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

(11) EP 2 393 070 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
07.12.2011 Bulletin 2011/49

(21) Application number: **10164694.1**

(22) Date of filing: **02.06.2010**

(51) Int Cl.:
G07F 19/00 *(2006.01)* ***G01D 5/12*** *(2006.01)*
G01N 27/02 *(2006.01)*

(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 SE SI SK SM TR
Designated Extension States:
BA ME RS

(71) Applicant: **3M Innovative Properties Company**
Saint Paul, MN 55133-3427 (US)

(72) Inventors:
- **Weinmann, Christian**
  52477, Alsdorf (DE)
- **Zilligen, Guenter**
  41514, Grevenbroich (DE)

(74) Representative: **Bergen, Katja**
3M Deutschland GmbH
OIPC
Carl-Schurz-Strasse 1
41453 Neuss (DE)

(54) Security system for data receiving unit

(57) The invention provides a security system for a data receiving unit comprising a user interface (2), the user interface comprising at least two components (3, 6; 15, 16) with at least partially conductive properties, the conductive components being electrically isolated from each other, and an electric field proximity sensor with emitting and/or receiving devices. According to the invention the conductive components of the user interface are used as emitting and/or receiving devices of the electric field proximity sensor.

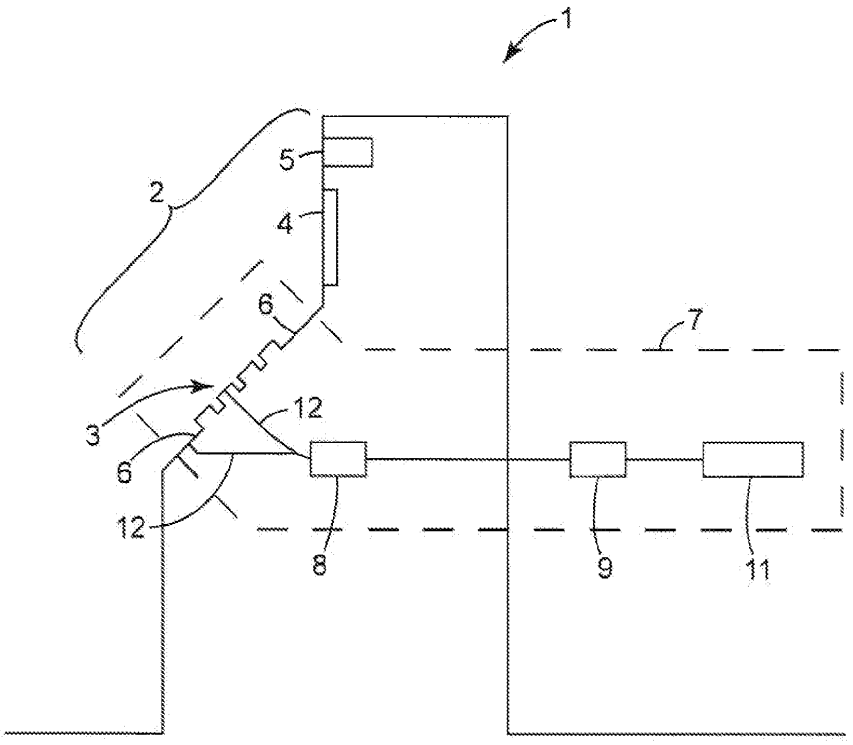

FIG. 1

EP 2 393 070 A1

Description

[0001] The invention relates to a security system for a data receiving unit comprising a housing with a user interface and an electric field proximity sensor.

[0002] Any kind of data receiving units may be object of a fraud attack, especially if the data sent to the data receiving unit is secret and if the data receiving unit is part of a system that protects anything of value. Self service terminals (SST), such as for example automated teller machines (ATM), are often the target of fraud-attacks to gain access to the valuables contained therein. To prohibit these attacks automated teller machines are in the mean time very heavily armoured. Thieves have created several ways to get access to the money. One is known as "skimming", where the thieves try to espy the relevant data to get access to the account and with it to the money of the account. The most important data for that is the personal identification number (PIN) which has to be entered in the automated teller machine through a keypad. In combination with a stolen or copied cash card or bank card access to the account and the money is possible. A common way to get access to the PIN is to attach a hidden camera above the keypad and capture the pressed keys. Another way is to overlay the keypad with a fake keypad which contains a key logger. These types of fraud-attacks are very hard to notice to an everyday user.

[0003] Other data receiving units, for example card readers, may also be subject to fraud-attacks. It is known to overlay card readers with fake card readers and to capture the data stored on a card while it is introduced into the card reader. This fraud-attack is also very hard to notice. Card readers may be part of self service terminals as well or they may be part of other systems such as for example any kind of access systems. It is generally known to use a card reader as a component to get access to buildings or rooms. A person that wants to get into a room has to put his card in or next to a card reader. If the card contains the right information the system grants access to the room. Other possible data receiving units for access systems are again keypads or touch pads, scanners, fingerprint sensors, cameras etc..

[0004] Security systems for automated teller machines that protect a card slot of a card reader are known in the prior art, such as the system described in EP 1 677 267 A1, that provides an optoelectric sensing barrier aligned to the card-in/card-out barrier and an electronic circuit that is connected to the sensing barrier. Furthermore US 2008/0110975 A1 describes a cash dispensing automated banking machine with a sensing device for a card-slot of a card reader as protection. A protection of the keypad is not described in these documents.

[0005] It is also known in the prior art to provide mechanical viewing barriers for automated teller machines' keypads such as described in WO 95/23421 A. The system described in this document provides a privacy filter that is made up of parallel lamellae or a criss-cross grid of parallel lamellae.

[0006] WO 2005/109358 A1 describes a security system for automated teller machines with a capacitive proximity sensor on an inner surface of a protective covering of the automated teller machines. The capacitive proximity sensor is able to detect any foreign components positioned at an outer surface of the machine.

[0007] GB 2 351 590 A describes a self service terminal with a sensor that is located as to capture objects in the area of data capture devices, e.g. underneath the keypad. The sensor described in this document may be a capacitive, an inductive or an ultra sonic sensor.

[0008] There is a need for an easy but dependable security system for a data receiving unit. Such a system should be easy to install as well as easy to retrofit to existing data receiving units. Furthermore such a system should be relatively cheap in production.

