



(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
11.11.2015 Bulletin 2015/46

(51) Int Cl.:
G07C 9/00 (2006.01)

(21) Application number: **14167535.5**

(22) Date of filing: **08.05.2014**

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME

(71) Applicant: **BASICWORX ENGINEERING GmbH**
70191 Stuttgart (DE)

(72) Inventor: **Khoury, Jean**
70191 Stuttgart (DE)

(74) Representative: **DREISS Patentanwälte PartG mbB**
Friedrichstrasse 6
70174 Stuttgart (DE)

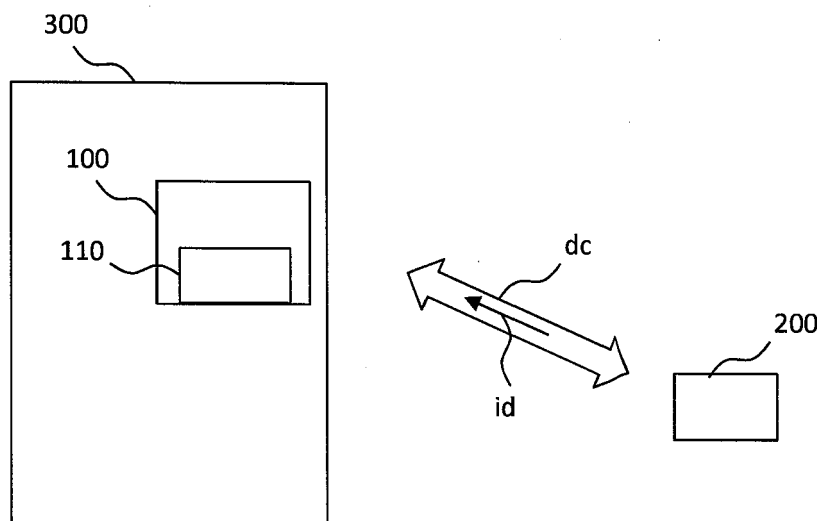
(54) **Security device and method of operating a security device**

(57) The invention relates to a security device (100) for granting access to a structure (300), particularly a vehicle or a building, wherein said security device (100) is configured to receive identification information (id) from a key device (200) by means of a contactless data connection (dc) and to grant or deny access to said structure (300) depending on said identification information (id), characterized in that said security device (100) is further

configured to

- receive (400) from said key device (200) information on at least one remote parameter of said key device (200), said remote parameter comprising at least one of a remote environmental parameter (rep) and a remote movement parameter (rmp) of said key device (200), and to
- grant (410) or deny access to said structure (300) depending on said at least one remote parameter.

Fig. 1



Description

[0001] The present invention relates to a security device for granting access to a structure, particularly a vehicle or a building, wherein said security device is configured to receive identification information from a key device by means of a contactless (i.e., wireless or the like) data connection and to grant or deny access to said structure depending on said identification information.

[0002] The invention further relates to a method of operating such security device. The invention also relates to a security unit for a security device.

[0003] Prior art security devices of the aforementioned type are e.g. used to control access to land vehicles such as cars, wherein the security device checks whether a key with which a data connection is established provides proper identification information prior to granting access to the vehicle. For example, the key may represent a car key with a wireless interface suitable for exchanging data with the security device by means of RF (radio frequency) signals in a per se known manner. After receiving identification information, which may preferably be encrypted, from the key, the prior art security device verifies whether the identification information is correct, e.g. by comparing to predetermined reference information.

[0004] Disadvantageously, the prior art security devices and keys do not prevent relay-type attacks, where a transceiver station is provided between the security device and the key extending a radio range for the contactless data connection therebetween. In these cases, an attacker may initiate a conventional key verification process e.g. by actuating a car door handle, which will trigger a contactless data transmission from the security device to the car key requesting said identification information of the car key. Due to the RF range extension by means of the transceiver station, said contactless data transmission from the security device will still arrive at the car key, even if the car owner with the key is comparatively far away from the car and thus cannot notice the attacker actuating said car door handle. If the conventional car key receives the contactless data transmission from the security device, it will respond, by means of a contactless data transmission, as usual with the proper identification information. Again, this response will also undergo RF range extension due to the transceiver of the attacker, so that the conventional security device of the car will properly receive suitable identification information of the car key and grant access to the car, although the owner carrying the key is far away.

[0005] In other words, since in this scenario, the security device still communicates with the original key device, the conventional identification processes may still be performed without the security device getting aware of the fact that a transceiver or relay station is arranged between the key device and the security device.

[0006] Thus, a proper authentication of a user of the security device (or its key) may be performed even if the user with its key device is at a remote location with respect

to the security device.

[0007] Without the aforementioned RF range extension, the conventional systems may offer an acceptable degree of security since in view of the limited RF range of the contactless data connection there is a high probability that a user carrying the key will notice the presence of an attacker actuating the door handle as long as the user with the key is in the nominal RF range of the security device.

[0008] However, as the aforementioned relay attacks do only require comparatively few specialized hardware components such as e.g. RF transceivers with a rather limited bandwidth, it is highly desirable to be able to prevent the relay-type attacks.

Summary of the invention

[0009] Thus, it is an object of the present invention to provide an improved security device and an improved method of operating a security device which avoid the disadvantages of the prior art, and which in particular prevent relay-type attacks.

[0010] Regarding the security device of the aforementioned type, this object is achieved by said security device being further configured to receive from said key device information on at least one remote parameter of said key device, said remote parameter comprising at least one of a remote environmental parameter and a remote movement parameter of said key device, and to grant or deny access to said structure depending on said at least one remote parameter. I.e., according to an embodiment, said remote parameter may comprise said remote environmental parameter. According to a further embodiment, said remote parameter may comprise said remote movement parameter. According to further embodiments, said remote parameter may comprise both remote environmental parameter(s) and remote movement parameter(s).

[0011] According to a preferred embodiment, the data connection may be a contactless or wireless data connection. According to a further embodiment, the data connection may also be a wired connection. Generally, the principle according to the embodiments may be applied independently of the specific type of the data connection, i.e. independent of a specific implementation of a physical layer in the sense of the ISO/IEC 7498-1 standard.

[0012] It is to be noted that the attribute "remote" in the context of parameters will be used herein to denote parameters associated with the location and/or surroundings of the key device, in contrast to the security device, whereas the attribute "local" in the context of parameters will be used herein to denote parameters associated with the location and/or surroundings of the security device.

