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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 December 2010 (16.12.2010)

PCT

(10) International Publication Number
WO 2010/142474 A1

(51) International Patent Classification:
G07C 9/00 (2006.01) *B60R 25/00* (2006.01)

(21) International Application Number:
PCT/EP2010/054015

(22) International Filing Date:
26 March 2010 (26.03.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PN2009A000038 10 June 2009 (10.06.2009) IT

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

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **REBULI, David** [IT/IT]; Via Camillo Bianchi 2, c/o Keyline S.p.A., I-31015 Conegliano (TV) (IT).

(74) Agent: **GIUGNI, Valter**; 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, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, 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, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, 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, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

(54) **Title**: DUPLICATION MEANS FOR AN ELECTRONICALLY CODED KEY AND RELATED METHOD

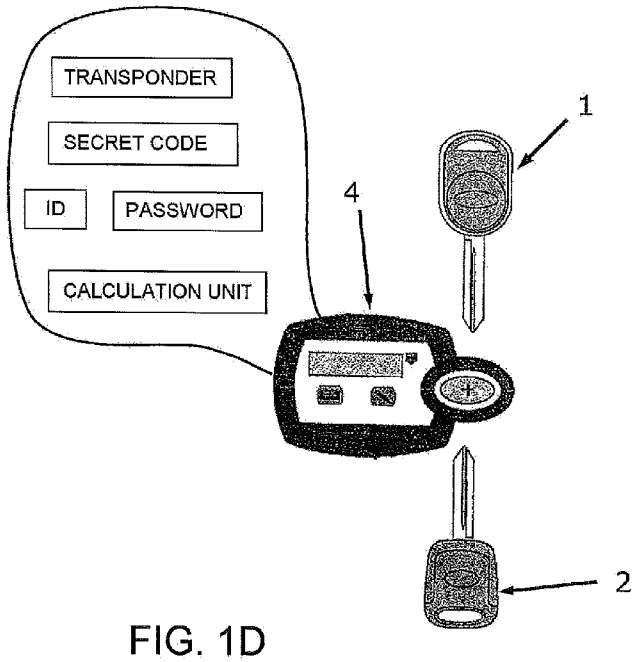


FIG. 1D

(57) **Abstract**: Method for the duplication of original electronic keys used in the automotive transports, and provided with coded and encrypted electronic authentication means, comprising: an Identification Code (ID), an encrypted secret code, a Password, an algorithm, data storage and computing means, able of being used in vehicles provided with a central processing unit able of storing an Identification Code (ID), an encrypted secret code, a Password, an algorithm, said duplication method being able of obtaining a duplicated key based on a blank key, which is originally provided with an algorithm, data storage means able of storing said Identification Code (ID), said secret code and said Password, wherein said data storage means are initially empty; said duplication is based on a duplication means and on a method which allows of using the blank key as intercepting means of secret codes sent by the vehicle central processing unit, and of transferring said information to the duplication means itself.

WO 2010/142474 A1

DUPLICATION MEANS FOR AN ELECTRONICALLY CODED KEY AND RELATED METHOD

DESCRIPTION

This invention refers to some means able of duplicating keys provided with both a mechanical code, of the conventional type, and of an electronic code, also in se known and employed for years in several technical applications.

The invention also refers to some methods in order to use said means and which allows the duplication of one of these keys.

In the following of this description, and in the attached claims, it will be specifically referred to the mechanical and electronic keys used in the nowadays produced vehicles, but it is intended that the invention applies also in different fields, as for instance in the armoured door, a safe etc..., provided a key with a double mechanical and electronic code, a respective lock and a related electronic central unit able of processing the data stored into the electronic codes of the key to be duplicated, and transmitted by it, is used.

Moreover it is stressed that, even if it will be useless to the man skilled in the art, the invention applies to a central processing units and electronic keys wherein, before the central unit to allow the operation of the various vehicle functions, a double and mutual authentication between the electronic key and the central unit mounted in the vehicle itself is implemented.

The means and the method of said mutual authentication are broadly described in the patent US 7,387,235 B2: "MUTUAL AUTHENTICATION SECURITY SYSTEM WITH RECOVERY FROM PARTIAL PROGRAMMING", assigned to Lear Corporation.

Just for it, in the facts, the original key, and therefore the duplicated one, are provided with a double code for the reciprocal authentication, one being called «Secret code», and the other «Password».

In the facts one of said codes is used by the central unit to authenticate the original key, and the second code is used by the original key to authenticate the central unit.

Furthermore, in order to easier introduce the man skilled in the art into the

field and technique of electronic keys with mutual authentication, it is referred to the Fig. 6 of said prior patent, which shows a method of mutual authentication between an electronic key and a respective central unit, which is activated when the key is being inserted in its lock and turned until a suitable «start» signal is sent to the central unit itself; based on said Figure, the man skilled in the art is with no doubts able of identifying the technique field involved, and of easily guessing its innovation with respect to said technique field.

It is known that when it is desired, or it needs to duplicate in a legal way a mechanical or electronic key as described, several aspects have to be evaluated.

The second aspect regards the time-length and the cost required for the key duplication activity; usually the duplication request is urgent as the user has lost one of its keys, or he has to provide one or more extra keys to trustworthy peoples, as relatives, assistants etc.

The third aspect refers to the practicality and actual feasibility of the duplication operation; in particular it is wanted that the duplication activity be available in a indeterminate plurality of different stations for key duplication, well spread on the territory where the vehicle usually travels, so that the user, who wishes to duplicate a key may reach easily and quickly, and with the same quickness may get the required duplicated key which has to be therefore handed to the same station.

Various methods and means are known, which allow the duplication of electronic keys; such means and methods are extensively described in a number of patents, or related applications, among these we here cite:

US 5,838,251 A,

US 2004/078563 A1,

EP 1 339 024 A,

WO 2006/032354,

GB 2 340 644 A,

PCT/EP2007/060856, (of the same applicant),

US 2001/049066 A1.

All such means and methods require, to duplicate an electronically coded key, a unique storing and processing center of a large quantity of keys of the considered type, and of the transmission means, typically on-line (internet), which

are used to transmit and receive information from a local station that has to physically generate and deliver the duplicated key, and to which the client addresses, towards and from such storing, processing and coding/decoding center.

The teaching and the information showed in such documents can be generally well implemented, and some are actually realized.

However all of them show a common drawback which limits the operability and the quickness, and finally makes them less operable; such common drawback consists in that the key duplication requires:

a) the availability of an usually remote center, able of receiving, processing and generate the needed codes to make out the required key, and

b) telecommunication means to transmit and receive the coded data, from the local station to said processing center, and vice-versa.

Such requirements obviously imply the existence and the correct operation of a specific organization, of trained and co-ordinated personnel and distributed on the territory, and of specific procedures which have to be carried out by said personnel both in the local station and in the processing center.

Obviously all that implies a higher operation complexity, organizational limits and so less reliable and convenient for an user who only asks the duplication of its key, in an easy way and without depending on outer and far-away centers, and on transmission and receiving means for the coded data.

It is then desirable, and is the purpose of the present invention, of making out a method for the duplication of electronic keys which eliminates the described drawbacks, be easily and safely usable and which can be carried out with means available in the technique.

This and further purposes are achieved by a method according to the attached claims.

Features and advantages of the invention will result apparent from the following description, as non-limiting example, with reference to the attached figures, wherein:

-Figures 1A, 1B, 1C represent respective means which have to be operated in the invention, and which show in a simplified and symbolic way their type and content both in the hardware and in the software, which take part to the invention method,

-Figures 1E and 1F show respectively in a simplified form the logical flow-chart of the various devices comprised in the original key and in the vehicle central unit,

-Fig. 2 shows a flow-chart of the various steps of the method according to the principle of the invention,

-Fig. 3 shows a schematic of the relationship among the various steps of the method of Fig. 2, and of the relationship among the various means which take part in the method of the invention,

-Fig. 4 shows a flow-chart of the various steps of an improved embodiment of the method according to the invention,

-Fig. 5 shows a schematic of the relationship among the various steps of the method of Fig. 4, and of the relationships among the several means operating in each of said steps,

-Fig. 6 shows a logical and schematic flow-chart of the sequence of the functions and of the reciprocal relationships between an electronic key and the respective central unit, implemented to work at a «mutual authentication» mode,

With reference to the Figures from 1A to 1D, the method of the invention uses the following means:

A) an original key 1, which has to be duplicated, and provided with:
- a memory able of storing a secret code, a Password and an Identification code ID,
- a transponder comprising a suitable algorithm,
- a logical or computing unit,
- further devices, per se generally known, which allow to transmit and to receive, modulate/de-modulate the radio-electric signals transmitted and received.

