

A method for electronically coupling a mobile terminal with a housing configured to receive the mobile terminal, related device and housing

5 The present invention relates to a method for electronically coupling a mobile terminal with a housing configured to receive the mobile terminal.

The invention also relates to a computer program comprising software instructions which, when executed by a computer, implement such a method.

The invention also relates to a device for electronically coupling a mobile terminal with a housing configured to receive the mobile terminal.

10 The invention also relates to a housing configured to receive a mobile terminal.

The invention relates to the field of telecommunications in general and, more particularly, to the field of information security, in particular during the implementation of security or surveillance operations.

15 For these operations, high levels of assurance in operational security and computer security are required, which lead to communications architectures, also known as Multiple Independent Levels of Security (MILS) architectures, wherein subsets of hardware and software resources are strictly separated, and wherein the communication flow is controlled or encrypted. Such architectures require heavy investments as a function of their missions,
20 and are developed according to their own life cycle.

At the same time, the professional use of mobile devices has evolved to keep pace with the developments of COTS (Commercial Off-The-Shelf) wireless mobile terminals for personal use. In fact, mobile terminals are experiencing even shorter life cycles compared to radio infrastructures, in particular because of ongoing improvements in terms of ergonomics,
25 and because of the continuous improvement of the efficiency of the man-machine interface.

The use of BYOD (Bring Your Own Device) personal terminals in the context of professional activities has therefore developed. To mitigate possible security breaches occasioned by the use of personal terminals in a professional context, hardware management approaches have been introduced, for example the COPE (Corporate Owned Personally
30 Enabled) approach aims to control (in particular by Secure Boot) and administer COTS terminals provided by a company in accordance with the company's MDM (Mobile Device Management) policy while allowing staff.

However, these hardware-based management approaches for COTS mobile terminals provided by companies are implemented in a centralized manner, which thus leaves little autonomy to users, and does not allow local adaptation of the security rules to unique and/or transient situations.

5

The object of the invention is thus to propose a method of communication for a mobile terminal for professional and personnel use which offers more autonomy in terms of radio-communication security while optimizing the ergonomics and customizing use without, however, deviating from the security policy to be applied.

10

To this end, the subject-matter of the invention is a method for electronically coupling a mobile terminal with a housing configured to receive the mobile terminal, the mobile terminal comprising a first radio-communication module, the housing comprising a second radio-communication module and an electronic coupling device configured to implement the method,

15

the method comprising at least:

- inhibition of the operation of the first radio-communication module, wherein the inhibition is triggered when the mobile terminal is secured to the housing, and
- activation of the second radio-communication module.

20

The electronic coupling method according to the invention then makes it possible, on the one hand, to separate the use, for example professional, and the life cycle of the housing configured to receive a mobile terminal, and, on the other hand, the use, for example personal, and the life cycle of the mobile terminal as such.

25

These two elements, i.e. the mobile terminal and the housing, form, once secured together, a new communicating object in accordance with predetermined communication rules and associated with the second radio-communication module by inhibiting the first radio-communication module of the mobile terminal dedicated to a first use (for example personal), and activation of the second radio-communication module that is integrated in the housing and is dedicated to a second use (for example professional) that is distinct from the first use.

30

In what follows, "housing" means a "shell" or a "casing" that is intended to accommodate a mobile terminal.

In other words, the coupling method according to the invention allows the housing to communicate in a secure mode while taking advantage of the ergonomics of use and the

man-machine interface of the mobile terminal 12 to which the housing is secured upon coupling.

According to other advantageous aspects of the invention, the electronic coupling method comprises one or more of the following features, taken separately or in any technically feasible combination:

the method further comprises:

- backup in a first dedicated memory space of the electronic coupling device, of at least one item of information that is representative of the configuration of the mobile terminal prior to the inhibition;

- transmission of at least one command for deleting any information stored by the mobile terminal during the period of connection of the mobile terminal to the housing;

and prior to separation of the mobile terminal from the housing:

- downloading to the mobile terminal by the electronic coupling device of the information that is representative of the configuration of the mobile terminal, prior to the inhibition, and
- deactivation of the second radio-communication module;

the activation of the operation of the second radio-communication module is conditioned by the receipt and verification of at least one item of authentication data of the user entered via an input interface of the mobile terminal;

the coupling method further comprises, prior to the activation of the second radio-communication module, downloading to the mobile terminal by the electronic coupling device of at least one software tool that is configured to:

