(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 675 073**

(51) Int. CI.:

G06F 21/55	(2013.01)
G06F 21/86	(2013.01)
G06Q 20/34	(2012.01)
G07F 7/08	(2006.01)
G07F 7/10	(2006.01)
H04L 9/08	(2006.01)
H04L 9/32	(2006.01)
H05K 5/02	(2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **22.05.2008 PCT/FR2008/050883**

(87) Fecha y número de publicación internacional: **04.12.2008 WO08145942**

(96) Fecha de presentación y número de la solicitud europea: **22.05.2008 E 08805828 (4)**

(97) Fecha y número de publicación de la concesión europea: **18.04.2018 EP 2158721**

(54) Título: **Procedimiento y dispositivo de detección de un intento de sustitución de una parte de carcasa original de un sistema electrónico por una parte de carcasa de reemplazo**

(30) Prioridad:

24.05.2007 FR 0755232

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
06.07.2018

(73) Titular/es:

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

(72) Inventor/es:

COUSSIEU, ALAIN y
ECK, ALAIN

(74) Agente/Representante:

SUGRAÑES MOLINÉ, Pedro

DESCRIPCIÓN

Procedimiento y dispositivo de detección de un intento de sustitución de una parte de carcasa original de un sistema electrónico por una parte de carcasa de reemplazo

Campo de la invención

La presente invención se refiere a un dispositivo y a un procedimiento de detección de un intento de sustitución de una parte de carcasa original de un sistema electrónico por una parte de carcasa de reemplazo.

Descripción de la técnica anterior

Para numerosos sistemas electrónicos, es deseable evitar a terceros no autorizados el acceso a los componentes internos del sistema electrónico y/o a los datos intercambiados por los componentes internos del sistema electrónico. Para ello, pueden preverse dispositivos de seguridad que permiten la detección de un intento de acceso no autorizado al sistema electrónico.

Es el caso, por ejemplo, de un lector de tarjetas, concretamente de tarjetas bancarias, utilizado para realizar operaciones de pago. Generalmente, el lector de tarjetas está constituido por una carcasa que comprende al menos una parte inferior de carcasa unida a una parte superior de carcasa. La carcasa contiene un circuito impreso al que están unidos los componentes electrónicos del lector.

El lector puede comprender un circuito integrado, denominado criptoprocesador, que se encarga del tratamiento de datos sensibles, por ejemplo, los códigos confidenciales de las tarjetas introducidas en el lector. Es deseable evitar que terceros no autorizados accedan a estos datos sensibles. Para ello, el criptoprocesador también puede encargarse de la detección de intentos de acceso no autorizado al lector. Entonces, recibe señales de alarma proporcionadas por dispositivos de seguridad que equipan el lector. Un ejemplo de dispositivo de seguridad corresponde a un circuito que comprende una pista conductora en forma de enrejado. Se considera que una interrupción de la pista conductora representa un intento de acceso no autorizado al lector y se traduce en la provisión de una señal de alarma al criptoprocesador. Otro ejemplo de dispositivo de seguridad corresponde a una tecla falsa prevista a nivel del teclado. En funcionamiento normal, la tecla garantiza de manera permanente la conexión eléctrica entre dos pistas conductoras del circuito impreso. Se considera que la interrupción de la conexión eléctrica representa un intento de acceso no autorizado al lector y se traduce en la provisión de una señal de alarma al criptoprocesador. Cuando el criptoprocesador detecta que se produce un intento de acceso no autorizado, interrumpe el funcionamiento normal del lector y, en particular, borra los datos sensibles.

No obstante, la simple detección de los intentos de acceso no autorizado puede ser insuficiente para garantizar una protección aceptable de los datos sensibles. En efecto, puede concebirse un tipo particular de fraude que consistiría, al conseguir neutralizar temporalmente los dispositivos de seguridad, en reemplazar la parte superior de carcasa original por una parte superior de carcasa que se habría modificado previamente con el fin de poder retirarse fácilmente con posterioridad sin conllevar la detección de un intento de acceso no autorizado por el criptoprocesador. Por ello, un usuario podría entonces hacer uso del lector sin darse cuenta de la modificación efectuada y proporcionar su código confidencial. A continuación, el código confidencial podría recuperarse fácilmente por terceros retirando la parte de carcasa modificada.

