(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 588 996**

(51) Int. CI.:

G06K 7/00 (2006.01)
G06F 21/00 (2013.01)
G07F 19/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **18.10.2012 E 12188996 (8)**

(97) Fecha y número de publicación de la concesión europea: **13.07.2016 EP 2722788**

(54) Título: **Dispositivo para lectura de una tarjeta de chip y procedimiento para la detección de un módulo de Skimming**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.11.2016

(73) Titular/es:

WINCOR NIXDORF INTERNATIONAL GMBH (100.0%)
Heinz-Nixdorf-Ring 1
33106 Paderborn, DE

(72) Inventor/es:

SCHLIEBE, DIETER y
HAMANN, WOLFGANG

(74) Agente/Representante:

UNGRÍA LÓPEZ, Javier

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Dispositivo para lectura de una tarjeta de chip y procedimiento para la detección de un módulo de Skimming

La invención se refiere a un dispositivo para la lectura de una tarjeta de chip, que presenta una unidad de lectura para la lectura de una tarjeta de chip que puede ser recibida en esta unidad de lectura y a una unidad de suministro de corriente para la alimentación del chip de la tarjeta de chip con energía eléctrica, cuando esta tarjeta de chip está alojada en la unidad de lectura. Además, la invención se refiere a un procedimiento para la detección de un módulo de Skimming colocado en un dispositivo para la lectura de una tarjeta de chip.

Para acceder ilegalmente a los datos de las tarjetas de tarjetas-EC, tarjetas de dinero y/o tarjetas de crédito y al PIN correspondiente, se manipulan aparatos de autoservicio, como por ejemplo cajeros automáticos o terminales de pago en filiales de comercios individuales, con los llamados módulos de Skimming, con cuya ayuda deben espiarse los datos de las tarjetas y el PIN correspondiente.

En el pasado era especialmente habitual que se intentase a través de los módulos de Skimming leer las cintas magnéticas de una tarjeta. A tal fin se han instalado en cajeros automáticos especialmente unidades de lectura de cintas magnéticas, con cuya ayuda se leían inadvertidamente los datos registrados en la cinta magnética. Adicionalmente, se ha espiado el in correspondiente, por ejemplo, con la ayuda de cámaras colocadas ocultas o con un teclado colocado adicionalmente, que ha sido dispuesto sobre el teclado propiamente dicho, de manera que la persona que realiza el ataque de Skimming espía tanto los datos de la cinta magnética como también el PIN correspondiente.

La seguridad en los cajeros automáticos se ha elevado a través del empleo de los llamados módulos antiskimming. Por una parte, se conocen procedimientos antiskimming, en los que a través de la determinación de la modificación de magnitudes físicas a través de la colocación de módulos de Skimming, por ejemplo por medio de la supervisión de la modificación del peso y de las dimensiones de componentes del cajero automático se ha detectado la presencia del módulo de Skimming. Por otra parte, se conocen procedimientos basados en cámaras, en los que con la ayuda de cámaras se determina la colocación o la presencia de un módulo de Skimming. Además, se conocen procedimientos antiskimming, en los que se impide la lectura de los datos de las tarjetas con la ayuda del módulo de Skimming. Por otro lado, se conocen procedimientos antiskimming, en los que se detectan las modificaciones de un campo electromagnético provocadas a través del módulo de Skimming.

Además, cada vez más cajeros automáticos utilizan el chip de la tarjeta-Eco bien tarjeta de crédito y no ya la cinta magnética, de manera que la lectura de los datos de las cintas magnéticas no es ya suficiente para la persona que realiza el ataque de Skimming.

En virtud de que los cajeros automáticos son cada vez más seguros, en los últimos tiempos los ataques de Skimming se han concentrado, por lo tanto, más en terminales de pago de establecimientos comerciales individuales, irrumpiendo con los nuevos ataques de Skimming durante la noche en los establecimientos comerciales individuales y manipulando los terminales de pago de forma inadvertid. A tal fin se inserta un módulo Skimming en forma de una unidad de construcción en miniatura pequeña con un circuito impreso (llamado Miniaturprints) con un componente eléctrico en la ranura, en la que se inserta normalmente la tarjeta de chip, estando configurada esta unidad de construcción de miniatura de tal manera que se puede leer al mismo tiempo o incluso influir en la comunicación de datos entre la tarjeta de chip o el terminal de pago.