While the Figures from 1A to 1D describe in a preferred way the content of the devices needed to the invention, Figure 1E and 1F in particular show the constructional and circuital content of the key and of the central unit installed into the vehicle, and which are needed to make the just cited devices to operate.

These devices are for long time mounted and working in the presently made vehicles, and therefore they are not new, but they represent without any exception the prior art, and moreover they do not need specific explanations as the man skilled in the art is perfectly able to immediately identify the construction type and

the related working.

B) a blank key 2; such blank key comprises the same electronic and mechanical devices of the original key 1, but logically, it misses the own codes to allow the working of the same blank key, i.e. the secret code, The ID, and the Password; however the algorithm, identical to that one installed in the original key, and already known, is already installed into the blank key 2; furthermore logically the blank key 2 is provided with a mechanical profile, in se known, able of permitting the introduction of the key itself into the vehicle lock, and of operating on said lock just as the original key.

C) the vehicle or central unit 3, the original key 1 is used with, and that has to use the duplicated key 2 too, comprises means and devices which basically perform the same function of the original key, i.e.

- a memory able of storing a secret code, a Password, and an Identification Code ID,
- a transponder containing a suitable algorithm, in se known,
- a logical or computing unit,
- further devices, in se generally known, which allow of transmitting, receiving, modulating/demodulating the radio-electric transmitted and received signals.

Moreover said central unit 3 is provided with transmission means able of transmitting an enough powerful radio-electric signal to the original key engaged to the vehicle lock, so as to start the procedure for the mutual authentication between the original key and the central unite itself.

D) a duplicating device 4, whose composition and operation are, in the principle, still similar to those of the blank key 2, and which therefore, for the sake of brevity, will not again be explained.

However it is reminded that said duplicating device is provided with the same algorithm installed into the two keys 1 and 2, and with a particularly quick and powerful computing unit, whose function will be described later on.

As for the duplicating device 4, it is generally divulgated in the patent application No. PCT/EP2007/060856 and there described as «reading/writing unit 13».

Therefore it acquires a data that is randomly encrypted into a first encryption form.

Then it is provided with:

a) an inner memory and a reading knob to write the code contained into said inner memory,

b) a small antenna able of receiving a radio-electrical signal containing a code, of transferring said code into said inner memory and, on a defined command on the writing knob, of re-transmitting outwards said code stored into it,

c) computing means particularly designed and produced to process at a high speed the encrypted secret code, and to identify in a very reliably way the secret code after its decryption,

E) a device able of receiving the electro-magnetic signals coming from the central unit 3 of the vehicle, and that therefore will be called sniffer 5.

Said sniffer 5 is a device able of receiving a radio-electric signal comprising one or more codes, to store said codes without making any processing on them, and to re-transmit them, according to a pre-determined command given to it, to said duplicating device 4.

It will be also apparent that the sole function of the sniffer 5 is to intercept the signal coming from the central unit 3, to store it and to deliver it, on a command of the duplicating device 4, into the same duplicating device 4 which stores it into the suitable memories.

The method of the invention is based on the following strategy: shortly speaking, said strategy is based on the «interception» of a part of the communication between central unit and original key, on the «substitution» of the central unit itself through a proper means (the duplicating means 4 which is therefore enabled to perfectly emulate the central unit 3), on the interrogation - for the second time - of the original key in order to catch also the last part of its information, and therefore in the transferring all information to the blank key.

To sum up, going now to the operating modes, in order to implement the duplication of the blank key, the original key is as «interrogated»; such interrogation is achieved by introducing it into the vehicle lock.

(it is here omitted the step of the recognition of the ID of the original key by the central unit 3; however such step will be resumed in the complete sequence of the operating steps, which will be repeated and explained with great detail in the

following).

So the central unit 3, in a known way, transmits a radio-electric interrogation signal, properly coded and encrypted by the algorithm in it installed; said interrogation encrypted signal, sent to the original key, is however received also by the sniffer 5.

The sniffer intercepts the communication between the original key and central unit, i.e.:

- the interrogation code transmitted by the central unit, and
- the secret code transmitted, as the answer, from the original key.

The sniffer 5 however stores only the encrypted code coming from the central unit 3 and neglects the encrypted code, as the answer, coming from the original key 1.

At this time the duplicating device 4, provided from the beginning with the same algorithm, is also provided with the interrogation code of the central unit 3.

This duplicating unit 4 is then enabled to implement a very complex and quite long-lasting mathematical processing, in order to exploit the algorithm installed into it to decrypt the secret code from the encrypted signal generated by the central unit 3.

Such very complex processing is based on specific mathematical functions, and in se well known to the man skilled in the art, and must be implemented by proper processing means, which may be either comprised inside the duplication device 4 itself, or made-up by external means, to be connected to the duplication device 4 itself; however such type of embodiment is not included in the present invention, and therefore it will not further detailed.

However it is possible that, from one interrogation only of the central unit, a decrypted signal which could result insufficient to identify in a reliable way the true central unit secret code; therefore an advantageous improvement of the instant method consists in the acting the original key into its lock a number of times and successively, so as to receive from said central unit a corresponding plurality of encrypted signals which are different from each other, but which are all, if properly decrypted, to supply information in all suitable to identify the exact secret code.

It is obviously possible to carry out only one activation of the central unit 3, which therefore replies with only one coded decrypted code; however said signal

could be insufficient for the duplicating device 4 to identify in an unambiguous way the secret code, and therefore it comes out to be particularly profitable to make out a sequence of activations of the central unit 3, what is practically done by making, at the beginning of the method, a series of successive rotations of the original key into its lock, which allows to give raise respective answering signals from the central unit which, properly recorded by the sniffer 5, are all flown into the duplicating device 4.

After having processed the received encrypted codes, the duplication device 4 selects the secret code from the central unit 3, and stores it into its memory.

By introducing then into the duplicating device 4 the original key 1, it, correctly interrogated by the duplication device 4 which transmits the secret code-encrypted by the algorithm now recognized by the central unit 3, replies as it received the signal of the central unit 3, as it receives the same signal; it therefore «believes» to be interrogated by the central unit, and therefore replies transmitting its own Password.

At this time the duplicating device is also informed about the Password of the original key, and therefore may store it and transfer it into the blank key, which successfully and as last operation is introduced into the duplication device 4.

To sum up, the invention strategy is based on the circumstance of «intercepting» the exchange of some information (Identification number ID, and secret code) between the original key and the vehicle central unit, of storing them and of transferring them on a proper storing means, i.e. the duplicating device 4.

It may code the central unit secret code, and then emulate the central unit working; therefore, when interrogated by the original key, receives from it the password too.

Then the duplicating device is informed of the secret data of the original key, i.e. the ID, the secret code and the PASSWORD.

Finally all these information are transferred from the duplicating device 4 into the blank key, which then acquires all information of the original key.

With reference to the Fig. 2, the actual practical method, represented in great detail through a flow-chart, is the following:

Step A) the original key is inserted into the vehicle lock, and is rotated until it closes the electric circuit which activates the central unit of the vehicle itself; profitably such rotation of the original key, and the relevant activations of the

central unit 3, are more than one, and are made up in sequence.

It was also verified and evaluated that the optimum number to get a sufficient number of encrypted codes, and that may be afterwards certainly decrypted by the duplicating device 4 to get the secret code, is of three activations/rotations of the original key inside the respective lock.

It is in the fact apparent that the more the information available on a certain condition, the more are the chances of faithfully representing that condition and of avoiding identification mistakes.

