(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 587 987**

(51) Int. CI.:

***G06K 7/00*** (2006.01)
***G07F 19/00*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **14.09.2011 E 11181299 (6)**

(97) Fecha y número de publicación de la concesión europea: **25.05.2016 EP 2431911**

(54) Título: **Dispositivo de protección de un conector y de un hilo de comunicación de un lector de tarjeta de memoria**

(30) Prioridad:

**15.09.2010 FR 1057383**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**28.10.2016**

(73) Titular/es:

**INGENICO GROUP (100.0%)**
**28-32 Boulevard de Grenelle**
**75015 Paris, FR**

(72) Inventor/es:

**ROSSI, LAURENT y**
**SCHANG, BERNARD**

(74) Agente/Representante:

**CARPINTERO LÓPEZ, Mario**

## DESCRIPCIÓN

Dispositivo de protección de un conector y de un hilo de comunicación de un lector de tarjeta de memoria

### 1. Campo de la invención

La presente invención se refiere al campo de la protección de los lectores de tarjeta de memoria que comprenden un conector de tarjeta de memoria (TDM). Los lectores de tarjetas de memoria se emplean en particular en numerosos aparatos como terminales de pago, dispositivos de autentificación o de identificación o incluso dispositivos de lectura de contenidos.

La presente invención se refiere de manera más particular a la seguridad de un conector y de un enlace de comunicación de dichos lectores de tarjeta de memoria, con el fin de protegerlos contra cualquier intrusión de terceros malintencionados.

### 2. Técnica anterior

Los aparatos que integran los lectores de tarjeta de memoria, como los terminales de pago electrónicos (TPE) y los distribuidores automáticos de billetes (DAB) constituyen una pieza maestra del dispositivo de seguridad de los pagos electrónicos realizados por los usuarios.

En efecto, los terminales de pago electrónicos permiten vincular a la tarjeta de pago y a su portador, al proveedor y a la red. Además, graban la transacción.

Los distribuidores automáticos de billetes permiten la retirada de billetes de banco tras la identificación del portador. Están constantemente conectados al centro informático de los bancos emisores de tarjeta durante cada transacción. Las entidades de crédito son responsables de su funcionamiento.

Estos terminales de pago comprenden numerosos dispositivos de seguridad e implementan numerosos métodos que permiten garantizar que los aparatos se utilizan de conformidad con los usos para los cuales se han previsto y cumplen las normas de seguridad que imponen los organismos de certificación.

Por ejemplo, en el campo de los terminales de pago electrónicos (TPE) los fabricantes están obligados a cumplir, desde el 1 de enero de 2008, la norma PCI PED 2.0 (del inglés *Payement Card Industry Pin Entry Device*, estándar de Seguridad de Datos para la Industria de Tarjeta de Pago).

Esta norma de seguridad consiste en particular en asegurar el teclado de entrada de los terminales protegiendo la entrada del código confidencial, y en bloquear el terminal en caso de intrusión (fraudulenta o accidental).

Sin embargo, además de la seguridad del teclado, la experiencia muestra que poner a disposición terminales de pago en los puntos de venta permite a terceros malintencionados un acceso relativamente fácil a estos terminales de pago. Uno de los fraudes constatado últimamente corresponde al hecho de espiar los datos confidenciales en el enlace de comunicación de entrada/salida habitualmente designado por el acrónimo “IO_TDM”, procedente del inglés “Input/Output” (entrada/salida en español), correspondiendo el acrónimo TDM a la expresión “tarjeta de memoria”. Por otra parte, se llaman Entradas-Salidas a los intercambios de información entre el procesador del terminal de pago y los periféricos que este tiene asociados. Este enlace de comunicación de entrada/salida está directamente conectado al conector de tarjeta de memoria del terminal de pago.

En enero de 2010, Ross Anderson, profesor de Cambridge, especialista en seguridad informática, ha saltado a los titulares en relación con la seguridad de los datos. En efecto, ha descubierto cómo falsear el diálogo entre una tarjeta y un terminal de pago, de modo que se haga creer equivocadamente a este que el portador de tarjetas ha tecleado su código.

De este modo, un nuevo fraude corresponde a la introducción en el terminal de pago de un señuelo que hace creer al terminal de pago que el portador de tarjeta bancaria ha teclado en realidad su código confidencial. Dicho fraude corresponde en concreto a la inserción de un micro “bug” (error, en inglés) o anomalía de software en la ranura de inserción del conector de tarjeta de pago.

Dicho “bug” puede adoptar diversas formas, por ejemplo el “bug” puede ser un micromontaje electrónico que sirve para espiar los datos transaccionales entre la tarjeta de pago y el terminal de pago. El “bug” también puede corresponder a un simple enlace insertado en el conector de tarjeta de memoria, que une el enlace de comunicación de entradas/salidas del terminal de pago con un montaje externo destinado a espiar, o a cualquier otra acción maliciosa contra los datos bancarios de un usuario.

Con el fin de proteger el enlace de entradas/salidas y el conector de tarjeta de memoria, se han desarrollado algunas soluciones de protección. Una primera solución consiste en detectar una variación de la capacidad de las pistas conductoras del circuito impreso como se da a conocer en el documento FR 2 934 070. El inconveniente de esta técnica es que dicha detección se produce después del daño que modifica la capacidad de una de las pistas del circuito impreso. Otras soluciones son de tipo “electromecánico”, implementando por ejemplo una malla flexible (en

inglés, “wire mesh”) o incluso un enrejado de enlaces en el que se llevan a cabo, por ejemplo, unas pruebas de resistencia.

