(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 453 291**

(51) Int. CI.:

G06F 21/51 (2013.01)
G06F 21/83 (2013.01)
G07F 7/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **24.01.2011 E 11151888 (2)**

(97) Fecha y número de publicación de la concesión europea: **15.01.2014 EP 2378453**

(54) Título: **Terminal de pago electrónico portátil adaptado para ejecutar programas no certificados**

(30) Prioridad:

25.01.2010 FR 1050465

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
07.04.2014

(73) Titular/es:

COMPAGNIE INDUSTRIELLE ET FINANCIÈRE D'INGÉNIERIE INGENICO (100.0%)
28/32 boulevard de Grenelle
75015 Paris, FR

(72) Inventor/es:

CARABELLI, ANDRÉ

(74) Agente/Representante:

CURELL AGUILÁ, Mireia

DESCRIPCIÓN

Terminal de pago electrónico portátil adaptado para ejecutar programas no certificados.

Campo de la invención

La presente invención se refiere a un terminal portátil de pago electrónico adaptado para ejecutar a la vez programas relacionados con operaciones de pago y programas relacionados con aplicaciones anexas, por ejemplo programas de navegación por internet.

Exposición de la técnica anterior

La figura 1A es una vista en perspectiva que representa de manera muy simplificada un terminal portátil de pago electrónico 1.

La figura 1B es una vista en sección del terminal 1 de la figura 1A, según el plano B-B representado por trazos de puntos en la figura 1A.

El terminal 1 comprende una caja 3, que contiene en particular una placa de circuitos electrónicos (no representada), a la cual están conectados diversos componentes periféricos, en este caso un teclado 5, una pantalla de visualización 7, y un lector 9 de tarjetas chip (figura 1B). El lector 9 está situado al fondo de una hendidura 10, abierta únicamente por el frente, en la cual un usuario puede introducir una tarjeta con chip de pago 11 (figura 1A). Están previstos en general otros componentes periféricos, no representados, tales como una impresora, un módulo de modulación/demodulación de datos adaptado para conectarse a una red de intercambio de datos, etcétera.

El terminal 1 comprende en particular un microprocesador 13 (figura 1B), destinado a ejecutar programas adaptados para gobernar los componentes periféricos del terminal, con el fin de llevar a cabo operaciones de pago. A título de ejemplo, está previsto un programa de introducción de código confidencial (PIN). Cuando una tarjeta con chip se introduce correctamente en la hendidura 10 y es autentificada por el terminal, este programa visualiza, en la pantalla 7, mensajes de invitación a la introducción del PIN. Cerca del fondo de la hendidura está previsto en general un detector, por ejemplo un interruptor mecánico 14, para validar la introducción completa de la tarjeta. El código introducido por el usuario transita por los circuitos electrónicos del terminal para ser verificado por el chip de la tarjeta de pago. El programa de introducción del PIN visualiza, llegado el caso, un mensaje de confirmación del éxito de la introducción.

Está prevista una zona 15 securizada, representada por trazos de puntos, cuyo acceso físico está protegido por dispositivos anti-intrusión. Los componentes sensibles del terminal, por ejemplo los bornes de contacto de las teclas del teclado 5, y los circuitos electrónicos por los cuales transita el código PIN introducido por el usuario, están colocados dentro de la zona 15. Estos componentes están protegidos contra cualquier tentativa de manipulación fraudulenta. Se pueden prever unos mecanismos para poner fuera de servicio el terminal 1 cuando se detecta una intrusión dentro de la zona 15.

Están previstos diversos mecanismos de seguridad para garantizar que solamente se puedan ejecutar programas certificados, o securizados, y para comunicarse con los diferentes componentes periféricos del terminal (teclado, pantalla, etcétera). Por programa certificado, o securizado, se entiende un programa auditado y reconocido como fiable, por ejemplo, por un organismo de seguridad de una entidad interbancaria tal como el PCI SSC (del inglés “Payment Card Industry Security Standards Council”). En la práctica, los programas certificados disponen de una firma digital. Todo programa que no dispone de una firma auténtica ve rechazado el acceso al microprocesador y a los componentes periféricos del terminal.