Para impedir tales ataques de Skimming a través de la introducción de un módulo de Skimming en la ranura de la tarjeta, se conoce construir los terminales de pago de tal manera que se pueden reconocer fácilmente las intervenciones correspondientes, de modo que la introducción de un módulo de Skimming se puede detectar fácilmente por un operador, antes de que se produzca un daño. Sin embargo, aquí es problemático que estos mecanismos de protección pueden ser eludidos con habilidad por las personas que realizan los ataques de Skimming.

Se conoce a partir del documento US 2006/0038011 A1, con respecto al cual se han limitado las reivindicaciones, un procedimiento para el reconocimiento de módulos de micro skimming insertados en una unidad de lectura, en el que se calculan una corriente alimentada a una tarjeta de chip y un corriente retornada desde la tarjeta de chip. Si se diferencias estas dos corrientes entre sí, se deduce la presencia de un módulo de Skimmng.

El cometido de la invención es indicar un dispositivo para la lectura de una tarjeta de chip y un procedimiento para la detección de un módulo de Skimming, con los que se puede detectar de una manera sencilla cuándo ha sido introducido un módulo se Skimming en una ranura de tarjeta del dispositivo.

La invención se define en las reivindicaciones dependientes.

Los ejemplos de realización preferidos se deducen a partir de las reivindicaciones dependientes.

En particular, de esta manera se puede determinar si se ha introducido un módulo de Skimming en la unidad relectura, especialmente en una ranura para la inserción de la tarjeta de chip.

La unidad de suministro de corriente determina en este caso especialmente la corriente en aquella trayectoria de la corriente, que sirve para el suministro de la tarjeta de chip con energía eléctrica. La determinación se realiza en este caso con preferencia en la zona de la trayectoria de la corriente, en la que, además de la tarjeta de chip introducida eventualmente en el dispositivo, no están conectados otros consumidores eléctricos regulares del dispositivo.

Los módulos de Skimming para la lectura de los datos de la tarjeta de chip necesitan una alimentación con energía eléctrica, que adquieren desde el dispositivo de la misma manera que la tarjeta de chip desde la unidad de suministro de corriente del dispositivo. De esta manera se puede calcula de manera especialmente sencilla a través de la supervisión de la corriente eléctrica cedida por la unidad de suministro de corriente si han sido introducido un módulo de Skimming.

A tal fin, en la unidad de control está registrado un valor límite, con el que la unidad de control compara las corrientes eléctricas calculadas a través de la unidad de sensor y cedidas por la unidad de suministro de corriente. Si de esta comparación resulta que la corriente cedida es mayor que el valor límite preajustado, entonces la unidad de control deduce a partir de ello la presencia de un módulo de Skimming en la unidad de lectura. El valor límite está preajustado en este caso especialmente de tal manera que corresponde al consumo máximo nominal de la corriente de la tarjeta de chip, es decir, aquellos valores de la corriente cedida por la unidad de suministro de corriente, que ésta cede para la alimentación de una tarjeta de chip introducida en la unidad de lectura con energía eléctrica a ésta. Si la corriente eléctrica cedida es, por lo tanto, mayor que este valor límite, debe estar presente otro consumidor de corriente adicionalmente a la tarjeta de chip, de manera que se puede deducir de una manera fiable y sencilla que ha sido insertado un módulo de Skimming.

En una forma de realización preferida, también pueden estar registrados dos valores límites o más de dos valores límites en la unidad de control. En este caso a cada uno de los valores límites registrados en la unidad de control está asociada, respectivamente, al menos un tipo de tarjeta de chip, estando asociado exactamente un valor límite cada tipo de tarjeta de chip utilizable en el dispositivo. El valor límite corresponde en este caso, respectivamente, a aquella corriente eléctrica, que ha sido necesitada por una tarjeta de chip de este tipo de tarjetas de chip. La unidad de control compara la corriente actual calculada a través de la unidad de sensor en este caso especialmente, respectivamente, con aquel valor límite, que está asociado al tipo de tarjeta de chip utilizado o a utilizar.