Por tanto, es deseable, además de la detección de los intentos de acceso no autorizado, que el criptoprocesador verifique de manera permanente si al menos determinadas piezas que constituyen el lector corresponden correctamente a las originales.

Sumario de la invención

La presente invención se refiere a un procedimiento y a un dispositivo de detección de un intento de sustitución no autorizada de una pieza original de un sistema electrónico por una pieza de reemplazo.

Según otro objeto, el dispositivo de detección modifica poco el sistema electrónico a nivel del cual está previsto.

Así, un ejemplo de realización de la presente invención prevé un sistema electrónico que comprende una carcasa constituida al menos por una primera parte de carcasa unida a una segunda parte de carcasa y que contiene un dispositivo de detección de la sustitución de la primera parte de carcasa. El dispositivo comprende un primer circuito integrado destinado a fijarse a la primera parte de carcasa; y un segundo circuito integrado destinado a fijarse a la segunda parte de carcasa y adaptado para transmitir al primer circuito integrado señales digitales sucesivas aleatorias o pseudoaleatorias, estando el primer circuito integrado adaptado para reenviar al segundo circuito integrado, para cada señal digital, una primera firma encriptada a partir de dicha señal digital, estando el segundo circuito integrado adaptado para determinar una segunda firma encriptada a partir de dicha señal digital y para detectar una sustitución de la primera parte de carcasa si las firmas encriptadas primera y segunda son diferentes.

Según un ejemplo de realización, el primer circuito integrado comprende una primera memoria en la que se almacenan un número de identificación y una primera clave y el segundo circuito integrado comprende una segunda memoria en la que se almacena una segunda clave, estando el primer circuito integrado adaptado para transmitir el número de identificación al segundo circuito integrado, estando el segundo circuito integrado adaptado para transmitir el número de identificación a una herramienta de activación exterior al lector y para recibir la segunda clave, igual a la primera clave, determinada por la herramienta de activación mediante una primera función de encriptado a partir del número de identificación y de una tercera clave, estando el primer circuito integrado adaptado para determinar, para cada señal digital, la primera firma encriptada mediante una segunda función de encriptado a partir de dicha señal digital y de la primera clave, estando el segundo circuito integrado adaptado para determinar la segunda firma encriptada mediante la segunda función de encriptado a partir de dicha señal digital y de la segunda clave.

Según un ejemplo de realización, el primer circuito integrado está unido al segundo circuito integrado mediante una conexión por cable.

Según un ejemplo de realización, el primer circuito integrado está unido al segundo circuito integrado mediante una conexión capacitiva.

Según un ejemplo de realización, el sistema corresponde a un lector de tarjetas, concretamente para la realización de operaciones de pago.

También está previsto un procedimiento de detección de la sustitución de una primera parte de carcasa de un sistema que comprende, además, una segunda parte de carcasa unida a la primera parte de carcasa. El procedimiento consiste en proporcionar un primer circuito integrado fijado a la primera parte de carcasa y un segundo circuito integrado fijado a la segunda parte de carcasa; en hacer que el segundo circuito integrado transmita al primer circuito integrado señales digitales sucesivas aleatorias o pseudoaleatorias; en hacer que el primer circuito integrado reenvíe al segundo circuito integrado, para cada señal digital, una primera firma encriptada a partir de dicha señal digital; y en hacer que el segundo circuito integrado determine una segunda firma encriptada a partir de dicha señal digital y detecte una sustitución de la primera parte de carcasa si las firmas encriptadas primera y segunda son diferentes.

Según un ejemplo de realización, el procedimiento comprende las siguientes etapas:

a) almacenar en el primer circuito integrado un número de identificación y una primera clave que no es accesible desde el exterior del primer circuito integrado;
b) hacer que, en una fase de activación, el primer circuito integrado transmita el número de identificación al segundo circuito integrado;
c) hacer que, en la fase de activación, el segundo circuito integrado transmita el número de identificación a una herramienta de activación exterior al lector;
d) hacer que, en la fase de activación, la herramienta de activación determine una segunda clave, igual a la primera clave, mediante una primera función de encriptado a partir del número de identificación y de una tercera clave;
e) hacer que, en la fase de activación, la herramienta de activación transmita la segunda clave al segundo circuito integrado;
f) hacer que, en una fase de funcionamiento normal, el segundo circuito integrado transmita al primer circuito integrado las señales digitales sucesivas aleatorias o pseudoaleatorias;
g) hacer que, en la fase de funcionamiento normal, el primer circuito integrado reenvíe al segundo circuito integrado, para cada señal digital, la primera firma encriptada determinada mediante una segunda función de encriptado a partir de dicha señal digital y de la primera clave; y
h) hacer que, en la fase de funcionamiento normal, el segundo circuito integrado determine la segunda firma encriptada mediante la segunda función de encriptado a partir de dicha señal digital y de la segunda clave, y detecte una sustitución de la primera parte de carcasa si las firmas encriptadas primera y segunda son diferentes.