El documento US-2006/0138241-A1 da a conocer un mecanismo de detección de una tarjeta con chip en un lector de tarjetas chip basado en la detección de la banda magnética, en sensores de apertura y de cierre de la cubierta de la hendidura del lector de tarjetas chip, así como en sensores ópticos que permiten la detección de la tarjeta con chip.

El documento EP-1808834-A1 da a conocer un mecanismo de detección de tarjetas que garantiza que no se introduce ningún cuerpo extraño con una tarjeta con chip dentro del lector. Este mecanismo utiliza diferentes sensores dentro del lector y en el nivel de la hendidura que permiten la introducción de la tarjeta con chip.

Resultará deseable poder utilizar los terminales portátiles de pago electrónico para otras aplicaciones que no sean aplicaciones de pago, por ejemplo aplicaciones de navegación por internet, de presentación publicitaria y/o multimedia, de geo-localización de tipo GPS, de telefonía, etcétera. No obstante, esto implica la apertura del terminal y de ciertos componentes periféricos, tales como la pantalla y el teclado numérico, a programas no certificados por organismos de seguridad bancaria. Esto plantea problemas de seguridad evidentes. A título de ejemplo, un atacante podría prever fácilmente un programa fraudulento destinado a recoger informaciones confidenciales y a comunicarlas por internet. Un programa de este tipo podría imitar, por ejemplo, los mensajes auténticos de invitación

a la introducción del PIN, para engañar al usuario e incitarlo a introducir su código, el cual podría entonces ser recuperado y utilizado de manera fraudulenta.

Resumen

Así, un objetivo de un modo de realización de la presente invención consiste en proponer un terminal de pago que evite, por lo menos en parte, los inconvenientes de los terminales de pago actuales.

Un objetivo de un modo de realización de la presente invención consiste en proponer un terminal de pago, adaptado para ejecutar programas no certificados por organismos de seguridad bancaria.

Un objetivo de un modo de realización de la presente invención consiste en proponer un terminal del tipo mencionado que presenta una seguridad óptima para el usuario.

Así, un modo de realización de la presente invención prevé un terminal portátil de pago electrónico, que comprende: una hendidura destinada a recibir una tarjeta con chip; cerca de la entrada de la hendidura, un detector de ausencia de una tarjeta; y cerca del fondo de la hendidura, un detector (14) de acoplamiento completo de una tarjeta en la hendidura.

Según un modo de realización de la presente invención, el terminal está adaptado para conmutar de un primer modo de funcionamiento a un segundo modo de funcionamiento, cuando el detector señala la presencia de una tarjeta en la hendidura.

Según un modo de realización de la presente invención, el detector comprende: por el lado de una primera pared de la hendidura, un emisor de señales no deterministas; por el lado de una segunda pared de la hendidura, frente al emisor, un receptor de señales; y un elemento adaptado para determinar si las señales recibidas se corresponden con las señales emitidas.

Según un modo de realización de la presente invención, el receptor y el elemento están situados dentro de una zona securizada.

Según un modo de realización de la presente invención, el emisor comprende un diodo electroluminiscente conectado a un generador de señales no deterministas.

Según un modo de realización de la presente invención, el receptor comprende un fototransistor.

Según un modo de realización de la presente invención, el elemento comprende un comparador que comprende un primer y un segundo bornes de entrada conectados respectivamente a un borne de entrada del emisor y a un borne de salida del receptor.

Según un modo de realización de la presente invención, el elemento comprende un microprocesador que comprende un primer y un segundo bornes de entrada conectados, respectivamente, a un borne de entrada del emisor y a un borne de salida del receptor.

