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

(11) EP 1 544 386 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
22.06.2005 Bulletin 2005/25

(51) Int Cl.[7]: **E05B 39/02**, B65D 90/00, G09F 3/03, G06F 17/60

(21) Application number: **03425806.1**

(22) Date of filing: **17.12.2003**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PT RO SE SI SK TR
Designated Extension States:
AL LT LV MK

(71) Applicant: **HT S.r.l.**
57014 Collesalvetti LI (IT)

(72) Inventor: **Sestini, Quirino Fausto**
24100 Bergamo BG (IT)

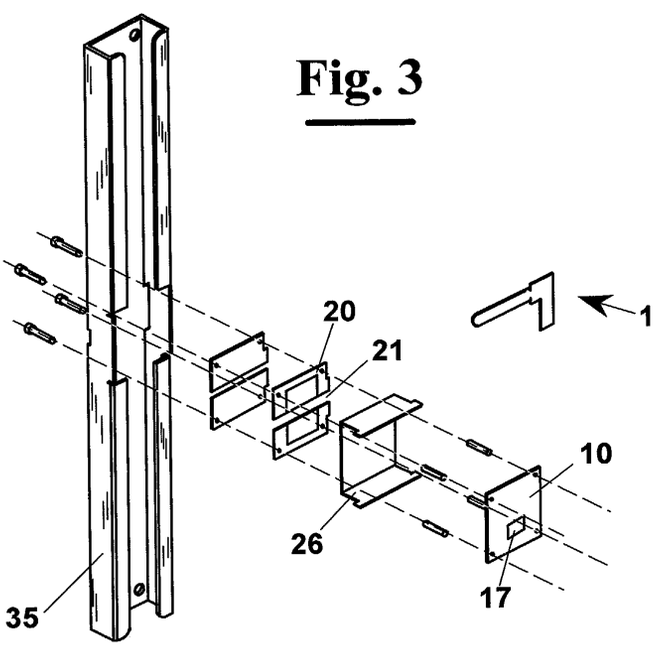
(74) Representative: **Celestino, Marco**
ABM, Agenzia Brevetti & Marchi,
Viale Giovanni Pisano, 31
56123 Pisa (IT)

Remarks:
In accordance with the last part of Article 14 (2) EPC the applicant has filed a text with which it is intended to bring the translation into conformity with the original text of the application.

(54) Method to attest an occurred tampering of a container and electronic lock that carries out this method

(57) Method to attest an occurred tampering of the lock of a container carried out by means comprising a transponder (10) associated to the container with relative circuit (17) and security member (1). The transponder (10) can be mounted on a support (35) that is integral to the container and that in use remains inside it, whereby the transponder is not accessible without leaving apparent tampering evidence on the container same or on a lock (101). The transponder (10) comprises a circuit (17) in which a non-duplicable identification code is recorded for identifying univocally the container (100). Similarly, the security member (1) is associated univocally to a non-duplicable identification code recorded in another circuit (7) to it fastened. In particular, each circuit (7, or 17), is of passive type, i.e. it does not need a battery and is activated only within an electromagnetic field and not out of it. Each circuit (7, or 17), is, furthermore, capable of radio communication with a transreceiving apparatus (55) for returning its identification code.

Fig. 3



EP 1 544 386 A1

Description

Field of the invention

[0001] The present invention relates to a method to attest an occurred tampering or an unauthorized opening of a container for carrying goods of many kinds.

[0002] Furthermore, the invention relates to an electronic lock that carries out this method.

Description of the prior art

[0003] As known, various solutions exist adopted for preventing an unauthorized opening of containers of many kinds, in particular, containers set to travel without surveillance in freight compartments of transport means such as ships and trains. In particular, locks exist with traditional closing/opening mechanisms and also locks much more sophisticated that provide opening/closing devices of electronic type, for example that require a combination. However, such locks, even the more sophisticated, if tampered and opened by expert burglars, have the drawback that they can be closed again without that an occurred tampering can be detected. In particular, in case the containers keep confidential documents, dangerous substances, military equipment, or if they are sent to protected areas, it is important to attest whether if they have been tampered during transport.

[0004] Devices also exist to attest an occurred tampering of a container. For example, a simple solution is described in US 2013299. It provides the application of an adhesive tape at the opening line of the container with the signature or stamp of the owner to avoid opening by unauthorised people. Other solutions provide the use of seals of various material, for example, plastics or metal, with serial numbers or symbols printed or engraved on. Such solutions do not solve appropriately the problem since they can be easily tampered as described in US 6265973.

[0005] Antitampering systems also exist that provide a security member inserted in a lock which prevents mechanically the opening operation of the container. The extraction of the security member or its rupture causes the transmitting an alarm signal.

[0006] Also this solution, however, does not assure full safety and furthermore, an electric supply is necessary.

Summary of the invention.

[0007] It is therefore a first feature of the present invention to provide a method to attest an occurred tampering of a container for testing with certainty a possible unauthorized opening of the container.

[0008] It is another feature of the present invention to provide such a method that allows trailing the container, its content, and any control steps carried out on them, i.e. tracing and reconstructing with precision its movements carried from forwarding to delivery.

[0009] These and other features are accomplished with one exemplary method to attest an occurred tampering of a container whose main feature is to provide the following steps:

- associating to said container a first non-duplicable code which can be read by radio waves reading means;
- choosing a security member having a second non-duplicable code which can be read by radio waves reading means;
- opening a surveillance procedure of the container by a first operator authorized to close the container in a forwarding station, to said first operator an ID code being given;
- reading said first and second identification codes by radio waves receiving means and storing said codes associated to each other in registration means;
- transmitting said recorded codes to a remote terminal;
- arranging said security member in integral association to said container in order to block mechanically the opening operation of said container unless breaking said security member;
- transporting said container from the forwarding station to the delivery station;
- repeating the step of reading said codes by a second operator in the delivery station and checking the coincidence of the recorded codes with the read data.