Según un ejemplo de realización, el procedimiento comprende además la etapa que consiste en hacer que el segundo circuito integrado borre la segunda clave en el caso de que las firmas encriptadas primera y segunda sean diferentes en la etapa h), necesitando entonces la reutilización del lector de nuevo la puesta en práctica de las etapas b) a e).

Según un ejemplo de realización, la primera función de encriptado es una función de tipo DES o triple DES y/o la segunda función de encriptado es una función de tipo SHA.

Breve descripción de los dibujos

Estos objetos, características y ventajas, así como otros, se expondrán en detalle en la siguiente descripción de un ejemplo de realización particular realizada a modo no limitativo en relación con las figuras adjuntas en las que:

la figura 1 es una vista en perspectiva esquemática de un ejemplo de lector de tarjeta;

la figura 2 es una sección esquemática del lector de la figura 1 y representa un ejemplo de dispositivo de detección de un intento de sustitución no autorizada de una parte de la carcasa del lector;

la figura 3 representa, en forma de un diagrama de bloques, etapas de un ejemplo de procedimiento de detección de intento de sustitución no autorizada de una pieza original durante una fase de activación; y

la figura 4 representa, en forma de un diagrama de bloques, etapas sucesivas del procedimiento de detección durante una fase de funcionamiento normal.

Descripción detallada

Por motivos de claridad, elementos iguales se han designado mediante referencias iguales en las diferentes figuras.

Ahora va a describirse la presente invención para un lector, por ejemplo, un lector de tarjetas, utilizado, por ejemplo, para la realización de operaciones de pago. No obstante, es evidente que la presente invención puede aplicarse a cualquier sistema electrónico para el que es deseable que se detecte un intento de sustitución no autorizada de una parte de carcasa original del sistema electrónico por una parte de carcasa de reemplazo.

La figura 1 representa de manera esquemática un ejemplo de realización de un lector de tarjeta 10. El lector 10 comprende una carcasa 12 constituida por una parte superior de carcasa 14 y por una parte inferior de carcasa 16. Están previstas aberturas 17 a nivel de la parte superior de carcasa 14 para una pantalla de visualización 18 y teclas de un teclado 20. Además, está prevista una abertura, no representada, en la carcasa 12 para permitir la introducción de tarjetas.

La figura 2 es una sección esquemática del lector 10 de la figura 1. La carcasa 12 contiene un circuito impreso 22, denominado placa base, fijado a la parte inferior de carcasa 16 y en el que se conectan los componentes electrónicos del lector 10. En particular, un circuito integrado 24, denominado criptoprocesador, se conecta a la placa base 22 y se encarga de la manipulación de datos sensibles utilizados por el lector 10. A modo de ejemplo, los datos sensibles pueden corresponder a claves utilizadas durante operaciones de encriptado puestas en práctica por el criptoprocesador 24. También puede tratarse de los códigos confidenciales de las tarjetas utilizadas con el lector 10.

El criptoprocesador 24 también se encarga de la detección de intentos de acceso no autorizado al lector 10. Para ello, el criptoprocesador 24 está unido a dispositivos de seguridad, no representados, adaptados para proporcionar al criptoprocesador 24 señales de alarma en el caso de que se produzca un intento de acceso no autorizado. Los dispositivos de seguridad pueden comprender circuitos de seguridad de tipo enrejado y/o teclas de teclado falsas o cualquier otro dispositivo de detección de intento de intrusión. En el caso de que el criptoprocesador 24 detecte que se produce un intento de acceso no autorizado, pasa a un modo de desactivación en el que interrumpe el funcionamiento del lector 10 y borra los datos sensibles.

