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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 December 2008 (04.12.2008)

PCT

(10) International Publication Number
WO 2008/145199 A1

(51) International Patent Classification:
G07C 9/00 (2006.01)

(21) International Application Number:
PCT/EP2007/060856

(22) International Filing Date: 11 October 2007 (11.10.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PN2007A000040 29 May 2007 (29.05.2007) IT

(71) Applicant *(for all designated States except US)*: **BIANCHI 1770 S.P.A.** [IT/IT]; Via Camillo Bianchi 2, I-31015 Conegliano (Treviso) (IT).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **CHIES, Ezio** [IT/IT]; c/o BIANCHI 1770 S.p.A., Via Camillo Bianchi 2, I-31015 Conegliano (Treviso) (IT). **LONGATO, Stefano** [IT/IT]; c/o BIANCHI 1770 S.p.A., Via Camillo Bianchi 2, I-31015 Conegliano (Treviso) (IT).

(74) Agents: **GONELLA, Mario** et al.; PROPRIA S.R.L., Via della Colonna, 35, I-33170 Pordenone (IT).

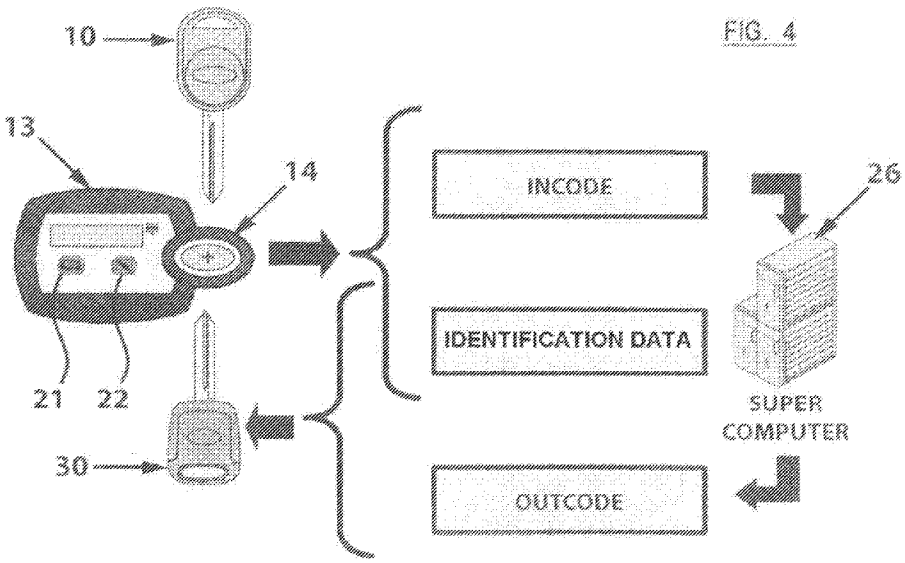
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN,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

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

Published:
— *with international search report*

(54) **Title:** METHOD FOR THE DUPLICATION OF ELECTRONIC-CODE KEYS

FIG. 4



(57) **Abstract:** Method for the duplication of keys provided with code-based electronic recognition means, said method being based on the use of a data read/write unit (13) and telematic data transmission means. The data read/write unit (13) acquires the code of the original key to be duplicated (10), wherein part of such code is in an encrypted form. The data read/write unit transmits the encrypted part of the code in the form of first encrypted and indexed data to a data processing centre (26). These first encrypted and indexed data are recognized at said data processing centre, which in response processes them into second encrypted data. These second encrypted data, which will have been indexed in accordance with the first encrypted data, are transmitted back to the sender peripheral data read/write unit, where they are associated to the remaining part of the code of the key to be duplicated. The thus reconstructed code is decrypted and stored in a blank key (30) that will form the duplicate of the original key.

WO 2008/145199 A1

METHOD FOR THE DUPLICATION OF ELECTRONIC-CODE KEYS

DESCRIPTION

The present invention refers to a method and an apparatus for the duplication of keys provided with code-based electronic recognition means. Keys of this kind are increasingly being used in connection with security locks of various kinds, in particular in connection with motor-vehicle starting systems.

As largely known in the art, the general problem associated with the duplication of an electronically coded key is a multi-faceted one with a number of different aspects that need to be taken into due consideration.

A first such aspect involves the connection and the access to the centres that keep in store, handle and manage the programming codes of the keys of the various manufacturers. These centres are in fact located remotely from the site where a key is materially duplicated, so that the related duplication process has to be performed under telematic transmission and control conditions, i.e. via a blend of computer and wireless telecommunications technologies.

A second aspect of said general problem is security; the user, who for any reason whatsoever needs a duplicate of his/her key, shall be sure and certain that the duplication of his/her key, or the generation of a new duplicate thereof, will be solely possible to the legitimate owner of such key and is by no means accessible to third, possibly ill-intentioned parties.

A further aspect is the rapidity of the service, considering that, usually, a duplication request has an urgent nature, since it derives from a particular, specific need of the user, and – as such – it must therefore be complied with in as short a time as possible.

Various systems and solutions have in fact been proposed hitherto in view of solving such problems.

The recently filed patent application WO 2006/032354 describes a telematic system for the duplication of electronic-code keys, which is based on the use of at least a central unit containing at least an electronic file, in which to each code there are associated the data pertaining or relating to the corresponding key to be duplicated. The duplication process itself requires the code to be transmitted from a peripheral unit to the central unit, the transmitted code to be recognized in the central unit, and a composite signal to be finally transmitted from the central unit to the peripheral unit, where the duplication is performed, i.e. takes place. This system, which might seem quite simple at a first sight, is rather complicated, actually, owing to the need arising for the peripheral unit to be provided with means for hiding or even deleting or erasing the data it receives from the central unit. Such means are needed in view of ensuring full secrecy and, therefore, security to the duplication process itself.