[0010] In particular, the arrangement of the security member in integral association to the container is made introducing a portion of the security member in a housing created in a support integral to the container and accessible through an opening created in the wall of the container.

[0011] Advantageously, the container can be opened only breaking the seal, i.e., causing a detachment of a portion thereof which exceeds the external surface of the container. This allows attesting a possible unauthorized opening observing directly the integrity of the seal.

[0012] In particular, the identification code of the container is recorded in a circuit arranged in a housing that in use is in the container in an area not accessible from outside without leaving apparent tampering evidence on the container same.

[0013] Similarly, the identification code of the security member is recorded in a circuit that in operative conditions is not accessible from outside without leaving apparent tampering evidence on the security member same or on the container. This prevents from possible tampering of the circuits by unauthorised individuals.

[0014] In particular, at least one intermediate verification station can be provided arranged between the forwarding station and the delivery station. The surveil-

lance procedure of the container as above described thus provides a traceability of the container same. In other words, it is possible to reconstruct and follow the path of the container from the forwarding station to the delivery station at any intermediate station to attest a possible tampering and to date back the moment when this tampering occurred.

[0015] According to another aspect of the invention, an apparatus to attest an occurred tampering of a container provides:

- an electronic lock comprising:
    - a housing having a first circuit in which an non-duplicable identification code is recorded associated to a container;
    - a security member having a second circuit in which another non-duplicable identification code is recorded;
    - means for engaging said security member with said container suitable for blocking mechanically the opening operation of said container, after said engagement said security member being not separable from said container without break;
    - radio waves transreceiving means capable of communicating with said first and second circuit for reading said codes and writing various data.

[0016] In particular, a housing is provided accessible through an opening created in the wall of the container, said housing being mounted on a support integral to the container that in use remains in the container same.

[0017] Advantageously, the security member and the housing have cooperating means suitable for causing a mutual engagement.

[0018] Advantageously, the housing has a protection shield that cannot be set if the security member is not correctly engaged in it.

[0019] In an exemplary embodiment of the invention the cooperating means of the security member and of the housing have a unidirectional pliability. In particular they allow the introduction of the security member in the housing along an advancing direction, but preventing from the extraction of the security member from the housing in the opposite direction. This prohibits that an unauthorised individual removes the security member as a whole from the housing and that the lock is opened without leaving tampering evidence.

[0020] Advantageously, the security member comprises an elongated portion connected by a weakened portion to a head. Once inserted correctly the security member in the housing in order to cause the respective cooperating means to mutually engage, the container can be opened only detaching the head from the seal, i.e. detaching the head from the elongated portion at the weakened portion.

[0021] In particular, the used circuits have a read only memory (ROM) whereby the identification code that is preprogrammed at the moment of the production of the circuits cannot be altered. More in detail, each circuit queried by the transreceiving means returns its identification code. This is carried out through an antenna that forms with the queried circuit a transreceiving element, or transponder, which interacts with the transreceiving means by a system of transmitting/receiving radio waves according to the RFID technology (Radio Frequency IDentification). In the extent of the present application radio waves comprise also microwaves.

[0022] More in detail, the transponder associated to the container is mounted on the support integral to the container and in operative conditions is in the inner side of the container, whereby it is not possible to reach it without leaving tampering evidence on the container same.

Brief description of the drawings

[0023] Further characteristics and the advantages of the method to attest an occurred tampering of a container according to the present invention will be made clearer with the following description of an exemplary embodiment thereof, exemplifying but not limitative, with reference to the attached drawings wherein:

- figure 1 shows diagrammatically a perspective view of a transponder associated to the container mounted on the relative frame;
- figure 2 shows a perspective view of a possible exemplary embodiment of the security member with relative transponder and of the cooperating means of the housing that allow their mutual engagement;
- figure 3 shows in an exploded view the support on which the housing and the transponder associated to the container are mounted;
- figures 4 and 5 show perspective views respectively in an exploded and in an assembled configuration of the upright with the opening that allows the access to the housing of the lock and relative protection shield;
- figures from 6 to 11 show diagrammatically a possible succession of steps through which the method according to the invention is carried out;
- figure 12 shows diagrammatically a partially cross sectioned elevational side view of the position in which the lock means are arranged for preventing the opening operation of the container;
- figure 13 shows diagrammatically a partially cross sectioned elevational side view of the position in which the lock means allow opening the container;
- figure 14 shows in a perspective rear view the relative position of the support and of the upright of figures 11 and 12;
- figure 15 shows a perspective view of a container on which an electronic lock according to the inven-

tion is installed.

Description of the preferred exemplary embodiments

[0024] A container which applyies the present invention is described in EP 02020011 incorporated by reference to the present description.

[0025] In figures 1 and 2 respectively transponder 10 associated to the container with relative circuit 17 and security member 1 with relative circuit 7 are shown by means of which it is possible to carry out the method to attest an occurred tampering of the lock of a container, according to the invention. Even if in the following description reference is made to a transponder 10 operating at a frequency of 13,56 MHz, in any case it is possible to use a transponder operating at much higher frequencies, for example 900 MHz or 2.4 GHz. More in detail, the use of transponder operating at much higher frequencies allows longer reading distances and higher data transmission rates, even if the higher frequencies have some drawbacks, for example a higher sensitivity to humidity for GHz frequencies.