Los componentes del lector, incluido el criptoprocesador 24, se alimentan a partir de una misma fuente de alimentación general, por ejemplo, la alimentación de la red. El lector 10 puede comprender una fuente de alimentación de emergencia, que corresponde, por ejemplo, a una batería de litio, que garantiza la alimentación del criptoprocesador 24 en el caso de que la fuente de alimentación general no esté presente. Cuando se alimenta mediante la fuente de alimentación de emergencia, el criptoprocesador 24 funciona en un modo degradado en el que solamente garantiza la detección de intentos de acceso no autorizado.

La presente invención prevé asociar un chip de circuito integrado 26 a cada elemento del lector 10 para el que se desea que se detecte un intento de sustitución no autorizada. En el presente ejemplo, el chip 26 se fija a la parte superior de carcasa 14. Por ejemplo, se adhiere a la parte superior de carcasa 14, o se sobremoldea a la misma, de manera que no sea posible retirar el chip 26 de la parte superior de carcasa 14 sin interrumpir el funcionamiento del chip 26.

El chip 26 está unido al criptoprocesador 24 con el fin de permitir el intercambio de señales entre el chip 26 y el criptoprocesador 24. La alimentación del chip 26 puede garantizarse por el criptoprocesador 24. A modo de ejemplo, el chip 26 puede estar unido al criptoprocesador 24 mediante una conexión por cable 28 de manera que el menor desplazamiento de la parte superior de carcasa 14 con respecto a la parte inferior de carcasa 16 conlleva la interrupción de la conexión eléctrica entre el chip 26 y el criptoprocesador 24. A modo de variante, la conexión entre el criptoprocesador 24 y el chip 26 puede realizarse mediante cualquier medio adaptado. A modo de ejemplo, puede proporcionarse una conexión sin cable, por ejemplo, una conexión capacitiva.

El chip 26 comprende una memoria en la que se almacena un número de serie N que corresponde por ejemplo a una señal binaria codificada en varias decenas de bits, por ejemplo 32 bits. Además, se almacena una clave K_f a nivel del chip 26. La clave K_f corresponde, por ejemplo, a una señal binaria codificada en varias decenas de bits, por ejemplo, 64 bits. La clave K_f se almacena a nivel del chip 26 mediante cualquier procedimiento habitual con el fin de no poder leerse por un usuario que tiene acceso al chip 26. El número de serie N y la clave K_f se almacenan en el

chip 26 durante su fabricación y permanecen memorizados incluso cuando el chip 26 no se alimenta.

El chip 26 está adaptado para recibir una señal R, denominada a continuación alea, proporcionada por el criptoprocesador 24. La alea R es una señal binaria codificada en varias decenas de bits, por ejemplo, de 64 bits a 128 bits. El chip 26 está adaptado para proporcionar al criptoprocesador 24 una señal binaria S, denominada a continuación firma de chip. La firma de chip S se obtiene mediante la siguiente relación:

$$S=F_1(N,\ R,\ K_f) \qquad (1)$$

en la que F_1 es una función de encriptado puesta en práctica por el chip 26 y corresponde, por ejemplo, a una función de resumen criptográfica de tipo SHA (acrónimo del término en inglés Secure Hash Algorithm). La función de encriptado F_1 puede ponerse en práctica mediante un medio material (por cableado) o mediante un programa informático.

El criptoprocesador 24 también está adaptado para poner en práctica la función de encriptado F_1 mediante un medio material (por cableado) o mediante un programa informático. Además, el criptoprocesador 24 está adaptado para proporcionar nuevos valores de la alea R según un proceso aleatorio o pseudoaleatorio. La provisión de la alea R puede realizarse mediante un medio material (por cableado) o mediante un programa informático.

El lector 10 está adaptado para intercambiar señales con una herramienta de activación (no representada) exterior al lector 10. La herramienta de activación puede corresponder a un sistema electrónico manipulado por un operario o a uno o varios ordenadores separados del lector 10 y a los que puede unirse el lector 10 por medio de una red de comunicación. Una clave base K_m se almacena a nivel de la herramienta de activación. La herramienta de activación está adaptada para poner en práctica una función de encriptado F_2, por ejemplo, de tipo triple DES (siendo DES un acrónimo del término en ingles Data Encryption Standard). La clave K_f del chip 26 se define de manera que puede determinarse por la herramienta de activación a partir del número de serie N y de la clave base K_m mediante la siguiente relación:

$$K_f=F_2(N,\ K_m) \qquad (2)$$

Ahora va a describirse un ejemplo de procedimiento de detección de un intento de sustitución de la pieza a la que se fija el chip 26, es decir, la parte superior de carcasa 14 en el presente ejemplo de realización. El procedimiento comprende una fase de activación y una fase de funcionamiento normal.