Estas soluciones caras pretenden de forma explícita impedir el acceso por un tercer malintencionado a los enlaces de entradas/salidas y al conector de tarjeta de memoria.

De forma general, se asocian en paralelo varias “wire mesh” o enrejados de enlaces para proteger el enlace de entradas/salidas “IO_TDM”. Se puede utilizar un enrejado de enlaces implantado en una de las capas internas del PCB (circuito electrónico impreso, del inglés *Printed Circuit Board*) para proteger el lado inferior del conector “TDM”, mientras que se dispondrá una “wire mesh” (malla flexible que tiene unas pistas adyacentes que cubren la superficie que hay que proteger) en el lado superior del conector, un tercer dispositivo (caché IO) se podrá desplegar justo frente a las patillas de conexiones que unen el conector con el PCB. Este último dispositivo es un minicircuito impreso en el que se implanta un enrejado de enlaces, estando todo conectado (soldado) en el circuito impreso principal de modo que se realice una “mini pared” entre las patillas de conexiones y la ranura de inserción del conector.

Estos diversos dispositivos se prueban en niveles de tensión o señales.

El inconveniente de estas soluciones reside en el hecho de que el enrejado por naturaleza tiene unos orificios que hacen posible una eventual intrusión dentro del conector de tarjeta de memoria o incluso una eventual degradación del enlace de entradas/salidas.

De este modo, en la actualidad, los inventores no han identificado ninguna solución simple y económica que permita una protección pero también una vigilancia eficaz del enlace de entradas/salidas y del conector de tarjeta de memoria contra cualquier intrusión de terceros malintencionados.

## 3. Resumen de la invención

La invención no presenta los inconvenientes de la técnica anterior. En efecto, la invención se refiere a un dispositivo según la reivindicación 1.

Según una característica particular de la invención, dicho dispositivo de protección utiliza un detector (*wire mesh*) existente y realiza una medición de capacidad en dicho detector.

Según una forma particular de realización, dicho dispositivo de protección comprende, además, unos medios de calibración que suministran dicha capacidad de referencia.

Según una forma particular de realización, dicho dispositivo de protección comprende, además, un sistema de compensación ambiental que modifica dicha capacidad de referencia en función de un criterio predeterminado.

Según una característica particular, dicho al menos un detector capacitivo se dispone sobre el llamado primer detector capacitivo en un conector de tarjeta de memoria.

Según una característica particular, dicho dispositivo de protección comprende, además, un segundo detector capacitivo conectado a un enlace entrada/salida del conector de tarjeta de memoria.

Según una forma particular de realización, dicho primer detector capacitivo es una pista de cobre de forma espiral cuadrada.

Según una forma particular de realización, dicho primer detector capacitivo se despliega en un plano completo.

Según otro aspecto, la invención se refiere también a un procedimiento según la reivindicación 7.

Según una característica particular, dicho procedimiento de protección comprende, además, una etapa de calibración que suministra dicha capacidad de referencia.

Según otro aspecto, la invención trata también de un terminal de pago. Según la invención, dicho terminal de pago comprende un dispositivo de protección según la reivindicación 1.

Según otro aspecto, la invención se refiere también a un programa de ordenador que comprende unas instrucciones de código de programa para la implementación del procedimiento según la reivindicación 7 cuando el programa lo ejecuta un procesador.

## 4. Lista de las figuras

Se mostrarán otras características y ventajas de la invención de manera más clara con la lectura de la siguiente descripción de una forma preferente de realización, dada a título de simple ejemplo ilustrativo y no limitativo, y de los dibujos adjuntos, en los que:

- la figura 1 ilustra un esquema de un dispositivo de protección según la invención;

- la figura 2 ilustra unas curvas de calibración del dispositivo de protección según la invención;
- las figuras 3A a 3D presentan la disposición y el funcionamiento de un detector capacitivo en un conector de tarjeta de memoria, así como dos variantes de detector capacitivo;
- las figuras 4A y 4B presentan respectivamente el esquema de una segunda forma de realización de la invención, y la estructura electrónica del segundo detector capacitivo asociado;
- la figura 5 ilustra el procedimiento de protección según la invención;
- la figura 6 esquematiza un terminal de pago según la invención.

**5. Descripción detallada de la invención**

5.1 Recordatorio del principio de la invención

La invención propone vigilar de forma eficaz y simple el enlace de entradas/salidas y del conector de tarjeta de memoria contra cualquier intrusión de terceros malintencionados, utilizando un dispositivo de protección que implementa una medición capacitiva de al menos un detector capacitivo dispuesto en el conector de tarjeta de memoria de un terminal de pago.

Como el dispositivo de protección implementa una medición capacitiva, la intrusión de un elemento conductor se detecta debido a que la intrusión modifica las líneas de campos magnéticos, y por consiguiente la capacidad de referencia del detector capacitivo más allá de un umbral predeterminado.