[0026] As shown in figure 1, transponder 10 can be mounted on a support 35 that is integral to the container and that in use remains inside it, whereby the transponder is not accessible without leaving apparent tampering evidence on the container same or on a lock 101. Transponder 10 comprises a circuit 17 in which at the production a non-duplicable identification code is recorded for identifying univocally a container 100. Similarly, security member 1 is associated univocally to a non-duplicable identification code recorded at the production in a circuit 7 to it fastened. In particular, each circuit 7, or 17, is of passive type, i.e. it does not need a battery and is activated only within an electromagnetic field and not out of it. Each circuit 7, or 17, is, furthermore, capable of radio communication with a transreceiving apparatus 55 for returning its identification code (figures 7 and 9).

[0027] In the exemplary embodiment shown in figure 2 the security member comprises an elongated portion 2 on which the circuit 7 is applied. Elongated portion 2 is connected by a weakened portion 6 to a head 3. Always in figure 2 a possible exemplary embodiment is shown of the cooperating means 5 of between security member 1 and a part of cooperating means 25 associated to housing 21 that allow to them a mutual engagement. In particular, the interaction between the teeth 25 of a lock 20 and side recesses 5 of security member 1 allows an easy introduction of security member 1 in housing 21, but prohibit any extraction of security member 1.

[0028] The method to attest an occurred tampering of the lock of container 100 begins when an operator 50 uses a transreceiving apparatus 55, for example a palm-sized computer, associated to a plurality of identification data. These identify the operator entrusted with the surveillance procedure of container 100 in the forwarding station (figure 6). Then, operator 50 by a radio waves transreceiver, for example integrated in the palm-sized computer 55, queries circuit 17 that returns the identification code associated to container 100 and in it recorded. Then, operator 50 chooses a security member 1 among a plurality of security member and reads its relative identification code recorded in circuit 7 by the radio waves transreceiver integrated in the palm-sized computer 55 (figure 9). Both identification codes of circuits 7 and 17 are recorded in the memory of the palm-sized computer 55 without being displayed on the display 56 and then associated univocally to each other. In particular, the identification codes of the security member and of the container are encrypted and kept inaccessible to avoid any possible manipulation.

[0029] Security member 1 is then inserted, through an opening 45 made in an upright 40, in a housing 21 mounted on support 35 obtaining a physical matching between security member 1 and housing 21. This allows to attest a possible unauthorized opening of container 100 since the cooperating means 5 and 25 of security member 1 and of housing 21 prohibit the extraction of security member 1 as a whole from housing 21. Once executed correctly the engagement between security member 1 and housing 21, container 100 can be opened only breaking security member 1, causing a detachment of head 3 from elongated portion 2 at weakened portion 6 (figure 11). This would make apparent a possible tampering of the container or of the housing by unauthorised individuals. A possible change of a broken security member 1 with another identical security member would be recognized at the moment of the control in a station of verification, owing to the uniqueness of the identification code of each security member.

[0030] The foregoing description of a specific embodiment will so fully reveal the invention according to the conceptual point of view, so that others, by applying current knowledge, will be able to modify and/or adapt for various applications such an embodiment without further research and without parting from the invention, and it is therefore to be understood that such adaptations and modifications will have to be considered as equivalent to the specific embodiment. The means and the materials to realise the different functions described herein could have a different nature without, for this reason, departing from the field of the invention. It is to be understood that the phraseology or terminology employed herein is for the purpose of description and not of limitation.

Claims

1. Method to attest an occurred tampering of a container **characterised in that** it provides the following steps:

   - associating to said container a first non-duplicable code which can be read by radio waves

reading means;

- choosing a security member having a second non-duplicable code which can be read by radio waves reading means;
- opening a surveillance procedure of the container by a first operator authorized to close the container in a forwarding station, to said first operator an ID code being given;
- reading said first and second identification codes by radio waves receiving means and storing said codes associated to each other in registration means;
- transmitting said recorded codes to a remote terminal;
- arranging said security member in integral association to said container in order to block mechanically the opening operation of said container unless breaking said security member;
- transporting said container from the forwarding station to the delivery station;
- repeating the step of reading said codes by a second operator in the delivery station and checking the coincidence of the recorded codes with the read data.

2. Method, according to claim 1, wherein said arranging step of said security member in integral association to said container is made introducing a portion of said security member in a housing created in a support integral to said container, said housing being accessible through an opening created in the wall of said container.

3. Method, according to claims 1 and 2, where the opening operation of said container is possible only causing a detachment of a portion of said security member exceeding the external surface of said container.

4. Method, according to claim 1, wherein said identification code of said container is recorded in a circuit arranged in a housing that in use is in the container in an area not accessible from outside without leaving apparent tampering evidence on the container same.

5. Method, according to claim 1, wherein said identification code of said security member is recorded in a circuit that in operative conditions is not accessible from outside without leaving apparent tampering evidence on the security member same or on the container.

6. Method, according to claim 1, wherein at least one intermediate verification station is provided arranged between said forwarding station and said delivery station.

7. Apparatus to attest an occurred tampering of a container **characterised in that** of providing:

- an electronic lock comprising:

- a housing having a first circuit in which an non-duplicable identification code is recorded associated to a container;
- a security member having a second circuit in which another non-duplicable identification code is recorded;
- means for engaging said security member with said container suitable for blocking mechanically the opening operation of said container, after said engagement said security member being not separable from said container without break;
- radio waves receiving means capable of communicating with said first and second circuit for reading said codes;
- registration means suitable for memorizing said codes.