Step B) The central unit transmits a radio-electric signal comprising a code of identification request of the original key, that is the ID, which is an «open» code;

Step B-B) The original key receives such signal requesting of said «open» ID, and transmits that code to the central unit 3;

Step B-C) The central unit receives said open ID code and compares it to a previously stored ID code; if it is recognized, such recognition allows the procedure continuation;

Step C) The procedure goes on; the central unit 3 sends a random encrypted code which comprises the secret code, from the algorithm, to the original key 1;

Step D) An intercepting device 5, called sniffer, arranged close to the original key, intercepts the radio-electric signal which contains both the ID of the original key, and the interrogation of the central unit, and the key reply, i.e. its secret code in an encrypted form; however the latter is not stored, and the sniffer records and stores the central unit 3 interrogation only (the sniffer positioning close to the lock is preferably done before introducing the original key);

Step E) Said sniffer 5 is introduced into said duplicating device 4;

Step F) Said duplicating device 4 emits a radio-electric signal which reaches said sniffer 5;

Step G) Said sniffer transmits to said duplicating device 4 an electric signal with the random code encrypted by the algorithm which comprises the secret code, stored during the Step D;

Step H) The duplicating device 4 stores the random code generated by the central unit 3 and, through a plurality of mathematical functions and proper computing means decrypts said encrypted code, so obtaining the sought code.

Now the duplicating device contains the secret code, decrypted, of the original key 1.

Step I) The sniffer 5 is removed from the duplicating device 4;

Step L) Into the duplicating device 4 the original key is inserted;

Step M) The duplicating device interrogates the original key with a suitable radio-electric signal which comprises the secret code encrypted by its algorithm, so emulating the central unit operation;

Step N) The original key replies by transmitting a further own code, i.e. the encrypted password;

Step O) The duplicating device stores such Password;

Step P) The original key is removed from the duplicating device;

Step Q) The blank key is introduced into the duplicating device;

Step R) The duplicating device transmits a radio-electric signal to said blank key, so transferring to it the PASSWORD, the secret code and the ID;

Step S) The blank key stores into a definite memory all said three codes.

So the duplication of the blank key is completed.

To be noted now a profitable improvement of the method, which allows a certain simplification; in the facts, if in the Step D or of interception, the sniffer 5 intercepts and stores also the secret code of the original key, the Steps M and N would be no more needed, as the secret code transmitted by the original key would have been already transmitted to the sniffer 5, and then from it to the duplicating device 4, which could immediately emulate the central unit 3 to interrogate the original key to let it transmitting to himself the respective Password.

However such methodological simplification raises the risk that, as the signal carrying the secret code of the encrypted key is very weak, due to the fact that it is emitted by the original key which is supplied by the radio-electric signal emitted by the central unit, then such signal with the encrypted secret code may be easily jammed, or anyway may be received in an incomplete or wrong, which obviously causes the interruption of the key duplication procedure.

It is to be noted moreover that some of the above described Steps are typical manual operations, that an outer operator must perform on the described means, as introduce a key and rotate it inside the lock, extract a key, activate the duplicating device, move the sniffer etc...., as the remaining steps are automatic steps which are carried out by said means in a known way.

More specifically the manual steps are Steps A, E, I, L, Q.

Steps B-C, H, O, S are steps of mere processing/comparison /storage into

the respective devices, without any relationship to the other devices and therefore are only symbolically drafted.

Step D regards the intercepting action of the sniffer 5, which however shall be manually arranged and prepared close to the lock, and therefore it is intended that the sniffer positioning 5 requires an additional operation which here is not listed as a real operating Step.

By carefully observing the figure 2, it turns out to be apparent, also only by a visual check, the nature of the method strategy; as a matter of facts the original key 1 and the central 3 are put into relationship to each other (Steps A and B), so that the central unit is made to recognize and store the content of the codes stores in the original key; afterwards said codes are intercepted by the sniffer 5 (Steps C and D), which provides to transmit them to the duplicating device 4 (Steps E, F and G).

At this time the original key 1 also is introduced into the duplicating device 4 (Steps I, L), which interrogates said original key (Steps M, N) to get the answer with the password (Steps M, N).

Finally, after the Step P all coded information, originally stored in the original key 1, are contained inside the duplicating device 4, and therefore it is now possible to introduce the blank key 2 and transfer to it all said coded information.

The just described solution, which is effective, sure, and innovative, allows then a complete duplication of a blank key from an original key which uses the technique of the "mutual authentication", without having to connect to any data-base placed in a remote site, accessible only with on-line means to assure the security of the code transfer.

However such method implies the presence and the working of the sniffer 5; but such constraint and need are not deprived of penalization; in the facts the presence of the sniffer 5 shows some critical aspects, as it has to work with radio-electric signals that may be miss-received and therefore may introduce errors in the transmission of information and codes; moreover the sniffer operations are delicate, and precise operations which must be carried out with great caution and with the right sequence; all that may be troublesome and unpleasant in a working environment which is little trained and sensible to the remarkable technical complexity of the involved means and methods. Such drawback often is considered not agreeable, even because it requires a cost increase and a higher

complexity of the duplication procedure.

In order to avoid such problems, in the following a method is described which allows to carry out the duplication of an original key without using the sniffer.

The strategy of such improvement consists in that the blank key is used as sniffer, in the meaning that the central unit codes are introduced into the duplicating device through the blank key itself.

However to make it possible to use the blank key as "carrier" of such information, the blank key must have been previously loaded with the ID of the original key.

To this purpose, the duplicating device is employed as means to transfer the ID from the original key to the blank key; this one, after having been loaded with the ID, is used to receive from the vehicle central unit its secret code, and to store it, which then may be acquired, into the decrypted form, by the blank key itself.

It is here reminded that the secret code is the same both for the central unit 3 and for the original key 1; in the facts it could not be different, as if it were the case, it would be impossible to carry out the mutual authentication.

Therefore the blank key may transfer its still encrypted secret code into the duplicating device, which decrypts the secret code through suitable computing means and with advanced mathematical techniques.

Said computing means and said mathematical techniques are in se easily deductable from the prior art and generally are in the knowledge of the man skilled in the art, and therefore they will not be repeated.

The duplicating device now is informed of the central unit secret code, and therefore it is able of emulating it.

At this time the duplicating device is brought exactly in the same conditions where it is according to the previous procedure after the Step L, i.e. it contains both the ID and the decrypted secret code.

Therefore from this time on the procedure goes on exactly according to the Steps N, O, P, Q, R, S above described, obviously after having introduced the original key into the duplicating device.

More precisely, and with reference to Fig. 3, the flow diagram of said procedures as follows:

A-1) the original key is introduced into the duplication device 4,

B-1) the duplication device emits a radio-electric signal which interrogates the

original key,

C-1) the original key responds by emitting a radio-electric signal which contains its ID,

D-1) Said ID is received and stored into the blank key,

E-1) The blank key is introduced into the vehicle lock and one or more attempts of starting the engine is made (the reason of carrying out more than one attempt has been already explained before),

F-1) at each attempt of starting the engine, the vehicle center unit transmits to the blank key an electric signal which contains a random code encrypted by the algorithm which comprises the secret code,

G-1) The blank key is removed from the vehicle lock and introduced into the duplication device,

H-1) The duplicator through suitable computing and mathematical functions, in se known, decrypts the secret code and stores it,

L-1) the blank key is removed from the duplicating device,

M-1) the original key is introduced into the duplicating device.

From this time on, the procedure goes on as from the previous Step L, i.e.:

N-1) the duplicating device interrogates the original key with a proper radio-electric signal containing the secret code, so emulating the central unit operation,

Step O-1) the original key responds by transmitting a new own code, the PASSWORD;

Step P-1) the duplicating device stores such PASSWORD,

Step Q-1) the original key is removed from the duplicating device,

Step R-1) the blank key is introduced into the duplicating device,

Step S-1) the duplicating device transmits a radio-electric signal which contains: said PASSWORD, and the secret code, to said blank key; in the facts the ID has been already transmitted and stored during the previous Steps C-1 and D-1,

Step T-1) The blank key stores into a defined memory said PASSWORD and the secret code.

It should have been noted that the flow diagram of said Figure 3 describes the procedure only from the initial Step A-1 until the Step M-1.

As a matter of facts, the procedure goes on exactly as from the Step L of Figure 2, to which it is referred for better clarity and brevity.