- check input and output data of the mobile terminal during the activation of the second radio-communication module, and/or
- check the integrity of the mobile terminal, and/or
- detect the separation of the mobile terminal from the housing;

the activation of the second radio-communication module comprises an activation of a specific communication mode that is selected as a function of at least one parameter that is representative of a predetermined use of the second radio-communication module, wherein the at least one parameter was previously stored in a second dedicated and secure memory space that is accessible by the electronic coupling device;

- the coupling method further comprises a restitution that is initiated by the electronic coupling device of an item of information that is representative of the activation of the second radio-communication module, via a restitution module of the mobile terminal.

5 The invention also relates to a computer program comprising software instructions which, when executed by a computer, implement an electronic coupling method as defined above.

 The invention also relates to a device for electronically coupling a mobile terminal with a housing that is configured to receive the mobile terminal, the mobile terminal
10 comprising a first radio-communication module, the housing comprising a second radio-communication module, said device being configured to implement the electronic coupling method according to the invention.

 The invention also relates to a housing that is configured to receive a mobile terminal comprising at least one radio-communication module and the aforementioned
15 electronic coupling device.

 In other words, the present invention relates to a communicating housing (or shell) adapted to be secured to a mobile terminal, wherein it inhibits the communication module while taking advantage of its ergonomics and its man-machine interface when it is secured.

 According to other advantageous aspects of the invention, the housing comprises
20 one or more of the following features, taken separately or in any technically feasible combination:

- the radio-communication module of the housing is a secure radio-communication module;
- the housing further comprises an electromagnetic shield that is adapted to
25 extend over at least the largest reception area of the mobile terminal;
- the housing is made of a material that is obtained by nano-reinforced plastic processing.

 These features and advantages of the invention will become clearer upon reading the description which follows, given solely by way of a non-limiting example, and with
30 reference to the appended drawings, wherein:

 Fig. 1 shows a schematic representation of the coupling (i.e. assembly) of a mobile terminal with a housing configured to receive the mobile terminal; F

Fig. 2 shows a schematic representation of the electronic layer of the housing configured to receive this mobile terminal according to the invention;

Fig. 3 shows a schematic representation of the integrated coupling device within the electronic layer of the housing according to the invention;

5 Fig. 4 shows a flowchart of an electronic coupling method according to the invention.

Conventionally in the present application, the terms "substantially equal to" and "approximately" each express a relationship of equality plus or minus 10%.

10 Fig. 1 shows the assembly 10 of the mobile terminal 12 and the housing 14 that is configured to receive the former. In other words, a new communicating object 10 is obtained by coupling the mobile terminal 12 with the housing 14.

The mobile terminal 12 is manufactured in series (COTS - Commercial Off-the-shelf), and is, for example, a smartphone managed by an operating system, such as the Android operating system from Google®, or, as another example, a touch tablet. The mobile
15 terminal 12 comprises a first radio-communication module R_1 . Such a radio-communication module comprises, for example, a radio antenna and a radio transceiver (not shown). The transceiver of the mobile terminal 12 is connected to an information processing unit (not shown) formed, for example, by a first processor and a first memory associated with the first processor.

20 Moreover, such a mobile terminal 12 comprises a keyboard, a screen (for example a touch screen), and, for example, a digital camera (not shown).

The housing 14 comprises a cavity 16 that is intended to receive and protect at least two faces of the mobile terminal 12 in order to form the new communicating object 10 that results from the coupling of the mobile terminal 12 and the housing 14. In other words, the
25 height of the cavity 16 is substantially equal to the thickness of the mobile terminal 12.

Moreover, the housing 14 also comprises a communicating part 18 comprising, in particular, a second radio-communication module R_2 . In other words, the housing 14 is a smart shell.

30 Preferentially and subsequently, the second radio-communication module R_2 is a secure radio-communication module. In other words, the data exchanged via the second radio-communication module R_2 are inviolable and are processed according to predetermined information security rules.

According to a particular aspect, as shown in Fig. 1, the communicating part 18 and the cavity 16 are secured along a length of the housing so that the housing has an L-shape.

The housing 14 has, for example, a functional architecture (i.e. software and hardware) in dedicated layers distributed within the cavity and/or within the communicating part 18. In the example of Fig. 1, the architecture is, for example, formed by four layers 20, 22, 24 and 26.