De esta manera se consigue que también con diferentes tipos de tarjetas de chips se pueda determinar de manera fiable a través de la corriente calculada con la ayuda del sensor si ha sido introducido un módulo de Skimming para el espionaje de datos.

El dispositivo comprende especialmente una unidad de sensor de tarjetas, con cuya ayuda se puede determinar qué tipo de tarjeta de chip ha sido introducido en el dispositivo. En función del tipo de tarjeta de chip calculado, la unidad de control selecciona entonces el valor límite asociado correspondiente para la comparación. Alternativamente el tipo de tarjeta de chip se puede registrar, por ejemplo, también en el chip de la tarjeta de chip y se puede leer a través de la unidad de lectura. De la misma manera es posible alternativamente que el tipo de tarjeta de chip utilizado sea ajustado en la puesta en funcionamiento del dispositivo y la unidad de control utilice de manera correspondiente el valor límite asociado.

De manera alternativa, el valor límite puede corresponder también a 1,05 a 1,5 veces, opcionalmente a 1,1 a 1,3 veces, en particular a 1,15 a 1,2 veces el consumo máximo de corriente de la tarjeta de chip. De esta manera se asegura que en el caso de oscilaciones ligeras del consumo de corriente máximo normalmente habitual de la tarjeta de chip a través de influencias del medio ambiente no se deduzca inmediatamente de forma errónea la presencia de un módulo de Skimming.

En una forma de realización especialmente preferida, está previsto un sensor de tarjetas para la determinación de la presencia de una tarjeta de chip en la unidad de lectura. En esta forma de realización, la unidad de control deduce la presencia de un módulo de Skimming en la unidad de lectura cuando se ha calculado con la ayuda del sensor de tarjetas que no se ha introducido ninguna tarjeta de chip en la unidad de lectura y a pesar de todo se ha determinado con la ayuda de la unidad de sensor que se emite desde la unidad de suministro de corriente una corriente eléctrica. De esta manera debe cederse corriente a otro consumidor distinto a una tarjeta de chip, de modo que debe existir un intento de manipulación con la ayuda de un módulo de Skimming.

Además, es ventajoso que la unidad de control ponga el dispositivo fuera de servicio cuando ha determinado la presencia de un módulo de Skimming. De esta manera se asegura que no se puedan espiar los datos de un operador. Por puesta fuera de servicio se entiende especialmente que el dispositivo es accionado en un modo, en el que se rechaza la lectura de datos desde la tarjeta de chip.

Adicional o alternativamente, la unidad de control puede emitir también una señal de alarma con la ayuda de una unidad de salida. A tal fin se puede emitir, por ejemplo, a través de una pantalla una alarma óptica correspondiente.

Adicional o alternativamente, se puede emitir también una alarma acústica. Por lo demás, es posible que a través de una conexión de transmisión de datos se transmita un mensaje de alarma correspondiente a una unidad de supervisión central.

El dispositivo tiene especialmente una carcasa, en la que está prevista la ranura para la introducción de la tarjeta de chip. La unidad de lectura está dispuesta especialmente detrás de esta ranura, de manera que un módulo de Skimming insertado a través de la ranura está dispuesto en esta unidad de lectura. La ranura se puede cerrar especialmente a través de una corredera. En el caso de detección de un ataque de Skimming, la unidad de control cierra con preferencia la corredera, de manera que no se puede introducir ninguna tarjeta de chip.

Además, es ventajoso que la unidad de sensor para la determinación de la corriente emitida por la unidad de suministro de corriente sea un componente de la unidad de lectura, de manera que se consigue una estructura sencilla especialmente compacta. En el dispositivo se trata especialmente de un cajero automático, pudiendo tratarse tanto de un puro cajero automático de pago como también de un cajero automático de ingresos y de pago. Alternativamente, el dispositivo puede ser también un sistema de caja automática, una caja fuerte automática, un terminal de pago u otro aparato de autoservicio. De manera correspondiente, en la tarjeta de chip se trata especialmente de una tarjeta-EC, una tarjeta de dinero, una tarjeta de cliente o una tarjeta de crédito.

