

(19)



(11)

EP 3 128 490 A1

(12)

EUROPEAN PATENT APPLICATION

(43) Date of publication:
08.02.2017 Bulletin 2017/06

(51) Int Cl.:
G07F 19/00 ^(2006.01) **G07F 7/10** ^(2006.01)
H03K 3/0231 ^(2006.01)

(21) Application number: **15180144.6**

(22) Date of filing: **07.08.2015**

(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
Designated Validation States:
MA

(72) Inventor: **O'REILLY, Dave**
Co. Wicklow, W91 E202 (IE)

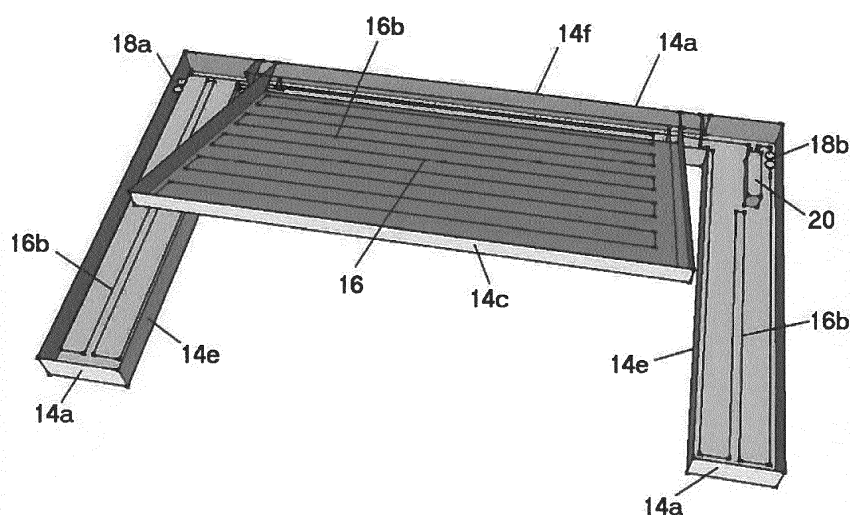
(74) Representative: **Boyce, Conor et al**
Hanna Moore + Curley
Garryard House
25/26 Earlsfort Terrace
Dublin 2, D02 PX51 (IE)

(71) Applicant: **Coraza Holdings Limited**
W91 E202 Co. Wicklow (IE)

(54) A SECURITY SHIELD FOR A DATA ENTRY KEYPAD

(57) A PIN shield 14 for a PIN pad 10 set into a fascia 12 comprises one or more components 14a, 14b, 14c which restrict a full view of the keypad to a person located directly in front of the keypad. At least one shield component has embedded therein a mesh 16 (Figures 2 and 3) comprising an electrical conductor extending continuously between input and output contacts 18b on the component. A microcontroller is connected to the input

and output contacts 18b to detect if the value of the mesh resistance falls outside a predetermined range. In a second embodiment (Figure 6), at least one shield component has a capacitive element closely associated therewith whose capacitance value is influenced by the presence of the shield. A microcontroller is connected to the capacitive element to detect changes in its capacitance value.

**Figure 3**

Description

[0001] This invention relates to a security shield for a data entry keypad, for example, a PIN entry pad (PIN pad) of an automated teller machine (ATM).

[0002] In the case of an ATM the security shield is commonly referred to as a PIN shield. In the present specification the invention will be described in its application to ATMs, but the invention is applicable generally to data entry keypads, such as other types of terminals where customers enter a PIN, as well as keypads mounted on walls for opening doors.

[0003] PIN shields are used at ATMs to prevent shoulder surfing or the use of a camera unit or other technique by a criminal in an attempt to capture a customer's PIN while the customer is performing a transaction at the PIN pad. The PIN shield comprises components fitted around and over the PIN pad to restrict a full view of the PIN pad to a person located directly in front of the PIN pad, so that a person off to one side, or looking over the person's shoulder, obtains only a partial view of the PIN pad, if any.

[0004] Once the PIN shield has been fitted, there is no way to know whether the PIN shield has been damaged, removed or replaced without visually inspecting the ATM.

[0005] It is an object of the invention to provide the ability to remotely detect whether a shield for a data entry keypad, in particular but not limited to, a PIN shield for an ATM PIN pad, has been damaged or removed.

[0006] According to a first aspect the present invention provides a security shield for a data entry keypad set into a fascia, the shield being secured to the fascia and comprising one or more components which restrict a full view of the keypad to a person located directly in front of the keypad, at least one component having embedded therein an electrical component extending between input and output contacts on the component, the shield further comprising a circuit coupled to the input and output contacts to detect changes in the electrical characteristics of the electrical component.

[0007] By embedding a conductive mesh in one or more component(s) of the PIN shield, a change or break in this conductive mesh can be detected by a microcontroller. The microcontroller can then generate an alert. In the present embodiment, in which the invention is implemented in an ATM, the alert can be sent either to a local or remote monitoring station via USB, or locally by disconnecting power from another component in the ATM (e.g. the card reader or the keypad or indeed the ATM core).