[0013] Thus, according to the principle of the embodiments, in addition to the conventional identification process of the prior art devices, at least one parameter ("remote parameter") of the key device is evaluated, e.g. for plausibility, prior to granting/denying access to the struc-

ture by means of the security device. Thereby, an increased degree of security is attained.

[0014] For example, according to one embodiment, a remote movement parameter of the key device may comprise data of an acceleration sensor which detects the acceleration of the key device in one or more spatial dimensions. The key device may determine such acceleration data and forward it as remote movement parameter in the sense of the present embodiment to the security device, i.e. together with the conventionally transmitted identification information and/or separated therefrom. Instead of only considering the identification received from the key device, the security device may now additionally consider the remote movement parameter of the key device, i.e. according to the present embodiment the acceleration data of the key device. For example, if the acceleration data of the key device as received by the security device indicate that no substantial acceleration values are recorded by the key device, the security device may conclude that the key device is presently not substantially moved or accelerated, but may e.g. be placed on a table top or the like. From this conclusion it may further be derived that in the present configuration, no manual interaction with the key device such as a manual handling of the key device has taken place, because this would have led to some non-vanishing acceleration values related to the key device. From this analysis, the security device may advantageously conclude that no authorized access to the security device or the structure protected thereby is currently made. Consequently, the security device may deny access to the structure.

[0015] According to a further embodiment, said security device is configured to determine at least one local parameter of said security device, said local parameter comprising at least one of a local environmental parameter and a local movement parameter. This enables to even further increase the security of the overall system since said at least one remote parameter of the key device received by the security device may e.g. be checked for plausibility with the at least one local parameter of the security device.

[0016] I.e., according to an embodiment, said local parameter may comprise said local environmental parameter. According to a further embodiment, said local parameter may comprise said local movement parameter. According to further embodiments, said local parameter may comprise both local environmental parameter(s) and local movement parameter(s).

[0017] According to a further embodiment, the security device is configured to compare said at least one local parameter with said at least one remote parameter, and to grant or deny access to said structure depending on the comparison of said at least one local parameter with said at least one remote parameter. For example, both the key device and the security device may determine air pressure information of their respective surroundings as environmental data in the sense of the present embodiment. By comparing its local air pressure with the air

pressure data received from the key device in the form of the remote environmental parameter, the security device may determine whether it is likely that the key device is positioned close to the security device or not. For instance, if there is a significant difference in the air pressure as determined by the security device as a local air pressure and the air pressure from the key device, it may be concluded that there is a non-vanishing altitude difference between both devices. Such constellation may e.g. occur when the security device is built in into a land vehicle such as a car parking in front of a building. The owner of the car carries a key device according to the embodiment with him. When the owner of the car enters the building and moves upwards some levels of the building the afore-explained altitude difference between the security device and the key device may be obtained. From this constellation, it can be concluded that even if the security device and the key device are currently maintaining a contactless data connection, no access to the car is desired at the moment. Insofar, the security device may deny access to the car. However, if the pressure difference between the air pressure at the security device and the air pressure at the key device does not exceed a predetermined threshold, the security device may conclude that the key device, and thus most probably also the owner of the car, is sufficiently close to the car and its security device so that access to the car may be granted.

[0018] According to a further embodiment, said security device comprises a sensor device for determining at least one local environmental parameter, wherein said sensor device is configured to determine at least one of the following parameters: air pressure, temperature, humidity, concentration of one or more gases such as e.g. carbon monoxide or nitrogen dioxide, electric and/or magnetic and/or electromagnetic signals, acoustic signals, radioactive radiation.

[0019] According to a further embodiment, said security device is configured to determine at least one local movement parameter of said security device, wherein said local movement parameter comprises at least one of: acceleration of said security device, direction of movement of said security device, position of said security device.

[0020] According to a further embodiment, it is possible that a single sensor device which may comprise plurality of different sensors, may be provided to gather one or more of the aforementioned parameters (environmental and/or movement).

[0021] According to a further embodiment, one or more of the aforementioned parameters may be determined by the security device and by the key device, and a comparison based the so determined data may be made, e.g. by means of the security device upon receiving remote parameter data of the key device.

[0022] According to a further embodiment, a sensor device of the security device and/or key device may e.g. comprise a global positioning system (GPS) receiver

and/or an inertial navigation system relying on acceleration measurements for determining position and/or orientation of the sensor device or the security device, respectively in space. Also, rotational rate and/or earth magnetic field sensors may be comprised within such sensor device according to an embodiment.

[0023] According to a further embodiment, alternatively or additionally to the above-mentioned parameters, radio signals may be evaluated such as e.g. from base stations of cellular mobile communications systems which may e.g. adhere to the well-known GSM (global system for mobile communications), UMTS (universal mobile telecommunications system), LTE (long term evolution) or LTE-A (LTE advanced) systems or the like. Alternatively or additionally, radio signals from wireless access points such as W-LAN (wireless local area network) access points may be used.

[0024] Alternatively, or in addition, according to a further embodiment, triangulation methods as per se known in the art may be used to determine a position and/or orientation in space of said security device and/or said key device. Also according to a further embodiment, typical movement profiles (i.e., a series of movement measurements over time) may be recorded in advance or in a training phase of said security device.

[0025] Alternatively or additionally such movement profiles may e.g. be periodically be recorded during regular use of the security device or its key device(s). Such movement profiles may e.g. be used to enable an even more precise evaluation of whether to grant or deny access by means of the security device.

[0026] A further solution to the object of the present invention is given by a method of operating a security device according to claim 6. Advantageous embodiments are presented by claims 7, 8.

[0027] Yet another solution to the object of the present invention is given by a key device according to claim 9 and a method of operating a key device according to claim 11. Further advantageous embodiments are presented by the dependent claims.

[0028] A further solution to the object of the present invention is given by a security unit for a security device and/or a key device, particularly for a security device according to the embodiments and/or for a key device according to the embodiments. The security unit may e.g. be provided in form of an ASIC (application specific integrated circuit) and/or FPGA (field programmable gate array) (or a portion of an FPGA) or another type of integrated circuit.