La unidad de suministro de corriente presenta especialmente al menos una zona de contacto para el contacto de un contacto del chip de la tarjeta de chip. A través de este contacto se transmite la energía eléctrica necesaria para el suministro del chip. Los módulos de Skimming, que se introducen en la unidad de lectura para la reproducción de los datos, utilizan especialmente también esta alimentación de corriente para la alimentación propia con energía eléctrica.

Alternativamente, se pueden utilizar también tarjetas de chip sin contacto, como por ejemplo tarjetas de chip con un chip-RFID y/o chip-NFC. En este caso, se realiza también la alimentación de corriente sin contacto. La alimentación de corriente se realiza en este caso especialmente por medio de inducción.

Otro aspecto de la invención se refiere a un procedimiento para la detección de un módulo de Skimming, en el que con la ayuda de una unidad de sensor se calcula la corriente cedida por una unidad de suministro de corriente para la alimentación de una tarjeta de chip con energía eléctrica. En función de esta corriente calculada se supervisa si ha sido introducido un módulo de Skimming en una unidad de lectura para a lectura de datos desde la tarjeta de chip.

A tal fin se compara especialmente si la corriente cedida por la unidad de suministro de corriente es mayor que la corriente normalmente necesaria por la tarjeta de chip. Cuando éste es el caso, debe estar presenta otro consumidor eléctrico, especialmente un módulo de Skimming, de manera que en este caso se deduce que se ha introducido de forma ilegal un módulo de Skimming en esta unidad.

Además, se puede deducir también la presencia de un módulo de Skimming cuando con la ayuda de un sensor de tarjetas se determina que no se ha introducido ninguna tarjetas de chip en la unidad de lectura y a pesar de todo se cede corriente eléctrica desde la unidad de suministro de corriente. Tampoco en este caso la corriente puede servir para el suministrote una tarjeta de chip, sino que debe estar presente un módulo de Skimming.

En todos los datos se puede detectar de manera sencilla con seguridad la presencia de un módulo de Skimming.

Otras características y ventajas de la invención se deducen a partir de la siguiente descripción, que explica en detalle la invención con la ayuda de ejemplos de realización en conexión con las figuras adjuntas. En este caso:

La figura 1 muestra una representación esquemática de un aparato de autoservicio según una primera forma de realización; y

La figura 2 muestra una representación esquemática de un aparato de autoservicio según una segunda forma de realización.

En la figura 1 se representa una representación esquemática muy simplificada de un dispositivo 10 configurado como aparato de autoservicio para la lectura de una tarjeta de chip. El aparato de autoservicio 10 se emplea especialmente en filiales de comercios individuales para el pago de los productos adquiridos con la ayuda de una tarjeta-EC o una tarjeta de crédito, es decir, en general, una tarjeta de banda magnética y/o tarjeta de chip.

El aparato de autoservicio 10 presenta una carcasa 12, en la que está prevista una ranura 14, a través de la cual se puede alimentar la tarjeta de chip a una unidad de lectura 16 para la lectura de los datos registrados en el chip de la tarjeta de chip. Además, el aparato de autoservicio 10 comprende una unidad de suministro de corriente 18, con cuya ayuda la tarjeta de chip, cuando ésta es introducida en el aparato de autoservicio 10 y, por lo tanto, en la unidad de lectura 16, se puede alimentar con una corriente eléctrica. A tal fin, la unidad de suministro de corriente 18 presenta especialmente elementos de contacto, a través de los cuales se contacta con contactos del chip y de esta manera se puede realizar un suministro de corriente eléctrica del chip.

