(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 590 658**

(51) Int. CI.:

G06K 19/073 (2006.01)
G06K 19/07 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **24.06.2010 PCT/EP2010/058965**

(87) Fecha y número de publicación internacional: **29.12.2010 WO10149730**

(96) Fecha de presentación y número de la solicitud europea: **24.06.2010 E 10726502 (7)**

(97) Fecha y número de publicación de la concesión europea: **10.08.2016 EP 2446399**

(54) Título: **Procedimiento, soporte de datos portátil, dispositivo de autorización y sistema para autorizar una transacción**

(30) Prioridad:

25.06.2009 DE 102009030456

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.11.2016

(73) Titular/es:

GIESECKE & DEVRIENT GMBH (100.0%)
Prinzregentenstrasse 159
81677 München, DE

(72) Inventor/es:

FINKENZELLER, KLAUS y
RANKL, WOLFGANG

(74) Agente/Representante:

ARPE FERNÁNDEZ, Manuel

DESCRIPCIÓN

Procedimiento, soporte de datos portátil, dispositivo de autorización y sistema para autorizar una transacción

[0001] La invención se refiere a un procedimiento, un soporte de datos portátil, un dispositivo de autorización y un sistema para autorizar una transacción por medio de sensores de aceleración.

[0002] En el sentido de la solicitud, se entiende por sensor de aceleración un sensor que detecta la aceleración de un cuerpo, por ejemplo por el método de determinar la fuerza de inercia que actúa sobre una masa de ensayo. En el estado actual de la técnica se conocen sensores de aceleración y sensores de rotación basados en semiconductores. Un sensor de aceleración de este tipo mide aceleraciones y movimientos propios lineales y a continuación, por medio del resultado de medición, dispara procesos de conmutación en función del movimiento propio en el espacio. Un sensor de rotación detecta el movimiento giratorio propio alrededor de un eje. En este contexto pueden mencionarse, solamente a modo de ejemplo, el sensor de rotación de un eje LY530AL y el sensor de rotación de 3 ejes LIS344ALH de la firma ST Microelectronics como componentes electrónicos.

[0003] La posibilidad de integrar un sensor de movimiento en un soporte de datos portátil, especialmente en forma de una tarjeta chip, se conoce por el documento de publicación DE 102 48 389. El sensor de movimiento se emplea aquí exclusivamente para registrar un trazo.

[0004] Un problema de los soportes de datos portátiles consiste en que éstos pueden leerse a distancia sin que lo advierta el poseedor, por ejemplo a través de un bolsillo, mediante una interfaz sin contacto. En este contexto es particularmente crítica la posibilidad de un *relay-attack* (ataque de retransmisión), ya que aquí se establece, mediante un radioenlace, una conexión con un equipo lector "real". Un ataque de este tipo se describe por ejemplo en el capítulo 8 del libro "Handbuch für Chipkarten" de Rankl, Effing, o en el capítulo 8 del libro "RFID-Handbuch" de Finkenzeller. El *relay-attack* se denomina en la bibliografía también ataque de retransmisión o ataque *ghost-and-leech*.

[0005] Según el estado actual de la técnica, para evitar este problema se propone por ejemplo equipar los soportes de datos portátiles con un pulsador. Sin embargo, la instalación de un pulsador en una tarjeta chip o en un testigo (*token*) de seguridad es muy costosa y ocasiona grandes gastos de producción. Como componente mecánico, un pulsador está además sometido siempre a un desgaste y puede también causar dificultades por problemas de contacto.

[0006] Por la publicación "*RFIDs and Secret Handshakes: Defending Against Ghost-and-Leech Attacks and Unauthorized Reads with Context-Aware Communications*", presentada en la 15 ACM Conference of Computer and Communications Security 2008, páginas 479 a 490, se conoce la posibilidad de registrar gestos característicos mediante un sensor de aceleración para autorizar el acceso a un soporte de datos.