[0009] The present invention provides a security system for a data receiving unit with a user interface and an electric field proximity sensor. The user interface comprises at least two components with at least partially conductive properties, the conductive components being electrically isolated from each other. The electric field proximity sensor has emitting and/or receiving devices. According to the invention the conductive components of the user interface are used as emitting and/or receiving devices of the electric field proximity sensor.

[0010] Data receiving units in the sense of the invention are all kind of electric systems that are able to collect, receive etc. data. The data may be any kind of data, especially but not limited to secret data, such as for examples personal identification numbers (PINs), passwords, keywords, fingerprints, pictures etc.. Those data may for example be used to get access to private or secret information, access to money but also access to buildings, rooms in buildings etc.. Data receiving units usually have an user interface with means for receiving the above mentioned data, such as for example a keypad, a card reader, a RFID reader, a USB stick reader a touch pad, a scanner, a fingerprint sensor, a camera etc. If someone wants to get access to data, the data receiving units may be manipulated as described above.

[0011] As described above, it is known to use electric field proximity sensors in security systems for automated teller machines. Such systems are based on electric field proximity sensing. Usually an alternating voltage is applied and an electric field is created that has a certain impedance. The impedance may be measured and any change in the impedance may be registered and analysed. Electric field proximity sensors usually have devices for emitting and/or receiving the electric field. Such emitting and/or receiving devices need to have at least partially conductive properties. For creating an electric field two such at least partially conductive components are needed. Those components need to be electrically isolated from each other.

[0012] According to the invention conductive parts or components of the data receiving unit are used as emit-

ting and/or receiving devices of an electric field proximity sensor. This is a very smart solution since existing parts are used to build up the proximity sensor of a security system. This has the advantage that this solution is a cost saving one since less parts are needed. Furthermore this solution may be integrated in data receiving units such that the system itself is not visible for possible attackers, since no visible additional components need to be installed. Additionally existing data receiving units may be retrofitted very easily. Conductive and electrically isolated components only need to be electrically connected to a sensing unit of a proximity sensor of the security system. Sensing unit and emitting and/or receiving devices build up the electric field proximity sensor that is part of the security system according to the invention.

[0013] According to one embodiment of the invention the sensing unit of the proximity sensor applies an alternating voltage to the conductive components of the user interface for propagating an electric field in the area of the user interface. On one side the amplitude of the applied voltage is chosen low enough so that the user will not recognize it when using the data receiving unit. On the other side the amplitude of the applied voltage is chosen high enough so that the resolution is high enough for the system to identify any significant changes in the impedance. The Voltage range could be from couple of Milivolts up to several Volts, such as for example from 2 mV up to 25 V, which is the maximal voltage for low-voltage equipment according to DIN VDE 0100. The electric field has a characteristic impedance. The impedance is measured by the sensing unit of the system and compared with a reference value of the impedance. Any change of the impedance or any discrepancy of the measured impedance and the reference value is recognized by the system and any possible further steps may be initiated such as for example activation a warning system.

[0014] The proximity sensor may apply one single or several different frequencies or even a range of frequencies to the conductive components of the user interface. Applying more than one frequency to the conductive components has the advantage that the system can be adapted to the frequency with the most dynamic response. The impedance of the system depends among other things on the physical dimensions of the sensor, that are e.g. the emitting and/or receiving devices. Therefore the impedance changes from system to system and in every system the change of the impedance in the situation of an approaching object is depending on the specific frequency. In other words every system has its own preferred frequency, where the best measuring results may be achieved. To avoid complicated calibration procedures when installing a security system it is possible to run the system with more than one frequency or even with a range of frequencies and to use the sum or the maximum of all discrepancies of the measured impedance from the reference value.

[0015] The proximity sensor may be electrically connected with at least two of the conductive components of the user interface. For propagating an electric field, it is enough to apply an alternating voltage to two electrically isolated conductive components - two poles. The sensing unit of the proximity sensor may also be electrically connected with more than two conductive components such as for example three or four. In such a case two or more conductive components need to be short-circuited to build up two electrically independent poles. This opens the possibility to select and to design the two needed poles such that the electric field created by these poles extends in the area of the data receiving unit that needs to be secured.

[0016] The sensing unit of the proximity sensor may be electrically connected from a rear side with the at least two conductive components of the user interface. The rear side of the electrical conductive components of the user interface is the side that faces the interior of the data receiving unit and that is invisible for a user. Such an arrangement has the advantage that the security system itself is invisible for potential attackers. The system may be integrated into a housing of the data receiving unit such that the outer appearance of the receiving unit is not influenced at all.

[0017] The user interface of the data receiving unit may comprise a faceplate and a keypad. That may for example be the case when the data receiving unit is part of a self service terminal such as for example an automated teller machine. The faceplate and/or the keypad may have conductive properties. The sensing unit of the proximity sensor may be electrically connected with either two keys of the keypad or with one key of the keypad and the faceplate. If the sensing unit of the proximity sensor is electrically connected with more than two conductive components it may be connected with more than one key of the keypad and the faceplate. It is also possible that the faceplate comprises several parts that are electrically isolated from each other. In that case it is also possible that the sensing unit of the proximity sensor is electrically connected with two or more parts of the faceplate. Any other combination is possible as well. In every case the components that are electrically connected with the sensing unit need to be designed such that they build up two electrically independent poles as described above.

[0018] The user interface of the data receiving unit may comprise a card reader. That may also be the case when the data receiving unit is part of an automated teller machine. Another possible application of a data receiving unit comprising a card reader is the card reader being part of an access control system providing for example physical access to e.g. buildings, rooms or virtual access to data rooms, TV channels etc. or authorize money transactions for cashless payment systems or authorize treatment-payments with a health insurance card.

[0019] The card reader may comprise two electrically isolated components with at least partially conductive properties. The sensing unit of the proximity sensor according to the invention may be electrically connected

with those two components of the card reader and use them as emitting and/or receiving device. To build up two poles the card reader may comprise a block out of electrically conductive material. The block may be divided in two parts that are electrically isolated from each other. The block may also comprise a screw or bolt or something similar that is sitting in the block and that is also electrically isolated from the block.