The first layer 20 is, for example, configured to act as an electromagnetic radio-communication shield for the communicating object 10 resulting from the coupling of the mobile terminal 12 and the housing 14.

To do this, this first layer 20 is, for example, formed by a metal shield that is adapted to extend at least over the largest reception area, or on all four sides of the cavity 16 of the housing 14 that receives the mobile terminal 12. Such a metal shield is designed to protect in the sense of a faraday cage, the second secure radio-communication module R_2 from electrical and subsidiary electromagnetic nuisances produced by the first radio module R_1 of the terminal. In other words, the electromagnetic shield 20 is configured to inhibit, scramble, quarantine or degrade the communications transmitted by the first radio-communication module R_1 of the mobile terminal 12, while allowing the second secure radio-communication module R_2 to transmit correctly.

According to one variant (not shown), the communicating part 18 and the cavity 16 are stacked vertically, so that:

- the electromagnetic shield 20 is positioned under the cavity 16, and therefore under the first radio communication module R_1 of the mobile terminal 12 whose protective shield degrades or even inhibits the communication capacity,
- the second secure radio-communication module R_2 of the housing 14 is located outside the electromagnetic protection conferred by the electromagnetic shield 20, so that the communication capacity of the second secure radio-communication module R_2 is not impaired.

The communicating part 18 comprises at least one software and hardware (i.e. functional) layer dedicated to the purely electronic aspect of the secure radio-communication module R_2 , while the software and hardware (i.e. functional) layer 24 is dedicated to the antennal aspect, and, more particularly, to one or more multiband antennas. The software and hardware (i.e. functional) layer 26 is, for its part, dedicated to the energy supply, for example in the form of a battery.

According to another variant (not shown), the housing forms an envelope in order to partially or completely cover each face of the mobile terminal 12. According to this other variant, the arrangement of the layers 20, 22, 24 and 26 is also designed to degrade or inhibit the operation of the first radio-communication module R_1 of the mobile terminal 12, while
5 allowing the second secure radio-communication module R_2 of the housing 14 to function properly.

The housing 14 is formed by a material obtained by nano-reinforced plastic processing. For example, the material used to form the housing 14 is a polyamide reinforced with carbon black.

10 Three-dimensional printing (3D) may, for example, be used to form a completely suitable housing 14 (i.e. a housing perfectly adapted to the dimensions of the mobile terminal 12). Thus, the housing 14 according to the present invention, may be produced in different sizes and/or shapes (i.e. polymorphic: adapted to house various types (i.e. models) of mobile terminals 12).

15 In Fig. 1, the housing 14 also has a notch 27 to facilitate the insertion or removal of the mobile terminal 12 in the cavity 16 of the housing 14.

The electronic elements of the software layer 22 are now described with reference to Fig. 2.

Structurally, the software and hardware (i.e. functional) layer 22 comprises, in
20 particular, a plurality of dedicated and distinct electronic stages.

The electronic first stage 28 is a hypervision stage. The hypervisor 28 is a virtualization platform allowing several operating systems to work on the same physical machine at the same time, i.e. the housing 14 or, preferably, the communicating object 10 resulting from the coupling of the mobile terminal 12 with the housing 14. In other words, the
25 hypervisor 28 acts as a processor manager for the electronic operation of the housing 14 (i.e. of the shell).

The hypervisor 28 is, for example, of the PikeOS type from SYSGO AG® having at least EAL5+ level certification.

According to the present invention, the hypervisor 28 controls an electronic coupling
30 device 30 configured to electronically couple the mobile terminal 12 and the housing 14 once these two elements are mechanically and/or electrically connected to one another, and, in particular, to couple their radio-communication modules R_1 and R_2 respectively.

The mechanical and/or electrical secure coupling of the mobile terminal 12 and the housing 14 consists of inserting the mobile terminal 12 in the cavity 16 of the housing 14 provided for this purpose, and, if necessary, connecting the mobile terminal 12 to the housing 14 by means of a wired link, for example a 32 USB (Universal Serial Bus) link.

5 To do this, the housing 14 has, for example, a USB connector (not shown) located in the cavity 16 that engages with the USB connector of the mobile terminal 12.

In what follows, "USB" means the different USB versions that are adapted to be implemented according to the type of mobile terminal 12 used, i.e. USB 1.0, USB 1.1, USB 2.0, USB 3.0, USB 3.1, etc.