Según la invención, el dispositivo de protección de un terminal de pago comprende al menos un detector capacitivo introducido dentro de un volumen formado por una primera placa de masa que se apoya sobre la superficie del circuito impreso del terminal de pago y una segunda placa de masa dispuesta en el fondo de la caja plástica del terminal de pago, un microprocesador de medición capacitiva y unos medios de transmisión de una información que indica una variación de la capacidad del detector capacitivo más allá de un umbral predeterminado, que indica dicho de otro modo una intrusión dentro del volumen vigilado.

Según una primera forma de realización de la invención, un primer detector capacitivo se despliega en un conector de tarjeta de memoria del terminal de pago.

Según otra forma de realización, un segundo detector capacitivo se añade en el dispositivo de protección y se une con una conexión de entrada/salida del conector de tarjeta de memoria.

Según la invención, el dispositivo de protección es apto para proteger mediante medición capacitiva un terminal de pago. Dicho dispositivo de protección puede presentarse con cualquier forma. La forma del dispositivo se puede adaptar en función de la caja, o también del conector de tarjeta de memoria que hay que proteger.

A continuación, se detalla una forma de realización de un dispositivo de protección según la invención. Sin embargo, es evidente que la invención no se limita a esta aplicación particular, sino que también se puede implementar en otros numerosos contextos de protección de circuitos impresos electrónicos y de manera más general en todos los casos en los que las características que se enumeran a continuación son interesantes.

*Estructura general de un dispositivo según la invención*

Se presenta en relación con la figura 1, la estructura general de un dispositivo 10 de protección según la invención. Dicho dispositivo comprende, en primer lugar, un detector 12 capacitivo que pertenece a un volumen definido por una primera placa 111 de masa de un circuito 11 impreso electrónico y por una segunda placa 112 de masa dispuesta en el fondo de la caja del terminal de pago.

Estas placas de masa producen una acción comparable a la de una jaula de Faraday, es decir que permiten proteger el dispositivo de protección de eventuales perturbaciones electromagnéticas exteriores.

La placa de masa dispuesta en el fondo de la caja del terminal de pago se obtiene, por ejemplo, por medio de un procedimiento conocido de aplicación de pintura conductora.

Por otra parte, unos medios 15 de calibración, unidos eléctricamente al detector capacitivo, permiten evaluar su capacidad de referencia. A continuación se detallarán más estos medios 15 de calibración.

Además, el dispositivo de protección según la invención comprende también un microprocesador 13 de medición capacitiva unido eléctricamente al detector 12 capacitivo y a la masa 16. Dicho microprocesador de medición utiliza por ejemplo un sensor capacitivo que corresponde a una sonda para medir la capacidad del detector capacitivo.

Dicha sonda se realiza por lo general con un electrodo plano de medición rodeado de un anillo protector. El electrodo forma por tanto con el detector capacitivo un condensador plano. Un electrodo protector contenido dentro del anillo protector se coloca alrededor del de medición y su potencial se lleva al mismo valor con el fin de mejorar la linealidad volviendo las líneas de campo normales (perpendiculares) al electrodo de medición. De este modo, el electrodo protector permite eliminar los efectos de borde.

Por medio de estos medios 13 de medición, se detecta una variación de la capacidad del detector capacitivo. Esta variación se obtiene, por ejemplo, comparando la capacidad medida con la capacidad de referencia previamente determinada por los medios 15 de calibración. Esta medición se lleva a cabo de manera preferente en tiempo real con el fin de avisar de forma instantánea al procesador seguro de un terminal de pago a través de los medios 14 de transmisión.

Con independencia de la frecuencia de medición seleccionada por el usuario, el conjunto de las mediciones se controla mediante un programa de ordenador grabado en los propios medios de medición.

De manera más precisa, los medios de medición determinan una diferencia entre la capacidad del detector capacitivo medida por los medios 13 de medición, y la capacidad de referencia determinada por los medios de calibración. Si el valor absoluto de esta diferencia excede un umbral U predeterminado, los medios de transmisión del dispositivo de protección según la invención indican al procesador seguro del terminal seguro que se ponga en modo “ataque”.

De este modo, el dispositivo de protección según la invención permite determinar cualquier contacto con el detector capacitivo dispuesto dentro de un volumen definido por la primera placa 111 de masa del circuito 11 impreso electrónico y por la segunda placa 112 de masa dispuesta en el fondo de la caja del terminal de pago que hay que proteger. En particular, se detectará cualquier intrusión (incluso sin contacto directo con el sensor) por un tercero malintencionado, debido a que esta intrusión, en particular mediante la introducción de un elemento conductor modifica de forma significativa la capacidad del detector capacitivo.

Además, este dispositivo de protección saca provecho del detector capacitivo y de la medición capacitiva evitando implementar un enrutamiento geométrico complejo o también evitando utilizar un material de protección fácilmente degradable y caro como las mallas flexibles.

*Medios de calibración del detector capacitivo en cuestión*

La calibración implementada por los medios 15 de calibración, es necesaria debido a que el valor de la capacidad es sensible a las variaciones exteriores.

En efecto, se sabe que el valor de capacidad varía en función de diferentes factores. Por ejemplo, la capacidad de un detector capacitivo varía en función de la histéresis de carga causada por la magnetización de un material, el efecto de una batería del terminal de pago, o incluso la temperatura, la humedad, el envejecimiento en particular por la oxidación de los materiales que constituyen el detector capacitivo, etc.