La figura 3 representa un ejemplo de etapas sucesivas de la fase de activación que se produce la primera vez que se une el criptoprocesador 24 al chip 26. La fase de activación puede comenzar por la conexión del criptoprocesador 24 desactivado a la herramienta de activación.

En la etapa 30, tras una petición del criptoprocesador 24, el chip 26 transmite al criptoprocesador 24 el número de serie N. Entonces, el número de serie N se memoriza a nivel del criptoprocesador 24. El procedimiento avanza a la etapa 31.

En la etapa 31, el criptoprocesador 24 proporciona el número de serie N a la herramienta de activación. El procedimiento avanza a la etapa 32.

En la etapa 32, la herramienta de activación determina la clave K_f asociada al chip 26 a partir de la relación (2) descrita anteriormente. El procedimiento avanza a la etapa 33.

En la etapa 33, la herramienta de activación proporciona la clave K_f al criptoprocesador 24. Entonces, la clave K_f se memoriza a nivel del criptoprocesador 24. La clave K_f forma parte de los datos sensibles que se borran cuando el criptoprocesador 24 detecta un intento de acceso no autorizado al lector 10.

La figura 4 representa un ejemplo de etapas sucesivas de la fase de funcionamiento normal del procedimiento de detección de sustitución. La fase de funcionamiento normal se pone en práctica de modo idéntico ya se alimente el criptoprocesador 24 por la fuente de alimentación general del lector 10 o por la fuente de alimentación de emergencia. En la fase de funcionamiento normal, se intercambian señales entre el criptoprocesador 24 y el lector 26 de modo cíclico mientras que el criptoprocesador 24 no detecte ningún intento de sustitución no autorizada.

En la etapa 34, el criptoprocesador 24 determina un nuevo valor aleatorio o pseudoaleatorio de la alea R. La señal R se proporciona al chip 26 mediante la conexión 28. El procedimiento avanza a la etapa 36. A modo de ejemplo, puede marcarse el ritmo del criptoprocesador 24 mediante una señal de reloj a 100 kHz. Los nuevos valores de la alea R pueden emitirse mediante el criptoprocesador 24 a una frecuencia de 1 a 10 Hz, proporcionándose entonces los bits de la alea R a una frecuencia de 1 a 10 kHz.

En la etapa 36, el criptoprocesador 24 determina una señal S', denominada firma de criptoprocesador, que corresponde a una señal binaria codificada en varias decenas de bits y que se determina a partir del número de serie N, de la clave K_f y de la alea R según la siguiente relación:

$$S' = F_1 (N, K_f, R) \quad (3)$$

En paralelo, el chip 26 determina la firma de chip S según la relación (1) descrita anteriormente. El procedimiento avanza a la etapa 38.

En la etapa 38, el chip 26 proporciona la firma de chip S al criptoprocesador 24 mediante la conexión por cable 28. El procedimiento avanza a la etapa 40.

En la etapa 40, el criptoprocesador 24 compara las firmas S y S'. En el caso de que la firma de chip S sea igual a la firma de criptoprocesador S', esto significa que la parte superior de carcasa 14 a la que está conectada el chip 26 es auténtica. Entonces, el procedimiento vuelve a comenzar en la etapa 34 mediante la determinación de un nuevo valor de la alea R mediante el criptoprocesador 24.

Si en la etapa 40, el criptoprocesador 24 determina que la firma de chip S es diferente de la firma de criptoprocesador S', el procedimiento avanza a la etapa 42.

En la etapa 42, el criptoprocesador 24 ha detectado que se ha producido un intento de sustitución no autorizada. Entonces pasa, tal como durante la detección de un intento de acceso no autorizado, al modo de desactivación en el que interrumpe el funcionamiento del lector 10. Además, se borra el conjunto de los datos sensibles. Por ello, se borra la clave K_f almacenada a nivel del criptoprocesador 24 en la fase de activación. La detención del modo de desactivación del criptoprocesador 24 y la reanudación de un funcionamiento normal necesita la intervención de un operario autorizado y comienza por una nueva fase de activación con la herramienta de activación que dispone de K_m.