[0008] According to a second aspect the present invention provides a security shield for a data entry keypad set into a fascia, the shield being secured to the fascia and comprising one or more components which restrict a full view of the keypad to a person located directly in front of the keypad, at least one component having a capacitive element closely associated therewith whose capacitance value is influenced by the presence of the shield, the shield further comprising a circuit connected

to the capacitive element to detect changes in its capacitance value.

[0009] Embodiments of the invention will now be described, by way of example, with reference to the accompanying drawings, in which:

Figure 1 is a perspective view of a first embodiment of the invention showing an ATM with a PIN shield.

Figure 2 is a perspective view of the right hand side panel 14b of the first embodiment of the invention, the left hand side panel 14b being a mirror image of that shown.

Figure 3 is a perspective view of the base member 14a and flap 14c of a first embodiment of the invention.

Figure 4 is a partial underside view of the base member 14a.

Figure 5 illustrates how a connection is taken through the ATM fascia to a microcontroller in the body of the ATM.

Figure 6 is a perspective view of a second embodiment of the invention, the shield being shown prior to fixing to the fascia. In Figure 6 the same reference numerals have been used as in Figures 1 to 5 for the same or equivalent components.

[0010] In the Figures, only those parts of the ATM relevant to the invention are shown, i.e. the fascia and PIN shield. Figures 2 and 3 are shown with transparent shield components to reveal the circuitry within them.

[0011] Referring to Figures 1 to 5, a first embodiment of the invention comprises an ATM having a PIN pad 10 set into the ATM fascia 12. A PIN shield 14 is secured to the fascia 12 around the PIN pad 10 on three sides. The PIN shield 14 comprises:

- A three-sided generally U-shaped base member 14a that is secured to the ATM fascia 12 along the opposite sides and rear of the PIN pad 10.
- Two side panels 14b rising vertically or near vertically from the base member 14a on each side of the PIN pad.
- An upwardly and forwardly inclined "flap" or "lid" 14c extending upwardly and forwardly from the base member 14a at the rear of the PIN pad.

[0012] The PIN shield 14 may be formed: (a) of individual components 14a, 14b, 14c with the base member 14a secured on the fascia 12 and the flap 14c and side panels 14b secured on the base member, or (b) with one or more of the flap and side panels formed integrally with the base member, or (c) with the entire shield formed integrally as a single physical component. In the partic-

ular case of the embodiment of Figures 2 to 5 the side panels 14b are individual components secured to the U-shaped base member 14a by out-turned flanges 14d (Figure 2) which are fitted to the base member in register with the opposite side arms 14e thereof (Figure 3), while the flap 14c is formed integrally with the rear 14f of the base member 14a. The base member 14a is glued and/or screwed to the fascia 12 and the components 14b and 14c, when formed as separate components, are glued or screwed to the base member. The shield components 14a, 14b and 14c are typically moulded from a hard electrically insulating plastics material, whether the shield is formed as separate components or as a single physical piece. When fitted, the PIN shield 14 restricts a full view of the PIN pad 10 to a person located directly in front of the PIN pad, so that a person off to one side, or looking over the person's shoulder, obtains only a partial view of the PIN pad, if any.

[0013] A conductive wire mesh 16, which in the embodiment is made of 40AWG Nichrome wire, is embedded in each of the base member 14a, side panels 14b and flap 14c. Figure 2 shows the portion 16a of the mesh which is embedded in the right hand side panel 14b, the left hand side panel being a mirror image of the right hand panel, and Figure 3 shows the portion 16b of the mesh which is embedded in the base member 14a and integral flap 14c.

[0014] In each side panel 14b, Figure 3, the mesh 16a comprises a single wire extending in the body of the panel continuously between two flat, 2.5mm diameter, circular metal contacts 17 exposed substantially flush with the bottom surface of the flange 14d at the rear of the side panel. In the base member 14a and integral flap 14c, the mesh 16b comprises a single wire connected across respective pins 19 of a two pin connector, the wire being interrupted by respective pairs of flat, 2.5mm diameter, circular metal contacts 18a, 18b which are exposed substantially flush with the top surface of the base member side arms 14e. When the flanges 14d are fitted to the base member 14a in register with the side arms 14e, the pair of contacts 17 on the left hand side panel 14b engage the pair of contacts 18a and the pair of contacts 17 on the right hand side panel 14b engage the pair of contacts 18b. By this means the mesh portions 16a, 16b (right hand side) and 16b (left hand side) are connected in series between the contact pins 19 to form a continuous electrical conductor, comprising primarily the wire mesh 16 but locally by the contacts 17, 18a and 18b, extending from one contact pin 19 to the other contact pin 19 of the two pin connector. The contact pins 19 therefore constitute input and output terminals for the mesh 16 as a whole.