In the same way as the above-cited patent application, the US patent no. 5,838,251 refers to a method and an apparatus for programming operative data into component parts of a motor-vehicle, in particular motor-vehicle keys. The system covered by this patent calls for the data to be collected and stored in a central storage unit to be then transmitted in a coded form – via any suitable line, such as a telephone line – to a peripheral unit where the same data have to be used. The risk that an unauthorized person may gain access to or come into possession of the so transmitted data is reduced to a minimum thanks to the fact that the same data can solely be decoded in the final component part that has to be programmed with such data. Various information levels are provided along with special adapters to as best as possible protect the system against possible

intrusions.

In any case, prior-art systems that have been proposed and used up to these days make use of a plurality of centralized electronic files, in each one of which the data are repeatedly checked, i.e. undergo multiple controls by means of comparisons that are performed between the data transmitted by the peripheral units in connection with the operative request thereof and the data stored in the central units that must consent to such operative request being enabled to be complied with and carried out.

It therefore is a main object of the present invention to provide a method for the duplication of keys provided with code-based electronic recognition means, which ensures remote operativeness under conditions of absolute security, wherein any need for use to be made of special devices, such as proprietary databases with related inquiry means, is however done away with.

Within this object, a further purpose of the present invention is to provide a system that makes use of a single data processing centre, which all peripheral units concerned are connected to, so that these peripheral units are enabled to carry out the requested duplications through a proper data processing sequence. This data processing sequence – as performed based on an algorithm – enables the requested data to be coded and transmitted, without any need arising of setting up a plurality of files or storage capacities that have to be acceded to for the comparison and recognition of the requested data.

Still a further purpose of the present invention is to enable users to do away with the need to make use of a plurality of particularly sophisticated and smart, i.e. high-performance peripheral units, while limiting such use to a simple read/write unit of any known type.

Finally, the method according to the present invention can be readily extended to cover applications involving other security devices operating on the basis of or through electronic codes, such as in particular remote controls, radio controls, further to keys equipped with transponder means.

According to the present invention, these aims, along with further ones that will be apparent from the following description, are reached in a key duplication method and apparatus incorporating the features and characteristics as recited in the appended claims.

Features and advantages of the present invention will anyway be more readily understood from the description that is given below by way of non-limiting example with reference to the accompanying drawings, in which:

- Figure 1 is a diagrammatical view of the various functional blocks making up a code-based electronic recognition means;

- Figure 2 is a schematic view illustrating the method according to the present invention in a first embodiment thereof;

- Figure 3 is a schematic view illustrating the method according to the present invention in a second embodiment thereof;

- Figure 4 is a schematic view illustrating the data recognition method according to the present invention; and

- Figure 5 is a schematic view illustrating the method according to the present invention in a third, preferred embodiment thereof.

With reference in particular to Figures 1 and 4, the key to be duplicated 10 is provided with code-based electronic recognition means, such as a transponder. Figure 1 is a diagrammatical view of the various functional blocks that make up a code-based electronic recognition means.

The code-based electronic recognition means 11 is made up by a specially designed, i.e. dedicated microchip contained in a support, where an antenna 12 is provided for bi-directional radiofrequency communications. The code-based electronic recognition means is energized via an electromagnetic coupling

established through an antenna of a read/write unit 13 adapted to receive a key 10 or 30 in a pit or hole 14 (see Figure 4).

A first functional block is formed of an EEPROM programmable memory 5 that has for instance a capacity of 256 bits. This EEPROM programmable memory 5 is subdivided into some fragments that are arranged to host, i.e. store some identification data and a secret code of the key. The identification data of the key may for instance consist of a recognition code, a code identifying the manufacturer, a serial number, and the like, in which each one of them occupies a certain characteristic number of bits, whereas the secret code is an information consisting of data forming a string in the size of a few Bytes, e.g. five Bytes. The secret code can be neither copied nor read by the read/write unit 13 lodging the key, i.e. in which the key is received, but solely and merely interpreted in a mode that shall be explained in greater detail further on.

A second functional block includes a computing unit 16, in which a protected proprietary algorithm is implemented.

A third functional block refers to a control logic 17, which assigned the task of processing the secret code of the key 10 (contained in the block 5) through the algorithm implemented in the computing unit 16, in response to an inquiry signal that is sent in by the read/write unit 13 in which the key 10 is received. In addition, the functional block concerning to the control logic 17 implements a cryptanalysis, i.e. decryption routine that is retrieved and caused to run whenever and as soon as data are input in a form that is encrypted with the same protected proprietary algorithm. In a known manner, the electronic recognition means further contains some component parts that build up a contactless interface 18 (see Figure 1).

Figure 2 shows a flow diagram of the method according to the present invention, in which all involved devices are networked through the Internet, i.e. connect to a communication network such as the Internet.

The peripheral read/write unit 13 is connected to a computer 15, e.g. via a serial interface RS232 or a Universal Serial Bus (USB). The computer 15 is

interconnected with the Internet network and is located in proximity of the read/write unit 13. Installed in the same computer 15 there is an application program that is adapted to handle the flow of data coming in from the read/write unit 13.

The read/write unit 13 performs data reading and writing operations and is capable of identifying the type of key. Provided in the apparatus there is a built-in, i.e. internal memory having a storage capacity of for instance 64 kilobytes. Moreover, the read/write unit 13 is provided with a display 20, such as for instance a display formed of two lines by twenty digits, an antenna (not shown) for receiving and transmitting data, and two push-buttons, i.e. a read button 21 and a write button 22, by means of which an operator is able to interact, i.e. intervene interactively.