10 Such a link 32 between the housing 14 and the mobile terminal is detected by the hypervisor 28 which activates the electronic coupling device 30.

Alternatively, the link 32 may be an electrical connection and the housing 14, like the mobile terminal 12, may respectively comprise an electrical contact area (not shown), so that the insertion of the mobile terminal 12 into the housing 14 allows the establishment of an
15 electrical contact (i.e. the closing an electrical circuit previously in open circuit state) between the electrical contact area of the housing 14 and the electrical contact zone of the terminal 12.

The electrical contact thus established during the securing of the terminal 12 to the housing 14 makes it possible to trigger the electronic coupling device 30.

The electronic coupling device 30 is, moreover, connected by a link 34 to the battery
20 26.

In addition, the electronic coupling device 30 of the hypervisor 28 comprises an interface 36 with a security device 38 managed by a trusted third party 40, for example a radio-communication operator and/or a service provider.

Such a security device 38 is, for example, a chip comprising a microcontroller and
25 memory. Such a chip corresponds, for example, to a UICC (UMTS Integrated Circuit Card), also referred to as a SIM card (Subscriber Identity Module) or a USIM (Universal Subscriber Identity Module) card.

In particular, the security device 38 is designed to secure the radio-communications transmitted by the second secure radio-communication module R_2 of the housing 14 in
30 accordance with the security rules and services defined by the trusted third party 40.

For example, the security device 38 enables access to the Eiji service, while the trusted third party 40 might be Thales®, which offers a high-speed, resilient and secure

communication solution for operating and exchanging data safely in a context of multiple threats.

Via such an Eiji service, the trusted third party 40 is able, in particular, to download to the security device 38 at least one representative parameter of a predetermined use of the
5 second secure radio-communication module R_2 as a function of the mission or the profile of the user of the housing 14 and the mobile terminal 12.

The electronic coupling device 30 also has an exchange interface 42 with the second secure radio-communication module R_2 of the housing 14.

Such a second secure radio-communication module R_2 is integrated in a second
10 dedicated electronic stage of the housing 14. The second secure radio-communication module R_2 comprises a waveform manager module 44 capable of communicating data according to a mode of communication that is specifically selected from a plurality of available communication modes respectively corresponding to the implementation of specific standards and/or the use of dedicated and secure frequency bands.

15 To implement such a selection, the waveform manager module 44 is controlled by the electronic coupling device 30 via the interface 42.

In order to transmit data conforming to each communication mode, the secure radio-communication module R_2 in fact comprises different types of dedicated secure radio-communication transceivers 46, 47, 48, 50.

20 For example, the secure radio-communication module R_2 is designed to provide secure access to an LTE network and comprises for this purpose, a secure LTE transceiver 46, for example of the TWS8100 type developed by Thales®.

In Fig. 2, the secure radio-communication module R_2 is also designed to provide, according to another example, a secure access to a UHF (Ultra-High Frequency) network via
25 a dedicated transceiver 47 of the SDR (Software Defined Radio) type and secured according to the CNR (Combat Net Radio) standard.

The secure radio-communication module R_2 also comprises, according to another example, a transceiver 48 that is able to exchange data in a secure manner according to CNR (Combat Net Radio) in accordance with the Bluetooth® standard.

30 The second secure radio-communication module R_2 also comprises other types of transceiver 50 selected by the waveform manager module 44, which is itself controlled by the coupling device 30 according to the invention.

The coupling device 30 is, in fact, designed to read in the memory of the security device 38 at least one parameter that is representative of a predetermined use (i.e. mission) of the second secure radio-communication module R_2 . Such a parameter makes it possible to select the transceiver of the second secure radio-communication module R_2 that is adapted to the specific communication mode corresponding to the mission of the user of the communicating object 10 resulting from the coupling of the mobile terminal 12 and the housing 14.

Each of the different transceivers of the second secure radio-communication module R_2 may be connected to the software and hardware (i.e. functional) layer 24 that is dedicated to the antenna aspect, and comprises one or more selected multiband antennas of the same the type of transceiver, as a function of the specific communication mode associated with the user's current mission.

The structure of the electronic coupling device 30 according to the invention is now described with the aid of Fig. 3.

According to the example of Fig. 3, the electronic coupling device 30 firstly comprises a switch 52 for the operating mode of the housing 14.