La unidad de lectura 16 comprende una unidad de sensor 20, con cuya ayuda se puede detectar el valor de la corriente eléctrica cedida por la unidad de suministro de corriente 18. Además, está prevista una unidad de control 22, a la que se transmiten datos y/o señales con informaciones sobre la corriente eléctrica cedida por la unidad de suministro de corriente 18 desde la unidad de sensor 20. Además, el aparato de autoservicio 10 tiene un sensor de tarjetas 24, con cuya ayuda se puede determinar si en la unidad de lectura 16 se ha introducido o no una tarjeta de chip. También este sensor 24 está conectado especialmente a través de una conexión de transmisión de datos con la unidad de control 22 y transmite datos y/o señales con informaciones acerca de si en la unidad de lectura 16 está insertada o no una tarjeta de chip, a la unidad de control 22.

En el caso de nuevos ataques de Skimming, en los que se trata de manera ilegal de leer los datos registrados sobre el chip de la tarjeta de chip introducida, se introduce en la ranura 14 un módulo de Skimming muy pequeño, que está configurado en forma de una unidad de construcción de miniatura, que comprende un circuito impreso y una electrónica, con cuya ayuda el módulo de Skimming lee al mismo tiempo y/o manipula los datos transmitidos entre el chip de la tarjeta de chip y la unidad de lectura 16. En estos ataques de Skimming se irrumpe especialmente por la noche en las filiales de comercios individuales, en las que se utiliza el aparato de autoservicio 10 y se introduce de forma inadvertida el módulo de Skimming correspondiente en la ranura 14.

Para reconocer ataques de Skimming, antes de que los datos de una tarjeta de chip sean espiados de manera ilegal, se emplea según la invención el procedimiento descrito a continuación.

Con la ayuda de la unidad de sensor 20 se supervisa la corriente eléctrica cedida por la unidad de suministro de corriente 18. Cuando se ha introducido un módulo de Skimming en la ranura 14 y, por lo tanto, en la unidad de lectura 6, éste toma su energía eléctrica de manera similar a una tarjeta de chip introducida, a través de la unidad de suministro de corriente 18. De esta manera, para el caso de que se introduzca un módulo de Skimming, se detecta desde la unidad de sensor 20 una corriente eléctrica, incluso cuando no se ha introducido ninguna tarjeta de chip. La unidad de control 22 calcula de esta manera la presencia de un módulo de Skimming en la unidad de lectura 16 cuando con la ayuda de la unidad de sensor 20 se detecta una cesión de una corriente eléctrica de la unidad de suministro de corriente 18 y el sensor de tarjetas 24 detecta que no se ha introducido ninguna tarjeta de chip en el aparato de autoservicio 10. En este caso, la energía eléctrica desde la unidad de suministro de corriente 18 sólo puede ser cedida a un módulo de Skimming introducido ilegalmente, de manera que se puede detectar de una manera fiable y sencilla un ataque de Skimming correspondiente desde la unidad de sensor 22.

En cambio, si el sensor de tarjetas 24 detecta la presencia de una tarjeta de chip en la unidad de lectura 16, entonces la unidad de control 22 compara la corriente determinada por la unidad de sensor 20, que es cedida por la unidad de suministro de corriente 18, con un valor límite reajustado. Este valor límite está preajustado especialmente de tal manera que corresponde al consumo máximo nominal de corriente de la tarjeta de chip, es decir, aquel consumo de corriente, que se necesita como máximo para una sola tarjeta de chip. Alternativamente, el valor límite puede tener también un valor entre 1,05 veces y 1,3 veces el consumo máximo nominal de corriente de la tarjeta de chip.

En una forma de realización alternativa, se pueden preajustar también varios valores límites, sendo preajustado especialmente para cara tipo de tarjeta de chip posible a utilizar un valor límite. Los valores límites pueden ser preajustados en este caso especialmente de tal manera que corresponden, respectivamente, al consumo máximo nominal de la corriente de una tarjeta de chip del tipo de tarjetas de chip respectivo, es decir, a aquel consumo de corriente, que se necesaria como máximo por una unidad de tarjeta de chip del tipo respectivo de tarjeta de chip. Alternativamente, también en este caso de nuevo el valor límite respectivo puede corresponder a un valor entre 1,1 veces y 1,3 veces, del consumo máximo nominal de corriente de una tarjeta de chip del tipo de tarjetas de chip respectivo.