CLAIMS

1) Method for the duplication of original (1) electronic keys provided with coded and encrypted electronic authentication means, comprising:

- an Identification Code (ID),
- an encrypted secret code,
- a Password,
- an algorithm,
- data storage and computing means,

able of being used in vehicles provided with a central processing unit (3) able of storing:

- an Identification Code (ID),
- an encrypted secret code,
- a Password,
- an algorithm,

said duplication method being able of obtaining a duplicated key based on a blank key, which is originally provided with:

- an algorithm,
- data storage means able of storing said Identification Code (ID), said secret code and said Password,

wherein said data storage means being initially empty, **characterized in that** it comprises the following steps:

-an interception step of a radio-electric interrogating signal including a random code encrypted by the algorithm comprising the secret code transmitted by said central processing unit (3),

- a step of storing said random code by an external means (5),
- a step of transferring random code into an auxiliary means, as a key duplicating device (4),
- a decryption step of said secret code by said key duplicator (4),
- a step of interrogating, through a radio-electric signal including said secret code emitted by said duplicator, to said original key,
- a step of receiving a second code (Password) transmitted by said

original key to said duplicator, and of its storing into said duplicator,

- a step of transferring said second code (Password) to said blank key.

2) Method according to claim 1, **characterized in that** it comprises the following steps:

Step A) the original key (1) is introduced into the vehicle lock, and is rotated until an electric circuit is closed, which activates said central processing unit (3) of the same vehicle,

Step B) said central processing unit transmits a radio-electric signal comprising a code of requesting the identification of said Identification code (ID) of the original key,

Step B-B) the original key receives said Identification code, and transmits to the central processing unit the Identification code (ID) stored in it;

Step B-C) the central processing unit receives said code (ID) and compares it to a ID code previously stored; if it is recognized (authenticated), the present method is continued;

Step C) said central processing unit (3) sends its encrypted secret code to the original key (1),

Step D) an interception device (sniffer, 5), placed close to the original key, intercepts the radio-electric signal containing both the interrogation of the central processing unit, and the original key reply, i.e. its encrypted secret code, and stores said interrogation code of the central processing unit (3) and the Identification code (ID) transmitted by the original key;

Step E) said interception device (5) is introduced into said key duplicator (4),

Step F) said key duplicator sends a radio-electric signal to said interception device (5),

Step G) said interception device (5) transmits to said key duplicator (4) a radio-electric signal with the two codes stored in the Step D,

Step H) said key duplicator (4) stores the encrypted secret code produced by the central processing unit (3) and, through a plurality of mathematical functions and computation means decrypts said encrypted secret code, and obtains the secret code,

Step I) said interception device is removed from said key duplicator (4),

Step L) the original key is introduced into said key duplicating device (4),

Step M) the key duplicating device interrogates the original key with a proper radio-electric signal containing the secret code encrypted by its algorithm, so emulating the central processing unit operation,

Step N) the original Key replies by transmitting its encrypted Password,

Step O) the key duplicating device stores said Password,

Step P) the original key is removed from said key duplicating device,

Step Q) the blank key is inserted into the key duplicating device,

Step R) the key duplicating device transmits an radio-electric signal to said blank key, with said Password, the secret code and the ID,

Step S) the blank key stores into a defined memory said three codes (Password, secret code and ID).

3) Method according to claim 1, **characterized in that** it comprises the following steps:

A-1) the original key (1) is inserted into said key duplicating device (4),

B-1) said key duplicating device emits a radio-electric signal interrogating the original key,

C-1) the original key reacts by transmitting a radio-electric signal containing its Identification code (ID),

D-1) said ID is received and stored into the blank key,

E-1) the blank key is introduced into the vehicle lock, and one or more attempts for the vehicle ignition are tried,

F-1) at any attempt for the vehicle ignition the central processing unit transmits to the blank key a radio-electric signal containing its encrypted secret code,

G-1) the blank key is removed from the vehicle lock and introduced into the key duplicating device,

H-1) the key duplicating device through proper computing means and mathematical functions decrypts and stores the secret code,

L-1) the blank key is removed from the duplicating device,

M-1) the original key is introduced into the key duplicating device, and it also comprises the successive Steps (from Step A to Step S) according to claim 2.

4) Method according to claim 3, **characterized in that** the attempts described in said Step E-1 for the vehicle ignition are tried three times.

5) Method according to any of the previous claims, **characterized in that** during said Step D said interceptor device (5) receives and stores also the signal bearing the encrypted secret code stored into the original key (1), and in that during said Step G said interceptor device (5) transmits to said key duplicating device (4) a radio-electric signal which includes both said Identification code and said encrypted secret code of the original key itself.