Such a switch 52 is designed to detect the establishment of the wired link 32 (i.e. the electrical contact or the USB link) between the mobile terminal 12 and the housing 14, and to trigger respectively, as a function of the positive or negative result of this detection, a "coupled" mode of operation MC of the housing 14 and a "decoupled" operating mode MD of the housing 14, or even a transition operating mode MT between the coupled operation mode and the decoupled operating mode. In addition, the switch 52 makes it possible to establish, for the "coupled" operating mode MC, a physical path, exclusive of the other physical paths associated with the other modes of operation, between the mobile terminal 12 and a memory space of the housing 14 that is dedicated to the storage of at least one item of information that is representative of the configuration of the mobile terminal 12, prior to the electronic coupling with the housing 14.

The electronic coupling device 30 further comprises a module 54 for management of the decoupled MD, coupled MC, and transition MT, modes of operation of the housing 14.

When the mobile terminal 12 is secured to the housing 14 (i.e. when the switch detects the establishment of the wired link 32), such an operating mode management module 54 is able to handle the reception of an NMI 51 (Non-Maskable Interrupt) that is generated

automatically by the switch 52 in order to switch from the decoupled mode MD (via the transition mode MT) to the coupled mode MC as shown in Fig. 3.

Conversely, during the separation (untimely, or at the end of the mission) of the mobile terminal 12 from the housing 14 (i.e. the switch detects the disconnection of the wired link 32), such an operating mode management module 54 is adapted to manage the reception of an NMI 51 (Non-Maskable Interrupt) that is generated automatically by the switch 52 in order to switch from the coupled mode MC (via the transition mode MT) to the decoupled mode MD.

The operating mode management module 54 is also designed to be connected to the modules 56, 60, 62, 64 and 66 following the electronic coupling device 30 as described below.

The electronic coupling device 30 also comprises a module 56 comprising, in particular, at least one or more diodes whose blocking or passing state is intended to block or pass the signal leaving a filter 58 and applied to a radio-communication flow received by the second secure radio-communication module R_2 . Such a filter makes it possible to protect the second secure radio-communication module R_2 of the housing 14 from any communication flows associated with the mobile terminal 12.

The electronic coupling device 30 further comprises a first controller 60 of the telecommunications services which the second secure radio-communication module R_2 is authorized to access. Such a service controller 60 provides functionalities enabling resilient access to secure networks by multi-path transmission, in particular by applying an IPSEC (Internet Protocol Security) secure communication protocol.

The electronic coupling device 30 also comprises a second controller 62 connected to the security device 38 in order to apply the security rules associated with the specific communication mode defined by the trusted third party 40.

The electronic coupling device 30 also comprises at least two memory spaces 64 and 66 dedicated and isolated from each other.

A memory space 64 is, for example, dedicated to the storage of a software tool (micro kernel of operating system) configured to be downloaded into the memory of the mobile terminal 12 in order to:

- check the input and output data of the mobile terminal during the activation of the second secure radio-communication module R_2 , and/or
- check the integrity of the mobile terminal 12, and/or

- detect a separation of the mobile terminal 12 from the housing 14.

The other memory space 66 is, for example, dedicated to the storage of at least one item of information that is representative of the configuration of the mobile terminal 12 prior to the electronic coupling with the housing 14, and therefore prior to the inhibition of the first
5 radio-communication module R_1 of the mobile terminal 12.

According to one aspect (not shown), the memory space 66 is designed to prevent the disconnection of the housing 14 from the mobile terminal 12 until it is first emptied in order to reload this information that is representative of the configuration of the mobile terminal prior to uncoupling as described below in connection with the description of the operation of the
10 coupling device 30.

Optionally, the coupling device may comprise an authentication module (not shown) adapted to be connected via the link 32 to the man-machine interface (i.e. the input and output interface) of the mobile terminal 12 when the mobile terminal 12 is connected to the housing 14. Such an authentication module is capable of sending an authentication request
15 restituted to the user of the mobile terminal 12 via the interface.

The hypervisor 28 controls all the constituent modules of the electronic coupling device 30 in accordance with a Multiple Independent Levels of Security (MILS) architecture 68, wherein subsets of hardware and software resources are strictly separated, and wherein the communication flow is controlled or encrypted.