A remote service computer, i.e. server 25 is interconnected with the Internet network and the primary task thereof lies in managing in a queuing mode, such as for instance in the so-called F.I.F.O mode, the plurality of authentication requests coming in from the peripheral read/write units 13. Such server is connected to a data processing centre 26 (SuperComputer) having an elevated computing capacity as its peculiar property. Furthermore, this data processing centre 26 implements the same protected proprietary algorithm that is set up in the microchip included in the code-based electronic recognition means 11. All read/write units 13, irrespective of their actual location, refer to such data processing centre 26.

Owing to such data processing centre 26 being itself interconnected with the Internet network via the service computer, i.e. server 25, the telematic, i.e. remote communication circuit is completed.

According to the inventive method, a key 10 to be duplicated is introduced in the appropriate receptacle 14 of a read/write unit 13. Via the interactive read button 21, the read/write unit 13 reads the identification data of the key 10, thereby recognizing the type of key being handled, and temporarily stores such data in the internal memory thereof. In the assumption that the key 10 is of the type with a

secret (encrypted) code, the read/write unit 13 concurrently performs an inquiry operation to query the key 10. Such query occurs through a code that is implemented in the read/write unit 13 and is solely known by the manufacturer. Thus, a wireless communication is then established between the read/write unit 13 and the code-based electronic recognition means 11 of the key 10. The code-based electronic recognition means 11 processes the secret data, with the aid of the protected proprietary algorithm that is implemented inside its own microchip, in response to the inquiry signal. What the read/write unit 13 acquires is therefore a data-based information that is encrypted at random in a first encryption form, which shall be defined as INCODE hereinafter.

The read/write unit 13 automatically assigns the key 10 with an index, which may for instance be allotted following a numerical sequence. The read/write unit 13 transmits the INCODE, which contains also the information that identifies the key 10 to be duplicated in a univocal manner, owing to its having been assigned a log, to the computer connected thereto. The computer 15, as duly provided with the application program, receives such information and sends it to the serving computer or server 25. At this point, the INCODE contains also the information relating to the IP (Internet) address of the computer 15.

The INCODE received by the serving computer or server 25 is indexed in a sequence based on the IP address from which it has arrived, so as to be able to be classified. Afterwards, the authentication request will be handled and managed through the F.I.F.O. queue. As soon as the same authentication request becomes the first one in the queuing list, the same is served and, as a result, the INCODE is sent to the data processing centre 26, where a search is performed to find out the secret code contained in the microchip from which the INCODE has been derived.

The recognition of the secret code occurs following a data processing operation that requires an elevated computing capacity to be available. The basic steps thereof can be summarized as set forth below.

In the data processing centre 26, the INCODE is decrypted through the protected proprietary algorithm and – through an appropriate processing operation

– a correspondence is found with one of the afore-mentioned plurality of secret codes within the whole set of possible combinations relating to the size of the string of the secret code. As soon as this relation of correspondence is established, the secret code is recognized and authenticated, and – as a result – the single and sole secret code corresponding to the one contained in the microchip of the key 10 to be duplicated is acquired. The data processing centre 26 encrypts the corresponding secret code in a random way – through the protected proprietary algorithm – into a second encryption form, which shall be defined as OUTCODE hereinafter.

Via the same telematic network, the data processing centre 26 sends the OUTCODE to the read/write unit 13 from which the related request had originated. The encrypted response code obtained as OUTCODE will of course be different, even if to an INPUT code transmitted to the data processing centre there corresponds a single OUTPUT code. However, the encrypted response code, or OUTCODE, will be indexed in accordance with the INCODE input code arriving at the data processing centre 26, so that it is correctly addressed to the actual read/write unit 13, from which the processing and authentication request had originated.

The encrypted secret code transmitted by the data processing centre 26 is thus received by the read/write unit 13, in the receptacle 14 of which there has been inserted a blank key 30 to be programmed as a replacement, i.e. duplicate of the original key 10 to be duplicated. The read/write unit 13 is then activated and, by associating the OUTCODE response code received from the data processing centre 26 with the other previously stored identification data of the original key 10, transfers all identification data of such key into the microchip of the new blank key 30, wherein this operation is performed with the aid of the interactive write button 22. The OUTCODE response code – as it has been worked out at the data processing centre 26 – is decrypted and definitively stored – along with the other identification data – solely inside the microchip of the blank key 30. Once the duplication process has been completed, the key 30 turns out as being structurally constituted by a different recognition configuration that is anyway able to exactly emulate the functions of the configuration of the original key.

The read/write unit 13 is programmed to destroy – upon completion of each programming operation – all temporarily stored information and data. By virtue of the double encryption, i.e. on transmission and reception, respectively, of the codes transferred in the key system, the new key 30 is ensured that it will be identical to the original one and, thanks to the solely temporarily stored data being eventually destroyed, it is ensured that nobody will be able to gain access to the secret code of neither the original key nor – similarly – the duplicate one.

Figure 3 illustrates the same flow diagram that has been described in connection with Figure 2, with the difference, however, that the read/write unit 13 makes in this case use of a mobile telephone communication network 40 to transmit the INCODE and receive the OUTCODE.

In this case, the INCODE - as shown on the display of the read/write unit 13 - can be transmitted in a text message mode (SMS) with the aid of a mobile or cellular phone, and is indexed in a sequence mode with the phone number from which it has reached the computing server 25, to be classified accordingly.

The OUTCODE, which is received in a SMS mode, too, is input and logged in the read/write unit 13 through the combination of the two buttons 21 and 22; thereupon, through the interactive write button 22, the blank key is finally programmed as this has already been described above, wherein the possibility is contemplated for the programming operation to be repeated in the case that an error is made when striking, i.e. writing the OUTCODE.