Brief description of the figures

[0029] Further features, aspects and advantages of the present invention are given in following detailed description with reference to the drawings in which:

Figure 1 schematically depicts a security device and a key device according to an em-

bodiment,

Figure 2 schematically depicts an operational scenario with a relay attack,

Figure 3 schematically depicts a block diagram of a security device according to an embodiment,

Figure 4a, 4b schematically depict simplified flow charts of methods according to the embodiments,

Figure 5 schematically depicts a simplified block diagram of a key device according to an embodiment,

Figure 6 schematically depicts a simplified flow chart of a method of operating a key device according to an embodiment,

Figure 7 schematically depicts a side view of a further aspect according to the embodiments,

Figure 8 schematically depicts a block diagram of a security unit according to an embodiment,

Figure 9a, 9b schematically depict simplified flow charts of methods according to the embodiments, and

Figure 10 schematically depicts a block diagram of a conventional security device enhanced with a security unit according to an embodiment.

Detailed description

[0030] Figure 1 schematically depicts a simplified block diagram of a security device 100 according to an embodiment. The security device 100 is e.g. provided for granting access to a structure 300, which may be a vehicle or a building or the like. For instance, the security device 100 may be configured to operate together with a locking mechanism of a door (not shown) of the structure 300, e.g. to lock or release the locking mechanism of the door depending on whether access to the structure 300 is to be granted or denied by the security device 100. The locking mechanism may e.g. comprise an electromagnetic actuator (not shown) for this purpose that may be controlled by the security device 100.

[0031] Also depicted by figure 1 is a key device 200 which may in a per se known manner establish a contactless data connection dc with the security device 100, e.g. for exchanging identification information id. For example, according to an embodiment, the security device

100 may initiate said contactless data connection dc if a user actuates a door handle of structure 300. Alternatively or in addition, according to a further embodiment, said key device 200 may initiate said contactless data connection dc if a user of the key device presses a button on the key device 200 or the like.

[0032] As is well-known from conventional security devices and key devices, the security device may check identification information id received from a key device 200 in the course of the contactless data communication dc for predetermined features (e.g., comparison with reference identification information) and may make a decision on whether to grant or deny access to the structure 300 depending on such evaluation.

[0033] According to an embodiment, the contactless data connection dc may comprise one or more radio frequency channels of same and/or similar and/or different bandwidth and/or center frequency, which may be established by providing corresponding radio frequency transceivers (not shown) both in the security device 100 and the key device 200. For example, standardized ad-hoc-capable radio frequency systems may be used for establishing the data connection dc. Also, propriety radio frequency communications may be used for this purpose. Alternatively or additionally to using an RF channel for the data connection dc, an optical and/or acoustic channel (e.g., ultrasonic signals) or the like may be used according to a further embodiment. Generally, data transmissions via said data connection dc may be encrypted or not encrypted.

[0034] Figure 2 schematically depicts an operational scenario with components 100, 200 already described with reference to figure 1. In addition to the figure 1 embodiment, according to figure 2, a relay station 400 is arranged within the data connection path between the devices 100, 200. Suppose that an attacker installs the relay station 400, and that the relay station 400 is capable of receiving RF signals transmitted from the security device 100 to the key device 200 and of amplifying such received signals, thereby extending the radio range of the RF signal transmissions of the security device 100. Likewise, the relay station 400 may be configured to amplify radio frequency signal transmission received from the key device 200 in the same way to extend the radio range of the key device 200. In this context, the working range of the data connection dc (figure 1) may be extended to a degree which is highly undesired from a security point of view. For example, if a user of the structure 300 carries the key device 200 with him and if the user moves away from the structure 300, usually, it is not to be supposed that the user of the key device 200 intends to initiate a data communication dc with the security device 200, e.g. for accessing the structure 300. However, if the relay station 400 is present, the data connection dc (figure 1) between the devices 100, 200 is enhanced by providing two data connection branches dc1, dc2 in such a way that a proper RF communication between the devices 100, 200 in the sense of a user identification is still

possible even if the user or its key device 200 is comparatively far away from the structure 300 and its security device 100. Thus, even in the physical absence of the user and its key device 200 from the security device 100, a proper identification of the key device 200 can be performed by the security device 100 due to RF range extension by means of the relay 400 thus enabling to grant access to structure 300, which may be exploited by the attacker operating the relay station 400. In other words, by using the relay station 400 for extending the radio range of the devices 100, 200, the attacker may initiate a conventional identification session between devices 100, 200 without the user of the key device 200 becoming aware of this scenario. In this case, the attacker may gain access to the structure 300 without any effort of faking or even decrypting the identification information id in case of an encrypted transmission between devices 100, 200.

[0035] Rather, the relay station 400 may simply relay the identification information id, either decrypted or encrypted, as it has been sent from the key device 200 to the security device 100.

[0036] According to the present invention, in order to prevent attacks as described above with reference to figure 2, the security device 100 is configured to receive from the key device 200 information on at least one remote parameter of said key device 200, said remote parameter comprising at least one of a remote environmental parameter and a remote movement parameter of said key device 200, and to grant or deny access to said structure 300 depending on said at least one remote parameter.

[0037] Thus, the security device 100 is enabled to check specific properties - in addition to the conventional check of identification information id - of the key device 200 in the context of a radio communication to the key device 200, whereby a degree of security of the access procedure can be increased. According to an embodiment, said key device 200 may be configured to determine at least one of the following parameters as said remote environmental parameter: air pressure, temperature, humidity, concentration of one or more gases such as e.g. carbon monoxide or nitrogen dioxide, electric and/or magnetic and/or electromagnetic signals, acoustic signals, radioactive radiation. According to a further embodiment, the key device 200 may be configured to detect one or more of the following parameters as remote movement parameters: acceleration of said key device 200 in one or more dimensions, direction of the movement of said key device, position of said key device.

[0038] One or more of these remote environmental or movement parameters of the key device 200 may advantageously be provided to the security device 100 according to an embodiment, which is configured to receive such parameter(s) and to take into consideration such parameter(s) when determining whether or not to grant access to the structure 300.

[0039] For example, according to an embodiment, wherein the key device 200 is configured to determine

movement parameters comprising at least one acceleration value of the key device 200, upon receiving such acceleration values, the security device 100 may determine whether or not the acceleration values exceed a certain threshold. If the threshold is not exceeded, the security device 100 may conclude that the key device 100 is substantially not moving and thus not experiencing a significant acceleration. From this, the security device 100 may further conclude that is very unlikely that an authorized user of the key device 200 has currently pressed an actuator such as a button or the like to initiate the data connection dc with the security device 100. Rather, the situation as depicted in figure 2 may be present, i.e. a possible relay attack on the system, where a contactless data communication has e.g. been initiated by the attacker actuating a car door handle or the like. In this case, the security device 100 may conclude to deny access to the structure 300 depending on the evaluated remote parameter(s).