Se presenta en relación con la figura 2, que representa un ejemplo de curvas de calibración del dispositivo de protección según la invención, el método implementado por los medios de calibración que suministran la capacidad de referencia del detector capacitivo.

Los medios de calibración miden 21 (por ejemplo de una manera similar a la utilizada por los medios de medición descritos con anterioridad) la capacidad del detector capacitivo en función del tiempo. La curva 21 de medición representada en la figura 2 atestigua que la capacidad varía en función del tiempo, en particular en función de la temperatura ambiente.

Los medios de calibración promedian los datos de medición de capacidad de la curva de medición de modo que se obtiene un valor de referencia *Ref*.

Además, los medios de calibración determinan, por ejemplo, un umbral *U* de variación de capacidad más allá del cual la variación de capacidad es anormal. De este modo, los medios de calibración determinan el intervalo de valor de capacidades centrado en el valor de referencia que permite atestiguar un funcionamiento “*normal*” y seguro del circuito impreso del terminal de pago.

De manera preferente, el valor de referencia y el umbral *U* predeterminado se graban en una memoria y se transmiten a los medios de medición con el fin de que estos últimos determinen una intrusión de un tercero malintencionado que pretende deteriorar el circuito impreso electrónico.

De manera opcional, los medios de calibración comprenden, además, un sistema de compensación ambiental que pretende adaptar los valores de referencia y de umbral *U* predeterminado en función de un parámetro seleccionado por el usuario del terminal de pago.

Por ejemplo, al ser la temperatura ambiente en Singapur muy diferente de la temperatura en Estocolmo, el usuario adapta en función de su localización la referencia y el intervalo de variación de capacidad permitido.

Del mismo modo, según otro ejemplo, el usuario puede adaptar este intervalo de variación a medida que envejece el terminal de pago, según las recomendaciones del fabricante mencionadas en las instrucciones de uso.

5.2 Descripción de una primera forma de realización de un dispositivo según la invención

*Estructura del dispositivo de protección según esta primera forma de realización*

En esta forma de realización representada en las figuras 3A a 3D, se presenta un dispositivo de protección según la invención en el que se ha montado un primer detector capacitivo en el conector de tarjeta de memoria representado en la figura 3A.

El primer detector capacitivo colocado en el conector de tarjeta de memoria mide dentro un volumen, definido por una primera placa 111 de masa de un circuito 11 impreso electrónico y por una segunda placa 112 de masa dispuesta en el fondo de la caja del terminal de pago, la capacidad de este volumen.

De este modo, cualquier introducción de un objeto incluso muy pequeño, constituido por una o varias partes conductoras, entre el detector capacitivo y una de las placas de masa (que definen el volumen que contiene el detector capacitivo), modifica las líneas 32 de campos representadas en la figura 3B.

Esta modificación de líneas de campos provoca una variación de la capacidad del volumen más allá del umbral predeterminado definido con anterioridad por los medios de calibración.

*Tipo de detector capacitivo*

Se utiliza, por ejemplo, un detector capacitivo que adopta la forma de una simple pista de cobre y que se representa en la figura 3C. Esta pista adopta, por ejemplo, la forma de una espiral 33 cuadrada.

Según otra variante, el detector 12 corresponde a un plano 34 completo y está dispuesto sobre una superficie del conector de tarjeta de memoria del terminal de pago por ejemplo.

Un detector capacitivo que corresponde a un plano completo, adopta la forma de una superficie capacitiva. De manera más precisa, una tecnología capacitiva de superficie consiste en un revestimiento conductor uniforme sobre un aislante. Durante la utilización, unos electrodos colocados en el borde del aislante distribuyen una corriente de baja tensión de manera igual en toda la capa conductora, creando de este modo un campo eléctrico uniforme. Cuando un objeto entra en contacto con la superficie, esto tiene como efecto atraer la corriente de cada rincón del campo eléctrico.

De manera opcional, un controlador calcula las coordenadas del contacto midiendo la corriente. A continuación transmite estas coordenadas al procesador seguro del terminal de pago.

Según otra forma de realización, el detector capacitivo puede adoptar la forma de un enrejado (no representado) de hilos conductores muy finos (menos de 10 µm) sumergido entre dos capas de aislante por ejemplo vidrio o unas películas laminadas de plástico.

Dicho enrejado puede ser plano o tridimensional con un enmallado más o menos denso. Un simple hilo, que se dispone de una forma particular, también puede ser suficiente en algunos casos.

Por otra parte, el dispositivo de protección según la invención también se puede conectar eléctricamente a un circuito impreso que tiene un detector capacitivo existente constituido por una parte conductora y por una parte aislante. En este caso, el dispositivo de protección según la invención coloca unos electrodos en el borde del aislante con el fin de distribuir una corriente de baja tensión de manera igual en toda la parte conductora, creando de este modo un campo eléctrico uniforme. El detector existente se vuelve, de este modo, capacitivo.

5.3 Descripción de una segunda forma de realización de un dispositivo según la invención

En relación con la figura 4A, se representa el esquema de una segunda forma de realización de la invención. Esta segunda forma de realización añade, además del primer detector 41 capacitivo dispuesto en el conector de tarjeta de memoria, un segundo detector capacitivo con el fin de impedir el acceso a los enlaces del conector de tarjeta de memoria, en particular el enlace “IO_TDM” (del inglés por “Input/Output”, entrada/salida).