20 The operation of the electronic coupling device 30 according to the invention is now described with the aid of Fig. 4 which shows a flowchart of the method 70 according to the invention for the electronic coupling a mobile terminal 12 with a housing 14 configured to receive the mobile terminal.

The method 70 comprises, in particular, two phases, i.e. a first phase 72 for
25 coupling preparation and a second phase 74 for preparation for electronic decoupling of the mobile terminal 12 from the housing 14. Each of these phases 72 and 74 comprises a set of steps that are implemented automatically by the electronic coupling device 30 according to the invention.

The first coupling preparation phase 72 firstly comprises, according to the example
30 shown in Fig. 4, a back-up step 76, in a first dedicated memory space 66 of the electronic coupling device, at least one representative item of information, wherein the configuration of the mobile terminal prior to the inhibition of the first radio-communication module R_1 of the mobile terminal 12.

Such a step 76 is, in particular, triggered once the switch 52 detects the establishment of the link 32 between the housing 14 and the terminal 12. In other words, during this step, the current information contained in the memory of the mobile terminal 12 is saved in the memory location 66 of the housing 14 (i.e. the shell), wherein this memory location 66 is isolated from other locations via the hypervisor 28 of the housing 14 and which is dedicated security software (PikeOS®).

In the next step 78, the electronic coupling device 30 implements the downloading to the mobile terminal 12, of at least one software tool (kernel) configured to:

- check the input and output data of the mobile terminal during the activation of the second secure radio-communication module, and/or
- check the integrity of the mobile terminal, and/or
- detect a disconnection of the mobile terminal from the housing.

In other words, the shell 14 downloads to the mobile terminal 12 a set of software (kernel) which, on the one hand, is designed to disable the first radio-communication module R_1 of the mobile terminal 12, and, on the other hand, is designed to monitor the inadvertent disconnection (intentional or accidental) of the terminal of the shell 14.

Once this downloading 78 has been performed, the step 80 for inhibiting the operation of the first radio-communication module R_1 is implemented.

Depending on the type of mobile terminal 12, it is possible that the action of the set of software (kernel) downloaded by the electronic coupling device 30 to the mobile terminal 12 is incomplete with respect to the invalidation of the communication capabilities of the radio-communication module R_1 . To remedy and complete this action, the first layer 20 of the housing 14 previously described and designed to play the role of an electromagnetic shield can inhibit, scramble, quarantine, or degrade the communications issued by the first radio-communication module R_1 of the mobile terminal 12, while allowing the second secure radio-communication module R_2 to transmit correctly.

According to one particular aspect, a step 82 for receiving and verifying at least one user authentication data input via an input interface of the mobile terminal is implemented. To do this, the software tool (kernel) downloaded to the mobile terminal 12 and the coupling device 30 of the housing 14 (i.e. shell) exchanges information that is intended to verify the integrity of the mobile terminal 12 coupled to the shell 14 and/or to verify the integrity of its user.

Optionally, such a reception and verification step 82 may be implemented by an authentication module (not shown) of the coupling device 30 that is capable of being connected via the link 32 to the man-machine interface (i.e. data entry and restitution interface) of the mobile terminal 12 when the mobile terminal 12 is secured to the housing 14, and designed to issue an authentication request that is restituted via the interface to the user of the mobile terminal 12.

Then, according to a step 84, a restitution is initiated by the electronic coupling device 30, via a restitution module of the mobile terminal 12, of information that is representative of the activation of the second secure radio-communication module R_2 .

Such information that is representative of the activation of the second secure radio-communication module R_2 corresponds, for example, to the display of the "MC mode" message.

According to one variant, the coupling device 30 activates an indicator, for example a light indicator (a light diffused for example by a green LED in the coupled mode MC, orange in the transition mode MT, and red in the decoupled mode MD), or an audio indicator that is representative of the coupled mode MC, the transition mode MT or the decoupled mode MD.

According to a particular aspect, such a restitution step 84 is capable of being implemented continuously as soon as the coupling phase 72 is triggered or at any other time during this coupling phase 72.

Prior to the implementation of this restitution step 84, the communicating object 10 is in the transition mode MT, which corresponds to the intermediate period between the moment of connection of the mobile terminal 12 to the housing 14 and the effective activation of the second secure radio-communication module R_2 .