The illustration in Figure 4 highlights the fact that the identification data of the key and the secret code, which are required for programming the blank key, are by no way accessible or available concurrently at any moment and any link of the communication network whatsoever.

Schematically illustrated in Figure 5 there is a third preferred embodiment of the method according to the present invention, wherein the transmission of the INCODE and the reception of the OUTCODE occur via a mobile telephone system

using a communication protocol, such as GSM.

To this purpose, there has been devised a data transceiving unit 50 that imitates, i.e. resembles in all parts thereof a GSM transceiving module and, as such is capable of being activated with a so-called SIM (**S**ubscriber **I**dentity **M**odule) card that is compatible with those used and available on the international marketplace; it further implements – with a set of routines – an interface software for the interconversion of data with the read/write unit 13. The data transceiving unit 50 operating according to the mobile-telephone standard mode is energized with an electric current supplied by a power supply 60 connected to the power mains. Such power supply 60 may for instance be the same one of the read/write unit 13. A serial I/O interface 58, such as an interface RS232 or a USB, enables the data transceiving unit 50 operating according to the mobile-telephone standard mode to be connected with the read/write unit 13. The data transceiving unit 50 operating according to the mobile-telephone standard is provided with an interactive push-button 52 and two LEDs 54, 56 that have a different colour, e.g. green and red, respectively. The interactive push-button 52 allows the operator to perform the operations required to transfer both the INCODE to the data processing centre 26 and the OUTCODE to the read/write unit 13, whereas the green LED 54 and the red LED 56 indicate the state of the operations being carried out in search of a GSM network and to transfer encrypted data, respectively.

The data transceiving unit 50 operating according to the mobile-telephone standard mode carries out a search of the available GSM network immediately after being connected to the read/write unit 13, and indicates that a connection to the GSM network has been successfully completed by causing the green LED 54 to blink.

The routines provided to initialize the read/write unit 13 and the data transceiving unit 50 operating according to the mobile-telephone standard mode, respectively, in view of starting the key duplication process, are retrieved and set into running when the key 10 to be duplicated, as provided with its own encrypted transponder, is inserted in the receptacle 14 of the read/write unit 13. At this point,

the read/write unit 13 transmits the INCODE to the data transceiving unit 50 operating according to the mobile-telephone standard mode and – following the actuation of the interactive button 52 – the related encrypted data are sent via the GSM telematic network to the data processing centre 26, the latter being of course duly associated to a proper transceiving means (not shown).

The data processing centre 26 processes the so received encrypted data to generate the OUTCODE in the manner that has already been described afore in connection with the other embodiments of the inventive method, and – during the time interval in which the encrypted data are being transferred through the telematic network and then processed at the data processing centre 26 – the red LED 56 illuminates steadily. As soon as the OUTCODE is available, the data processing centre 26 sends such OUTCODE to the data transceiving unit 50 operating according to the mobile-telephone standard mode and the reception of such OUTCODE by said unit is indicated by the same red LED 56 switching to a blinking state. As a result, the blank key 30 can be inserted in the read/write unit 13 and, through the interactive button 52, the related encrypted data can be transferred to the read/write unit 13 for the OUTCODE to be programmed into the blank key 30 inserted in the same read/write unit 13, in the same manner as already described afore in connection with the other embodiments of the inventive method. In this phase, the red LED 56 is again illuminated steadily and, once programming the blank key 30 is completed, the red LED 56 goes off.

With reference to the other two embodiments of the inventive method that have been described afore, it is worth noticing that this further embodiment, based on the use of a data transceiving unit 50 operating according to the mobile-telephone standard mode, has the peculiar advantage of allowing for some devices, such as the computer 15 connected to the Internet and/or the mobile phone, to be excluded, i.e. done away with, thereby enabling the total time needed for a key to be duplicated to be drastically cut. In particular, the need is furthermore done away with for buttons or dials to be struck or actuated manually on the telephone and the read/write unit 13 (in the second embodiment), thereby eliminating any error possibility by the operator.

It will of course be readily appreciated that this further embodiment of the invention, based on the use of a data transceiving unit 50 operating according to the mobile-telephone standard mode, can be implemented in a number of different manners as far as both the configuration of the system and the use of other mobile-telephone standards are concerned. So, for example, the possibility is given for a data transceiving unit to be provided, which uses the UMTS standard, while providing the system with related hardware or software interfaces as appropriate. In addition, the data transceiving unit operating according to the mobile-telephone standard may be integrated in the read/write unit 13. In other words, all devices that can be connected to or integrated in the read/write unit 13, as provided to transmit and receive data to and from the remote data processing centre 26 and making use – to such purpose – of any communication protocol whatsoever, fall within the scope of the present invention.

Therefore, the whole key duplication process can be considered as being effectively and fully protected, since data are in all cases and invariably transmitted and received in an encrypted form, while the identification data of the key 10 to be duplicated are available in the read/write unit 13 solely for the time that is strictly required to complete the programming operation. The whole set of operations to be carried out requires a time varying from just a few seconds up to a maximum of three minutes, thanks to the rapidity of the telematic transmission mode and the huge computing and processing capacity available at the remote data processing centre.

The particularly important fact should further be noticed that the whole key duplication process does by no way make use of any fixed database to be accessed to for a recognition by direct comparison, but is rather based on an autonomous computing and processing operation dedicated to each single transaction.

Accordingly, the system according to the present invention fully reaches the afore-noted aims by in particular allowing electronic keys of the encrypted type to be duplicated in a process that is handled and managed in a fully centralized manner, without any need arising for access to be gained to proprietary

databases, which would make it necessary for additional security devices to be used in view of ensuring the required level of secrecy. Moreover, the use of a mainframe computer for processing the data enables extremely quick responses to be obtained for complete user's satisfaction.