[0015] The two-pin connector is of the low profile clip type and is fitted into a recess 20 in the bottom surface of the base member 14a. The connector is positioned horizontally in the PIN shield so that when a cable 22, Figure 5, for connecting the wire mesh 16 to a microcontroller is attached, as will be described, the combination

of the connector and its socket do not protrude beyond the bottom of the PIN shield. For clip details see:

www.molex.com/molex/products/family?key=mini-latch&channel=products&chanName=family&pageTitle=Introduction&parentKey=wire_to_board_connectors

[0016] Physical impacts on the PIN shield components are generally more likely to be incident on the components in the direction perpendicular to their largest face. Specifically, impacts on the flap 14c of the PIN shield 14 are more likely to be from above and impacts on the side panels 14b are more likely to be from the side. The mesh wire 16 is therefore threaded throughout the shield components in a regularly spaced set of horizontal lines, approximately 2 to 5mm apart. Horizontal in this sense means parallel to the longest available axis of the component.

[0017] In one embodiment, a microcontroller (not shown), based on an ATMEL ATmega328P, is mounted within the body of the ATM below the fascia. Miscellaneous supporting circuitry for the microcontroller includes:

- Power shaping
- Power LED
- Reset switch
- Clock crystals
- USB interface

and are as per the Arduino UNO Revision 3 design; see http://arduino.cc/en/uploads/Main/Arduino_Uno_Rev3-schematic.pdf.

[0018] The connector pins 19 (Figure 4) are connected to the microcontroller by a cable 22 passing through a hole 24 drilled in the fascia 12. The wire mesh 16, comprising the series connected portions 16a, 16b and 16b, is configured as one resistor in a voltage divider, along with a second resistor (not shown) having a fixed resistance. The resistance of the second resistor is selected to be low relative to the resistance of the mesh 16. Therefore, in the voltage divider, the majority of the voltage will be dropped across the wire mesh. One of the microcontroller analog input pins is connected at the point between the two resistors (the wire mesh and the fixed value resistor respectively) and the voltage dropped across the wire mesh is monitored.

[0019] If the monitored voltage changes to a value which corresponds to the resistance of the mesh falling outside a predetermined range, due for example to a fracture of the mesh 16 indicating a possible attack on the PIN shield, an error condition is raised and an information LED is illuminated. Other alert actions, as described below are also invoked. The error status is maintained until the microcontroller is reset.

[0020] In an alternative implementation each wire mesh portion 16a, 16b, 16b is connected to a separate input-output pin pair on the microcontroller. For each

mesh portion a random bit pattern is generated and transmitted on the respective output pin of the microcontroller. The bit pattern is then read, byte by byte, on the corresponding input pin. The received bit pattern is compared to the transmitted bit pattern. If the patterns do not match, an error condition is raised and an information LED is illuminated. Other alert actions, as described below, are also invoked. The error status is maintained until the microcontroller is reset.

[0021] This implementation can be modified by attaching all mesh portions 16a, 16b, 16c to a single microcontroller output pin, with separate input pins per mesh portion. The same bit pattern will then be received on all input pins.

[0022] Alerts can be generated in two ways; either by directly reporting an alert status through the ATM PC core or by indirectly creating an error condition that will be detected by the ATM PC core.

[0023] Direct reporting can be achieved by connecting the microcontroller via USB to the ATM PC core. When an error condition is detected, a message is sent over the USB port. The microcontroller can be configured to repeat the transmission of the alert message at periodic time intervals or to repeat the transmission of the alert message a specific number of times. A USB driver is installed on the PC Core to receive the data transmitted by the microcontroller and convert this into an alert to be reported centrally (via Base24, SNMP or other mechanism).

[0024] Indirect reporting can be achieved by disconnecting the power from another component within the ATM, for example, by disconnecting the power from the card reader or the PIN pad. This will cause an error to be generated by the PC core.

[0025] As described, for two portions of the PIN shield that do not, once installed, move relative to each other, for example the shield portions 14a and 14b, the electrical continuation of the respective wire mesh portions from one shield portion to the other is made by terminating the wire mesh of one shield portion in two flat, 2.5mm diameter, circular metal contacts. Two similar contacts on the second shield portion are positioned so as to come into contact with the contacts on the first shield portion. When the two mesh portions are connected together the continuity of the wire mesh as between those two shield portions loop will be complete.

[0026] However, in certain embodiments two pieces of the PIN shield may move relative to each other, such as, for example, the "flap" may move relative to the base of the PIN shield. In such cases, an electrical connection between the two components is required.

[0027] This can be achieved through the use of a metal hinge between the articulating components. The wire mesh portions are connected to either side of the hinge, completing the electrical connection through the PIN shield.

[0028] Although in the above embodiment the coupling between the mesh and microcontroller is a direct resistive

connection, other embodiments are possible in which the coupling is inductive or capacitive, avoiding the need for the cable 22 to pass through the fascia and so for a hole to be formed in the fascia.