En la etapa 40, una diferencia entre las firmas S y S' puede tener motivos diferentes. Según un primer ejemplo, la ausencia de transmisión de la firma S por el chip 26 conlleva la detección de un intento de sustitución por el criptoprocesador 24. Es el caso, por ejemplo, cuando se interrumpe la conexión 28 entre el chip 26 y el criptoprocesador 24. El chip 26 desempeña entonces el papel de un dispositivo de seguridad habitual. Según un segundo ejemplo, una diferencia entre las firmas S y S' puede tener como origen el reemplazo de la parte superior de carcasa 14 por una parte superior de carcasa que proviene de otro lector. En este caso, al ser diferente el número de serie del chip de la parte superior de carcasa sustituida del número de serie del chip de la parte superior de carcasa original, la clave K_f del chip es diferente de la clave K_f del criptoprocesador 24 de manera que la firma S proporcionada por el chip de la parte de carcasa sustituida es diferente de la firma S' determinada por el criptoprocesador 24.

De modo ventajoso, la función de encriptado F_1, puesta en práctica a nivel del criptoprocesador 24 y del chip 26, puede implementarse mediante un medio material (por cableado). La determinación de las firmas S y S' puede realizarse entonces con un número reducido de ciclos de reloj y para un bajo consumo. Esto es ventajoso en el caso de que el criptoprocesador 24 solamente se alimente por la fuente de alimentación de emergencia. Además, de modo ventajoso, siendo la alea R transmitida por el criptoprocesador 24 al chip 26 una señal aleatoria o pseudoaleatoria, la secuencia de señales intercambiadas entre el criptoprocesador 24 y el chip 26 no puede conocerse de antemano por terceros que tuvieran acceso a estas señales.

A modo de variante, la conexión entre el criptoprocesador 24 y el chip 26 puede ser cualquier tipo de conexión a distancia. Se trata, por ejemplo, de una conexión a distancia mediante antena, que pone en práctica un protocolo de intercambio de datos de tipo identificación por radiofrecuencia o RFID (acrónimo del término en inglés Radio Frequency Identification). No obstante, es deseable que la conexión entre el chip 26 y el criptoprocesador 24 se interrumpa en el momento en que la parte superior de carcasa 14, a la que está fijado el chip 26, se desplace con respecto a la parte inferior de carcasa 16. Por tanto, es necesario proporcionar una conexión por radiofrecuencia que tenga un alcance reducido al tiempo que garantiza una transmisión conveniente de las señales entre el chip 26 y el criptoprocesador 24 en funcionamiento normal.

Se han descrito modos de realización particulares de la presente invención. Diversas variantes y modificaciones resultarán evidentes para el experto en la técnica. En particular, aunque la invención se ha descrito en el caso en el que el chip 26 está fijado a la parte superior de carcasa 14 y el criptoprocesador 24 está fijado a la parte inferior de carcasa 16, el chip 26 y el criptoprocesador 24 pueden fijarse a otros elementos del lector 10. En particular, el chip 26 puede fijarse a una membrana que forma el teclado 20.

REIVINDICACIONES

1. Lector de tarjetas (10) que comprende una carcasa (12) constituida al menos por una primera parte de carcasa (14) unida a una segunda parte de carcasa (16), una pantalla de visualización (18), un teclado (20) que comprende teclas, comprendiendo la primera parte de carcasa aberturas (17) para la pantalla de visualización y las teclas, comprendiendo la carcasa un circuito impreso (22) fijado a la segunda parte de carcasa y un dispositivo de detección de la sustitución de la primera parte de carcasa (14), estando el dispositivo **caracterizado por que** comprende:

un primer circuito integrado (26) fijado a la primera parte de carcasa; y
un segundo circuito integrado (24) fijado al circuito impreso y adaptado para transmitir al primer circuito integrado señales digitales sucesivas aleatorias o pseudoaleatorias (R), estando el primer circuito integrado adaptado para reenviar al segundo circuito integrado, para cada señal digital, una primera firma encriptada (S) a partir de dicha señal digital, estando el segundo circuito integrado adaptado para determinar una segunda firma encriptada (S') a partir de dicha señal digital y para detectar una sustitución de la primera parte de carcasa si las firmas encriptadas primera y segunda son diferentes.