[0020] The invention will now be described in more detail with reference to the following Figures exemplifying particular exemplary embodiments of the invention:

Fig. 1 is a schematic drawing of an automated teller machine (ATM) with a security system according to the invention;

Fig. 2 is a schematic drawing of a card reader that is adapted to be equipped with a security system according to the invention;

Fig. 3 is a schematic diagram of one embodiment of the security system according to the invention;

Fig. 4 is a schematic diagram of another embodiment of the security system according to the invention;

Fig. 5a is a cross-section of a user interface of an automated teller machine with a diagram of a simulation of an electric field that is created in the area of the user interface with a frequency of 100 MHz in an undisturbed situation;

Fig. 5b is a cross-section of a user interface of an automated teller machine with a diagram of a simulation of an electric field that is created in the area of the user interface with a frequency of 100 MHz in a disturbed situation - the user interface is approached by a dielectric object;

Fig. 5c is a cross-section of a user interface of an automated teller machine with a diagram of a simulation of an electric field that is created in the area of the user interface with a frequency of 100 MHz in a disturbed situation - the user interface is approached by a conductive object;

Fig. 6a is a cross-section of a user interface of an automated teller machine with a diagram of a simulation of an electric field that is created in the area of the user interface with a frequency of 1000 MHz in an undisturbed situation;

Fig. 6b is a cross-section of a user interface of an automated teller machine with a diagram of a simulation of an electric field that is created in the area of the user interface with a frequency of 1000 MHz in a disturbed situation - the user interface is approached by a dielectric object;

Fig. 6c is a cross-section of a user interface of an automated teller machine with a diagram of a simulation of an electric field that is created in the area of the user interface with a frequency of 1000 MHz in a disturbed situation - the user interface is approached by a conductive object, and

Fig. 7a, 7b are diagrams indicating a possible method of operating the security system according to the invention of an automated teller machine.

[0021] Herein below various embodiments of the present invention are described and shown in the drawings wherein like elements are provided with the same reference numbers.

[0022] Fig. 1 is a schematic drawing of an automated teller machine 1. The automated teller machine 1 has a user interface 2 that comprises several different data receiving units such as a keypad 3, a display or a screen 4 and a card reader 5. In the embodiment shown the keypad 3 is surrounded by a faceplate 6. The keys of the keypad 3 and the faceplate 6 are made out of an electrically conductive material such as for example metal. Keys and faceplate 6 are electrically isolated from each other. Some of the keys may be electrically connected with each other to create one pole as will be described later.

[0023] The automated teller machine 1 further comprises a security system surrounded by a dashed line indicated with reference number 7. The security system consists of several components such as a proximity sensor comprising a sensing unit 8 as well as emitting and/or receiving devices - here faceplate 6 and keys of a keypad 3 - a control unit 9 and means for warning 11. The security system 7 may be completely positioned in the automated teller machine 1. In such a scenario the existing warning system of the automated teller machine 1 may be used. Such a solution has a big advantage if the system is used for retrofitting an automated teller machine 1. It is also possible that components of the security system 7 are positioned inside the automated teller machine 1 and other components of the security system 7 are positioned outside the automated teller machine 1, wherein the components are connected with each other by a data exchange interface, such as for example an electrical connection or a wireless connection. In the embodiment shown in Fig. 1 the sensing unit 8 of the proximity sensor is positioned inside the automated teller machine 1 while the control device 9 and the warning device 11 are located outside the automated teller machine 1. The emitting and/or receiving devices 3, 6 are located at the outer surface of the automated teller machine.

[0024] The sensing unit 8 of the proximity sensor of the security system 7 is electrically connected with a key of the keypad 3 and with the faceplate 7 over - for example - shielded cables 12. The sensing unit 8 uses these two electrically conductive components - key of keypad 3 and faceplate 7 - to generate an electric field in the area of

the user interface 2 by applying an alternating voltage to these components.

[0025] Fig. 2 is a schematic drawing of a card reader 13 that is adapted to be equipped with a security system according to the invention. The card reader 13 comprises a block 15 with a slot 14 for introducing a card. Above the slot 14 the card reader 13 comprises a screw 16. the screw 16 is electrically conductive but isolated from the block 15. Block 15 and screw 16 may be used as emitting and/or receiving device of an electric field proximity sensor for a security system according to the invention.

[0026] Fig. 3 is a schematic diagram of one embodiment of the invention showing the security system in more detail. From the left to the right it shows two emitting and/or receiving devices 21 that are positioned so that they are electrically isolated from each other. The two emitting and/or receiving devices 21 are electrically connected with a LC oscillator 22 in the sensing unit 8. The LC oscillator 22 produces a repetitive electronic signal, such as for example a sine wave. This signal is send to the emitting and/or receiving devices 21 and generates an electric field 24 in the area of the emitting and/or receiving devices 21. This field does have a certain impedance. This impedance may be used by the LC oscillator to create a frequency which can be measured by a frequency counter 23 within the sensing unit 8 which creates a signal. The created signal is further send to the control unit 9, where an algorithm, with for example a low-pass filtering function, fades out quick changes and filters out long term contents. The impedance of the system depends on the shape of, the material of, and the distance between the emitting and/or receiving devices 21 as well as on the frequency that is send to the devices 21. An approaching object 25 influences the impedance as well. Any change in the impedance is measured by the frequency counter and reflected by the signal send to the control unit 9. The control unit 9 further compares the measured and filtered signals with a threshold as will be described later. If the signal is above the threshold the control unit 9 sends out an information to the warning unit 11.

[0027] Fig. 4 is a schematic diagram of another embodiment of the invention showing the security system in more detail. Also from the left to the right it shows two emitting and/or receiving devices 21.The emitting and/or receiving devices 21 are electrically connected with a directional coupler 25 of the sensing unit 8. The sensing unit 8 also comprises a generator 26, a splitter 27 and a receiver. The generator 26 generates a wave like signal which is splitted at the splitter 27, going over the directional coupler 25 and send out as an incident wave 29 between the sending and/or receiving devices 21. The incident wave 29 is reflected somewhere and comes back as a reflected wave 31. The reflected wave 31 may have a displaced phase compared with the incident wave 29 as well as a different amplitude. The changes of the reflected wave depend on the distance to the object that reflects the wave. The reflected wave 31 is than received by the emitting and/or receiving devices 21 and send to the directional coupler 25. The directional coupler 25 sends it to the receiver 28 where the signal of the reflected wave 31 is compared with the original signal. This signal contains at least two information - one over the phase shift and the other over the difference in the amplitude. The compared signal is send to the control unit 9. The control unit 9 uses an algorithm - as in the embodiment described above - to fade out quick changes and to filter out long term contents and further compares the signal with a threshold. If the signal is above the threshold the control unit 9 sends out a signal to the warning unit 11.