Como se ilustra en la figura 4A, el conector 42 de tarjeta de memoria está montado en el circuito 43 impreso. El conector de tarjeta de memoria presenta una ranura 42.1 en el que se puede introducir la tarjeta. El conector de tarjeta de memoria comprende también un conjunto de enlaces 42.2 que permiten la conexión de la tarjeta, una vez esta insertada, con un procesador del aparato.

Estos enlaces 42.2 presentan un ligero abombamiento 42.3 a la altura de la zona de conexión con la tarjeta, en el interior del conector de tarjeta de memoria. A continuación se conforman los enlaces para que estos se extiendan hacia el circuito 43 impreso. Estos se juntan con este a la altura de una zona intermedia en la que los enlaces 42.4 se unen con el circuito 43 impreso.

El segundo detector 44 capacitivo está dispuesto de modo que impide el acceso a al menos algunos enlaces y, en particular, al enlace “IO_TDM”.

En relación con la figura 4B, se representa una estructura electrónica del segundo detector capacitivo. Según esta estructura, un condensador *CE* de enlace implementa un acoplamiento capacitivo que permite evaluar la capacidad del enlace IO_TDM. Por otra parte, este detector se alimenta con una tensión *Vtdm* nominal y comprende, además, una resistencia R y una capacidad *CP* parásita.

*Vtdm* y R dependen del terminal y de manera más particular de las normas EMV (acrónimo de “Europay MasterCard VISA", estándar de interoperabilidad de tarjetas) y están presentes en todos los terminales de pago. La capacidad CE de enlace está directamente ligada a la invención, es de un valor de 220 pF (a título indicativo), este valor puede variar en función de las dimensiones de las pistas.

5.4 Descripción de una forma de realización del procedimiento de protección según la invención

En relación con la figura 5, se presenta el procedimiento 50 de protección de un circuito impreso electrónico según la invención.

Dicho procedimiento comprende:

- una etapa de disposición 51 de al menos un detector capacitivo sobre una capa del circuito impreso del terminal de pago;
- una etapa de calibración 52 que suministra la capacidad de referencia del detector capacitivo;
- una etapa de medición 53 capacitiva implementada por un microprocesador de medición capacitiva unido eléctricamente con el detector capacitivo, estando el microprocesador configurado para detectar una variación de capacidad del detector capacitivo;
- una etapa de transmisión 54 de una información “¡Ataque!”, representativa de la variación de capacidad, cuando un valor absoluto de una diferencia entre la capacidad medida y la capacidad de referencia sobrepasa un umbral predeterminado.

Además, la etapa de calibración se podrá reiterar según un método operativo conocido por el usuario.

Según una forma particular de realización, la etapa de calibración comprende, además, una etapa de compensación ambiental, que pretende tener en cuenta la influencia natural de algunos parámetros como: la histéresis de carga a causa de la magnetización de un material, el efecto de una batería del terminal de pago, o también la temperatura, la humedad, el envejecimiento en particular por la oxidación de los materiales que constituyen el detector capacitivo, etc.

El procedimiento de protección implementado por un dispositivo de protección conforme con la segunda forma de realización descrita con anterioridad, implementa dos detectores capacitivos, disponiéndose uno en el conector de tarjeta de memoria y el otro unido con el enlace de entrada/salida del conector de tarjeta de memoria. Las etapas del procedimiento anteriormente descrito se llevan a cabo, por consiguiente, para cada detector capacitivo implementado.

Se presenta, en relación con la figura 6, una forma de realización de un terminal de pago según la invención.

Dicho terminal comprende una memoria 61 constituida por una memoria tampón, una unidad 62 de tratamiento, equipada por ejemplo con un microprocesador, y gestionada por el programa 63 de ordenador, que implementa el procedimiento de protección según la invención.

En la inicialización, las instrucciones de código del programa 63 de ordenador se cargan, por ejemplo, en una memoria RAM antes de que las ejecute el procesador de la unidad 62 de tratamiento. La unidad 62 de tratamiento recibe en la entrada al menos una información I, como unos identificadores de zonas de localización. El microprocesador de la unidad 62 de tratamiento implementa las etapas del procedimiento de protección descrito con anterioridad, según las instrucciones del programa 63 de ordenador, para suministrar una información T tratada, como la detección de un ataque que provoca la supresión de los datos protegidos. Para ello, el terminal comprende, además de la memoria 61 tampón, al menos un detector capacitivo dispuesto dentro de un volumen formado por una primera placa de masa de dicho circuito impreso y por una segunda placa de masa dispuesta sobre una superficie interna de dicha caja, estando dicho al menos un detector capacitivo configurado para suministrar una capacidad de referencia, un microprocesador de medición capacitiva unido eléctricamente con dicho al menos un detector capacitivo, estando dicho al menos un microprocesador configurado para detectar una variación de capacidad de dicho al menos un detector capacitivo, unos medios de transmisión de una información representativa de dicha variación de capacidad, cuando un valor absoluto de una diferencia entre dicha capacidad medida y dicha capacidad de referencia sobrepasa un umbral predeterminado.

Estos medios están gestionados por el microprocesador de la unidad 62 de tratamiento.