Esto tiene la ventaja de que el valor límite, con el que se compara la corriente determinada a través de la unidad de sensor 20 por la unidad de control, se puede adaptar al tipo de tarjeta de chip utilizado en cada caso, de manera que también en el caso de utilización de tarjetas de chip de diferente tipo de tarjeta de chip y, por lo tanto, de tarjetas de chip con un consumo de corriente nominal diferente se puede deducir de manera fiable a través de la comparación, la presencia de un módulo de Skimming.

El tipo de tarjeta de chip utilizado es determinado con preferencia automáticamente por el dispositivo y se selecciona el valor límite correspondiente para la comparación. Alternativamente, el tipo de tarjeta de chip utilizado puede ser preajustado también por un usuario y un operario de servicio.

Si de esta comparación resulta que el consumo de corriente real calculado por la unidad de sensor es mayor que el valor límite preajustado, la unidad de control 22 detecta de la misma manera la presencia de un módulo de Skimming y, por lo tanto, un ataque de Skimming. En este caso, en efecto, el consumo elevado de corriente puede ser provocado no sólo por la tarjeta de chip y debe estar presente otro consumidor eléctrico.

Cuando la unidad de control 22 ha detectado un ataque de Skimming, entonces pone fuera de servicio especialmente el aparato de autoservicio 10, de manera que el aparato de autoservicio 10 no s epuede utilizar ya

para el pago a través de una tarjeta de chip y de esta manera no es posible ningún daño a través del espionaje de datos de tarjetas de chip. Adicional o alternativamente, la unidad de control 22 puede emitir también a través de una unidad de salida 26 del aparato de autoservicio 10 una alarma a un operador del aparato de autoservicio 10. En la unidad de salida 26 se trata especialmente de una pantalla, con cuya ayuda se pueden emitir también durante el proceso de pago planificado informaciones e instrucciones al operador. Adicional o alternativamente, se puede emitir también una alarma acústica. Por lo demás, es posible que se transmita una alarma a través de una conexión de transmisión de datos, por ejemplo por cable o por radio, a una unidad de control central, de manera que se solicita a un operador que verifique el aparato de autoservicio 10.

En la figura 2 se representa una representación esquemática, muy simplificada de un aparato de autoservicio 100 de acuerdo con una segunda forma de realización. El aparato de autoservicio 100 de acuerdo con la segunda forma de realización se diferencia de la primera forma de realización según la figura 1 solamente porque la unidad de sensor 20 no es componente de la unidad de lectura 16, sino que es un componente autónomo.

En otra forma de realización alternativa, por ejemplo, también la unidad de suministro de corriente 18 puede estar configurada como una parte de la unidad de lectura 16.

Lista de signos de referencia

10, 100	Aparato de autoservicio
12	Carcasa
16	Unidad de lectura
18	Unidas de suministro de corriente
20	Unidad de sensor
22	Unidad de control
24	Sensor de tarjetas
26	Unidad de salida

REIVINDICACIONES

1.- Dispositivo para la lectura de una tarjeta de chip de un tipo determinado de tarjeta de chip,

con una unidad de lectura (16) para la lectura de una tarjeta de chip que puede ser recibida en la unidad de lectura (16),

con una unidad de suministro de corriente (18) para la alimentación del chip de la tarjeta de chip con energía eléctrica, cuando la tarjeta de chip es recibida en la unidad de lectura (16),

en el que está prevista una unidad de sensor (20) para la determinación de la corriente eléctrica cedida por la unidad de suministro de corriente (18), y

en el que una unidad de control (22) determina en función de la corriente eléctrica cedida por la unidad de suministro de corriente (18) y por la unidad de sensor (20) si el dispositivo ha sido manipulado con un módulo de Skimming para el espionaje de los datos registrados en la tarjeta de chip,

caracterizado porque en la unidad de control (22) está registrado al menos un valor límite,

porque el valor límite está preajustado de tal manera que corresponde al consumo máximo nominal de la corriente de una tarjeta de chip del tipo predeterminado de la tarjeta de chip, y

porque la unidad de control (22) determina la presencia de un módulo de Skimming cuando la corriente detectada por la unidad de sensor (20) excede este valor límite.