Breve descripción de los dibujos

Estos objetivos, características y ventajas, así como otros, se expondrán de forma detallada en la siguiente descripción de modos de realización particulares, efectuada a título no limitativo, en relación con las figuras adjuntas, entre las cuales:

la figura 1A, descrita anteriormente, es una vista en perspectiva muy esquemática de un terminal portátil de pago electrónico, habitual;

la figura 1B, descrita anteriormente, es una vista en sección del terminal de la figura 1A según el eje B-B;

la figura 2 es una vista en sección en el mismo plano que la figura 1B, de un modo de realización de un terminal de pago adaptado para estar abierto a programas no certificados; y

la figura 3 representa el esquema eléctrico de un modo de realización de un detector de presencia o de ausencia de una tarjeta con chip en la hendidura de un terminal de pago.

Descripción detallada

Por motivos de claridad, los elementos iguales se han designado con las mismas referencias en las diferentes figuras y, además, como es habitual en la representación de los sistemas electrónicos, las diversas figuras no se han trazado a escala.

Se propone un terminal portátil de pago electrónico adaptado para funcionar según un primer modo, denominado no securizado, cuando no hay ninguna tarjeta presente en la hendidura del lector de tarjetas chip, y de acuerdo con un segundo modo, denominado securizado, cuando está presente una tarjeta en la hendidura del lector de tarjetas chip.

En el modo de funcionamiento securizado, solamente se pueden ejecutar programas reconocidos como fiables, por ejemplo programas certificados por organismos de seguridad bancaria, y pueden acceder a los diversos componentes periféricos (teclado, pantalla, etcétera) del terminal. Unos mecanismos de seguridad, por ejemplo mecanismos de firma digital, garantizan que no se pueda ejecutar ningún programa no certificado cuando el terminal está en modo securizado.

En el modo de funcionamiento no securizado, se pueden ejecutar libremente programas no certificados y pueden tener acceso a ciertos componentes periféricos tales como el teclado y la pantalla. Aunque entonces sea posible para un atacante prever un programa fraudulento, destinado por ejemplo a engañar al usuario por medio de una imitación fraudulenta de los mensajes auténticos de invitación a la introducción del PIN, el riesgo de que el usuario se deje embaucar es extremadamente bajo. En efecto, si no hay ninguna tarjeta de pago introducida en la hendidura del lector de tarjetas chip, es muy improbable que el usuario acepte responder a dicha petición de introducción de PIN.

Tal como se explicará de forma más detallada posteriormente, se propone en la presente memoria un terminal adaptado para detectar la presencia o la ausencia de una tarjeta en la hendidura del lector de tarjetas chip, y para conmutar del modo no securizado hacia el modo securizado cuando se detecte una tarjeta en la hendidura, es decir cuando el detector niegue la ausencia de una tarjeta en la hendidura.

Por defecto, en ausencia de tarjeta dentro de la hendidura, el terminal funciona en modo no securizado y autoriza la ejecución de todo tipo de programa.

Cuando se introduce una tarjeta en la hendidura del lector de tarjetas chip, el terminal conmuta del modo no securizado hacia el modo securizado. Se bloquea entonces el acceso de los programas no certificados a los diversos componentes del terminal.

Cuando se retira del terminal la tarjeta del usuario, por ejemplo después de una operación de pago, un programa certificado, dedicado a esta tarea, pone en marcha la conmutación de retorno hacia el modo no securizado.

La figura 2 es una vista en sección en el mismo plano que la figura 1B, de un modo de realización de un terminal de pago 21 adaptado para detectar la presencia o la ausencia de una tarjeta en la hendidura del lector de tarjetas chip.