CLAIMS

1. Method for the duplication of keys provided with code-based electronic recognition means, said method being based on the use of a data read/write unit (13) and telematic data transmission means, **characterized in that**:

- said data read/write unit (13) acquires the code of the original key to be duplicated (10), part of such code being in an encrypted form;
- the data read/write unit (13) transmits the encrypted part of the code in the form of first encrypted and indexed data to a data processing centre (26);
- such first encrypted and indexed data are recognized at said data processing centre, which in response processes out second encrypted data bearing however the same indexation as said first encrypted data;
- such second encrypted data are transmitted back to the peripheral data read/write unit, where they are recognized, based on the indexation thereof, and are then associated to the remaining part of the code of the key to be duplicated;
- the thus reconstructed code is stored and decrypted in the blank key (30) that is due to form a duplicate of the original key.

2. Method for the duplication of keys provided with code-based electronic recognition means according to claim 1, **characterized in that** the data read/write unit (13) acquires and stores in a temporary memory the identification data contained in the code of the key to be duplicated (10), while it receives and transmits to the data processing centre (26) the encrypted part of the code.

3. Method for the duplication of keys provided with code-based electronic recognition means according to claim 1, **characterized in that** said first encrypted and indexed data reaching the data processing centre (26) are decrypted and compared with all data that can be processed or are available for processing by said data processing centre, until they are eventually recognized when a match is univocally found with one of the data processed by the data processing centre.

4. Method for the duplication of keys provided with code-based electronic recognition means according to claim 1, **characterized in that** said data processing centre (26) performs a second encryption of the thus received and recognized data and then transmits the resulting second encrypted and indexed data to the respective data read/write unit (13).

5. Method for the duplication of keys provided with code-based electronic recognition means according to claim 1, **characterized in that** said second encrypted and indexed data are transferred to the data read/write unit (13), where they are associated to the respective identification data of the key to be duplicated (10) stored in the temporary memory in view of reconstructing the code that is in turn transferred to the blank key (30) to complete the key duplication process.

6. Method for the duplication of keys provided with code-based electronic recognition means according to claim 1, **characterized in that** the various encryption and decryption operations are performed based on the use of a proprietary, protected algorithm.

7. Method for the duplication of keys provided with code-based electronic recognition means according to claim 1, **characterized in that** following completion of the key duplication process, the identification data of the duplicated key are automatically deleted from the temporary storage memory of the data read/write unit (13).

8. Apparatus for carrying out the method according to any of the preceding claims, comprising a data read/write unit (13) provided with a receptacle (14) adapted to receive a key to be duplicated (10) and a blank key (30),

characterized in that said data read/write unit (13) is further provided with means to generate a first encrypted code derived from the original data of the key to be duplicated (10), and is associated to means (15, 40, 50) for transmitting said first encrypted code to a data processing centre (26), which is adapted to transmit a second encrypted code back to the data read/write unit (13) for the duplication of the original data into the blank key.

9. Apparatus according to claim 8, **characterized in that** said data read/write unit (13) is associated to a transceiving unit (50) that is fitted with a mobile-telephone communication protocol.