Then, according to step 86, the activation of the second secure radio-communication module R_2 is implemented. More specifically, the coupling device 30 of the housing 14 triggers a specific communication mode corresponding to a set of communication functions available within the second secure radio-communication module R_2 , as well as the memory areas associated and isolated from each other.

Alternatively, such an activation step 86 may be implemented simultaneously with the previously described restitution step 84.

Such a specific mode is selected as a function of at least one parameter that is representative of a predetermined use of the second secure radio-communication module, wherein the parameter previously stored in a second memory space of the housing 14 is

accessible by the electronic coupling device 30 in a dedicated and secure manner. According to the example of Fig. 2 or 3, this secure memory space corresponds to the memory space of the security device 38 (i.e. the SIM card), while the parameter(s) correspond(s), for example, to a mission profile registered in the profile support of the SIM card 38 that is specific to the housing 14.

According to a particular aspect, such an activation 86 of the operation of the second secure radio-communication module R_2 is conditioned by the result of the step 82 of receiving and verifying at least one user authentication data input via a user interface that is input via the mobile terminal.

In other words, if the result of the authentication of the mobile terminal 12 and/or its user is positive, the second secure radio-communication module R_2 is triggered, while in the contrary case, the electronic coupling according to the present invention is interrupted, optionally with a step of restitution (not shown) of an authentication failure indicator.

As long as the secure "mission" of the user is in progress, the second secure radio-communication module R_2 of the communicating object 10 remains activated, while the operation of the first radio-communication module R_1 of the mobile terminal 12 is inhibited.

Once this "mission" is completed, the mobile terminal 12 is able to be disconnected from the housing 14 for use "off mission", for example, for personal purposes.

In order that such a disconnection of the communicating object 10, on the one hand, from the mobile terminal 12 and, on the other hand, from the housing 14, is carried out according to a controlled method, the second phase 74 of preparation for electronic decoupling shown on the Fig. 4 is implemented.

The second decoupling preparation phase 74 firstly comprises, according to the example shown in Fig. 4, a transmission step 88 by the electronic coupling device 30, of at least one command to delete all information stored in the mobile terminal 12 during the period of connection of the mobile terminal 12 to the housing 14.

Such a deletion step 88 is, in one variant, designed to be repeated several times during the connection of the terminal 12 and the housing 14 (i.e. during the mission). According to another variant, the deletion step 88 is only implemented after the mission has been completed prior to disconnecting the mobile terminal 12 from the housing 14.

Furthermore, prior to disconnecting the mobile terminal 12 from the housing 14, a step 90 of deactivating the second secure radio-communication module R_2 is implemented.

In addition, a step 92 of downloading by the electronic coupling device 30, of the information that is representative of the configuration of the mobile terminal prior to the inhibition, to the mobile terminal 12 is also implemented. In other words, the memory space 66 dedicated to the storage of at least one item of information that is representative of the configuration of the mobile terminal 12 prior to the electronic coupling with the housing 14 is downloaded from the electronic coupling device 30 of the housing 14 to the memory of the mobile terminal 12. In other words, the initial context of the mobile terminal 12, prior to the formation of the communicating object 10 is downloaded again to the mobile terminal 12 when the latter is about to resume its off-duty life cycle.

The deactivation step 90 and downloading step 92 are suitable for being implemented by the electronic coupling device 30, in parallel or in any order, wherein the deactivation step 90 (as shown in Fig. 4) precedes or succeeds the downloading step 92.

According to one particular aspect, once the decoupling preparation phase 74 is completed, a message informing the user that the terminal 12 is ready to be decoupled is, for example, restituted by the coupling device 30 via the restitution interface of the mobile terminal 12.

According to another particular aspect, once the decoupling preparation the phase 74 is completed, the separation of the mobile terminal 12 is prevented via an element (not shown) of electrical and/or mechanical blocking of the housing 14 under the control of the electronic coupling device 30.

Thus, the user is able to separate the mobile terminal 12 securely and return the latter to its initial configuration.

It is thus conceivable that the electronic coupling method and the electronic device 30 as well as the appropriate housing 14 make it possible to offer greater flexibility in the use of a mobile terminal 12, for example, on the one hand, in the context of the use in a personal area network (PAN) but also in a context of professional use, for example secure use in a wide area network (WAN). The hybridization of uses is enabled by the coupling between two dedicated electronic elements having distinct life cycles, i.e. on the one hand, the mobile terminal 12 and, on the other hand, the housing 14 according to the invention.