2.- Dispositivo (10, 100) de acuerdo con la reivindicación 1, **caracterizado** porque está previsto un sensor de tarjetas (24) para la determinación de la presencia de una tarjeta de chip en la unidad de lectura (16), y por que la unidad de control (22) determina la presencia de un módulo de Skimming cuando se ha determinado con la ayuda del sensor de tarjetas (25), que no está dispuesta ninguna tarjeta de chip en la unidad de lectura (16), mientras la unidad de sensor (22) ha detectado una corriente eléctrica.

3.- Dispositivo (10, 100) de acuerdo con una de las reivindicaciones anteriores, **caracterizado** porque la unidad de control (22) pone el dispositivo fuera de servicio cuando ha determinado la presencia de un módulo de Skimming.

4.- Dispositivo (10, 100) de acuerdo con una de las reivindicaciones anteriores, **caracterizado** porque la unidad de control (22) emite a través de una unidad de emisión (26) una alarma, cuando ha determinado la presencia de un módulo de Skimming.

5.- Dispositivo (10, 100) de acuerdo con una de las reivindicaciones anteriores, **caracterizado** porque el dispositivo (10, 100) presenta una carcasa (12) con una ranura (14) para la introducción de la tarjeta de chip.

6.- Dispositivo (10, 100) de acuerdo con una de las reivindicaciones anteriores, **caracterizado** porque la unidad de sensor (20) es componente de la unidad de lectura (16).

7.- Dispositivo (10, 100) de acuerdo con una de las reivindicaciones anteriores, **caracterizado** porque la unidad de suministro de corriente (18) comprende al menos una zona de contacto para el contacto de un contacto del chip de la tarjeta de chip para la transmisión de la energía eléctrica.

8.- Dispositivo (10, 100) de acuerdo con una de las reivindicaciones anteriores, **caracterizado** porque el dispositivo (10, 100) es un cajero automático, un sistema de caja automática, una caja fuerte automática o un terminal de pago.

9.- Dispositivo (10, 100) de acuerdo con una de las reivindicaciones anteriores, **caracterizado** porque el valor límite es un primer valor límite, porque en la unidad de control (22) está registrado al menos un segundo valor límite, porque al primer valor límite y al segundo valor límite está asociado, respectivamente, al menos un tipo de tarjeta de chip, y porque la unidad de control (22) compara la corriente detectada por la unidad de sensor (20) en función del tipo de la tarjeta de chip utilizada con el valor límite asociado a este tipo de tarjeta de chip.

10.- Procedimiento para la detección de un módulo de Skimming,

en el que con la ayuda de una unidad de sensor (20) se detecta la corriente cedida por una unidad de suministro de corriente (18) para la alimentación de una tarjeta de chip con energía eléctrica, y

en el que en función de esta corriente detectada, se supervisa la presencia de un módulo de Skimming,

caracterizado porque en una unidad de control (22) se registra al menos un valor límite,

porque el valor límite se preajusta de tal manera que corresponde al consumo máximo nominal de corriente

de una tarjeta de chip de un tipo predeterminado de tarjeta de chip, y

porque se determina la presencia de un módulo de Skimming cuando la corriente detectada por la unidad de sensor (20) excede este valor límite.

11.- Procedimiento de acuerdo con la reivindicación 10, **caracterizado** porque se deduce la presencia de un módulo de Skimming cuando se cede una corriente desde la unidad de suministro de corriente (18), mientras que con la ayuda de un sensor de tarjeta (24) se determina que no está presente ninguna tarjeta de chip.

