR ROLAND [AT]; THATER DIRK [DE]) 18 October 2001 (2001-10-18) * page 6, line 4 - page 8, line 23 *	1-18	
X	DE 100 63 381 A1 (T MOBILE DEUTSCHLAND GMBH [DE]) 4 July 2002 (2002-07-04) * paragraph [0017] - paragraph [0035] *	1-18	
A	WO 02/48979 A (SIEMENS AG [DE]; NEUMANN PETER [DE]) 20 June 2002 (2002-06-20) * abstract *	1-18	
			TECHNICAL FIELDS SEARCHED (IPC)
			G08B

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	30 May 2008	La Gioia, Cosimo

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 07 02 4625

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

30-05-2008

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1164555 A	19-12-2001	AT 312390 T	15-12-2005
		DE 60115542 T2	10-08-2006
		GB 2363504 A	19-12-2001
		JP 2002057789 A	22-02-2002
		US 2001052846 A1	20-12-2001
WO 2004112363 A	23-12-2004	CN 1810016 A	26-07-2006
		JP 2006527953 T	07-12-2006
		KR 20060018893 A	02-03-2006
		US 2006148449 A1	06-07-2006
DE 20112099 U1	18-10-2001	NONE	
DE 10063381 A1	04-07-2002	NONE	
WO 0248979 A	20-06-2002	DE 10062378 A1	20-06-2002

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82