[0029] Referring to now Figure 6 in which capacitive coupling is used.

[0030] There are two general approaches for capacitive coupling: a first comprises affixing a first set of electrodes 30 for a plurality capacitors to the underside of the fascia 12 and then forming a second set of electrodes (not shown) within each of the base members 14a and the flap 14c juxtaposed a respective one of the first set of electrodes. Each first set of electrodes 30 comprises an aluminium plate, approximately 2cm square and 1mm thick and surrounded by a non-conductive layer (and similarly for the second set of electrodes). The second set of electrodes can be interconnected with a pair of resistive meshes as in the first embodiment, so providing a pair of RC networks between a set of 3 leads 32 connecting the electrodes 30 to a microcontroller.

[0031] The microcontroller can now measure either: the capacitance of each of the RC networks; or the time constant of the RC networks; or the resistance of the RC networks, once for calibration purposes and subsequently for monitoring purposes to determine if the shield has been removed or tampered with.

[0032] Alternatively, in a second approach, the electrodes 30 can be used as one electrode of an open circuited arrangement where the shield does not incorporate discrete components interconnecting the electrodes 30. (The shield may however be formed of electrically conducting material which affects the electrical characteristics of the exhibited at the electrodes 30.)

[0033] In this case, each of the electrodes 30 are connected back to the microcontroller via a number of resistors (not shown) to provide a pair of RC networks between three pins of the microcontroller, so allowing the microcontroller to measure and monitor the capacitance of the RC networks and to determine if the shield has been removed or tampered with as follows:

When the device is powered on, a calibration process takes place comprising the following steps:

1. The capacitance of each of the two RC networks between three pins of the microcontroller is measured a configured number of times (default 5) with a configured delay between each measurement (default 15 seconds).
2. These values are averaged and form the baseline capacitance value.
3. The capacitance is measured again a configured number of times (default 5) with a configured delay between each measurement (default 15 seconds).
4. The difference between the baseline capacitance value and the measured capacitance value is calculated for each measurement. The av-

erage difference is then calculated.

5. A configured tolerance percentage (default 25%) is then used to calculate the upper and lower bounds of the change in capacitance value before an error condition is detected. These values form the tolerance window.

[0034] Readings of the capacitance are then taken periodically, with a configured delay between each measurement (default 30 seconds). The difference between the reading and the baseline capacitance value is calculated and a rolling average of a configurable number of readings (default 5) is calculated.

[0035] When the baseline value has been calculated and sufficient values have been read to allow calculation of the rolling average value, a status LED is illuminated to indicate that the device is now ready and able to detect deviations from the baseline.

[0036] If the rolling average moves outside the tolerance window, then an error counter is incremented. If the average remains outside the tolerance window for a configured number of consecutive readings (default 10) then an error condition is raised and an information LED is illuminated. Other alert actions, as described in relation to the first embodiment, may also be invoked. The error status is maintained until the microcontroller is reset.

[0037] Alert generation, direct reporting and indirect reporting are as described for the first embodiment.

[0038] While the above implementations are described in terms of a sensing circuit comprising a discrete microcontroller, it will be appreciated that alternative embodiments could be implemented with a circuit comprising discrete components connected to a compatible ATM core which is arranged to detect changes in the electrical characteristics of the shield.

[0039] The invention is not limited to the embodiments described herein which may be modified or varied without departing from the scope of the invention.

Claims

1. A security shield for a data entry keypad set into a fascia, the shield being secured to the fascia and comprising one or more components which restrict a full view of the keypad to a person located directly in front of the keypad, at least one component having embedded therein an electrical component extending between input and output contacts on the component, the shield further comprising a circuit coupled to the input and output contacts to detect changes in the electrical characteristics of the electrical component.
2. A security shield according to claim 1 wherein said electrical component is coupled to said circuit via one of a resistive connection, a capacitive coupling or an inductive coupling.

3. A security shield according to claim 2 wherein said electrical component is coupled to said circuit via a resistive connection and the electrical characteristic is a resistance of the electrical component.
4. A security shield according to claim 2 wherein said electrical component is capacitively coupled to said circuit and the electrical characteristic is one of a resistance of the electrical component, a capacitance of the electrical component or a time constant of the electrical component.
5. A security shield according to claim 1 wherein said electrical component comprises a conductive mesh.
6. A security shield according to claim 1 wherein said electrical component comprises a first plurality of electrodes for respective capacitors and wherein said circuit comprises a corresponding plurality of electrodes arranged to be affixed to an underside of said fascia juxtaposed said first plurality of electrodes.
7. A security shield for a data entry keypad set into a fascia, the shield being secured to the fascia and comprising one or more components which restrict a full view of the keypad to a person located directly in front of the keypad, at least one component having a capacitive element closely associated therewith whose capacitance value is influenced by the presence of the shield, the shield further comprising a circuit connected to the capacitive element to detect changes in its capacitance value.
8. A security shield according to claim 1 or 7 wherein said circuit includes a microcontroller which is arranged to generate an alert in response to a change in the electrical characteristics of the electrical component exceeding a threshold value.
9. A security shield according to claim 8 wherein the microcontroller is arranged to transmit said alert to either a local or remote monitoring station via a USB connection.
10. A security shield according to claim 8 wherein said data entry keypad is for an ATM and the microcontroller is arranged to transmit said alert by disconnecting power from another component in the ATM.