**REIVINDICACIONES**

1. Dispositivo (10) de protección de un terminal de pago electrónico, que comprende un circuito impreso electrónico y una caja, comprendiendo dicho dispositivo de protección:

- al menos un detector (12, 41) capacitivo que está configurado para suministrar una capacidad de referencia;
- un microprocesador (13) de medición capacitiva unido eléctricamente a dicho al menos un detector capacitivo, estando dicho al menos un microprocesador configurado para detectar una variación de capacidad de dicho al menos un detector capacitivo;
- unos medios (14) de transmisión de una información representativa de dicha variación de capacidad, cuando un valor absoluto de una diferencia entre dicha capacidad medida y dicha capacidad de referencia sobrepasa un umbral predeterminado,

**caracterizado porque** dicho detector capacitivo se dispone dentro de un volumen formado por una primera placa (111) de masa de dicho circuito impreso y por una segunda placa (112) de masa dispuesta sobre una superficie interna de dicha caja.

2. Dispositivo de protección según la reivindicación 1, **caracterizado porque** comprende, además, unos medios (15) de calibración que suministran dicha capacidad de referencia.

3. Dispositivo de protección según la reivindicación 1, **caracterizado porque** dicho al menos un detector (12) capacitivo, llamado primer detector (12, 41) capacitivo, se dispone en un conector (42) de tarjeta de memoria.

4. Dispositivo de protección según la reivindicación 1, **caracterizado porque** comprende, además, un segundo detector (44) capacitivo conectado a un enlace entrada/salida del conector (42) de tarjeta de memoria.

5. Dispositivo de protección según la reivindicación 1, **caracterizado porque** dicho primer detector (41) capacitivo es una pista de cobre de forma espiral (33) cuadrada.

6. Dispositivo de protección según la reivindicación 1, **caracterizado porque** dicho primer detector (12, 41) capacitivo se despliega según un plano (34) completo.

7. Procedimiento (50) de protección de un terminal de pago electrónico, que comprende un circuito impreso electrónico y una caja, comprendiendo dicho procedimiento de protección:

- una etapa de medición (53) capacitiva implementada por un microprocesador de medición capacitiva unido eléctricamente con al menos un detector capacitivo, estando dicho al menos un microprocesador configurado para detectar una variación de capacidad de dicho al menos un detector capacitivo;
- una etapa de transmisión (54) de una información representativa de dicha variación de capacidad, cuando un valor absoluto de una diferencia entre dicha capacidad medida y dicha capacidad de referencia sobrepasa un umbral predeterminado,

**caracterizado porque** dicho procedimiento de protección comprende una etapa previa de disposición (51) de dicho detector capacitivo dentro de un volumen formado por una primera placa de masa de dicho circuito impreso y por una segunda placa de masa dispuesta sobre una superficie interna de dicha caja, estando dicho al menos un detector capacitivo configurado para suministrar una capacidad de referencia.

8. Procedimiento de protección según la reivindicación 7, **caracterizado porque** comprende, además, una etapa de calibración (52) que suministra dicha capacidad de referencia.

9. Terminal de pago **caracterizado porque** comprende un dispositivo de protección según la reivindicación 1.

10. Programa de ordenador **caracterizado porque** comprende unas instrucciones de código de programa para la implementación del procedimiento de protección según la reivindicación 7, cuando el programa lo ejecuta un procesador.