8. Apparatus, according to claim 7, wherein a housing is provided accessible through an opening created in the wall of said container, said housing being mounted on a support integral to said container that in use remains inside it.

9. Apparatus, according to claims 7 and 8, wherein said security member and said housing have cooperating means suitable for causing a mutual engagement.

10. Apparatus, according to claim 9, wherein said cooperating means of said security member and said housing have an unidirectional pliability, said cooperating means allowing the introducing said security member in said housing along a direction of movement and blocking the extraction of the security member from the housing in the opposite direction.

11. Apparatus, according to claim 9, wherein said security member comprises an elongated portion connected by a weakened portion to a head, the opening operation of said container being possible only detaching said head from said security member causing a disengagement from the elongated portion at the weakened portion.

Fig. 1

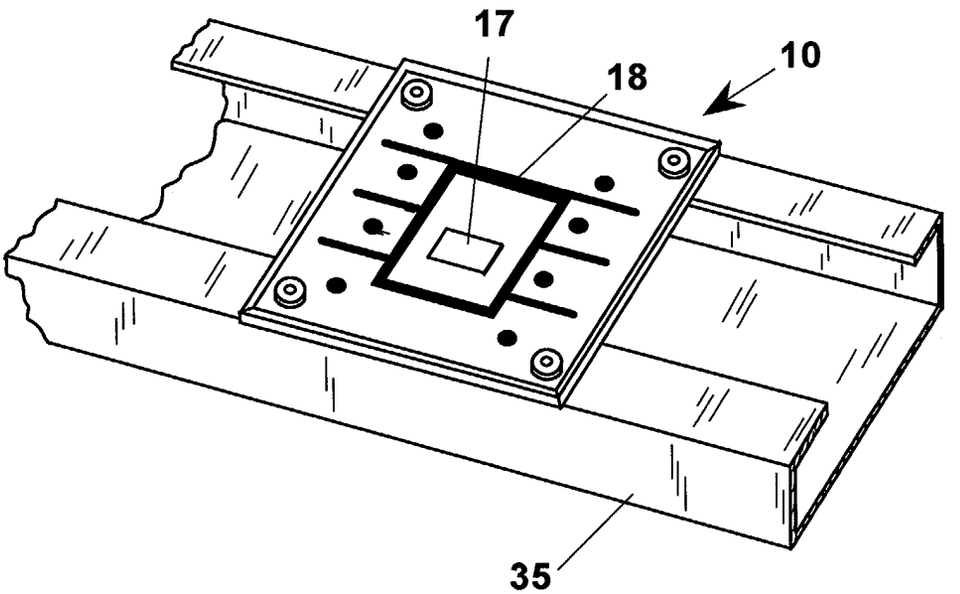


Fig. 2

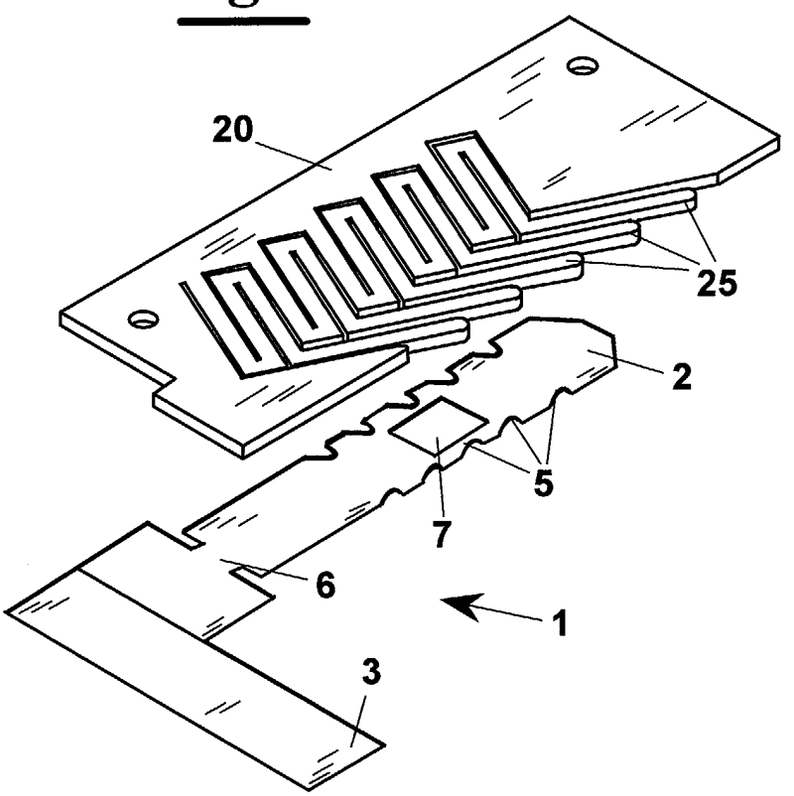


Fig. 3

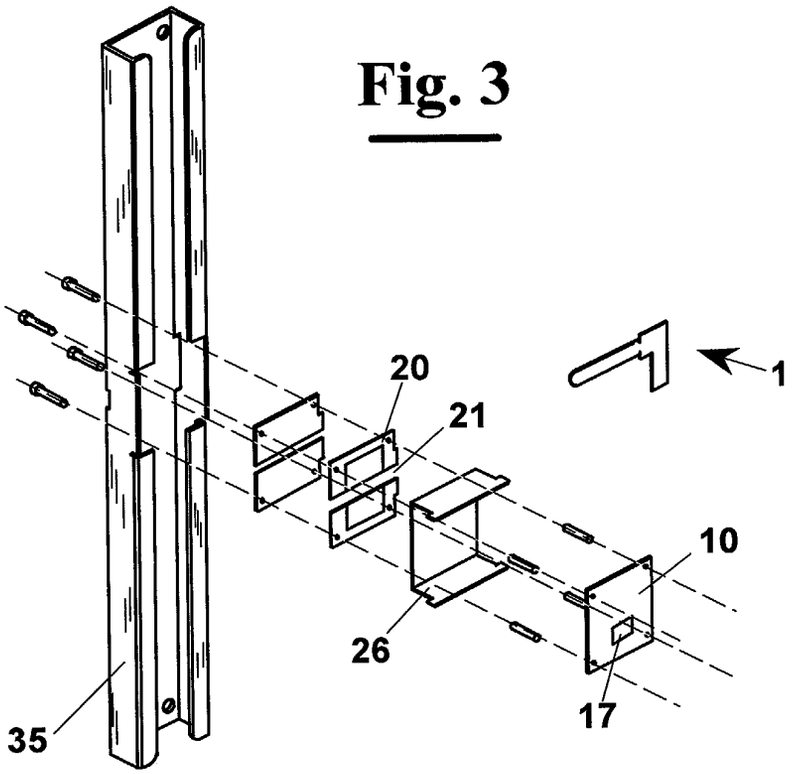


Fig. 4

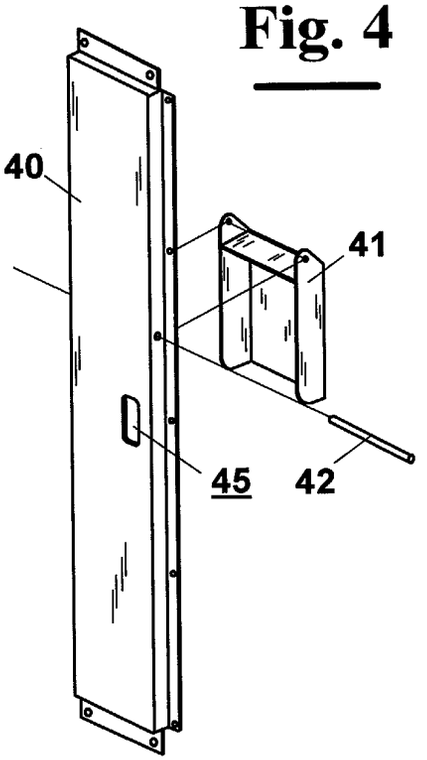


Fig. 5

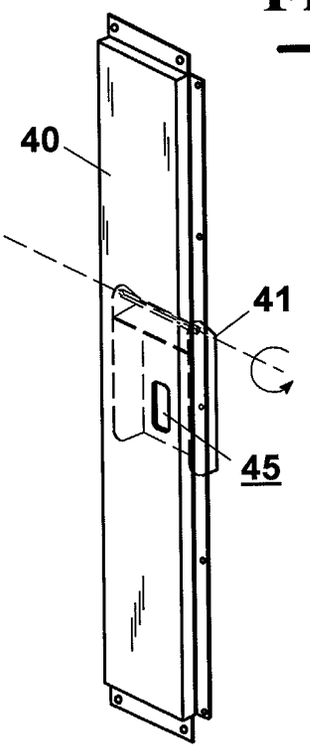


Fig. 6

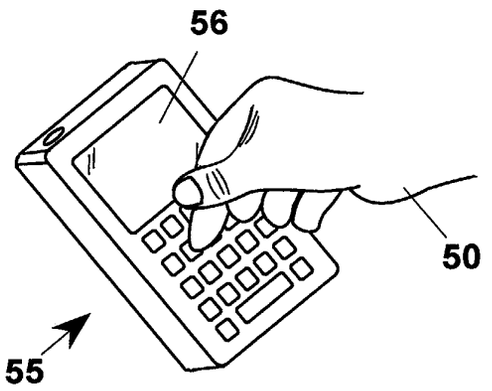


Fig. 8

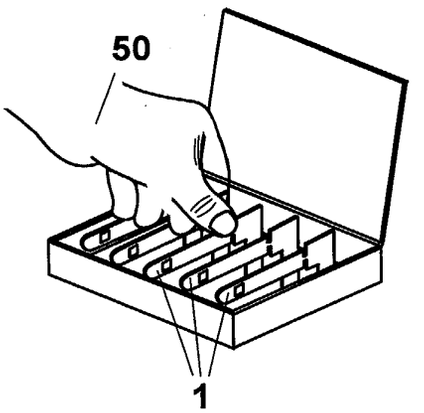


Fig. 7

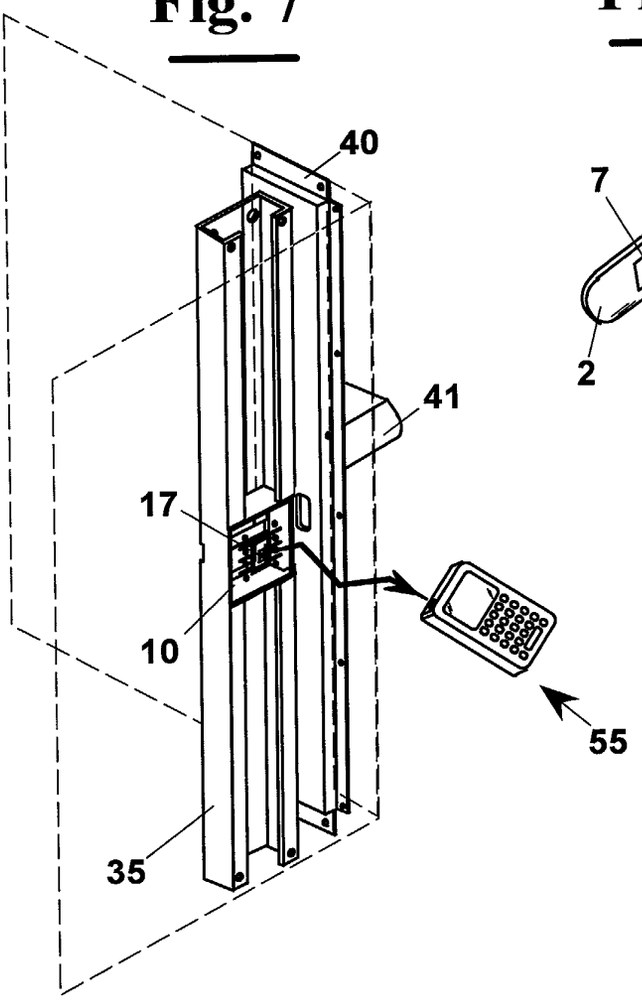


Fig. 9

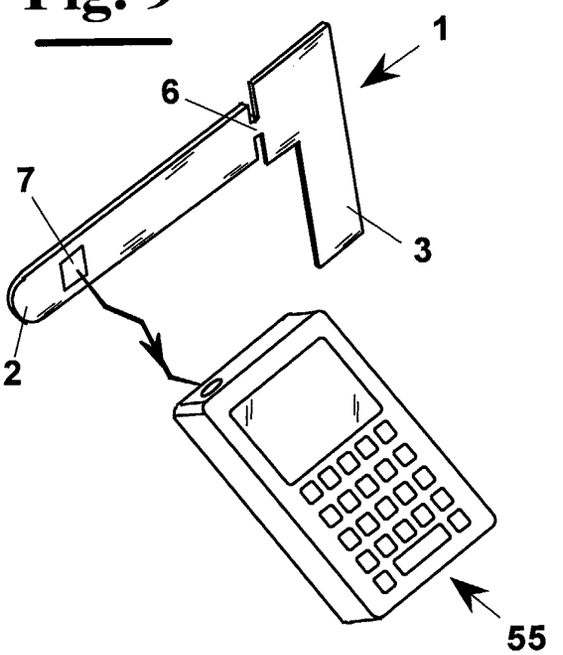