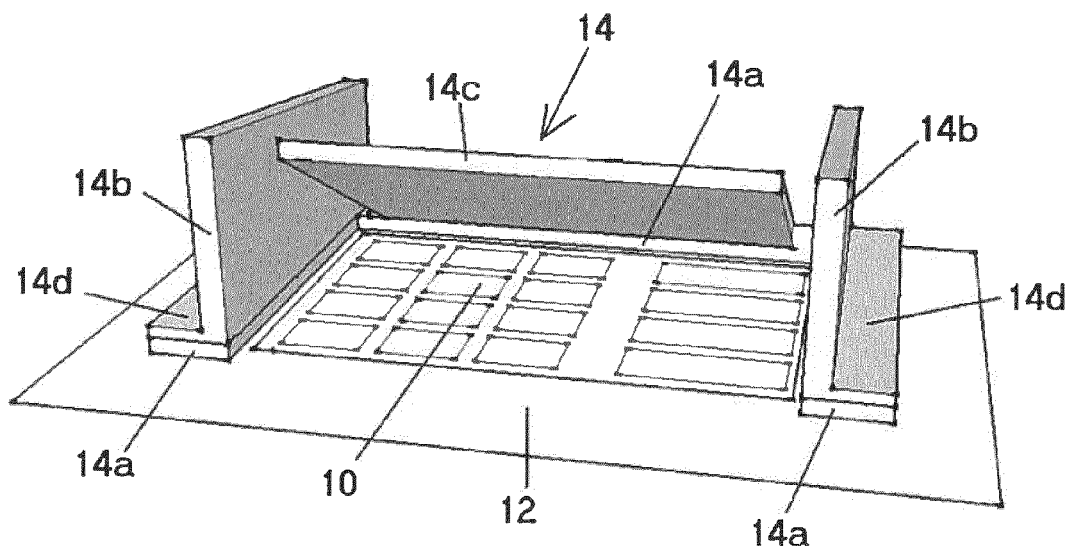


Figure 1

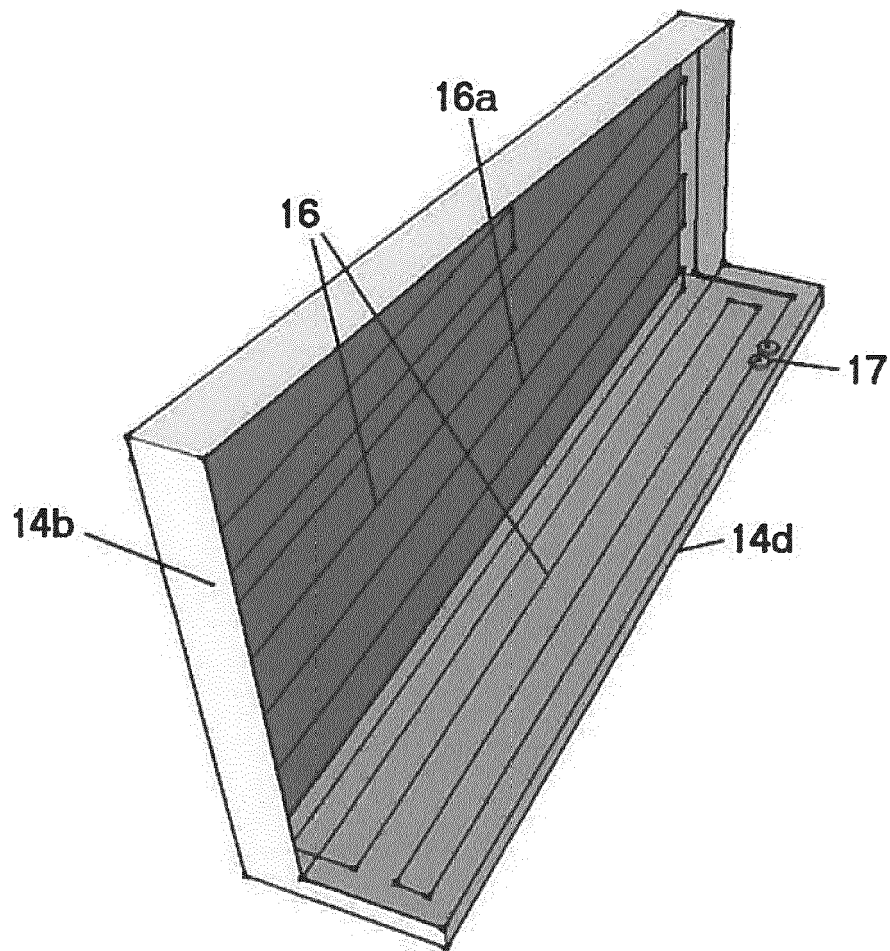


Figure 2

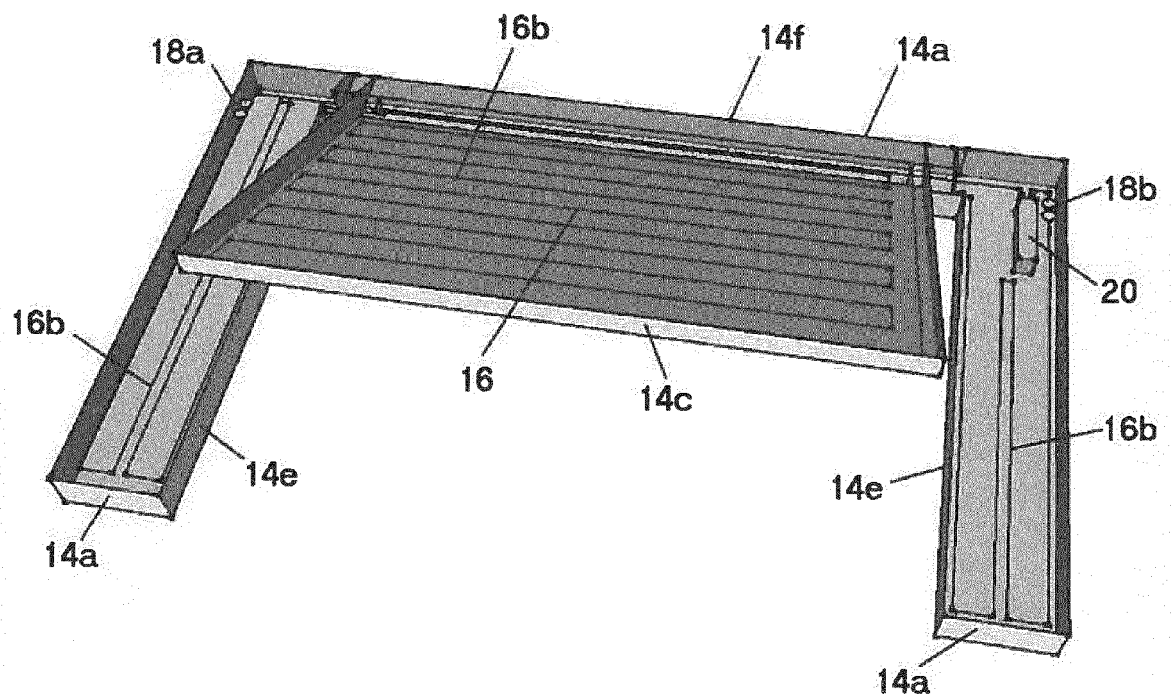


Figure 3

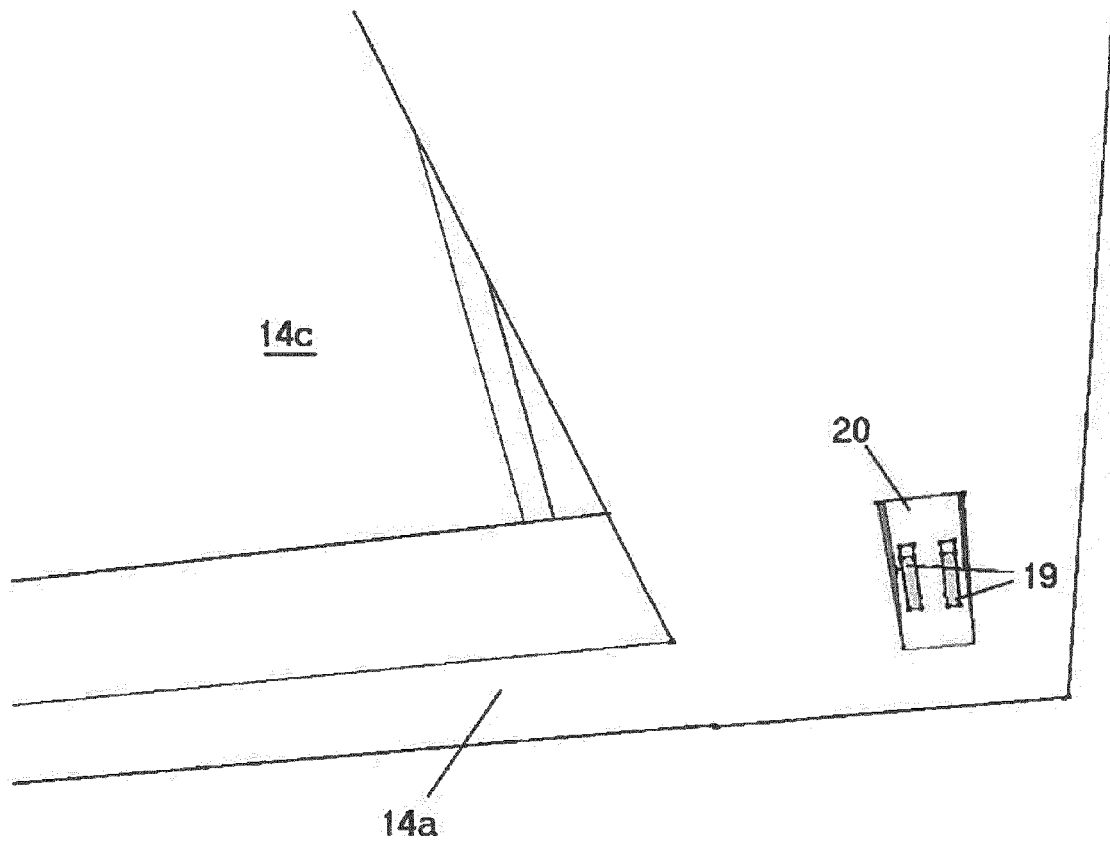


Figure 4

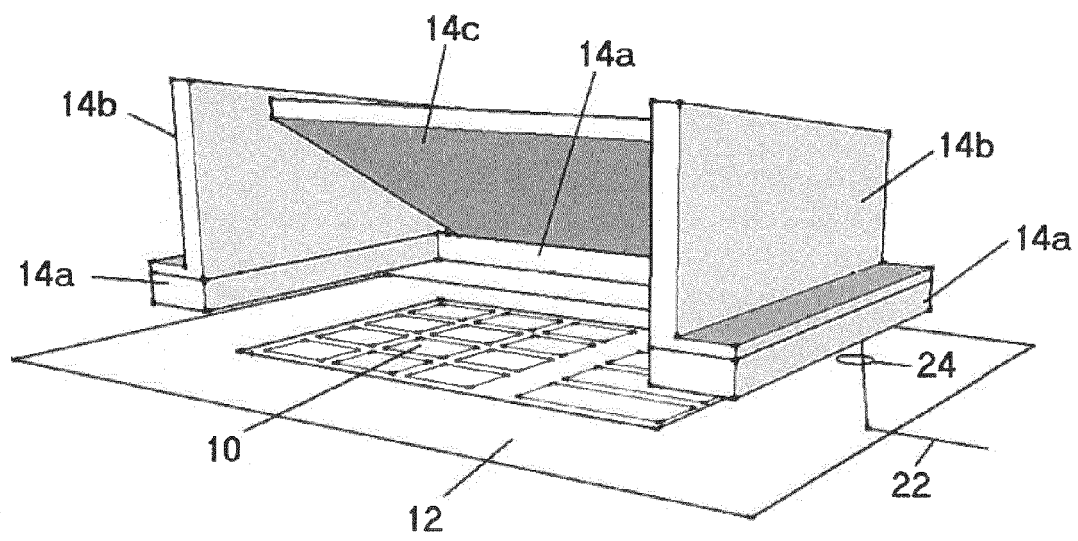


Figure 5

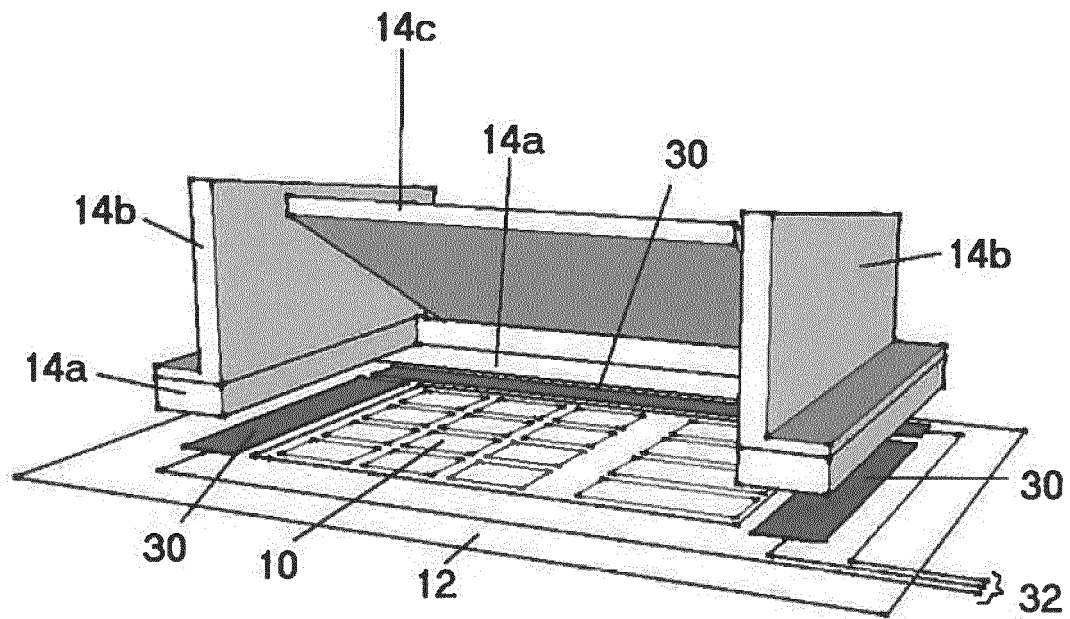


Figure 6



EUROPEAN SEARCH REPORT

 Application Number
 EP 15 18 0144

5

10

15

20

25

30

35

40

45

50

55

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	DE 10 2009 044794 A1 (WINCOR NIXDORF INT GMBH [DE]) 9 June 2011 (2011-06-09) * paragraph [0016] - paragraph [0021]; figures 1-3 *	1-10	INV. G07F19/00 G07F7/10 H03K3/0231
X	EP 2 793 202 A1 (WINCOR NIXDORF INT GMBH [DE]) 22 October 2014 (2014-10-22) * paragraph [0025] - paragraph [0037]; claims 1-5; figures 1-2 *	1-10	
X	DE 297 22 653 U1 (SIEMENS AG [DE]) 28 January 1999 (1999-01-28) * claims 1-7; figures 1-2 *	1-10	