Al igual que el terminal 1 de la figura 1B, el terminal 21 comprende una caja 3, que contiene en particular una placa de circuitos electrónicos (no representada), a la cual están conectados diversos componentes periféricos, en este caso un teclado 5, una pantalla de visualización 7, y un lector 9 de tarjetas chip. Cerca del fondo de una hendidura 10, abierta únicamente por el frente, y en la cual un usuario puede introducir una tarjeta con chip, están situados unos contactos de entrada-salida del lector 9. Se pueden prever otros componentes periféricos, no representados, tales como una impresora, un módulo de modulación/demodulación de datos, etcétera. El terminal 21 comprende además un microprocesador 13 destinado a ejecutar programas, y un detector 14 de introducción completa de una tarjeta de pago en la hendidura 10. Los componentes sensibles del terminal 21, tales como el microprocesador 13, los bornes de contacto de las teclas del teclado 5, el lector 9, etcétera, están colocados dentro de una zona 15 cuyo acceso físico está protegido por unos dispositivos anti-intrusión.

Hacia la abertura de la hendidura 10 del terminal, está previsto un detector 23 de ausencia de tarjeta dentro de la hendidura 10. El resultado de la detección llevada a cabo por el detector 23 se suministra a un mecanismo adaptado para conmutar del modo no securizado hacia el modo securizado cuando se detecta una tarjeta (es decir, cuando se niega la ausencia de una tarjeta) dentro de la hendidura 10.

Según una ventaja del modo de realización propuesto, la posición del detector 23, hacia la abertura de la hendidura 10 del lector de tarjeta con chip, permite garantizar que la conmutación hacia el modo securizado se lleva a cabo desde el inicio de la introducción de una tarjeta de pago en la hendidura 10. Esto permite en particular evitar que un usuario que, de manera inconsciente, hubiera introducido mal su tarjeta en el lector, pudiera ser embaucado por un programa fraudulento, por ejemplo, un programa que emite un mensaje auténtico de invitación a la introducción del PIN con vistas a recuperar el PIN del usuario.

A título de ejemplo, el detector 23 está posicionado a una distancia comprendida entre 4 mm y 1 cm de la abertura de la hendidura 10, con el fin de garantizar la conmutación hacia el modo securizado desde el inicio de la introducción de una tarjeta de pago en la hendidura 10. El detector 23 se posicionará preferentemente de manera que la conmutación tenga lugar antes de que el chip de la tarjeta de pago haya entrado en su totalidad en el interior de la hendidura.

Según un modo de realización preferido, el detector 23 comprende un emisor de señales luminosas que comprende un diodo electroluminiscente 23a, situado por el lado de la pared inferior de la hendidura 10, y, frente al diodo 23a, un receptor de señales luminosas que comprende un fototransistor 23b, situado por el lado de la pared superior de la hendidura 10. El diodo 23a está conectado, por ejemplo por medio del microprocesador 13, a un generador de señales no deterministas, por ejemplo un generador de señales aleatorias o seudoaleatorias. La señal eléctrica de salida del fototransistor 23b se compara con la señal de entrada del diodo 23a. Si la señal de salida del fototransistor 23b difiere con respecto a la señal de entrada del diodo 23a, el detector 23 informa al terminal de que ya no se puede garantizar la ausencia de una tarjeta en la hendidura 10. En efecto, cuando se introduce una tarjeta en la entrada de la hendidura, esta última enmascara la señal luminosa emitida por el diodo 23a, la cual entonces ya no es reproducida por el fototransistor 23b.

Para prevenir cualquier riesgo de manipulación fraudulenta del detector 23, destinada a simular una ausencia de tarjeta aunque esté presente una tarjeta en la hendidura, el fototransistor 23b y la conexión entre el fototransistor 23b y el dispositivo de comparación (por medio del microprocesador 13), se sitúan dentro de la zona 15 securizada. Esto permite, por ejemplo, evitar que un atacante pueda formar un cortocircuito entre la entrada del diodo 23a y la salida del fototransistor 23b, con vistas a embaucar al detector 23. Para evitar que la señal emitida por el diodo 23a sea reproducida y retransmitida hacia el fototransistor 23b, por medio de un sistema de recepción/emisión fraudulento, se puede prever un análisis de los tiempos de propagación de las señales.

A título de variante, las posiciones respectivas del diodo 23a y del fototransistor 23b están invertidas. Habrá que ocuparse entonces de que la conexión entre el generador y el diodo 23a se sitúe dentro de la zona securizada 15.