[0040] According to a further embodiment, the security device 100 may also be configured to determine at least one local parameter of the security device 100, said local parameter comprising at least one of a local environmental parameter and a local movement parameter. According to a further embodiment, the local parameters of the security device 100 may substantially be the same parameters as explained above with respect to the key device 200, i.e. air pressure temperature, humidity, concentration of one or more gases such as e.g. carbon monoxide or nitrogen dioxide, electric and/or magnetic and/or electromagnetic signals, acoustic signals, radioactive radiation, acceleration of said security device 100, direction of movement of said security device 100, position of said security device 100.

[0041] Thus, according to a further embodiment, the security device 100 may e.g. evaluate basically one or more parameters as also detected by the key device 200, and upon receiving such parameters from the key device 200, the security device 100 may advantageously perform one or more plausibility checks or comparison of its local parameters with the remote parameters of the key device 200 thus e.g. determining whether the key device 200 is comparatively close to the security device 100. In this situation, it is to be assumed that usually an authorized user uses the key device 200 for accessing the structure 300.

[0042] However, if according to a further embodiment, a difference between e.g. the local air pressure in the surroundings of the security device 100 and a remote air pressure in the surroundings of the key device 200 exceeds a predetermined threshold, it may be concluded that the devices 100, 200 are too far away from each other to allow an authorized access to the structure 300.

[0043] According to an embodiment, any local parameter(s) and/or remote parameter(s) of the devices 100, 200 may be encrypted for transmission over the contactless data connection dc.

[0044] According to a further embodiment, the security

device 100 may comprise a sensor device 110 (figure 1) which may be configured to determine one or more of the local parameters such as the local environmental parameters and/or the local movement parameters of the security device 100.

[0045] Figure 3 schematically depicts a simplified block diagram of a security device 100 according to an embodiment. The security device 100 comprises a sensor device 110 for determining one or more local environmental parameters lep and/or one or more local movement parameters lmp. The security device 100 also comprises a calculating unit 120 such as e.g. a microcontroller or a digital signal processor or the like. The functionality of these components 110, 120 and generally of device 100 may also be integrated into one or more ASICs (application specific integrated circuit) and/or FPGA (field programmable gate array).

[0046] The security device 100 may also comprise an RF interface 130 comprising e.g. a radio frequency transceiver which can be used to establish the contactless data connection dc with the key device 200 (figure 1).

[0047] Figure 4a schematically depicts a simplified flow chart of a method according to an embodiment. In a first step 400, the security device 100 (figure 1) receives from the key device 200 information on at least one remote parameter of the key device 200. Subsequently, in step 410, the security device 100 grants or denies access to the structure 300 depending on said at least one remote parameter that has been received from the key device 200 in step 400. Thus, alternatively to or in addition to a conventional evaluation of the identification information id also received from the key device 200 according to an embodiment, the security device 100 according to the embodiment also takes into consideration said at least one remote parameter received from the key device 200 for determining whether to grant or deny access to the structure 300.

[0048] Figure 4b schematically depicts a flow chart of a further method according to an embodiment. In step 500, the security device 100 determines at least one local parameter of the security device, i.e. at least one local environmental parameter lep (figure 3) and/or at least one local movement parameter lmp.

[0049] After that, in step 510 (figure 4b) said security device 100 compares said at least one local parameter determined in step 500 with said at least one remote parameter received from the key device 200, and grants 520 or denies access to the structure 300 (figure 1) depending on the comparison 510 of said at least one parameter with said at least one remote parameter.

[0050] Figure 5 schematically depicts a simplified block diagram of a key device 200 according to an embodiment. The key device 200 may comprise a sensor device 210 which is configured to determine one or more of the remote parameters 200 such as e.g. remote environmental parameters rep and/or remote movement parameters rmp of the key device 200. The key device 200 may also comprise a calculating unit 220 which is

configured to process said parameters rep and to transmit said parameters or information derived therefrom via the radio interface 230 by means of the contactless data connection dc to the security device 100 (figure 1).

[0051] According to a further embodiment, the calculating unit 220 may also comprise digital signal processing means which may provide for at least one of the following processes:

filtering and/or fusioning and/or comparison and/or weighting and/or correlation and/or prediction calculations related to the parameters rep, rmp. Likewise, according to an embodiment, the calculating unit 120 of the security device 100 may be configured to perform one or more of said aforementioned processes, either with local parameters lep, lmp and/or remote parameters rep, rmp. By applying these techniques, the precision regarding the security device's determination as to whether the key device 200 is sufficiently close to the security device 100 or as to a relay attack being carried out may even further be increased.

[0052] Figure 6 schematically depicts a simplified flow chart of a further method according to an embodiment. In step 600, the key device 200 determines at least one remote parameter rep, rmp of said key device 200, and in step 610 the key device 200 transmits, preferably in encrypted fashion, information on said at least one remote parameter to the security device 100, which may then evaluate the remote parameter(s) from the key device 200 in order to form a precise assessment whether to grant or deny access to the structure 300 based on the data from the key device 200 and/or on one or more local parameters lep, lmp evaluated according to the embodiments explained above.

[0053] Figure 7 schematically depicts a further aspect of the present invention. The security device 100 according to the embodiments may e.g. be comprised within a vehicle, especially land vehicle, particularly car 310. The key device 200 according to the embodiments may e.g. be used in form of a car key for operating together with the security device 100 as explained above.

[0054] According to further embodiments, any of the aforementioned aspects may be combined with each other to even further increase the overall security of the devices 100, 200, particularly against relay attacks.

[0055] Figure 8 schematically depicts a block diagram of a security unit 1000 according to an embodiment. The security unit 1000 may e.g. be implemented in form of an ASIC or FPGA (or functional block of an FPGA which also comprises one or more other functional blocks, e.g. for conventional purposes) or any other type of integrated circuit.