2. Lector de tarjetas según la reivindicación 1, en el que el primer circuito integrado (26) comprende una primera memoria en la que se almacenan un número de identificación (N) y una primera clave (K_f) y en el que el segundo circuito integrado (24) comprende una segunda memoria en la que se almacena una segunda clave (K_f), estando el primer circuito integrado adaptado para transmitir el número de identificación al segundo circuito integrado, estando el segundo circuito integrado adaptado para transmitir el número de identificación a una herramienta de activación exterior al lector (10) y para recibir la segunda clave, igual a la primera clave, determinada por la herramienta de activación mediante una primera función de encriptado a partir del número de identificación y de una tercera clave (K_m), estando el primer circuito integrado adaptado para determinar, para cada señal digital, la primera firma encriptada (S) mediante una segunda función de encriptado a partir de dicha señal digital y de la primera clave, estando el segundo circuito integrado adaptado para determinar la segunda firma encriptada (S') mediante la segunda función de encriptado a partir de dicha señal digital y de la segunda clave.

3. Lector de tarjetas según las reivindicaciones 1 o 2, en el que el primer circuito integrado (26) está conectado al segundo circuito integrado (24) mediante una conexión por cable (28).

4. Lector de tarjetas según las reivindicaciones 1 o 2, en el que el primer circuito integrado (26) está conectado al segundo circuito integrado (24) mediante una conexión capacitiva.

5. Procedimiento de detección de la sustitución de una primera parte de carcasa (14) de un lector de tarjetas (10) que comprende, además, una segunda parte de carcasa (16) unida a la primera parte de carcasa, formando la primera parte de carcasa y la segunda parte de carcasa una carcasa, comprendiendo el lector de tarjetas, además, un pantalla de visualización (18), un teclado (20) que comprende teclas, comprendiendo la primera parte de carcasa aberturas (17) para la pantalla de visualización y las teclas, comprendiendo la carcasa un circuito impreso (22) fijado a la segunda parte de carcasa, estando el procedimiento **caracterizado por que** comprende las siguientes etapas:

proporcionar un primer circuito integrado (26) fijado a la primera parte de carcasa y un segundo circuito integrado (24) fijado al circuito impreso;
hacer que el segundo circuito integrado transmita al primer circuito integrado señales digitales sucesivas aleatorias o pseudoaleatorias (R);
hacer que el primer circuito integrado reenvíe al segundo circuito integrado, para cada señal digital, una primera firma encriptada (S) a partir de dicha señal digital; y
hacer que el segundo circuito integrado determine una segunda firma encriptada (S') a partir de dicha señal digital y detecte una sustitución de la primera parte de carcasa si las firmas encriptadas primera y segunda son diferentes.

6. Procedimiento de detección según la reivindicación 5, que comprende las siguientes etapas:

a) almacenar en el primer circuito integrado (26) un número de identificación (N) y una primera clave (K_f) que no es accesible desde el exterior del primer circuito integrado;
b) hacer que, en una fase de activación, el primer circuito integrado transmita el número de identificación al segundo circuito integrado (24);
c) hacer que, en la fase de activación, el segundo circuito integrado transmita el número de identificación a una herramienta de activación exterior al lector (10);
d) hacer que, en la fase de activación, la herramienta de activación determine una segunda clave (K_f), igual a la primera clave, mediante una primera función de encriptado a partir del número de identificación y de una tercera clave (K_m);

e) hacer que, en la fase de activación, la herramienta de activación transmita la segunda clave al segundo circuito integrado;

f) hacer que, en una fase de funcionamiento normal, el segundo circuito integrado transmita al primer circuito integrado las señales digitales sucesivas aleatorias o pseudoaleatorias (R);

g) hacer que, en la fase de funcionamiento normal, el primer circuito integrado reenvíe al segundo circuito integrado, para cada señal digital, la primera firma encriptada (S) determinada mediante una segunda función de encriptado a partir de dicha señal digital y de la primera clave; y

h) hacer que, en la fase de funcionamiento normal, el segundo circuito integrado determine la segunda firma encriptada (S') mediante la segunda función de encriptado a partir de dicha señal digital y de la segunda clave, y detecte una sustitución de la primera parte de carcasa si las firmas encriptadas primera y segunda son diferentes.

7. Procedimiento según la reivindicación 6, que comprende además la etapa que consiste en hacer que el segundo circuito integrado (24) borre la segunda clave (K_f) en el caso de que las firmas encriptadas primera y segunda (S, S') sean diferentes en la etapa h), necesitando entonces la reutilización del lector (10) de nuevo la puesta en práctica de las etapas b) a e).