La figura 3 representa el esquema eléctrico de un modo de realización del detector 23 de presencia o de ausencia de tarjeta del terminal de pago 21 de la figura 2.

El detector 23 comprende un diodo electroluminiscente 23a, dispuesto enfrente de un fototransistor 23b. Un generador de señales no deterministas 31 está conectado entre un borne de alimentación alto V_{DD} y un borne de alimentación bajo, en este caso masa. La salida del generador 31 está conectada al electrodo de ánodo del diodo 23a. El electrodo de cátodo del diodo 23b está conectado a masa. El detector 23 comprende además un comparador 33, conectado entre un borne de alimentación alto V_{DD} y un borne de alimentación bajo, en este caso masa. Un primer y un segundo bornes de conducción del fototransistor 23b están conectados respectivamente a un primer borne de entrada del comparador 31 y a masa. La salida del generador 31 está conectada además a un segundo borne de entrada del comparador 33.

En ausencia de un objeto opaco entre el diodo 23a y el fototransistor 23b, la señal de salida del fototransistor 23b coincide con la señal de entrada del diodo 23a. La salida OUT del comparador 33 está entonces en un primer estado.

En presencia de un objeto opaco entre el diodo 23a y el fototransistor 23b, la señal de salida del fototransistor 23b ya no coincide con la señal de entrada del diodo 23a. La salida OUT del comparador 33 está entonces en un segundo estado.

La salida OUT del comparador 33 indica por lo tanto la presencia o la ausencia de un objeto opaco entre el diodo 23a y el fototransistor 23b.

Se observará que el comparador 33 podrá no ser un componente material independiente, pudiendo la función de comparación ser realizada por el microprocesador 13 de la figura 2.

Una ventaja del modo de realización de las figuras 2 y 3 es que el detector 23 ofrece una gran seguridad. En efecto, debido al carácter no determinista de las señales emitidas por el diodo 23a, resulta difícil, incluso imposible, que un atacante simule de manera fraudulenta una ausencia de tarjeta aunque esté presente una tarjeta dentro de la hendidura.

El terminal propuesto está adaptado por lo tanto para ejecutar programas no certificados por organismos de seguridad bancaria, y garantizar sin embargo una seguridad óptima al usuario.

Se observará que el detector de cambio de modo 23 no sustituye al detector habitual 14 de acoplamiento completo de la tarjeta dentro de la hendidura 10, sino que será complementario al mismo.

Se observará además que el detector 23 propuesto más arriba únicamente señala una ausencia de tarjeta si todos sus componentes permanecen íntegros y funcionales, lo cual refuerza todavía más la seguridad del dispositivo.

Se han descrito unos modos de realización particulares de la presente invención. Se pondrán de manifiesto diversas variantes y modificaciones para el experto en la materia.

En particular, la invención no se limita a la utilización del detector de ausencia de tarjeta descrito en relación con la

figura 3. El experto en la materia sabrá llevar a la práctica el funcionamiento previsto sea cual sea el medio utilizado para detectar la ausencia de una tarjeta en la hendidura del lector. A título de ejemplo, se podrá prever un detector similar al detector óptico descrito más arriba, pero en el que el emisor y el receptor funcionen a longitudes de onda no visibles. Se podrá prever también un detector mecánico, aunque un detector de este tipo resultará más difícil de securizar.

REIVINDICACIONES

1. Terminal (21) de pago electrónico portátil, que comprende:

una hendidura (10) destinada a recibir una tarjeta con chip (11);

cerca de la entrada de la hendidura, un detector (23) de ausencia de una tarjeta; y

cerca del fondo de la hendidura, un detector (14) de acoplamiento completo de una tarjeta en la hendidura,

caracterizado porque:

este terminal está adaptado, cuando el detector (23) señala la presencia de una tarjeta en la hendidura, para conmutar de un modo de funcionamiento no securizado, en el que se pueden ejecutar unos programas no certificados, a un modo de funcionamiento securizado, en el que unos mecanismos de seguridad garantizan que no se pueda ejecutar ningún programa no certificado.