[0028] Fig. 5a is a cross-section of a faceplate 6 and three keys of a keypad 3 of for example an automated teller machine. The faceplate 6 is electrically connected to the sensing unit 8 of the proximity sensor over a shielded cable 12 and the middle key of the keypad 3 is electrically connected to the sensing unit 8 of the proximity sensor over another shielded cable 12. The three keys shown in this Figure are electrical connected with each other to build up one pole. The second pole is the faceplate 6. Those two poles are used as an emitting and/or receiving device of the sensing unit 8. An alternating voltage is applied to the two poles. The electric field is created around the keys of the keypad 3, which is the area that needs to be secured. Fig. 5a further shows a simulation of an electric field (equipotential lines) that is created in the area of the faceplate 6 and the keypad 3 with a frequency of 100 MHz in an undisturbed situation. An undisturbed situation in the sense of the invention is a user interface 2 with a faceplate 6 and a keypad 3 of a data receiving unit standing alone with nothing or no one approaching it. In such a situation the electric flux lines of the electric field can deploy uninfluenced and generate a certain impedance that is measured by the sensing unit 8 of the proximity sensor of the security system 7 as described with reference to Fig. 3 and 4.

[0029] Fig. 5b is the same faceplate 6 and three keys of the keypad 3 of an automated teller machine in a disturbed situation, that means a dielectric object 15 is approaching the faceplate 6 and the keypad 3. Fig. 5b shows a simulation of an electric field (equipotential lines) that is created in the area of the faceplate 6 with the same frequency as in Fig. 5a. The electric flux lines are disturbed by the dielectric object 15. They still deploy - also through the dielectric object 15 - but the influence of the dielectric object changes the impedance. This change is measured by the sensing unit 8 of the security system 7 as described with reference to Fig. 2 and 3. Fig. 5c does show the same situation as Fig. 5b with the only difference that the object 16 approaching the faceplate 6 and the keypad 3 being electrically conductive. The electric flux lines are blocked by the electrically conductive object 16. The electrically conductive object 16 influences the impedance of the system dramatically. This change is also measured by the sensing unit 8.

[0030] Fig. 6a to 6c show the same situations as Fig. 5a to 5c with another frequency (1000 MHz) being applied

to the faceplate 6 and the keypad 3. Since the impedance of the system is influenced by the materials of the emitting and/or receiving unit, their shape, the distance between them etc. every system has its own characteristic impedance. Depending on the system a change of the impedance may be best measured at different frequencies. To get better results out of the measurements it is possible to send more than one or even a range of frequencies through the security system and to analyse or interpret the sum or the maximum of all discrepancies of the measured impedance from a reference value.

[0031] Fig. 7a, 7b are diagrams indicating a possible method of operating a security system for a data receiving unit as described above. The axis of the abscissas in Fig. 7a and 7b represents the times in seconds; the axis of ordinates in Fig. 7a represents a signal proportional to the measured impedance and the axis of ordinates in Fig. 7b represents two different stages: activated and not activated, wherein 1 is activated and 0 is not activated.

[0032] The dashed line at 50 in Fig. 7a indicates a possible threshold for the impedance. All measured impedances that are lying under that threshold are defined as not relevant and all measured impedances that are lying above the threshold are defined as being relevant. Relevant in the sense of the invention means a certain reaction is initiated, if relevant data are measured, e.g. a warning system is being activated. The bold graph in Fig. 7a is the measured impedance and the dashed graph is the calculated processed failure signal. This signal is calculated over the above mentioned algorithm with a low-pass filtering function. The measured impedance is shown for clarity reasons. For the method of operating the security system only the processed failure signal is relevant.

[0033] When the security system according to the invention has been installed in a data receiving unit, for example in an automated teller machine, it first has to be calibrated. This is done by storing the level (# 1 in the diagram) of the measured impedance and the processed failure signal, when there is no object in front of the data receiving unit. This level is stored as reference value of the system. At # 2 in the diagram a short disturbance of the electric field is detected. This could have been caused by a hand of a user, using the keypad for e.g. entering a PIN. It can be seen that this relatively short disturbance leads only to a short increase of the measured impedance and a slight increase of the failure signal. The failure signal does not reach the threshold level. Therefore no warning system is activated. If a longer impedance change is detected by the system (# 3 in the diagram), e.g. caused by an approaching object for example a fake front panel or a fake keypad mounted on the original parts of the user interface, the measured impedance and the failure signal increase. At # 4 the failure signal reaches the threshold. At that time the warning system will be activated. This is shown in Fig. 7b, when the graph is moving from zero to one. At # 5 the failure signal is moving below the threshold again. This may be the case if the object is being removed from the user interface. In this situation the warning system may be deactivated again as can be seen in Fig. 7b.

Claims

1. A security system for a data receiving unit comprising:

   - a user interface (2), the user interface comprising at least two components (3, 6; 15, 16) with at least partially conductive properties, the conductive components being electrically isolated from each other, and
   - an electric field proximity sensor with emitting and/or receiving devices, **characterized in that**

   the conductive components of the user interface being used as emitting and/or receiving devices of the electric field proximity sensor.

2. The security system according to claim 1, wherein a sensing unit (8) of the electric field proximity sensor applies an alternating voltage to the conductive components of the user interface (2) for propagating an electric field in the area of the user interface.

3. The security system according to claim 2, wherein the sensing unit (8) of the electric field proximity sensor applies one or different frequencies to the conductive components of the user interface (2).

4. The security system according to any of the preceding claims, wherein the sensing unit (8) of the electric field proximity sensor is electrically connected with at least two conductive components of the user interface (2).

5. The security system according to claim 4, wherein the sensing unit (8) of the electric field proximity sensor is electrically connected from a rear side with the at least two conductive components of the user interface (2).

6. The security system according to any of the preceding claims, wherein the user interface (2) comprises a faceplate (7) and a keypad (3).

7. The security system according to claim 6, wherein the faceplate (7) and/or the keys of the keypad (3) have conductive properties.

8. The security system according to any of the claims 1 to 5, wherein the user interface comprises a card reader (13).

9. The security system according to claim 8, wherein

the card reader (13) comprises two electrically isolated components (15, 16) with at least partially conductive properties.