FIG. 1

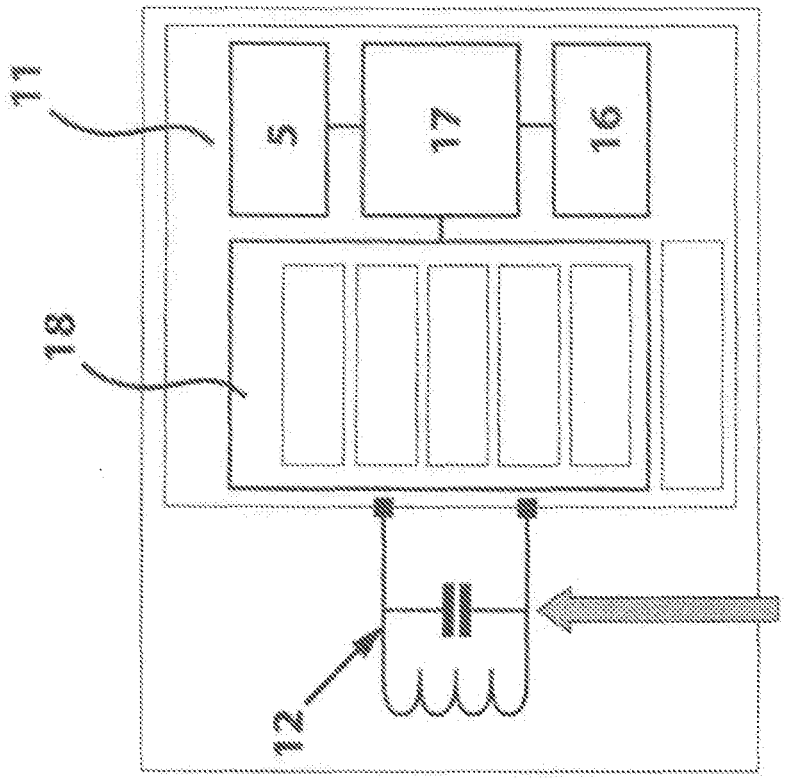


FIG. 2

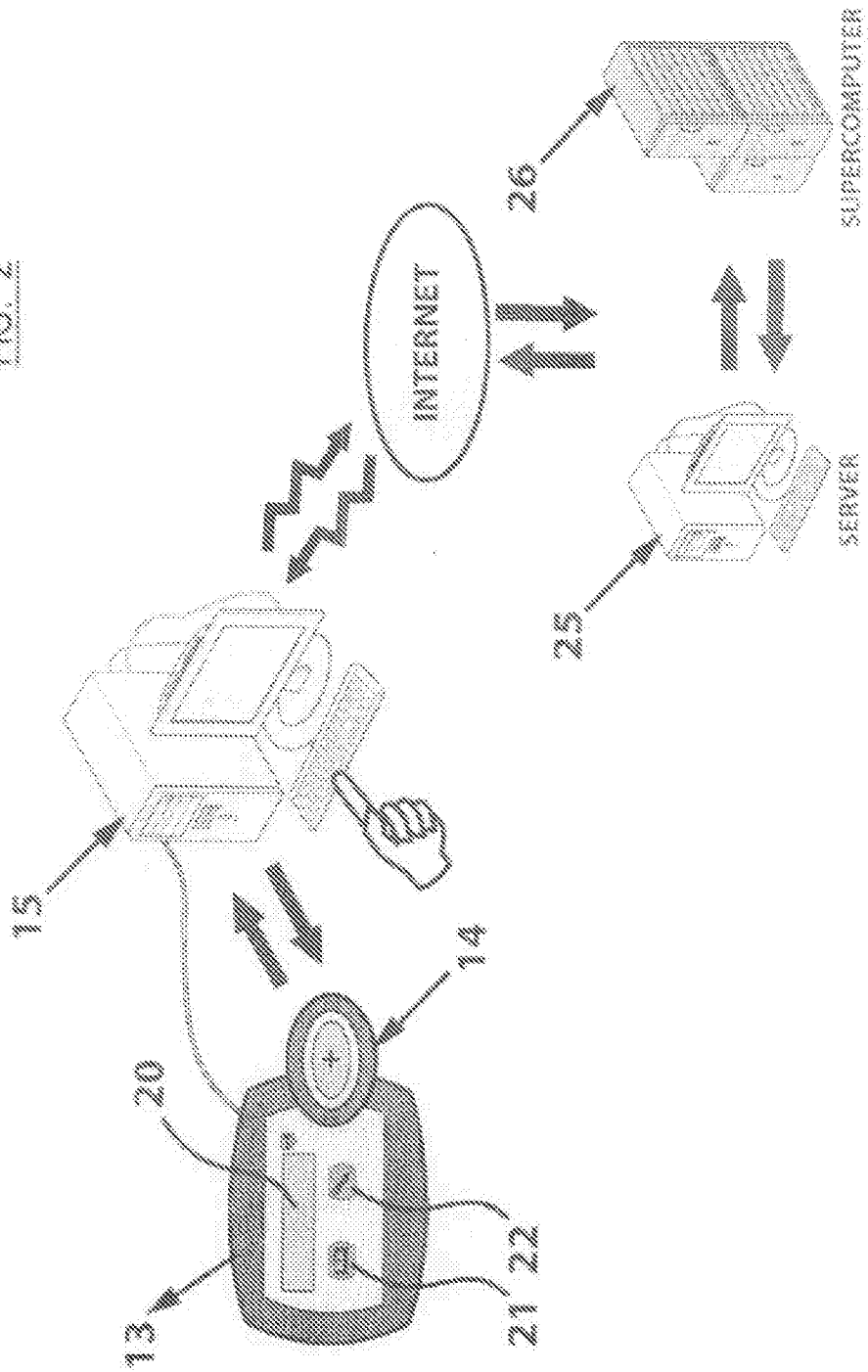