2. Terminal según la reivindicación 1, en el que el detector de ausencia (23) comprende:

por el lado de una primera pared de la hendidura (10), un emisor (23a) de señales no deterministas;

por el lado de una segunda pared de la hendidura, frente al emisor, un receptor (23b) de señales; y

un elemento (33) adaptado para determinar si las señales recibidas se corresponden con las señales emitidas.

3. Terminal según la reivindicación 2, en el que el receptor (23b) y dicho elemento (33) están situados dentro de una zona (15) securizada.

4. Terminal según la reivindicación 2 o 3, en el que el emisor comprende un diodo electroluminiscente (23a) conectado a un generador (31) de señales no deterministas.

5. Terminal según cualquiera de las reivindicaciones 2 a 4, en el que el receptor comprende un fototransistor (23b).

6. Terminal según cualquiera de las reivindicaciones 2 a 5, en el que dicho elemento comprende un comparador (33) que comprende un primer y un segundo bornes de entrada conectados respectivamente a un borne de entrada del emisor (23a) y a un borne de salida del receptor (23b).

7. Terminal según cualquiera de las reivindicaciones 2 a 5, en el que dicho elemento comprende un microprocesador (13) que comprende un primer y un segundo bornes de entrada conectados respectivamente a un borne de entrada del emisor (23a) y a un borne de salida del receptor (23b).