10. The security system according to any of the preceding claims comprising a control unit (9).

11. The security system according to any of the preceding claims comprising a warning unit (11).

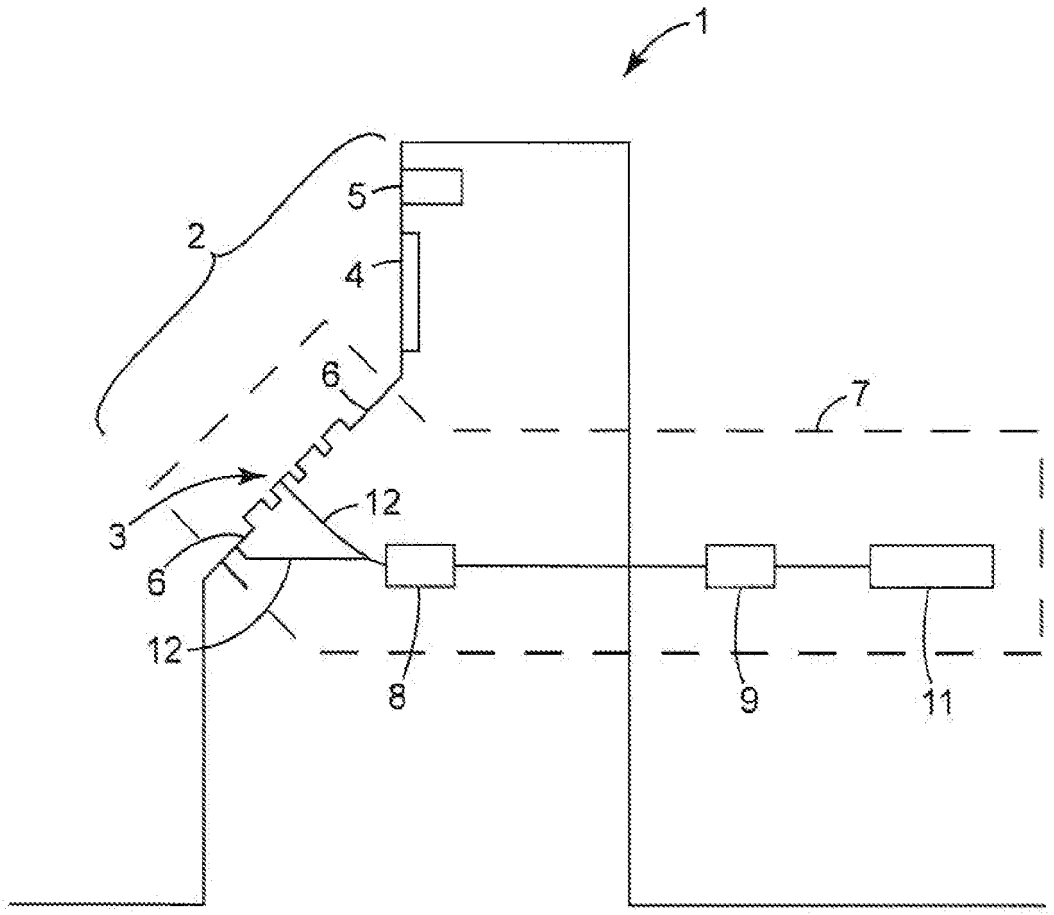

FIG. 1

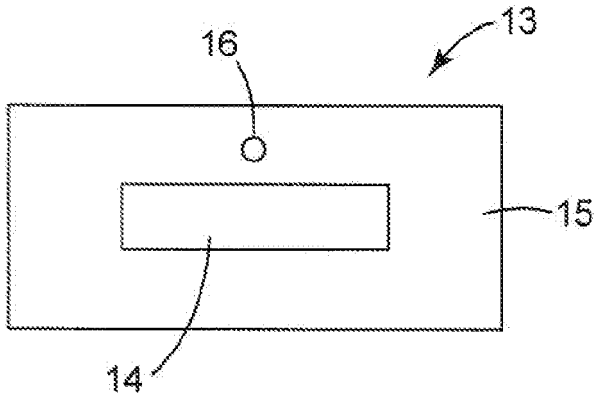

FIG. 2

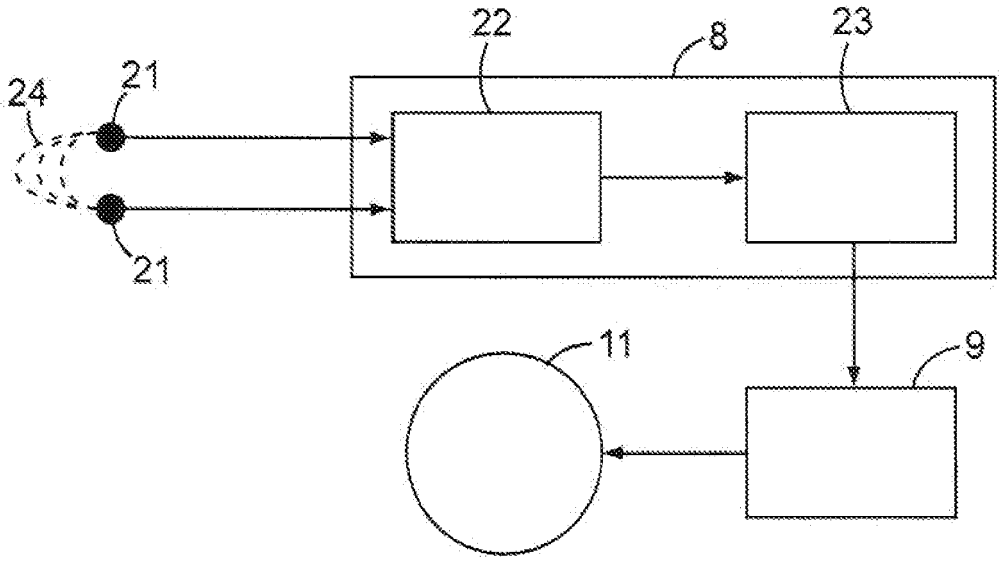

FIG. 3

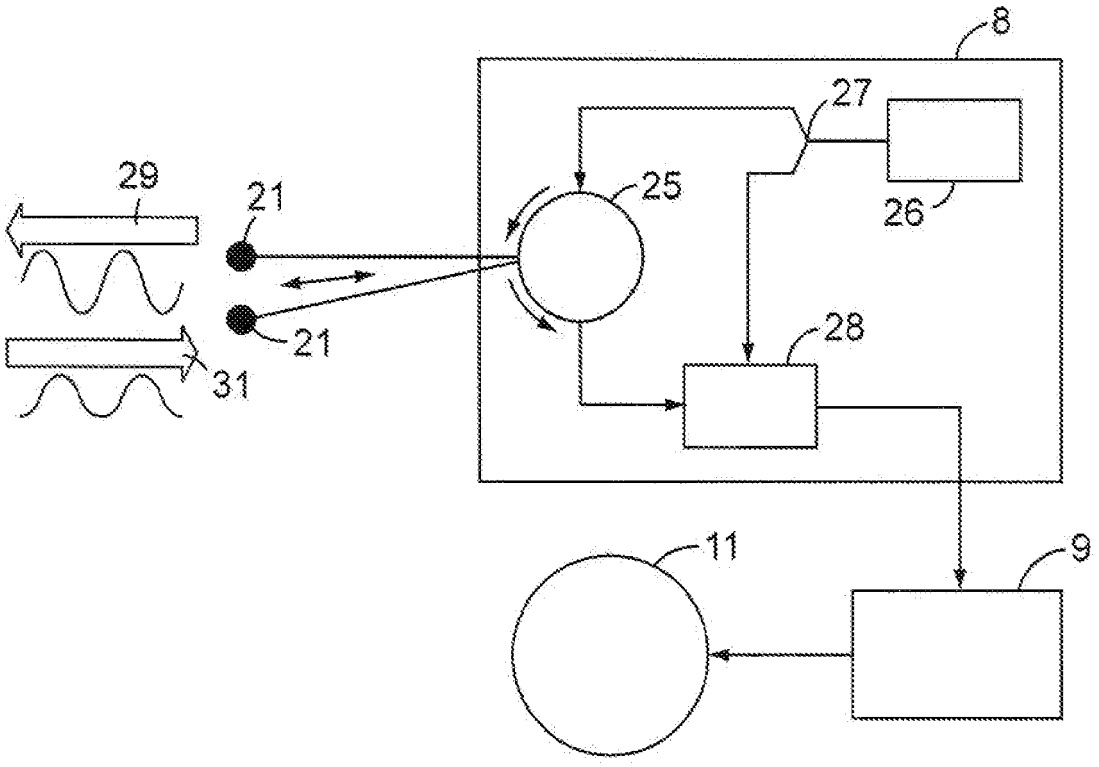

FIG. 4

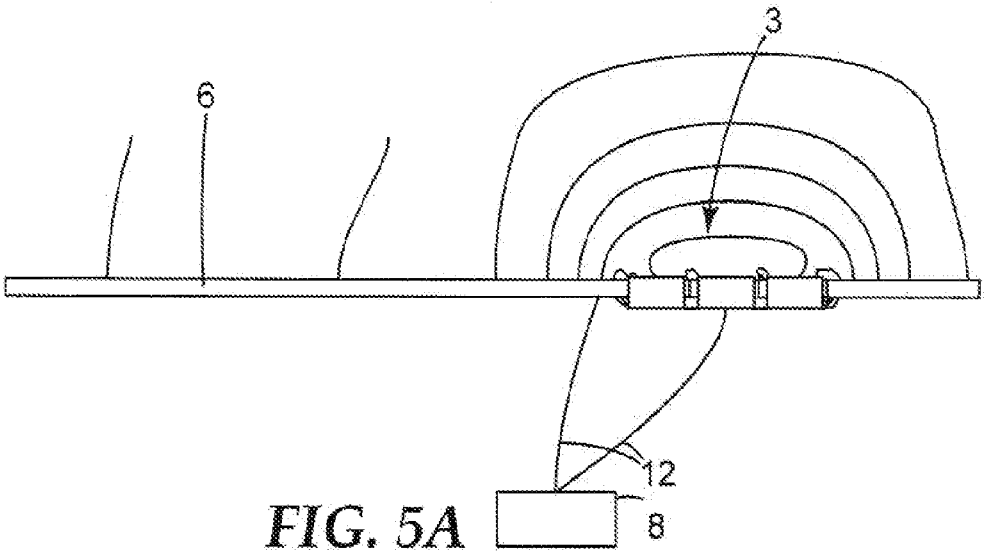

FIG. 5A

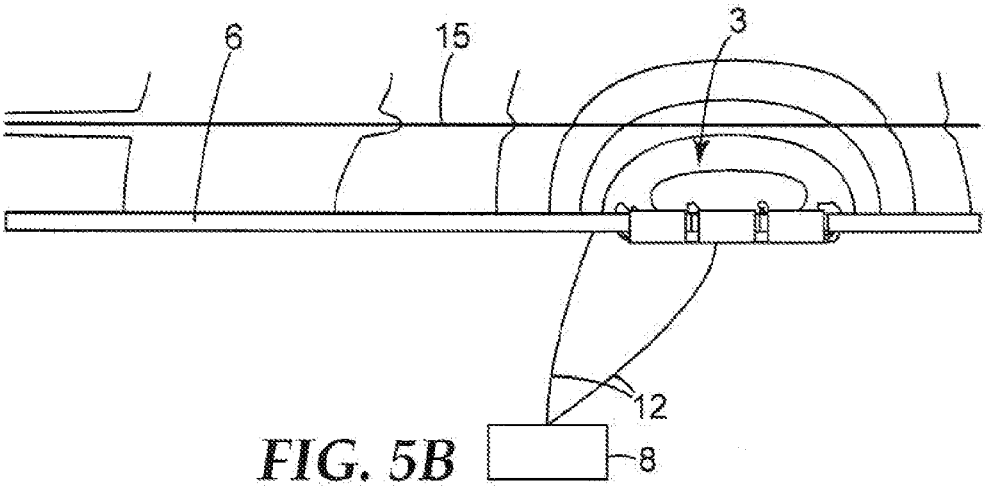

FIG. 5B

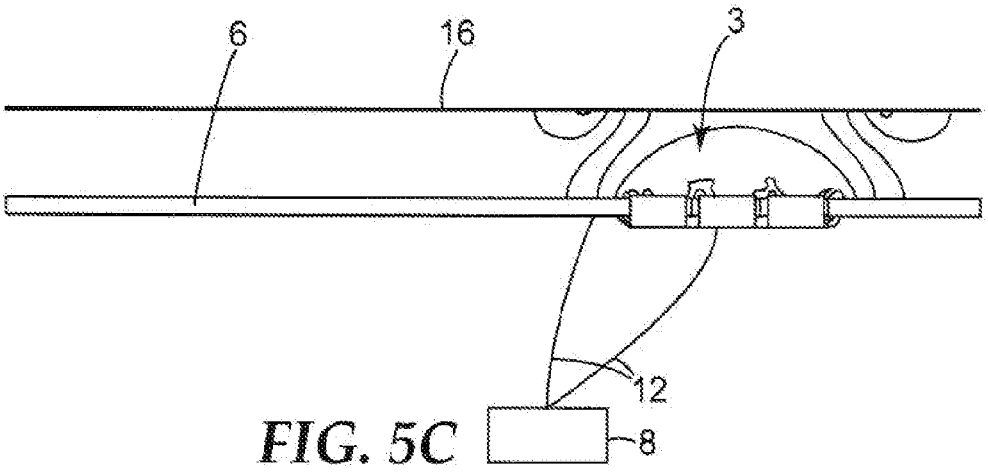

FIG. 5C

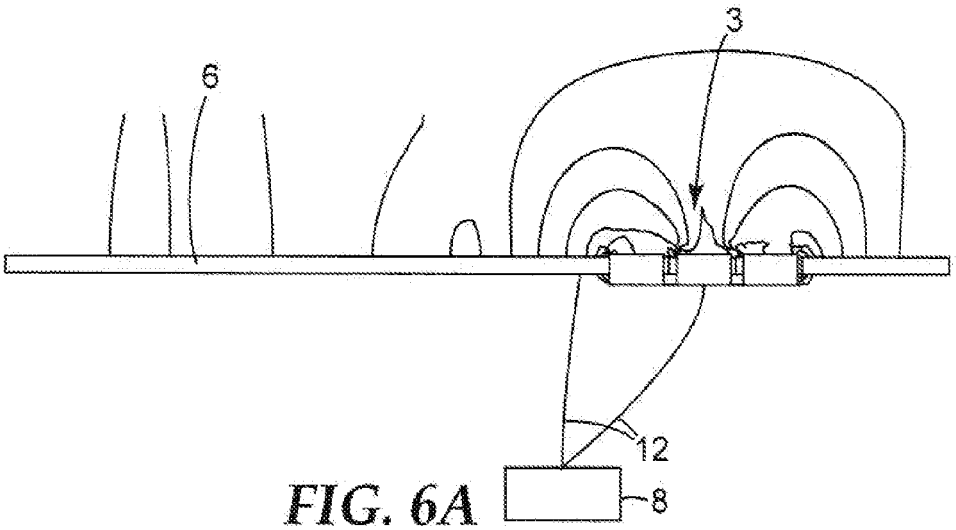

FIG. 6A

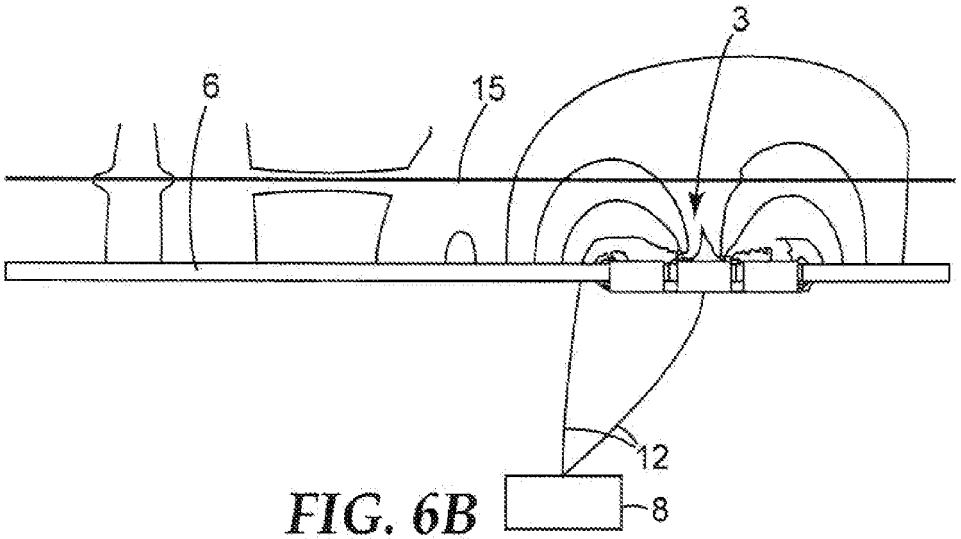

FIG. 6B

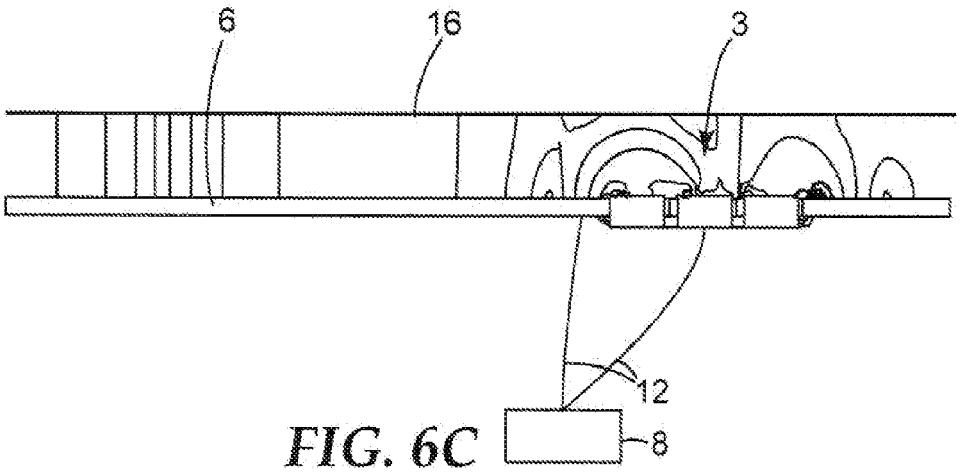

FIG. 6C

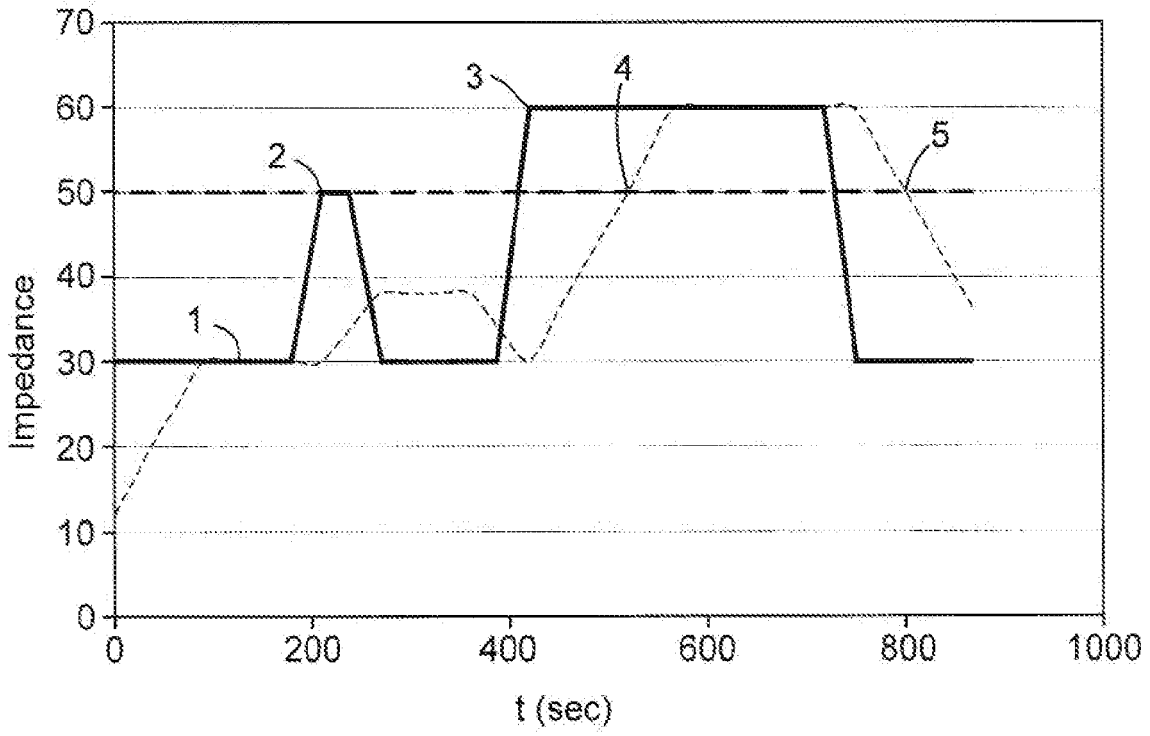
70
60
50
40
30
20
10
0
Impedance
0
200
400
600
800
1000
t (sec)
1
2
3
4
5

FIG. 7A