[0056] In the following, the operation of the security unit 1000 is described with reference to the flow charts of Fig. 9a, 9b. According to an embodiment, the security unit 1000 is configured to

receive 4000 from a key device 200 (Fig. 1) information on at least one remote parameter of said key device 200, said remote parameter comprising at least one of a remote environmental parameter rep and a remote movement parameter rmp of said key device 200, and to evaluate 4002 said at least one remote parameter of said key device 200 to obtain parameter evaluation information, and to indicate 4004 to a security device 100 whether to grant or deny access to a structure 300 depending on said parameter evaluation information.

[0057] According to the present embodiment, various aspects of the inventive principle are covered by the security unit 1000, which may e.g. be implemented as an integrated circuit, i.e. in form of a "security chip" 1000. As depicted by Fig. 8, the security chip 1000 may e.g. comprise a calculating unit 1100 for performing the above mentioned method steps and/or generally controlling an operation of the security chip 1000.

[0058] According to an embodiment, the security chip 1000 may also be configured to receive at least one of one or more local environmental parameters lep and/or one or more local movement parameters lmp, as indicated in Figure 8 by the dashed double arrow lep, lmp. Hence, the security chip 1000 may also make further determinations based on said information rep, rmp and/or lep, lmp, for determining which output signal I to indicate to a security device.

[0059] According to an embodiment, said security unit 1000 is configured to determine 5000 (Fig. 9b) at least one local parameter of said security device 100, said local parameter comprising at least one of a local environmental parameter lep and a local movement parameter lmp, and said security unit 1000 is configured to compare 5002 said at least one local parameter with said at least one remote parameter, and to perform said step of indicating 4004 depending on the comparison 5010 of said at least one local parameter with said at least one remote parameter.

[0060] According to an embodiment, said step 4000 of receiving from a key device 200 (Fig. 1) information on at least one remote parameter of said key device 200 may e.g. comprise receiving said data over a data connection between a control unit or a calculating unit 120 of a security device 100 (also cf. data connection 1000' of Fig. 10 explained below), which provides said data to the security chip 1000. According to a further embodiment, it is also possible that the security chip 1000 may receive the at least one local parameter via such data connection. The indication I may also be transmitted to the security device 100 or its calculating unit 120 by means of such data connection.

[0061] Figure 10 schematically depicts a block diagram of a conventional security device 600, which may be enhanced by applying the principle according to the embodiments. The conventional security device 600 comprises a calculating unit 620 such as e.g. a microcontroller or a digital signal processor or the like, and an RF interface 630 comprising e.g. a radio frequency trans-

ceiver which can be used to establish the contactless data connection dc with a key device 200 (figure 1). I.e., components 620, 630 may be conventional components that may e.g. be comprised in state of the art wireless identification key systems of cars or the like.

[0062] According to an embodiment, the conventional security device 600 is enhanced by providing a security chip 1000 according to the embodiments, which may e.g. be configured as explained above with reference to Fig. 8. The security chip 1000 is connected to the calculating unit 620 of the security device 600 by means of a data connection 1000', which may e.g. be a serial peripheral interface (SPI) or another chip-to-chip interface, and which may be used to provide the security chip 1000 with local and/or remote parameters of a key device 200 and/or a security device 600 as e.g. received and/or determined by the security device 600.

[0063] Also, according to an embodiment, it is possible to provide the calculating unit 620 in form of a first functional block of an FPGA (not shown), and to provide the functionality of the security chip 1000 according to an embodiment in the form of a second functional block of the same FPGA, wherein the data connection 1000' may e.g. be implemented in form of an on-chip-bus (data bus) of the FPGA.

[0064] According to an embodiment, the enhanced security device 600 of Fig. 10 may perform a method similar to the one explained above with reference to figure 4a. Firstly, the security device 600 receives from a key device 200 information on at least one remote parameter of the key device 200. Subsequently, the security device 600 grants or denies access to a structure 300 (figure 1) depending on said at least one remote parameter that has been received from the key device 200. Thus, alternatively to or in addition to a conventional evaluation of the identification information id also received from the key device 200 according to an embodiment, the security device 600 according to the embodiment also takes into consideration said at least one remote parameter received from the key device 200 for determining whether to grant or deny access to the structure 300.

[0065] According to one embodiment, for granting or denying access, the security device 600 may forward said at least one remote parameter that has been received from the key device 200 (or information derived therefrom) over data connection dc and its transceiver 630 to the security chip 1000, via data connection 1000'. The security chip 1000 may evaluate said at least one remote parameter.

[0066] For example, according to one embodiment, a remote movement parameter of the key device 200 may comprise data of an acceleration sensor which detects the acceleration of the key device in one or more spatial dimensions. The key device may determine such acceleration data and forward it as remote movement parameter in the sense of the present embodiment to the security device 600, i.e. together with the conventionally transmitted identification information and/or separated

therefrom. Upon receipt, the security device 600 may forward said acceleration data of the key 200 to the security chip 1000 via interface 1000' for performing e.g. a plausibility check.

[0067] For example, if the acceleration data of the key device 200 as received by the security device 600 and the security chip 1000 indicate that no substantial acceleration values are recorded by the key device, the security chip 1000 may conclude that the key device is presently not substantially moved or accelerated, but is e.g. be placed on a table top or the like. From this conclusion it may further be derived that in the present configuration, no manual interaction with the key device such as a manual handling of the key device has taken place, because this would have led to some non-vanishing acceleration values related to the key device. From this analysis, the security chip 1000 may advantageously conclude that no authorized access to the security device 600 or the structure protected thereby is currently made. Consequently, the security chip may indicate to the security device 600 or its calculating unit 120 a recommendation I (Fig. 8) to deny access to the structure.

[0068] The security device 600 may receive said recommendation I from the security chip 1000 and may now e.g. additionally consider this recommendation I for deciding whether to grant or deny access. According to an embodiment, the notification I may comprise a single binary value ("deny" or "grant"). According to further embodiments, the notification I may comprise a real number or a percentage or the like, which e.g. represents a confidence level associated with a determination of the security chip 1000. Optionally, a sensor device 610 may also be provided at (or in) the security device 600, for determining at least one or more of local parameters such as the local environmental parameters and/or local movement parameters of the security device 600. The sensor device 610 may be configured to provide its data lep, lmp to the control unit 620 (which may forward it to the security chip 1000) and/or directly (not shown) to the security chip 1000, and the security chip 1000 may e.g. perform the method according to Fig. 9b to evaluate said data and for providing an indication I derived therefrom to the security device 600 or its calculating unit 620.

[0069] The inventive aspect of the security chip 1000 advantageously enables to enhance existing security devices with the inventive functionality that offers increased security especially with respect to relay attacks.