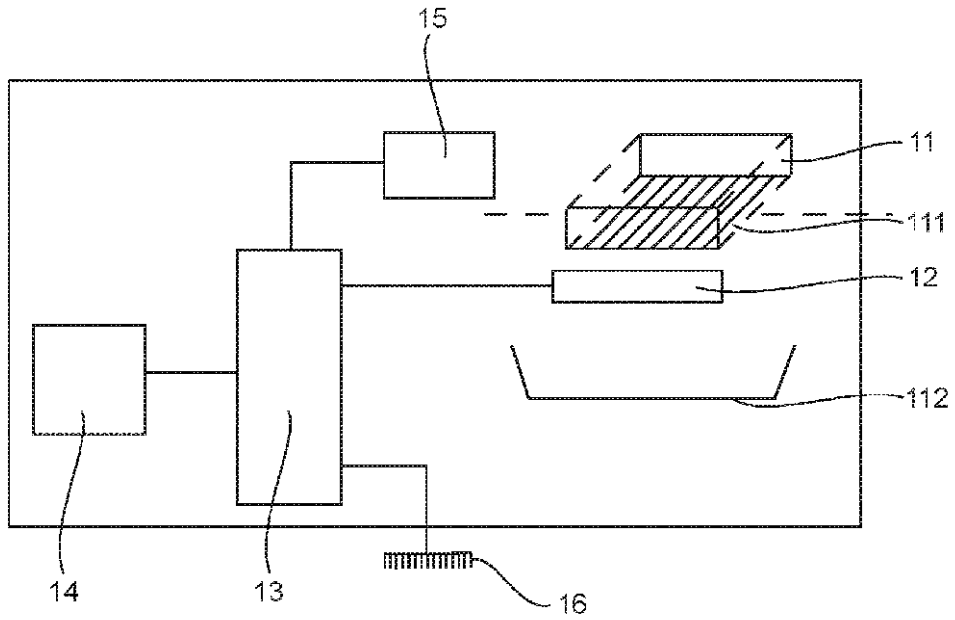


Fig. 1

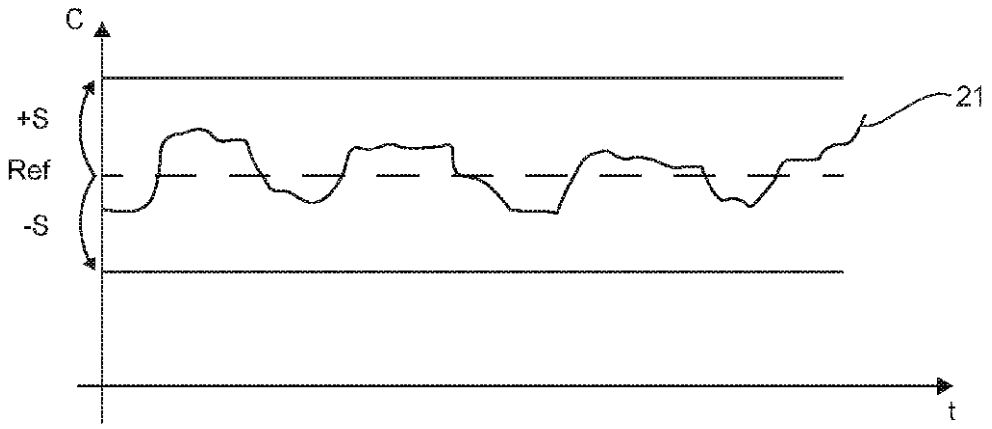


Fig. 2

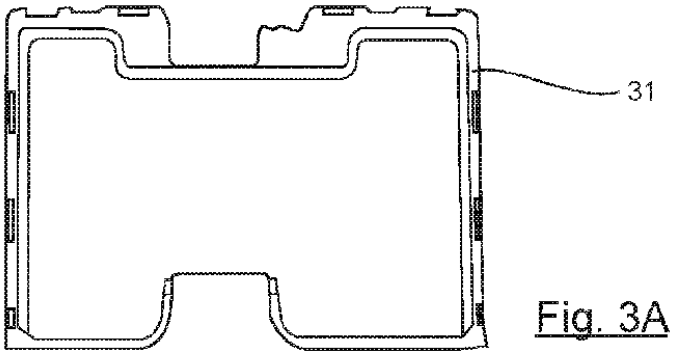


Fig. 3A

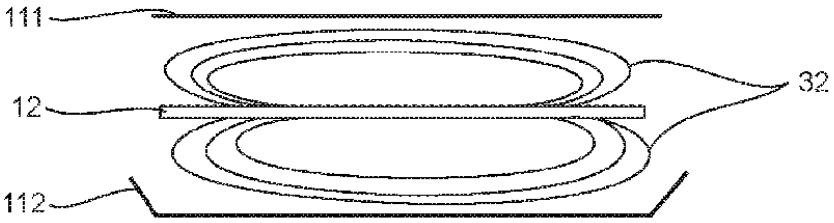


Fig. 3B

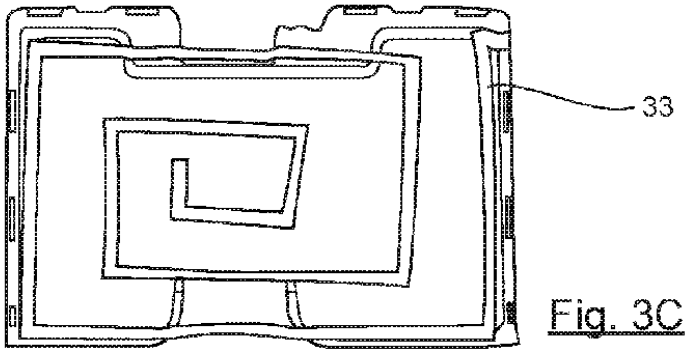


Fig. 3C