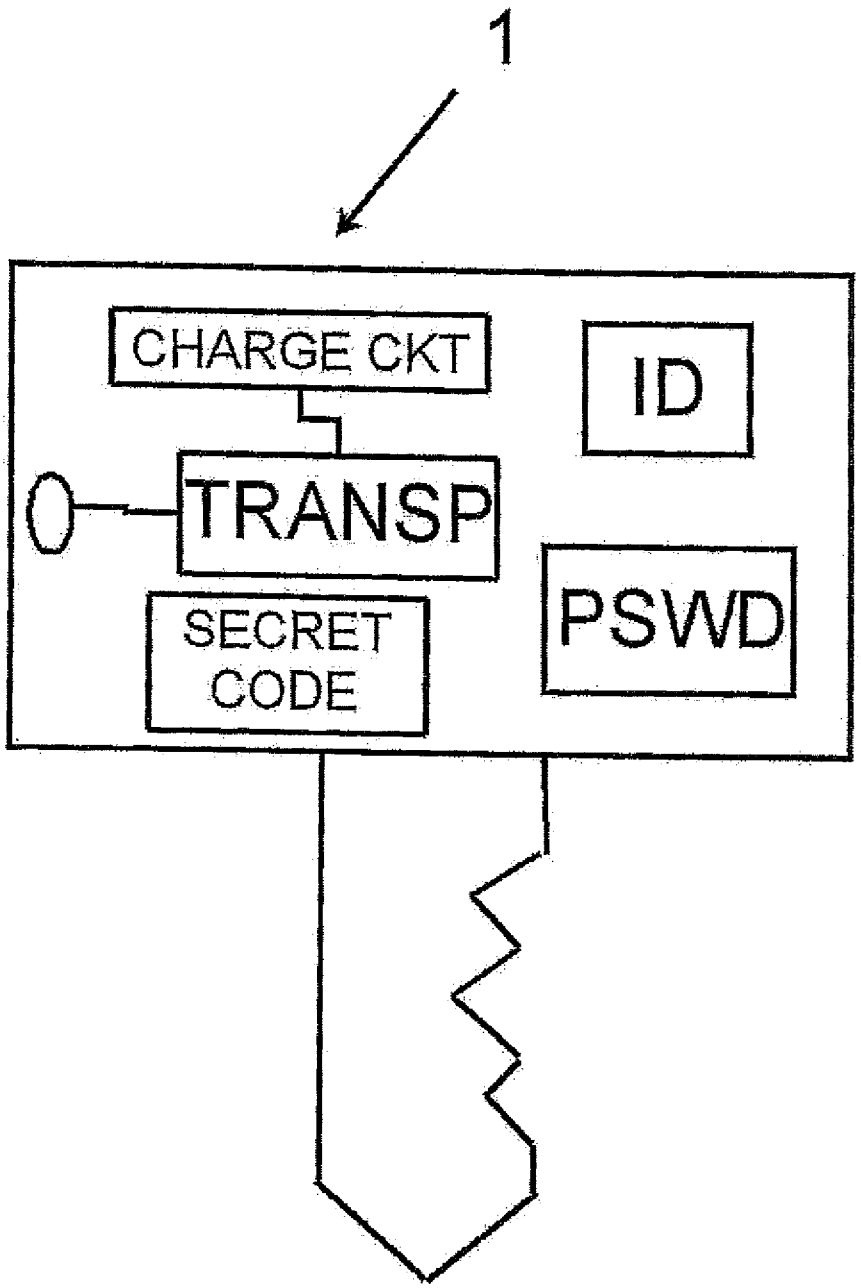


FIG. 1A

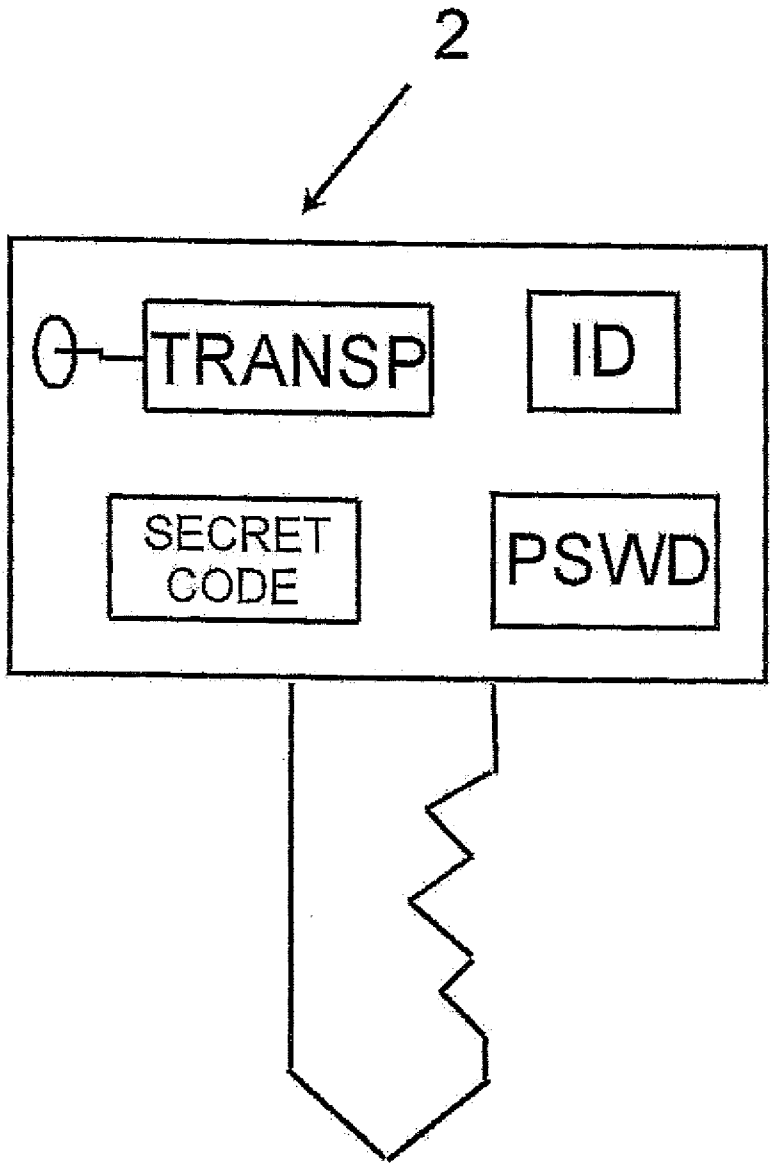


FIG. 1B

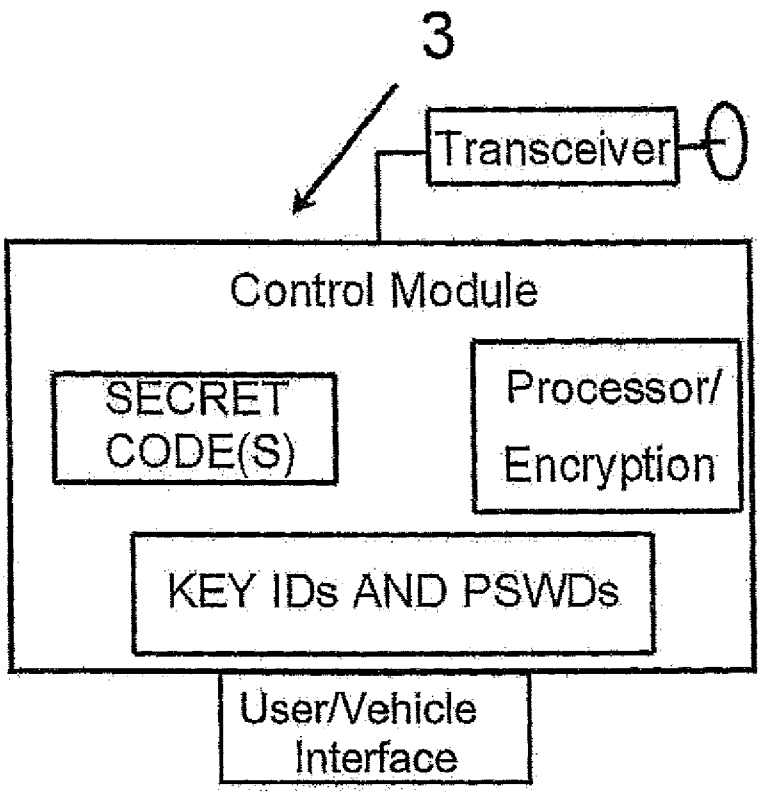

3
Transceiver
Control Module
SECRET CODE(S)
Processor/ Encryption
KEY IDs AND PSWDs
User/Vehicle Interface

FIG. 1C

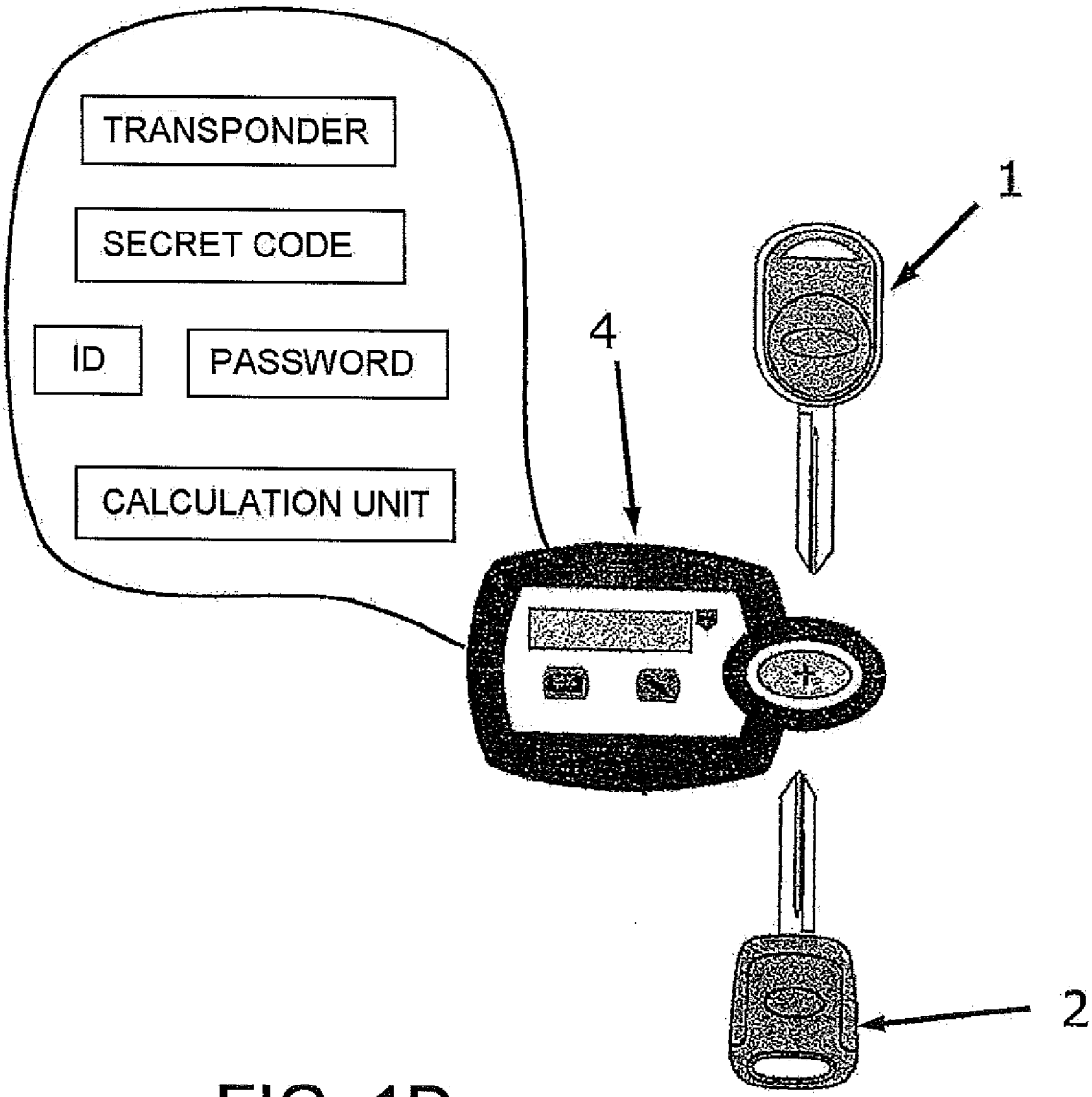


FIG. 1D

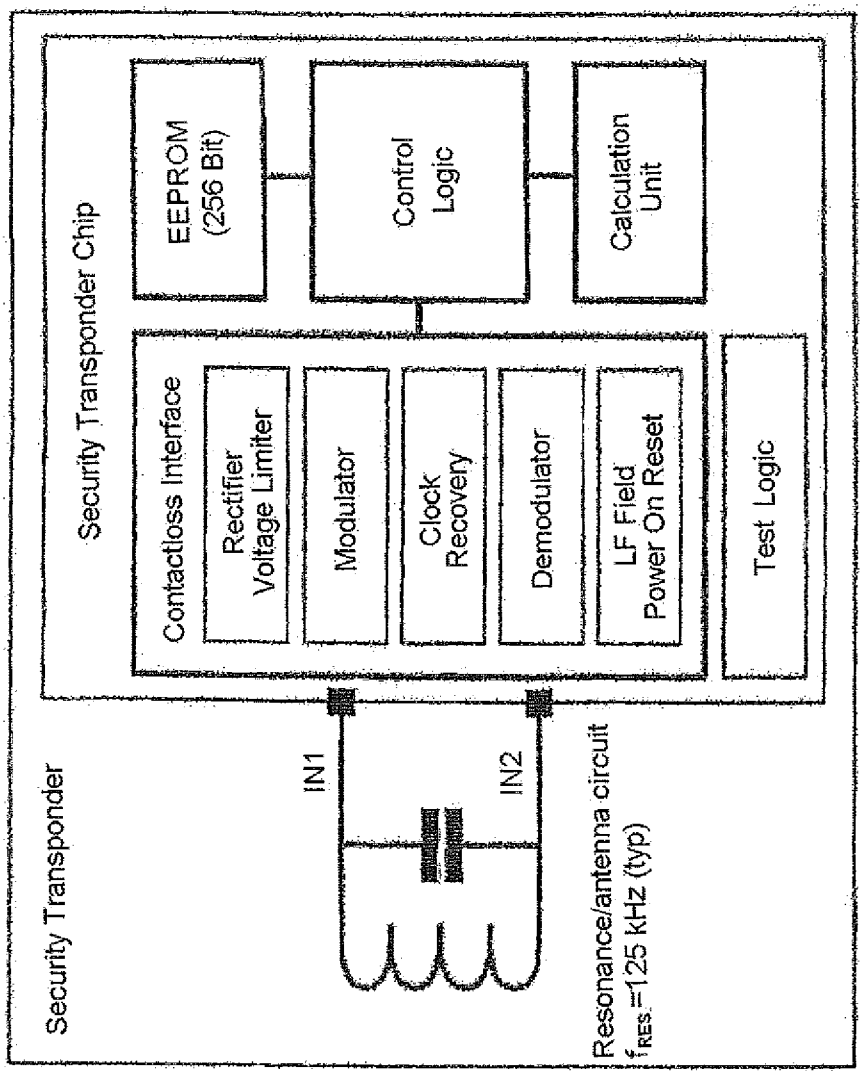

Security Transponder
Security Transponder Chip
EEPROM (256 Bit)
Control Logic
Calculation Unit
Contactless Interface
Rectifier Voltage Limiter
Modulator
Clock Recovery
Demodulator