X	EP 1 873 680 A1 (HOPT & SCHULER DDM [DE]) 2 January 2008 (2008-01-02) * paragraph [0009] - paragraph [0011]; figures 1-3a *	1-10	
X	DE 196 00 769 A1 (IBM [US]) 17 July 1997 (1997-07-17) * column 3 - column 5 *	1-10	TECHNICAL FIELDS SEARCHED (IPC)
A	US 2013/069784 A1 (KOIKE HIDETO [JP]) 21 March 2013 (2013-03-21) * abstract *	1-10	G07F H03K
A	US 7 337 955 B1 (BLOCK JAMES [US] ET AL) 4 March 2008 (2008-03-04) * figures 28-47 *	1-10	
A	EP 2 431 899 A1 (INGENICO SA [FR]) 21 March 2012 (2012-03-21) * abstract *	1-10	
A	EP 2 431 901 A1 (INGENICO SA [FR]) 21 March 2012 (2012-03-21) * abstract *	1-10	
		-/--	
The present search report has been drawn up for all claims			
Place of search Munich		Date of completion of the search 7 January 2016	Examiner 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)



EUROPEAN SEARCH REPORT

Application Number
EP 15 18 0144

5

10

15

20

25

30

35

40

45

50

55

1

EPO FORM 1503 03.02 (P04C01)

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
A	WO 2011/070355 A1 (TAVERNER ALISTAIR [GB]) 16 June 2011 (2011-06-16) * figure 4 *	1-10	
A	EP 0 622 719 A1 (SIEMENS NIXDORF INF SYST [DE]) 2 November 1994 (1994-11-02) * abstract *	1-10	
			TECHNICAL FIELDS SEARCHED (IPC)
The present search report has been drawn up for all claims			
Place of search Munich		Date of completion of the search 7 January 2016	Examiner 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	

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

EP 15 18 0144

5

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.

07-01-2016

10

15

20

25

30

35

40

45

50

55

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 102009044794 A1	09-06-2011	NONE	
EP 2793202 A1	22-10-2014	NONE	
DE 29722653 U1	28-01-1999	DE 29722653 U1 EP 0924592 A2	28-01-1999 23-06-1999