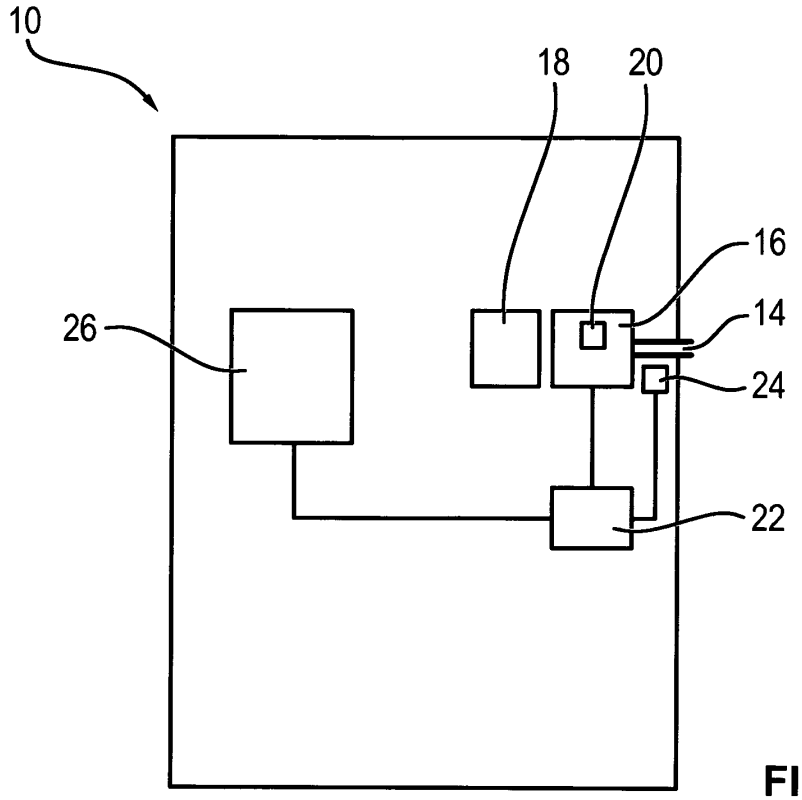

FIG. 1

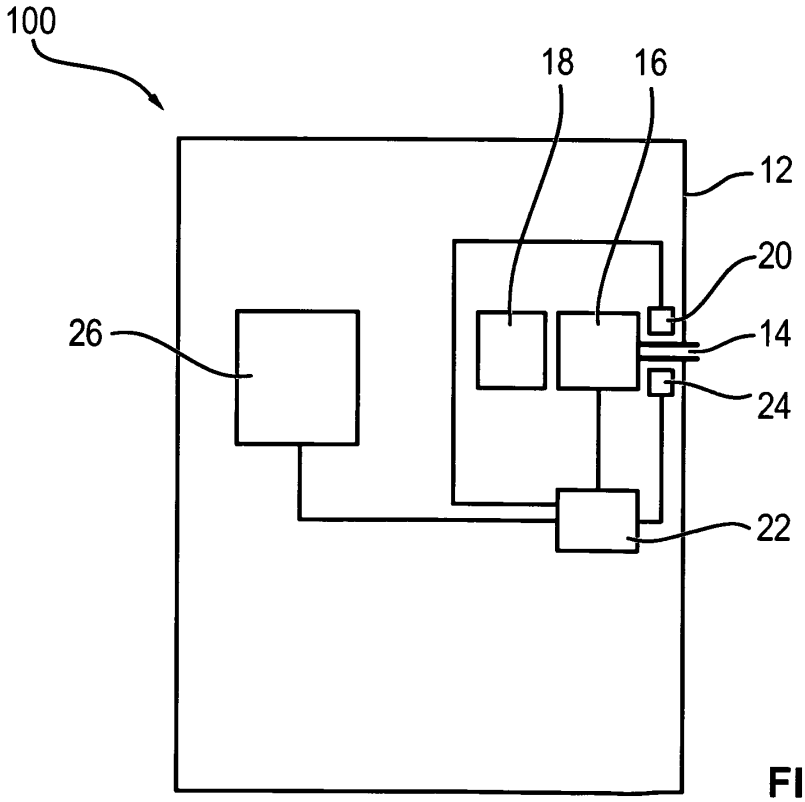

FIG. 2