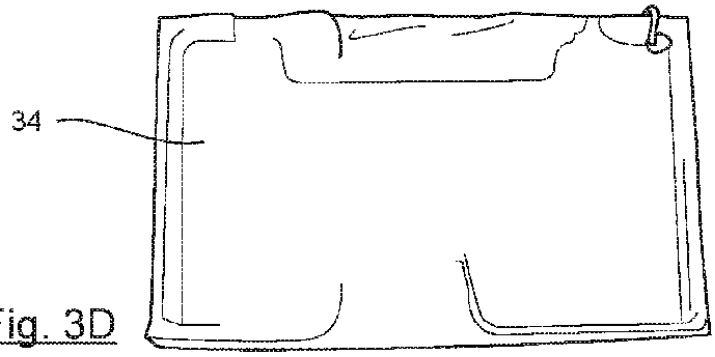


Fig. 3D

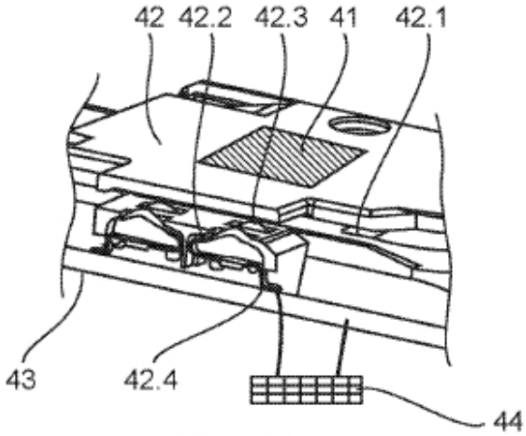


Fig. 4A

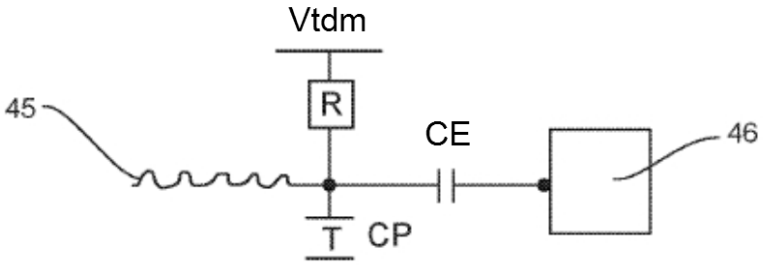


Fig. 4B

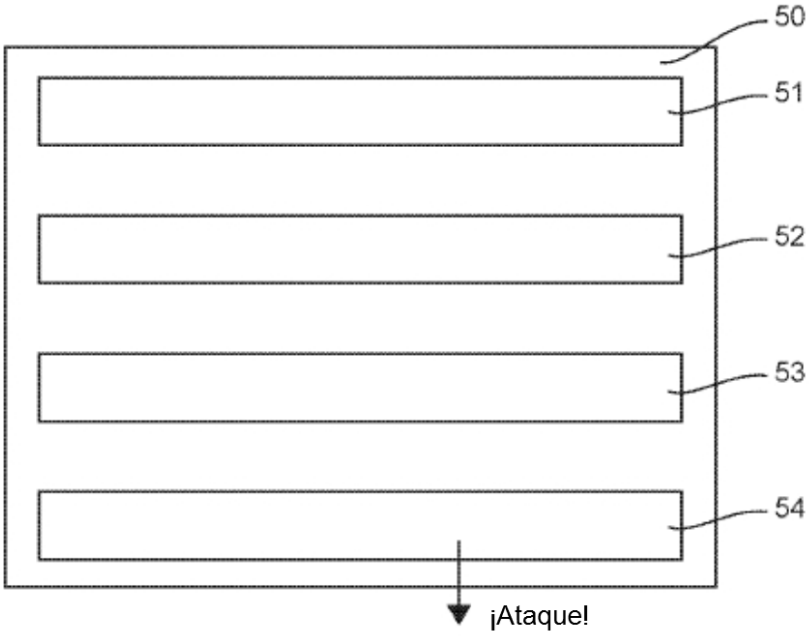


Fig. 5

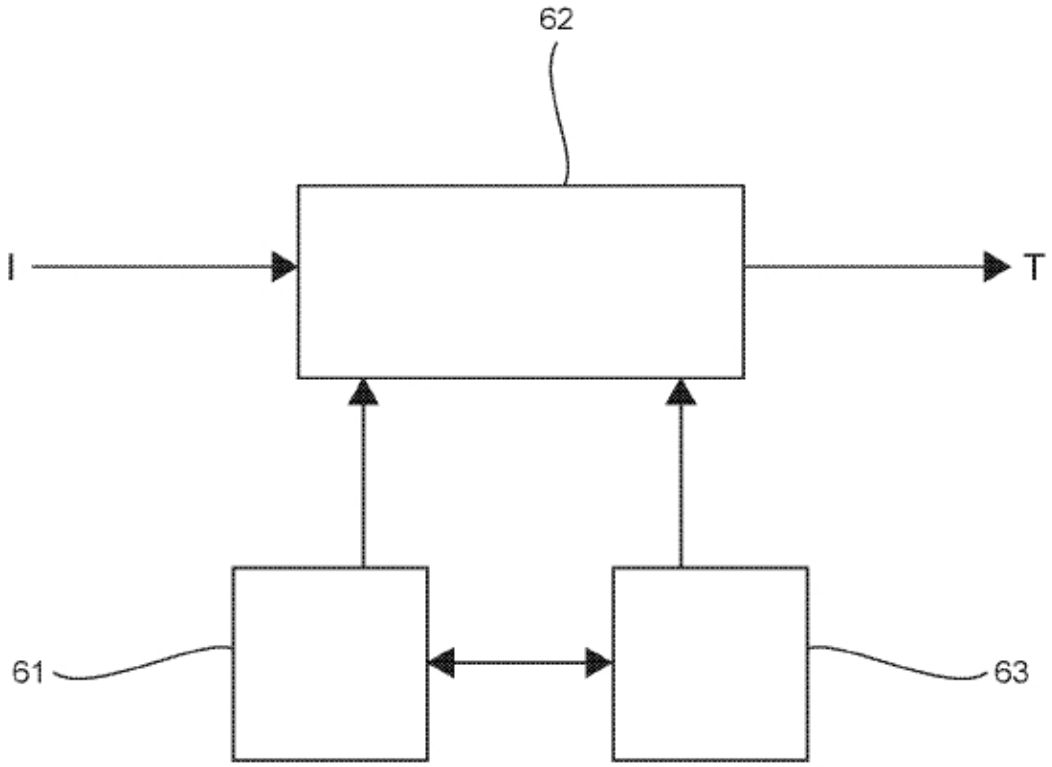


Fig. 6