[0070] According to further embodiments, the devices 100, 200 and/or at least some of their components may be implemented in form of hardware and/or firmware and/or software. For example, especially a determination step evaluating remote parameter(s) may be carried out by a software program running on a digital signal processor of the sensor device 100 or the key device 200. Alternatively or in addition, such functionality may also be implemented in form of hardware, e.g. in as a function block of an FPGA or the like.

Claims

1. Security device (100) for granting access to a structure (300), particularly a vehicle or a building, wherein said security device (100) is configured to receive identification information (id) from a key device (200) by means of a, preferably contactless, data connection (dc) and to grant or deny access to said structure (300) depending on said identification information (id), **characterized in that** said security device (100) is further configured to
 - receive (400) from said key device (200) information on at least one remote parameter of said key device (200), said remote parameter comprising at least one of a remote environmental parameter (rep) and a remote movement parameter (rmp) of said key device (200), and to
 - grant (410) or deny access to said structure (300) depending on said at least one remote parameter.
2. Security device (100) according to claim 1, wherein said security device (100) is configured to determine (500) at least one local parameter of said security device (100), said local parameter comprising at least one of a local environmental parameter (lep) and a local movement parameter (lmp).
3. Security device (100) according to claim 2, wherein said security device (100) is configured to compare (510) said at least one local parameter with said at least one remote parameter, and to grant (520) or deny access to said structure (300) depending on the comparison (510) of said at least one local parameter with said at least one remote parameter.
4. Security device (100) according to one of the preceding claims, wherein said security device (100) comprises a sensor device (110) for determining at least one local environmental parameter (lep), wherein said sensor device (110) is configured to determine at least one of the following parameters: air pressure, temperature, humidity, concentration of one or more gases such as e.g. carbon monoxide or nitrogen dioxide, electric and/or magnetic and/or electromagnetic signals, acoustic signals, radioactive radiation.
5. Security device (100) according to one of the preceding claims, wherein said security device (100) is configured to determine at least one local movement parameter (lmp) of said security device (100), wherein said local movement parameter (lmp) comprises at least one of: acceleration of said security device (100), direction of movement of said security device (100), position of said security device (100).
6. Method of operating a security device (100) for granting access to a structure (300), particularly a vehicle or a building, wherein said security device (100) is configured to receive identification information (id) from a key device (200) by means of a, preferably contactless, data connection (dc) and to grant or deny access to said structure (300) depending on said identification information (id), **characterized in that** said security device (100) receives (400) from said key device (200) information on at least one remote parameter of said key device (200), said remote parameter comprising at least one of a remote environmental parameter (rep) and a remote movement parameter (rmp) of said key device (200), and grants (410) or denies access to said structure (300) depending on said at least one remote parameter.
7. Method according to claim 6, wherein said security device (100) determines (500) at least one local parameter of said security device (100), said local parameter comprising at least one of a local environmental parameter (lep) and a local movement parameter (lmp), and wherein preferably, said security device (100) compares (510) said at least one local parameter with said at least one remote parameter, and grants (520) or denies access to said structure (300) depending on the comparison (510) of said at least one local parameter with said at least one remote parameter.
8. Method according to one of the claims 6 to 7, wherein said security device (100), by means of a sensor device (110), determines at least one of the following parameters: air pressure, temperature, humidity, concentration of one or more gases such as e.g. carbon monoxide or nitrogen dioxide, electric and/or magnetic and/or electromagnetic signals, acoustic signals, radioactive radiation, wherein preferably said security device (100) determines at least one local movement parameter (lmp) of said security device (100), wherein said local movement parameter (lmp) comprises at least one of: acceleration of said security device (100), direction of movement of said security device (100), position of said security device (100).
9. Key device (200) for transmitting identification information (id) to a security device (100), preferably according to one of the claims 1 to 5, wherein said key device (200) is configured to determine (600) at least one remote parameter of said key device (200), said remote parameter comprising at least one of a remote environmental parameter (rep) and a remote movement parameter (rmp) of said key device (200), and to transmit (610) information on said at least one remote parameter to said security device (100).
10. Key device (200) according to claim 9, wherein said

key device (200) is configured to determine at least one of the following parameters: air pressure, temperature, humidity, concentration of one or more gases such as e.g. carbon monoxide or nitrogen dioxide, electric and/or magnetic and/or electromagnetic signals, acoustic signals, radioactive radiation, acceleration of said key device (200), direction of movement of said key device (200), position of said key device (200).

11. Method of operating a key device (200) for transmitting identification information (id) to a security device (100), preferably according to one of the claims 1 to 5, wherein said key device (200) determines (600) at least one remote parameter of said key device (200), said remote parameter comprising at least one of a remote environmental parameter (rep) and a remote movement parameter (rmp) of said key device (200), and transmits (610) information on said at least one remote parameter to said security device (100).
12. Method according to claim 11, wherein said key device (200) determines at least one of the following parameters: air pressure, temperature, humidity, concentration of one or more gases such as e.g. carbon monoxide or nitrogen dioxide, electric and/or magnetic and/or electromagnetic signals, acoustic signals, radioactive radiation, acceleration of said key device (200), direction of movement of said key device (200), position of said key device (200).
13. Security unit (1000) for a security device and/or a key device, particularly for a security device (100) according to at least one of the claims 1 to 5 and/or for a key device (200) according to at least one of the claims 9, 10, wherein said security unit (1000) is configured to
 - receive (4000) from a key device (200) information on at least one remote parameter of said key device (200), said remote parameter comprising at least one of a remote environmental parameter (rep) and a remote movement parameter (rmp) of said key device (200), to
 - evaluate (4002) said at least one remote parameter of said key device (200) to obtain parameter evaluation information, and to
 - indicate (4004) to a security device (100) whether to grant or deny access to a structure (300) depending on said parameter evaluation information.
14. Security unit (1000) according to claim 13, wherein said security unit (1000) is configured to determine (5000) at least one local parameter of said security device (100), said local parameter comprising at least one of a local environmental parameter (lep)

and a local movement parameter (lmp), and wherein said security unit (1000) is configured to compare (5002) said at least one local parameter with said at least one remote parameter, and to perform said step of indicating (4004) depending on the comparison (5002) of said at least one local parameter with said at least one remote parameter.