LF Field Power On Reset
Test Logic
IN1
IN2
Resonance/antenna circuit
f_{RES}=125 kHz (typ)

FIG. 1E

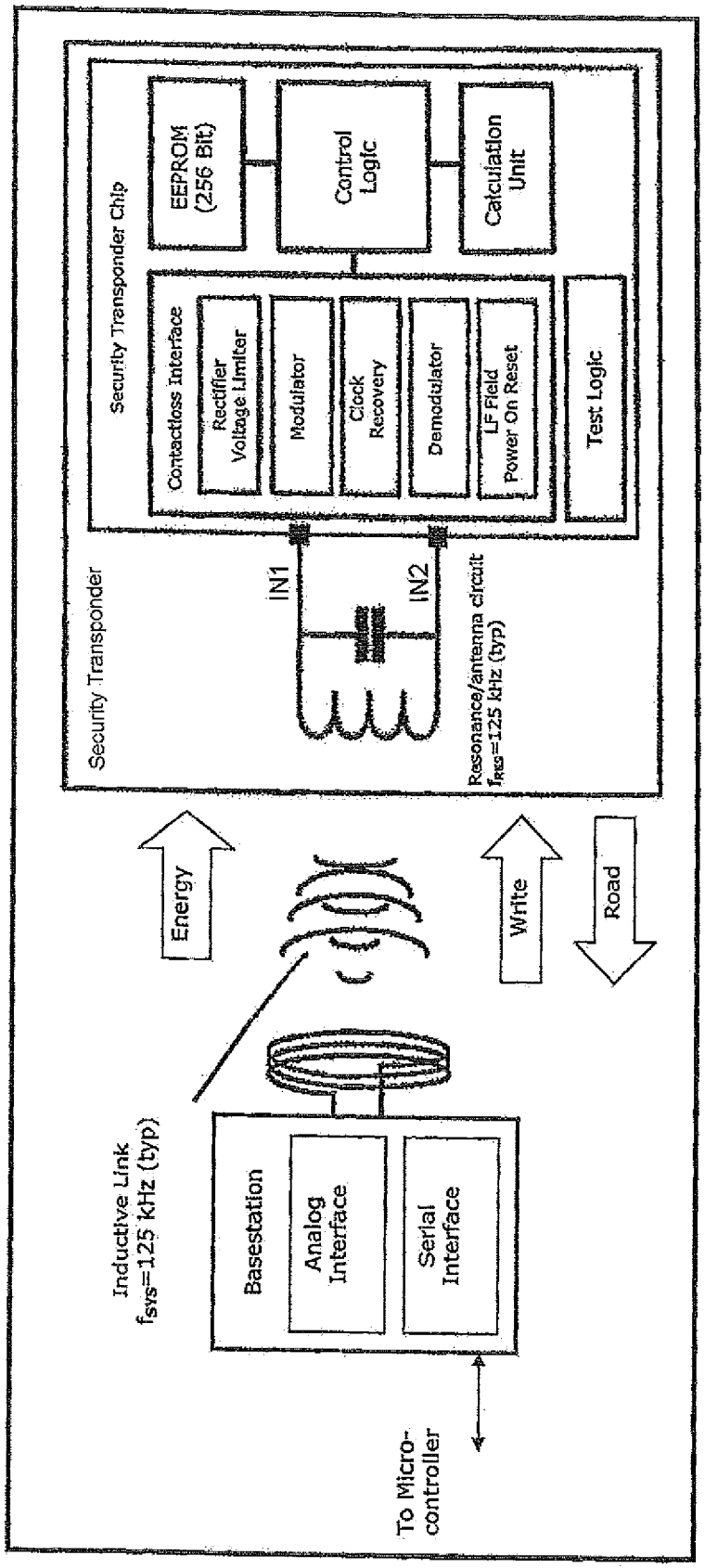

Security Transponder
Security Transponder Chip
EEPROM (256 Bit)
Control Logic
Calculation Unit
Contactless Interface
Rectifier Voltage Limiter
Modulator
Clock Recovery
Demodulator
LF Field Power On Reset
Test Logic
IN1
IN2
Resonance/antenna circuit f_{RES}=125 kHz (typ)
Energy
Write
Road
Inductive Link f_{sys}=125 kHz (typ)
Basestation
Analog Interface
Serial Interface
To Micro-controller