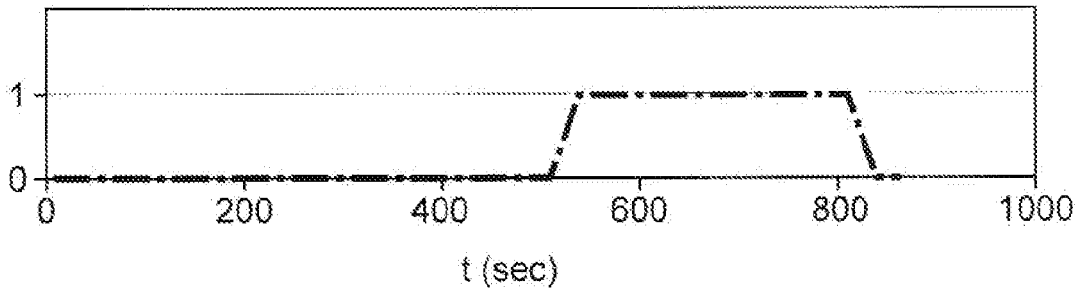
1
0
0
200
400
600
800
1000
t (sec)

FIG. 7B

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 10 16 4694

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
Y	US 6 390 367 B1 (DOIG ALISTAIR A [GB]) 21 May 2002 (2002-05-21) * column 3; claim 1; figures 1,2 *	1-11	INV. G07F19/00 G01D5/12 G01N27/02
Y	EP 0 742 448 A2 (EATON CORP [US]) 13 November 1996 (1996-11-13) * column 14; claim 1; figures 2,11,15 *	1-11	
A	GB 2 422 705 A (NCR INT INC [US]) 2 August 2006 (2006-08-02) * abstract; claim 1; figures 1-3 *	1	
A	WO 98/26506 A1 (CALDWELL DAVID W [US]) 18 June 1998 (1998-06-18) * page 16, line 15 - line 23; claims 1,26,27 *	1-11	
A	DE 10 2008 012231 A1 (WINCOR NIXDORF INT GMBH [DE]) 10 September 2009 (2009-09-10) * claims 1-11 *	1-11	