EP 1873680 A1	02-01-2008	CN 101093536 A EP 1873680 A1 US 2007295810 A1	26-12-2007 02-01-2008 27-12-2007
DE 19600769 A1	17-07-1997	NONE	
US 2013069784 A1	21-03-2013	CN 102999968 A JP 5360175 B2 JP 2013065072 A US 2013069784 A1	27-03-2013 04-12-2013 11-04-2013 21-03-2013
US 7337955 B1	04-03-2008	US 7337955 B1 US 7513420 B1 US 8870063 B1	04-03-2008 07-04-2009 28-10-2014
EP 2431899 A1	21-03-2012	CA 2751857 A1 EP 2431899 A1 FR 2964769 A1 US 2012065908 A1	15-03-2012 21-03-2012 16-03-2012 15-03-2012
EP 2431901 A1	21-03-2012	CA 2752279 A1 EP 2431901 A1 FR 2964768 A1 US 2012062252 A1	15-03-2012 21-03-2012 16-03-2012 15-03-2012
WO 2011070355 A1	16-06-2011	EP 2510507 A1 US 2012328350 A1 WO 2011070355 A1	17-10-2012 27-12-2012 16-06-2011
EP 0622719 A1	02-11-1994	AT 208918 T EP 0622719 A1	15-11-2001 02-11-1994

EPO FORM P0459

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