FIG. 1F

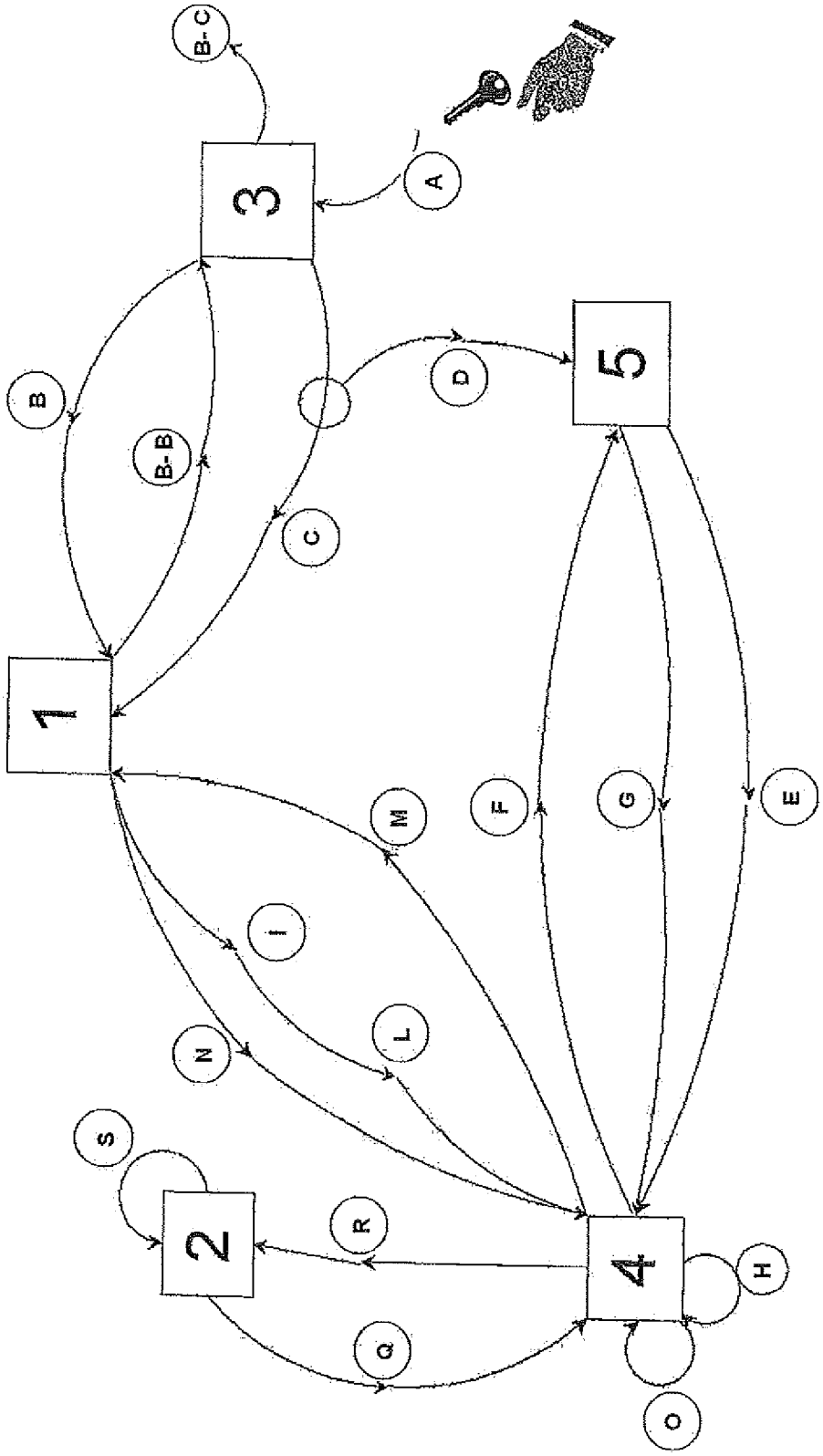
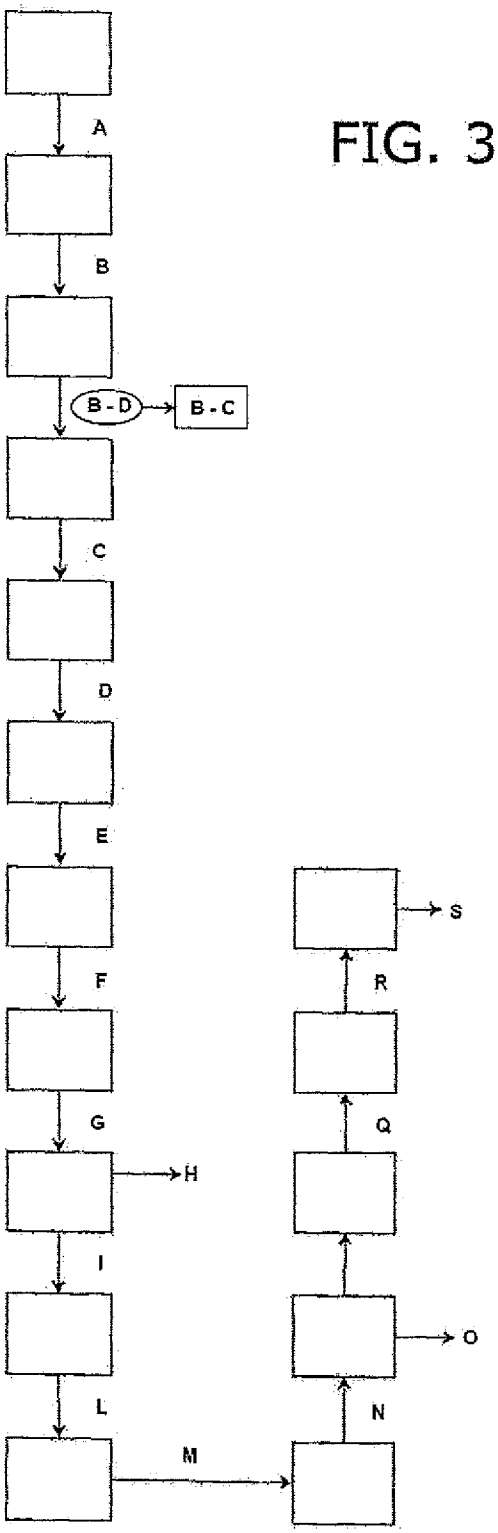