A	DE 10 2005 043317 B3 (WINCOR NIXDORF INT GMBH [DE]) 12 April 2007 (2007-04-12) * claims 1, 10, 11 *	1-11	TECHNICAL FIELDS SEARCHED (IPC) G07F G01D G01N
A	US 2006/237527 A1 (RAMACHANDRAN NATARAJAN [US] ET AL) 26 October 2006 (2006-10-26) * claims 1-17 *	1-11	
A	WO 96/06688 A1 (WHITAKER CORP [US]) 7 March 1996 (1996-03-07) * page 2, line 11 - line 35 * * page 21, line 19 - line 20; claim 1 *	1-11	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	25 October 2010	Lavin Liermo, Jesus

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 10 16 4694

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.

25-10-2010

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6390367 B1	21-05-2002	NONE	
EP 0742448 A2	13-11-1996	JP 9101104 A	15-04-1997
GB 2422705 A	02-08-2006	BR PI0519914 A2	07-04-2009
		CN 101147178 A	19-03-2008
WO 9826506 A1	18-06-1998	AT 295629 T	15-05-2005
		AU 759050 B2	03-04-2003
		AU 5696398 A	03-07-1998
		CA 2257920 A1	18-06-1998
		CN 1217835 A	26-05-1999
		DE 69733250 D1	16-06-2005
		DE 69733250 T2	02-02-2006
		EP 0883931 A1	16-12-1998
		ES 2242241 T3	01-11-2005
		HK 1020302 A1	06-05-2005
		JP 4162717 B2	08-10-2008
		JP 2001507882 T	12-06-2001
		NZ 331543 A	26-05-2000
DE 102008012231 A1	10-09-2009	WO 2009109543 A1	11-09-2009
DE 102005043317 B3	12-04-2007	CN 101263507 A	10-09-2008
		EP 1924948 A1	28-05-2008
		WO 2007048649 A1	03-05-2007
		US 2009159676 A1	25-06-2009
US 2006237527 A1	26-10-2006	US 2006243790 A1	02-11-2006
WO 9606688 A1	07-03-1996	NONE	

EPO FORM P0459

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

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- EP 1677267 A1 **[0004]**
- US 20080110975 A1 **[0004]**
- WO 9523421 A **[0005]**
- WO 2005109358 A1 **[0006]**
- GB 2351590 A **[0007]**