Fig. 10

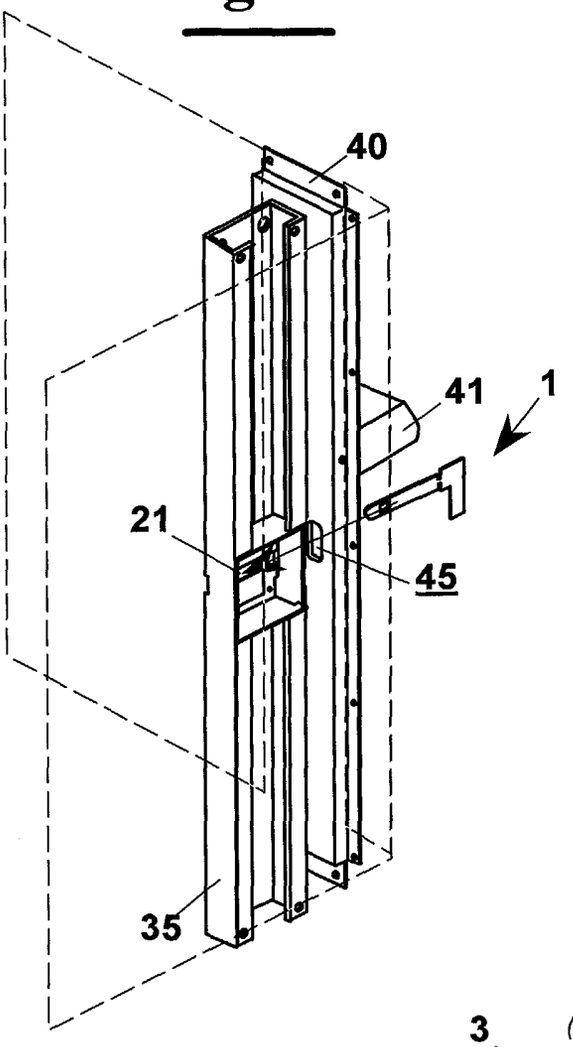


Fig. 11

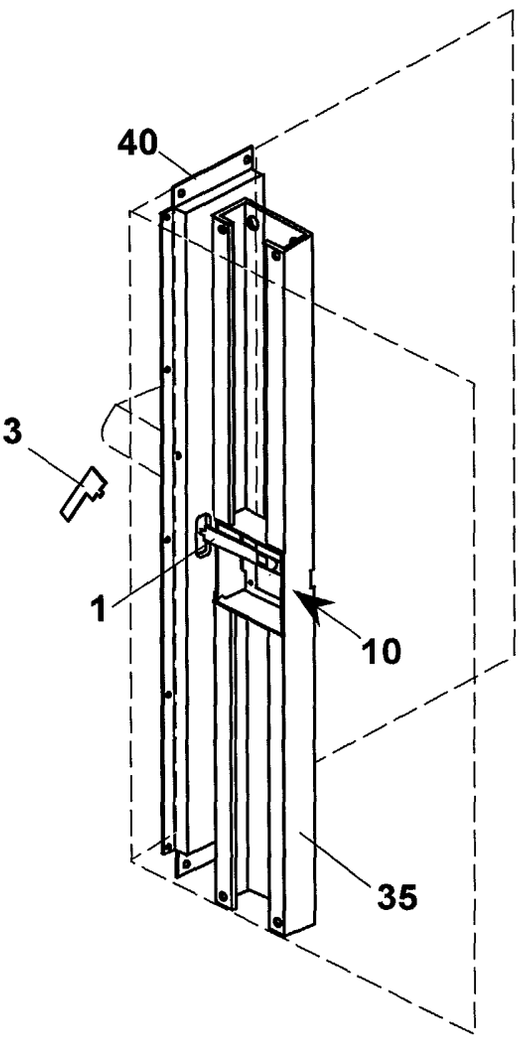


Fig. 12

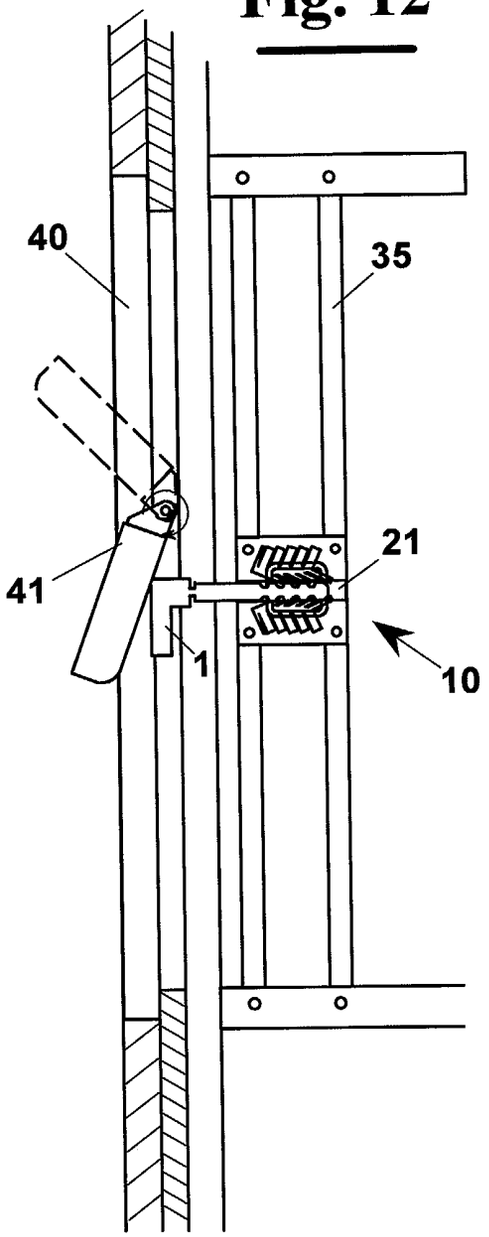


Fig. 13

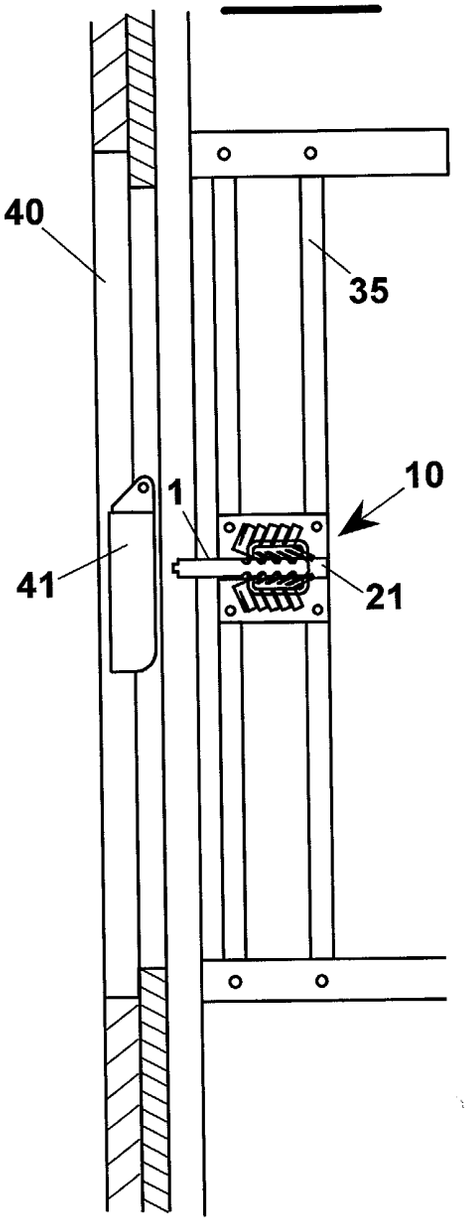


Fig. 14

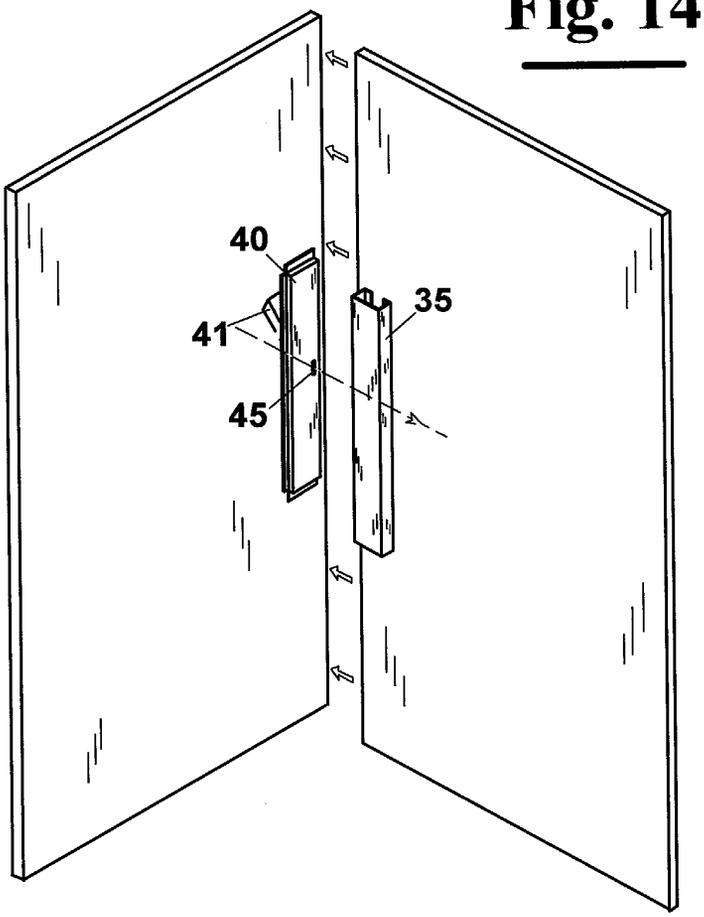
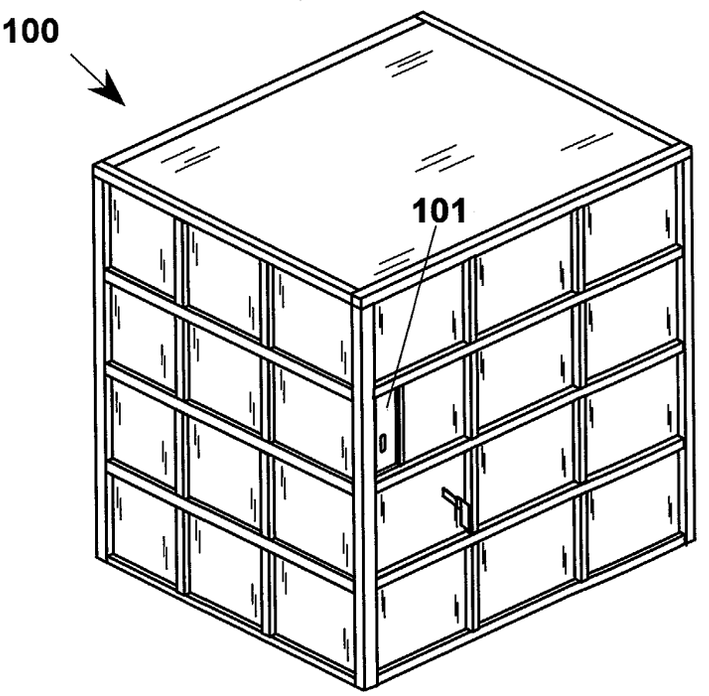


Fig. 15



European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 03 42 5806

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	EP 1 182 154 A (ISHIKAWAJIMA HARIMA HEAVY IND) 27 February 2002 (2002-02-27) * abstract; figures 11a,11b,12,13 * * paragraph [0022] * * paragraph [0025] * * paragraph [0028] * * paragraph [0032] - paragraph [0039] * * paragraph [0043] *	1,4,6,7	E05B39/02 B65D90/00 G09F3/03 G06F17/60
Y		2,3,5, 8-11	