15. Vehicle (310), preferably land vehicle, particularly car, comprising at least one security device (100) according to one of the claims 1 to 5.

Fig. 1

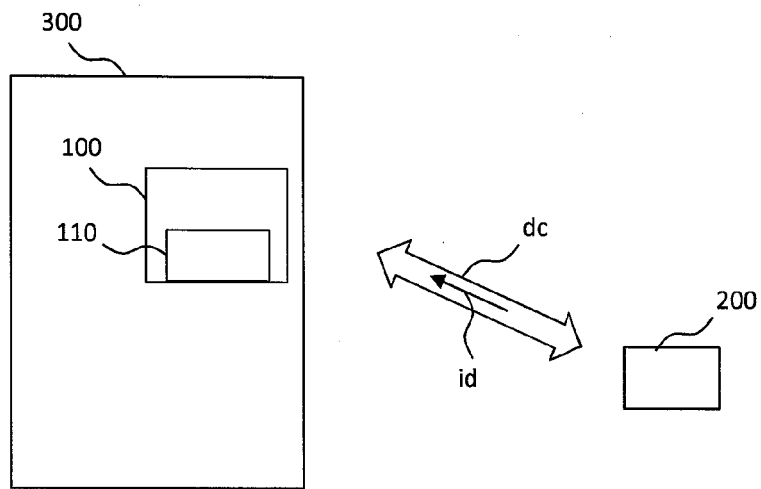


Fig. 2

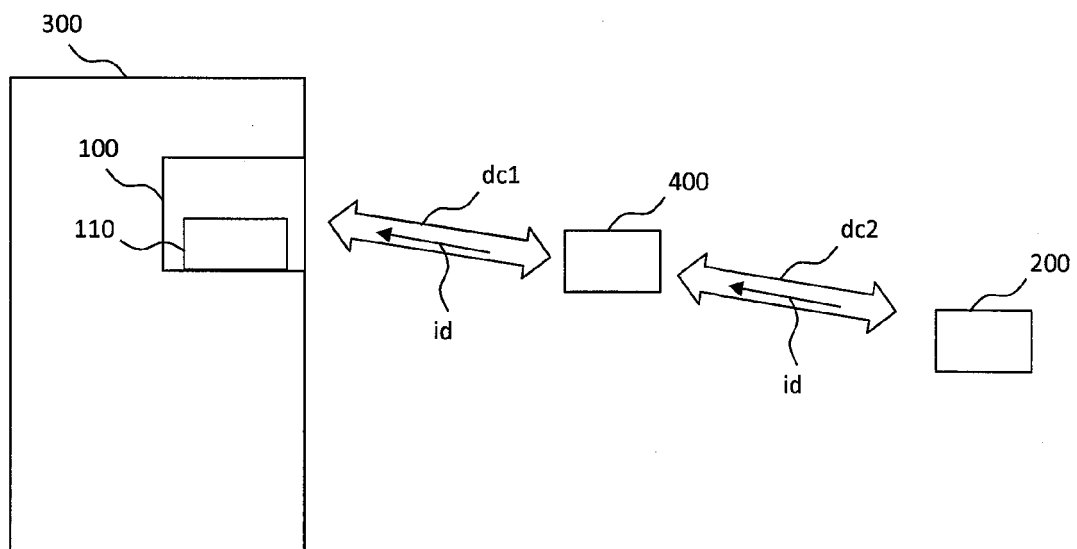


Fig. 3

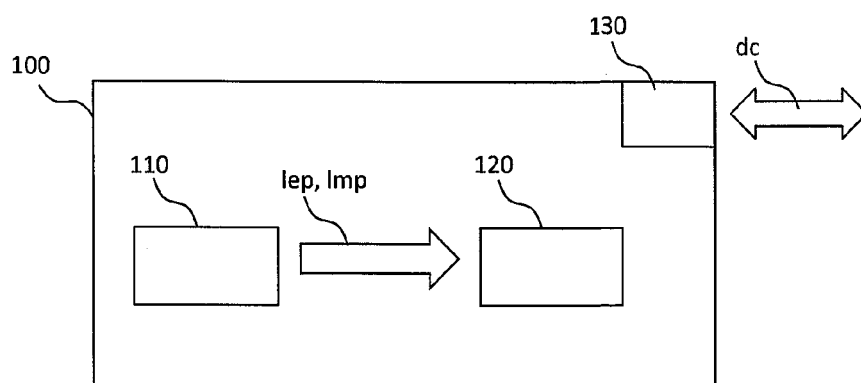


Fig. 4a

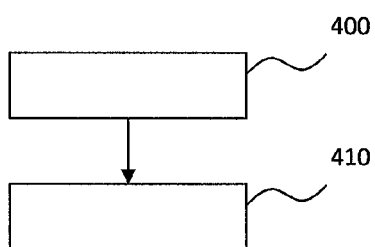


Fig. 4b

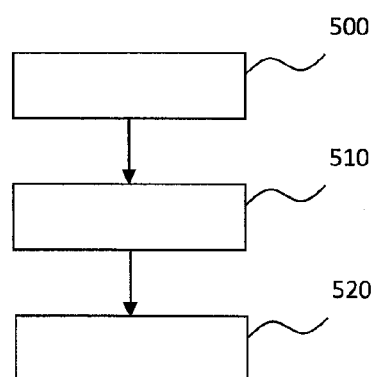


Fig. 5

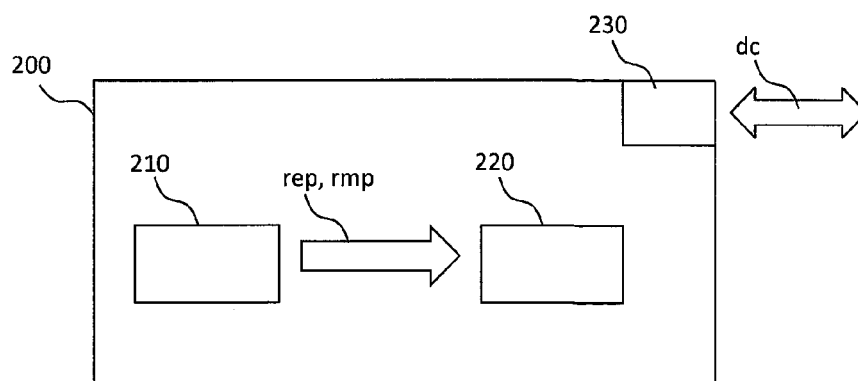


Fig. 6

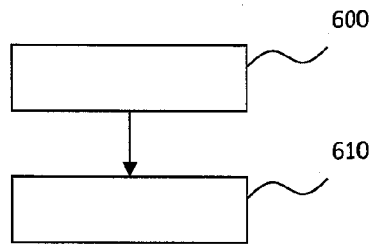


Fig. 7

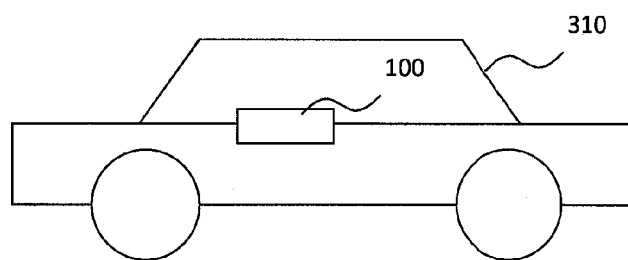


Fig. 8

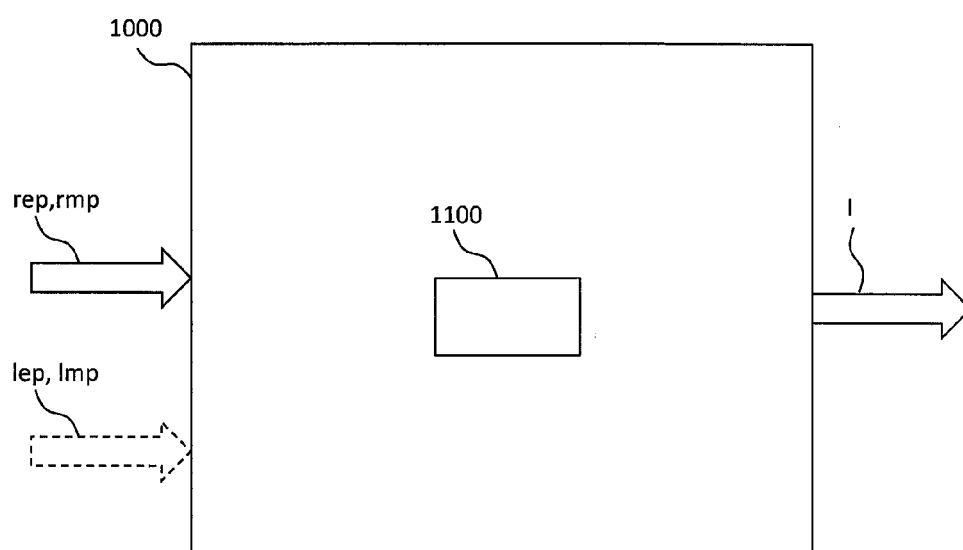


Fig. 9a

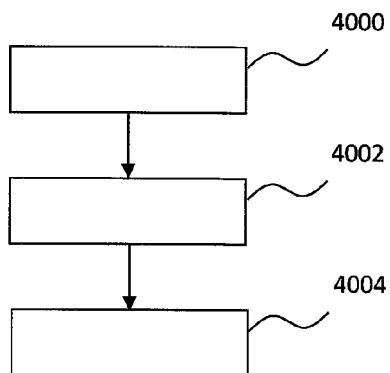


Fig. 9b

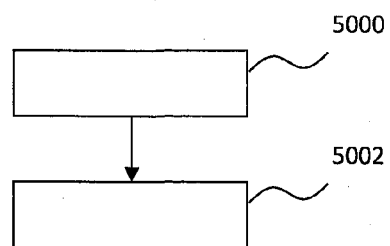
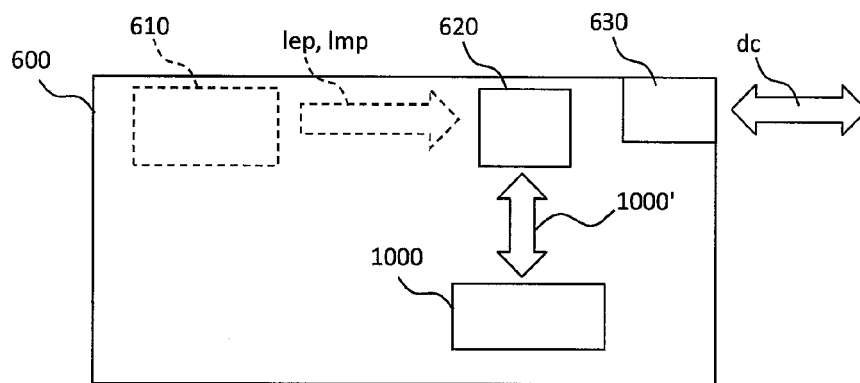


Fig. 10





EUROPEAN SEARCH REPORT

Application Number
EP 14 16 7535

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	FR 2 888 364 A1 (GEMPLUS SA [FR]) 12 January 2007 (2007-01-12) * abstract * * page 1, line 5 - line 23 * * page 3, line 16 - page 5, line 3 * * page 7, line 14 - page 10, line 13 * * page 13, line 7 - line 13 * * figure 1 *	1-15	INV. G07C9/00
X	EP 1 721 793 A1 (DELPHI TECH INC [US]) 15 November 2006 (2006-11-15) * abstract * * paragraph [0012] * * paragraph [0023] * * paragraph [0031] - paragraph [0037] * * paragraph [0051] *	1-15	
X	DE 198 50 176 C1 (SIEMENS AG [DE]) 31 August 2000 (2000-08-31) * abstract * * column 1, line 57 - column 2, line 9 * * column 2, line 22 - column 4, line 65 *	1-15	TECHNICAL FIELDS SEARCHED (IPC) G07C B60R
The present search report has been drawn up for all claims			
Place of search The Hague		Date of completion of the search 20 October 2014	Examiner Van der Haegen, D
CATEGORY OF CITED DOCUMENTS X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document			

EPO FORM 1503 03.82 (P04C01)

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 14 16 7535

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

20-10-2014

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
FR 2888364 A1	12-01-2007	FR 2888364 A1	12-01-2007
		WO 2007003656 A1	11-01-2007
EP 1721793 A1	15-11-2006	AT 369271 T	15-08-2007
		DE 602005001935 T2	08-05-2008
		EP 1721793 A1	15-11-2006
DE 19850176 C1	31-08-2000	NONE	