FIG. 2

FIG. 3



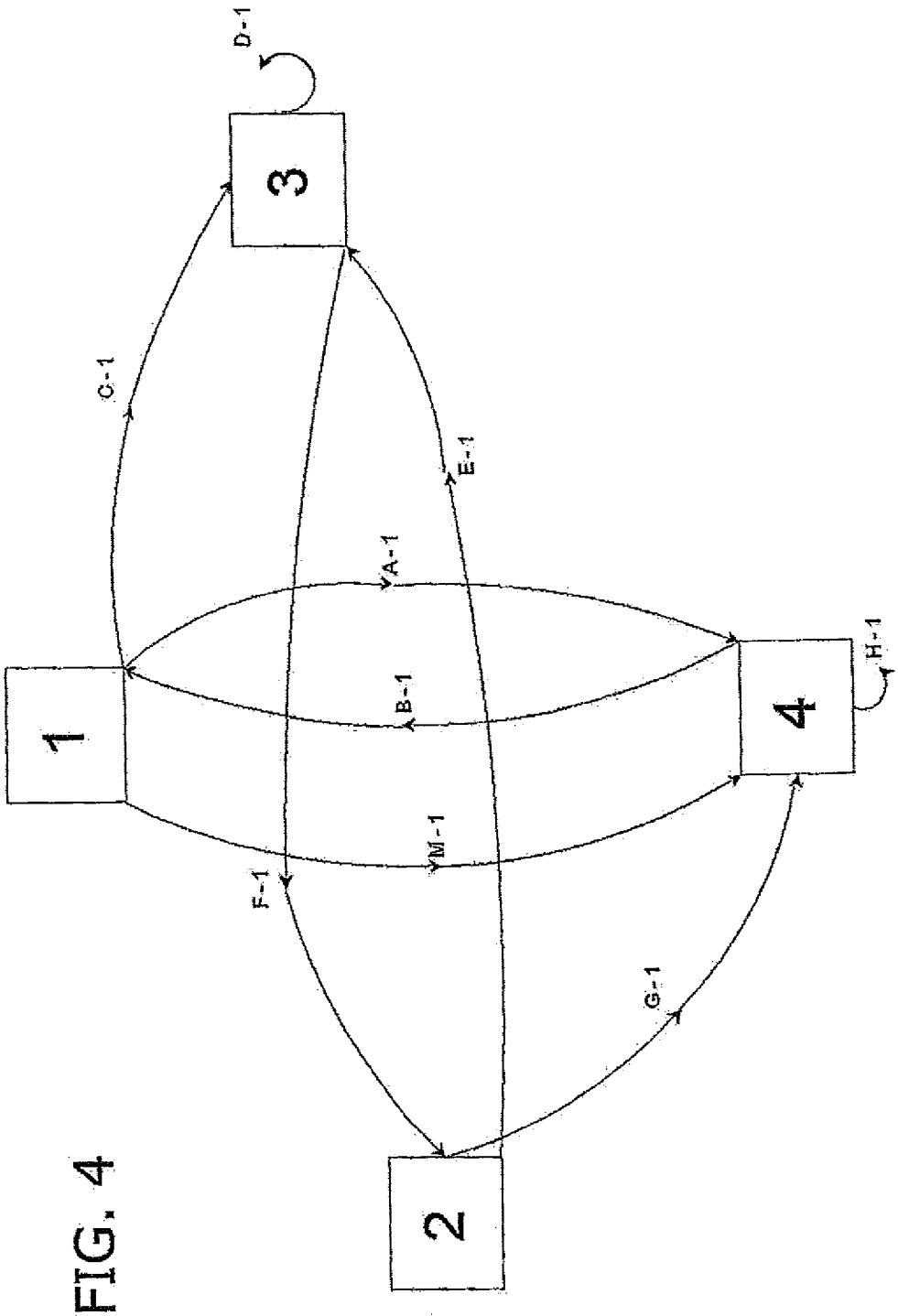


FIG. 4

FIG. 5

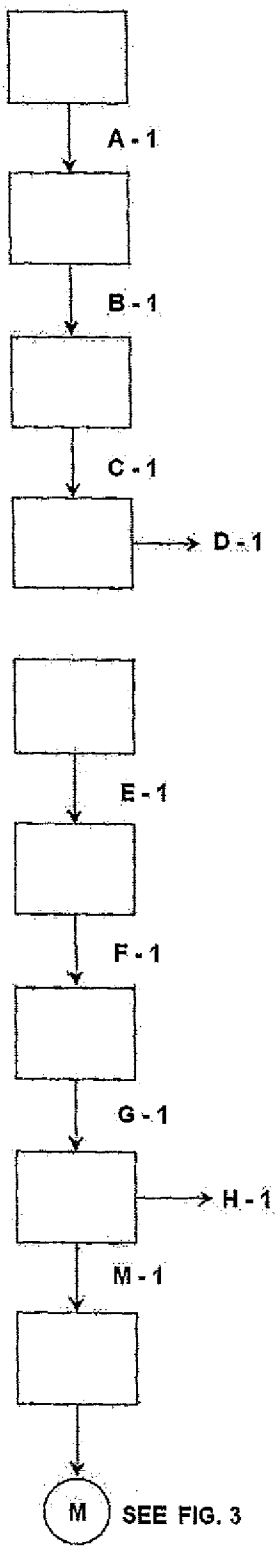
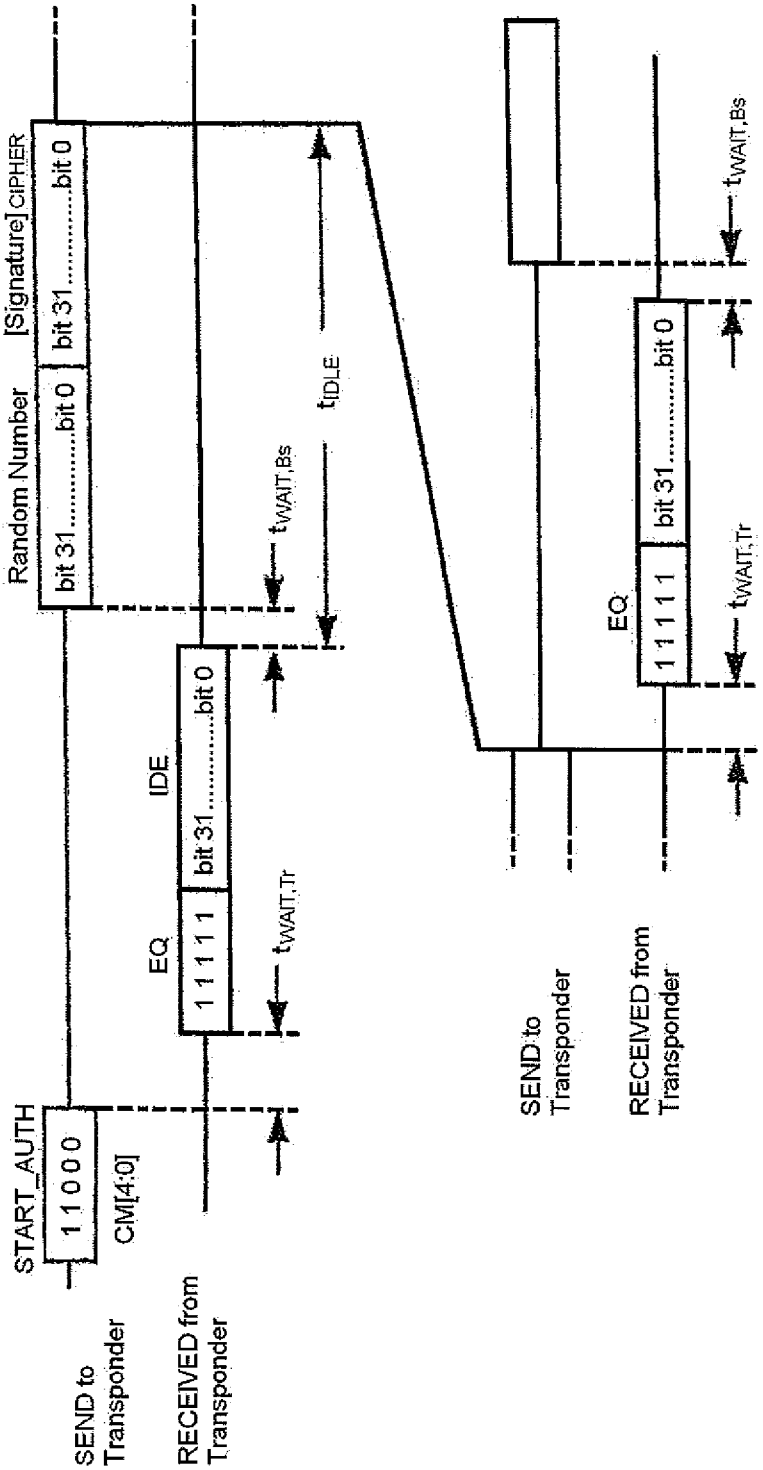


FIG. 6


START_AUTH
11000
CM[4:0]
SEND to Transponder
RECEIVED from Transponder
EQ
11111
IDE
bit 31.....bit 0
tWAIT,Tr
Random Number
[Signature] CIPHER
bit 31.....bit 0
tWAIT,Bs
tIDLE
SEND to Transponder
RECEIVED from Transponder
EQ
11111
bit 31.....bit 0
tWAIT,Tr
tWAIT,Bs

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2010/054015

A. CLASSIFICATION OF SUBJECT MATTER
INV. G07C9/00 B60R25/00
ADD.

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

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.
Y	WO 2008/145199 A1 (BIANCHI 1770 S P A [IT]; CHIES EZIO [IT]; LONGATO STEFANO [IT]) 4 December 2008 (2008-12-04) cited in the application abstract page 1, line 14 - page 2, line 26 page 4, line 26 - page 5, line 27 page 6, line 30 - page 9, line 8 figure 4	1-5
Y	DE 44 18 069 C1 (DAIMLER BENZ AG [DE]) 24 August 1995 (1995-08-24)	1,2,5
A	column 2, line 10 - line 36	3,4
Y	US 6 710 700 B1 (TATSUKAWA HIROFUMI [JP] ET AL) 23 March 2004 (2004-03-23)	3,4
A	column 11, line 50 - column 12, line 34	1,2,5

-/--

[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
23 April 2010	06/05/2010

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, Fax: (+31–70) 340–3016	Mandato, Davide

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2010/054015

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	GB 2 424 293 A (LEAR CORP [US]) 20 September 2006 (2006-09-20) page 1, line 30 - page 2, line 13 page 6, line 3 - line 23	1-5

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2010/054015

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2008145199 A1	04-12-2008	NONE	
DE 4418069 C1	24-08-1995	US 5596317 A	21-01-1997
US 6710700 B1	23-03-2004	DE 10047967 A1	31-10-2001
		JP 2001262890 A	26-09-2001
GB 2424293 A	20-09-2006	DE 102006011685 A1	21-09-2006
		US 2006208069 A1	21-09-2006