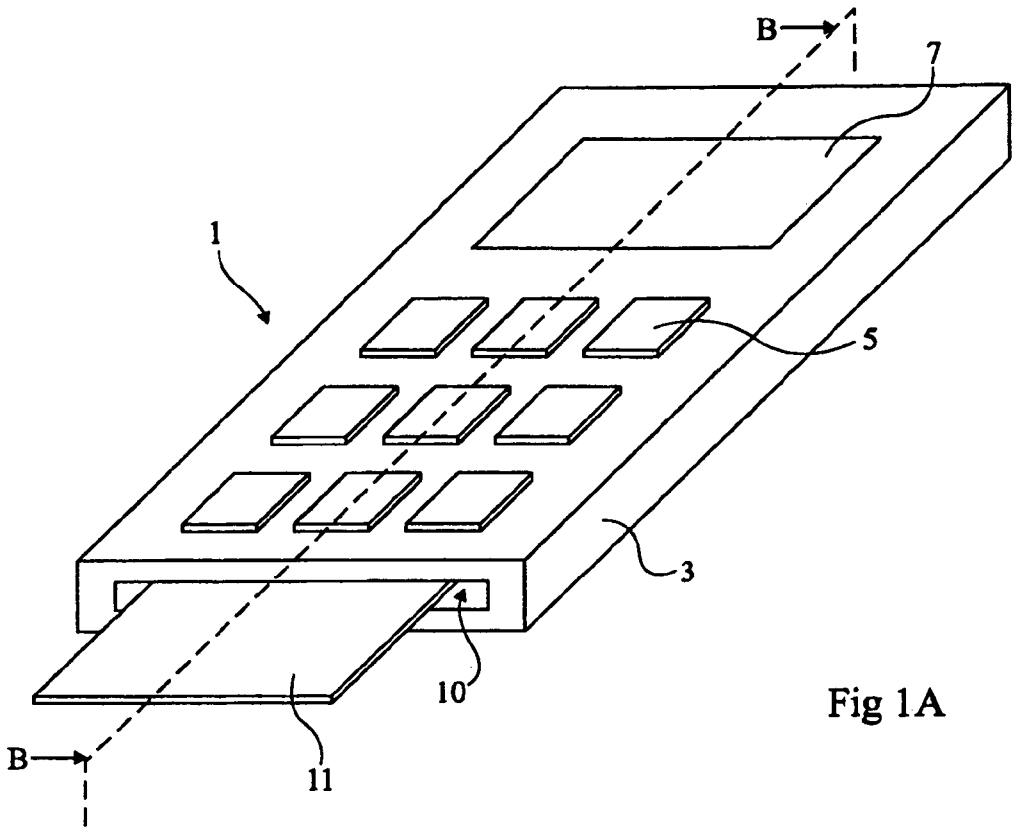

Fig 1A

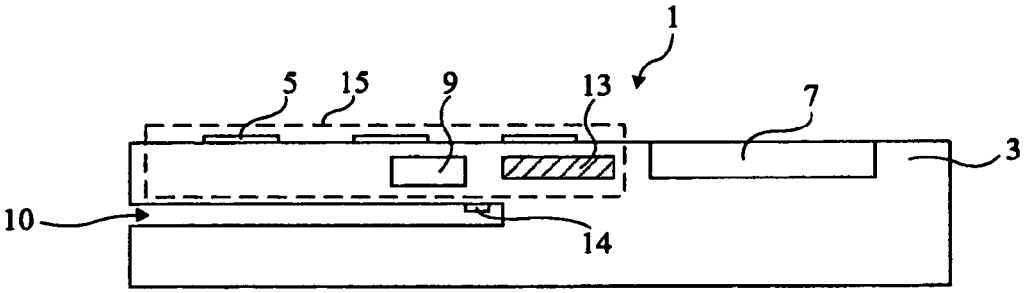

Fig 1B

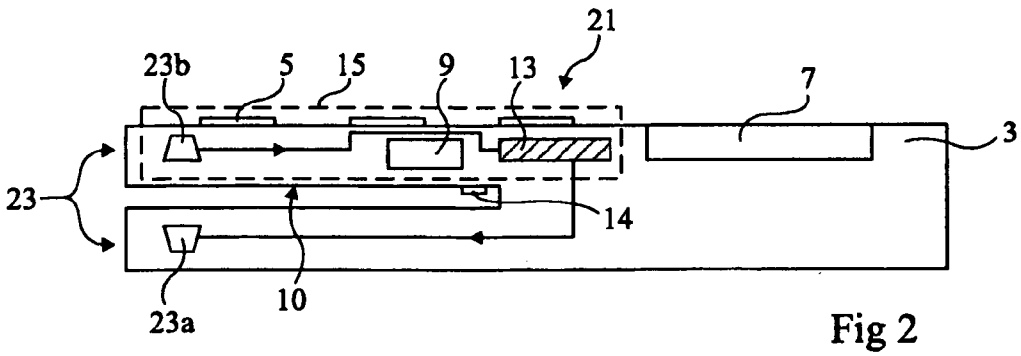

Fig 2

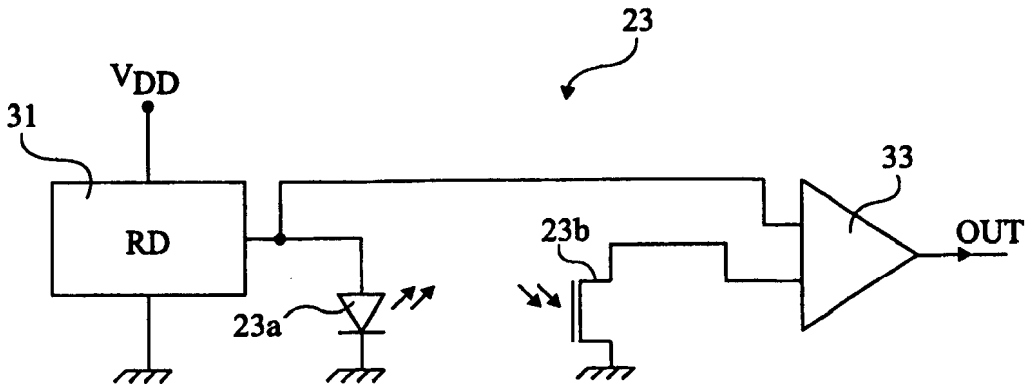

Fig 3