The housing 14 is easily reconfigurable as a function of the mission, secured or not, and regardless of the mobile terminal 12.

Furthermore, the housing 14 is preferably tamper-proof, and the communicating object 10 that is formed according to the invention, by coupling the mobile terminal 12 and the

housing 14, makes it possible to use the man-machine interface of the terminal 12 in favor of the communicating part of the housing 14. In other words, the communicating object 10 combines the inviolability, autonomy and reconfigurability of the housing 14 with the ergonomics of the mobile terminal 12.

5 As indicated above, the second radio-communication module R_2 is a secure radio-communication module that is able to exchange data that are processed according to predetermined information security rules. Those skilled in the art will thus understand that these data processed according to the predetermined security rules are data protected according to said security rules.

10 In optional addition, the second radio-communication module R_2 comprises several radio communication means that are distinct from each other, and preferably separate. The radio communication means are able to operate in parallel, i.e. simultaneously with each other, each radio communication mean being able to exchange data that are processed according to predetermined information security rules. This data is then protected according
15 to the security rules.

CLAIMS

1. Method (70) for electronically coupling a mobile terminal (12) with a housing (14) configured to receive the mobile terminal (12), the mobile terminal (12) comprising a first
5 radio-communication module (R_1), the housing (14) comprising a second radio communication module (R_2), and an electronic coupling device (30) being configured to implement the method (70),

the method (70) comprising at least:

- inhibition (80) of the operation of the first radio-communication module (R_1), the inhibition
10 being triggered when the mobile terminal (12) is secured to the housing (14), and
- activation (86) of the second radio-communication module (R_2), the second radio-communication module (R_2) being a secure radio-communication module that is able to exchange data that are processed according to predetermined information security rules.

15 2. Method (70) for coupling according to claim 1 further comprising:

- back-up (76) in a first dedicated memory space (66) of the electronic coupling device (30), of at least one item of information that is representative of the configuration of the mobile terminal (12) prior to the inhibition (80);
- transmission (88) of at least one command for deleting any information stored by the mobile
20 terminal during the period of coupling of the mobile terminal to the housing;
and before separation (94) of the mobile terminal (12) from the housing (14):
- downloading (92), by the electronic coupling device (30) of the information that is representative of the configuration of the mobile terminal, prior to the inhibition, to the mobile terminal, and
- 25 - deactivation (90) of the second radio-communication module (R_2).

3. Method (70) for coupling according to claim 1 or 2, wherein the method for coupling further comprises, prior to the activation (86) of the second radio-communication module (R_2), downloading (78), to the mobile terminal (12), by the electronic coupling device
30 (30) of at least one software tool that is configured to:

- check input and output data of the mobile terminal (12) during the activation of the second radio communication module (R_2), and/or
- check the integrity of the mobile terminal (12), and/or

- detect a separation of the mobile terminal (12) from the housing (14).

4. Method (70) for coupling according to any one of the preceding claims, wherein the activation (86) of the second radio communication module (R_2) comprises an activation of a specific communication mode selected according to at least one parameter that is representative of a predetermined use of the second radio communication module (R_2), said at least one parameter being previously stored in a second dedicated and secure memory space (38) that is accessible by the electronic coupling device (30).

5. Method (70) for coupling according to any one of the preceding claims, wherein the method (70) for coupling further comprises a restitution (84) initiated by the electronic coupling device (30), via a restitution module of the mobile terminal (12), of information that is representative of the activation of the second radio-communication module (R_2).

6. Device (30) for electronically coupling a mobile terminal (12) with a housing (14) configured to receive the mobile terminal (12), the mobile terminal (12) comprising a first radio-communication module (R_1), and the housing (14) comprising a second radio communication module (R_2), said device (30) being configured to implement the electronic coupling method (70) according to any one of claims 1 to 5.

7. Housing (14) configured to receive a mobile terminal, said housing comprising at least one radio-communication module (R_2) and an electronic coupling device (30) according to claim 6.

8. Housing (14) according to claim 7 wherein the radio-communication module (R_2) is a secure radio-communication module.

9. Housing (14) according to claim 7 or 8 comprising an electromagnetic shield (20) adapted to extend at least over the largest reception area of the mobile terminal (12).

10. Housing (14) according to any one of claims 7 to 9 that is formed by a material obtained by nano-reinforced plastic processing.