FIG. 3

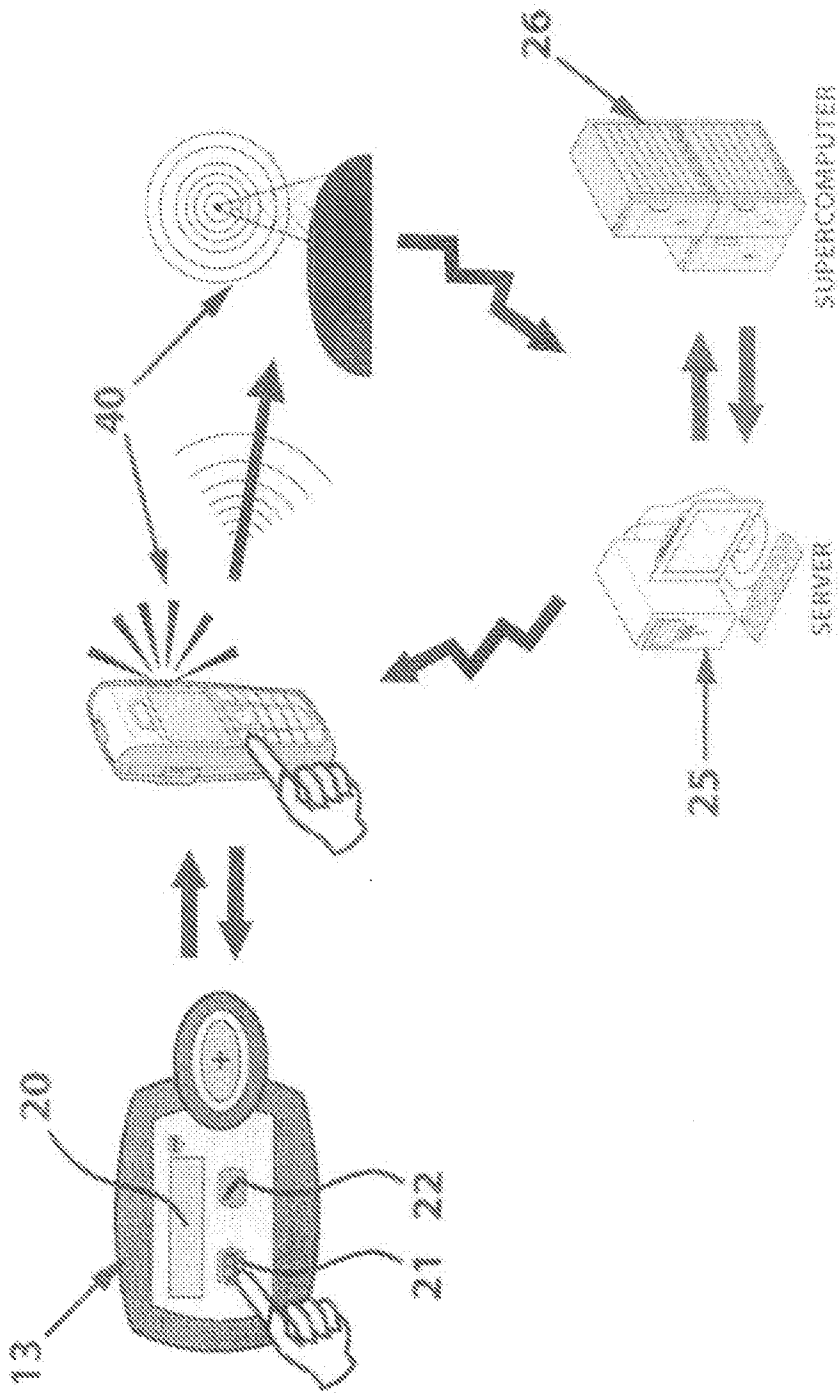
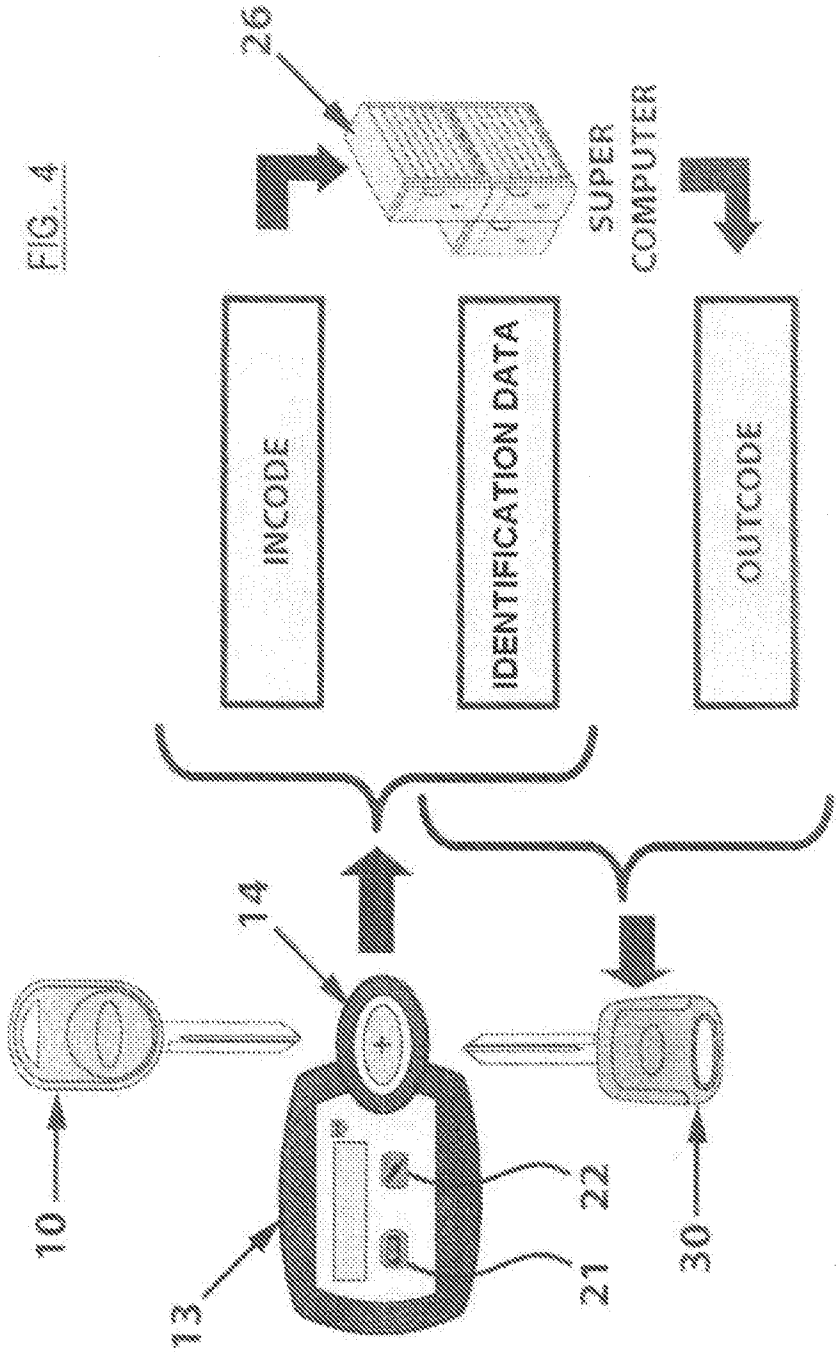