Y	FR 2 507 579 A (LEHNER MAX & CO AG) 17 December 1982 (1982-12-17) * figures 1,9,10 * * page 6, line 33 - page 7, line 16 *	2,3,5, 8-11	
A	US 4 682 688 A (BUDERT GUENTER H) 28 July 1987 (1987-07-28) * abstract; figures *	2,3,5, 8-11	
A	US 5 125 700 A (FATTORI LAZZARO A ET AL) 30 June 1992 (1992-06-30) * abstract; claim 9; figures 13,14 * * column 1, line 36 - line 50 * * column 2, line 3 - line 22 * * column 4, line 25 - line 28 *	1,7	TECHNICAL FIELDS SEARCHED (Int.Cl.7) E05B B65D G09F G06F
A	DE 197 04 210 A (ORGA KARTENSYSTEME GMBH) 6 August 1998 (1998-08-06) * the whole document *	1,7	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	12 July 2004	Buron, E

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 03 42 5806

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.

12-07-2004

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1182154 A	27-02-2002	JP 2001213523 A	07-08-2001
		JP 2001213524 A	07-08-2001
		JP 2001213522 A	07-08-2001
		JP 2001220019 A	14-08-2001
		JP 2001240246 A	04-09-2001
		JP 2001240247 A	04-09-2001
		JP 2001240248 A	04-09-2001
		EP 1182154 A1	27-02-2002
		US 2002161675 A1	31-10-2002
		WO 0156907 A1	09-08-2001
FR 2507579 A	17-12-1982	CH 652986 A5	13-12-1985
		DE 3220125 A1	30-12-1982
		FR 2507579 A1	17-12-1982
US 4682688 A	28-07-1987	DE 8501735 U1	21-03-1985
US 5125700 A	30-06-1992	AU 8309491 A	02-03-1992
		WO 9202918 A1	20-02-1992
		US 5120097 A	09-06-1992
DE 19704210 A	06-08-1998	DE 19704210 A1	06-08-1998

EPO FORM P0459

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