8. Procedimiento según la reivindicación 6 o 7, en el que la primera función de encriptado es una función de tipo DES o triple DES y/o en el que la segunda función de encriptado es una función de tipo SHA.

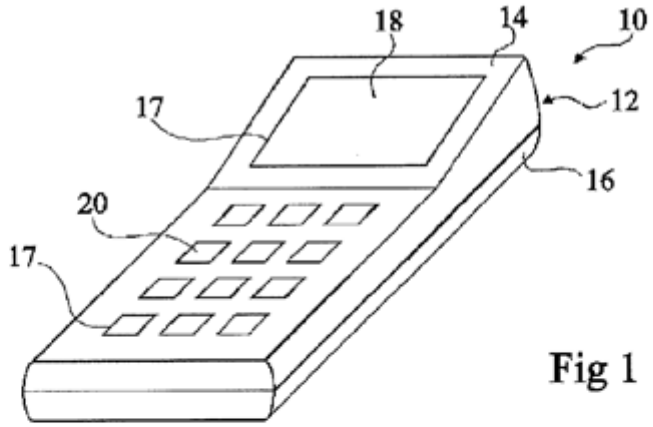

Fig 1

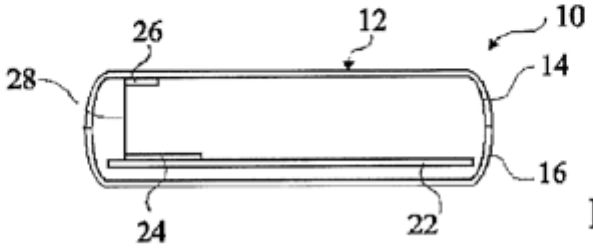

Fig 2

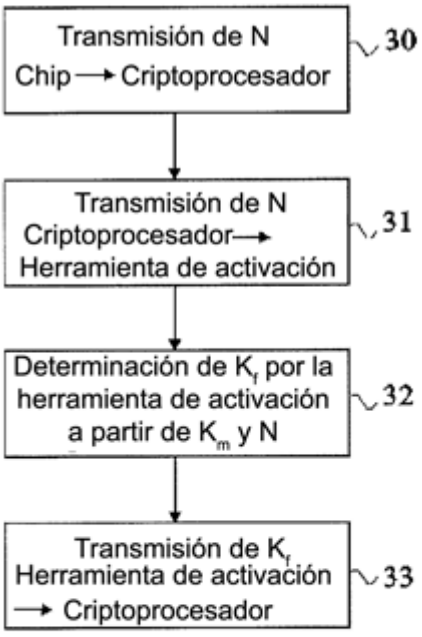

Fig 3

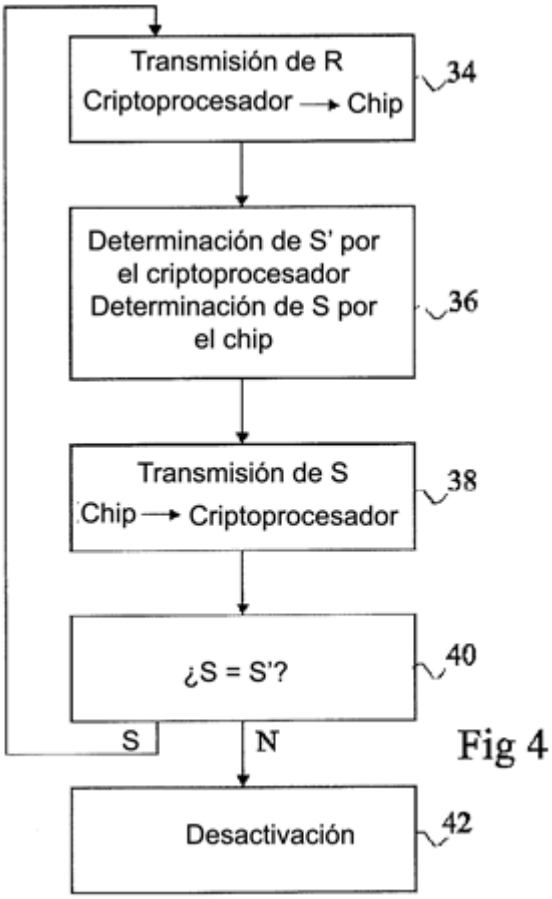

Fig 4