FIG. 4


26
SUPER COMPUTER
IMCODE
IDENTIFICATION DATA
OUTCODE
14
10
13
22
21
30

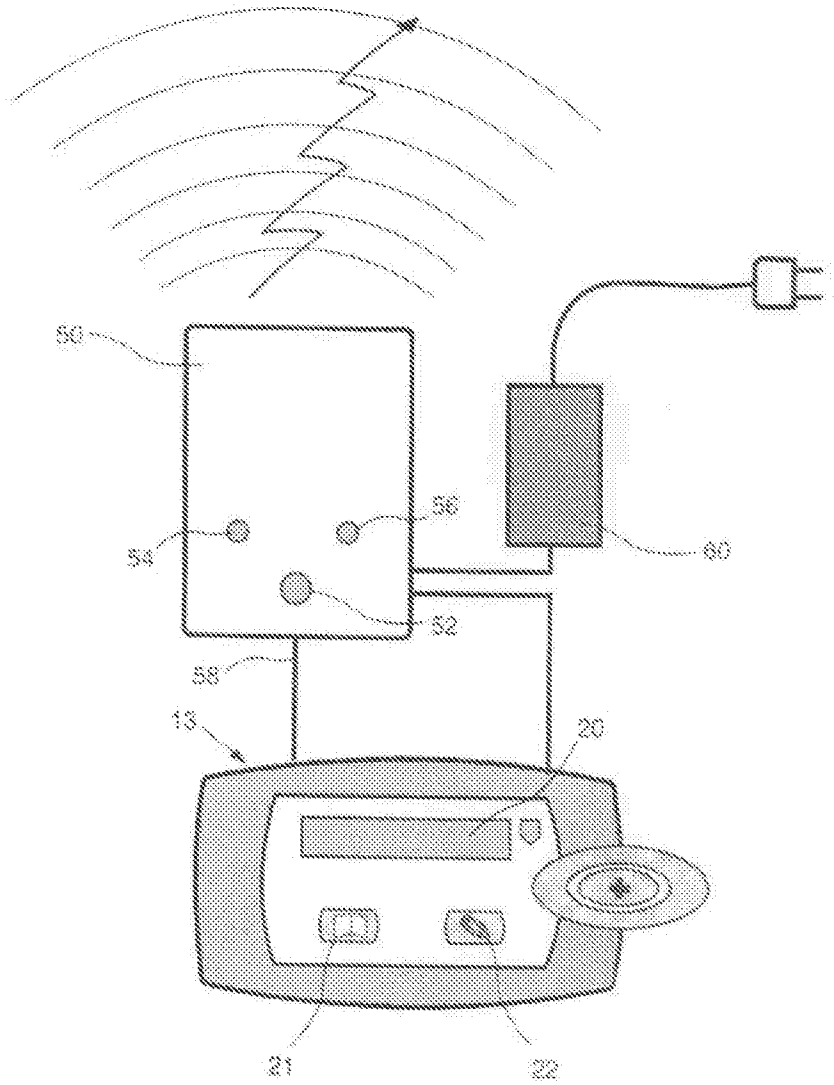


Fig 5

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2007/060856

A. CLASSIFICATION OF SUBJECT MATTER
INV. G07C9/00

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G07C B60R G07B

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2001/040966 A1 (BUHR WOLFGANG [DE] ET AL BUHR WOLFGANG [DE] ET AL) 15 November 2001 (2001-11-15) abstract paragraph [0001] - paragraph [0026] figure 1 claims 1-15	1-9
Y	GB 2 340 644 A (ROVER GROUP [GB]) 23 February 2000 (2000-02-23)	1-7
X	abstract page 3, paragraph 2 - page 12, paragraph 3 figures 1,2	8,9
	-/--	

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 February 2008	26/02/2008

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

Form PCT/ISA/210 (second sheet) (April 2005)

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 2006/032354 A (SILCA SPA [IT]; DONADINI MICHELE [IT]) 30 March 2006 (2006-03-30) abstract page 1, line 2 - page 6, line 18 figures 1,2	1-7
X	US 2002/133716 A1 (HARIF SHLOMI [US]) 19 September 2002 (2002-09-19) abstract figures 1-8 paragraph [0034] - paragraph [0054]	1-9
A	EP 1 324 276 A (MATSUSHITA ELECTRIC WORKS LTD [JP]) 2 July 2003 (2003-07-02) abstract paragraph [0035] - paragraph [0045] figures 1-14	1-9
A	EP 1 372 096 A (SAKAMURA KEN [JP]; KOSHIZUKA NOBORU [JP]; NTT DOCOMO INC [JP]) 17 December 2003 (2003-12-17) abstract paragraph [0024] - paragraph [0040] figures 1-7	1-9
A	EP 0 835 790 A (DENSO CORP [JP]) 15 April 1998 (1998-04-15) abstract column 1, line 35 - column 8, line 11 figures 1-9	1-9
A	EP 1 587 044 A (SOMFY [FR]) 19 October 2005 (2005-10-19) the whole document	1-9
A	US 2002/049904 A1 (NOWOTTNICK JUERGEN [DE] ET AL) 25 April 2002 (2002-04-25) the whole document	1-9

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2007/060856

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2001040966 A1	15-11-2001	DE 19633802 A1	26-02-1998
		EP 0825316 A2	25-02-1998
		JP 10107789 A	24-04-1998
GB 2340644 A	23-02-2000	NONE	
WO 2006032354 A	30-03-2006	NONE	
US 2002133716 A1	19-09-2002	NONE	
EP 1324276 A	02-07-2003	CN 1428737 A	09-07-2003
		US 2003122651 A1	03-07-2003
EP 1372096 A	17-12-2003	CN 1469273 A	21-01-2004
		JP 2004015665 A	15-01-2004
		US 2004059685 A1	25-03-2004
EP 0835790 A	15-04-1998	DE 69726681 D1	22-01-2004
		DE 69726681 T2	07-10-2004
		US 6160488 A	12-12-2000
EP 1587044 A	19-10-2005	AU 2005201517 A1	03-11-2005
		CN 1684011 A	19-10-2005
		ES 2246753 T1	01-03-2006
		FR 2869134 A1	21-10-2005
		JP 2005312040 A	04-11-2005
		KR 20060045795 A	17-05-2006
		US 2005237957 A1	27-10-2005
US 2002049904 A1	25-04-2002	EP 1182621 A2	27-02-2002
		JP 2002124943 A	26-04-2002