[0007] Desde el punto de vista actual, esta utilización de gestos no parece ser practicable. En los soportes de datos portátiles pasivos, que no están equipados con una batería, la zona para la realización de gestos es aproximadamente igual de grande que la zona en la que en realidad puede existir una comunicación entre el soporte de datos portátil y un equipo terminal, en particular un equipo lector, ya que el soporte de datos dispone sólo en esta zona de energía para realizar sus mediciones y cálculos. Si se utilizan equipos lectores según ISO/IEC 14443 con un alcance típico de por ejemplo 10 cm, el espacio libre de movimiento para realizar un gesto en la zona de lectura de una tarjeta es por lo tanto muy limitado. A esto se añade un posible umbral de inhibición relativo a la realización de gestos complejos con el soporte de datos portátil en un equipo terminal, por ejemplo un terminal punto de venta o una máquina expendedora de billetes, en público.

[0008] Por la memoria de patente EP 1745420 B1 se conoce por otra parte el método de configurar el cuerpo de una tarjeta chip con un material no homogéneo. Se evalúan las oscilaciones propias características que se producen a causa del material de la tarjeta al excitar la tarjeta chip y de este modo se identifica la tarjeta chip. Este procedimiento parece muy costoso, ya que cada cuerpo de tarjeta debe ser individual.

[0009] El documento WO 2008/092527 A1 se refiere a un procedimiento para hacer posible un acceso a datos almacenados en un soporte de datos móvil, como por ejemplo una tarjeta inteligente (*smartcard*). Para ello, el dispositivo móvil comprueba si un patrón de señales, generado por un sensor de aceleración, coincide con un patrón de referencia predefinido almacenado en el soporte de datos móvil.

[0010] Del documento US 2009/065575 A1 se desprende un dispositivo con el que es posible autorizar pagos sin contacto a corta distancia. Para ello se evalúan un movimiento y una posición y, en función del resultado de la evaluación, una transacción se autoriza o no.

[0011] Por consiguiente, el objetivo de la presente invención es mostrar un procedimiento, un sistema, un soporte de datos portátil y un dispositivo de autorización con los que la autorización de una transacción entre un soporte de datos portátil y un equipo terminal se realice de un modo más económico, más seguro y más sencillo.

[0012] En el sentido de la solicitud se entiende por transacción una secuencia lógica de operaciones. Una transacción es por ejemplo un proceso de pago entre un soporte de datos portátil y un equipo terminal a través de una interfaz sin contacto. Como alternativa, una transacción es también la lectura de información de nivel crítico de seguridad, por ejemplo de números PIN, de datos personales o de secretos generales, como números TAN, contraseñas y otros similares.

[0013] El objetivo se logra con todas las reivindicaciones independientes. En las reivindicaciones respectivamente dependientes se describen configuraciones ventajosas.

[0014] Según la invención, el objetivo se logra mediante un procedimiento para autorizar una transacción entre un soporte de datos portátil y un equipo terminal, en el que en primer lugar se introduce el soporte de datos portátil en un campo electromagnético. El campo EM lo genera el equipo terminal. El campo EM sirve de suministro de energía

y para la activación del soporte de datos portátil. De momento no se autoriza ninguna transacción entre el soporte de datos portátil y el equipo terminal que incluya información o datos relevantes para la seguridad. A continuación se excita el soporte de datos portátil mediante una oscilación mecánica. Estas oscilaciones mecánicas se registran luego en el soporte de datos portátil mediante un sensor de aceleración. A continuación se evalúa o se analiza la señal de salida del sensor de aceleración con respecto a propiedades características de la oscilación mecánica. En cuanto se detecta una propiedad característica de la oscilación por medio de la evaluación de la señal de salida, se autoriza la transacción mediante el soporte de datos portátil.

[0015] En el sentido de la solicitud, un soporte de datos portátil no está predefinido en principio en cuanto a su forma y configuración. Por soporte de datos portátil debe entenderse en particular una tarjeta chip, una tarjeta inteligente o en general un testigo de seguridad, por ejemplo con función de identificación. También son concebibles configuraciones alternativas, por ejemplo como tarjeta de memoria de gran capacidad, por ejemplo una tarjeta µSD. En el sentido de la solicitud se entiende además un pasaporte electrónico o un medio de identificación de otro tipo que contenga información de nivel crítico de seguridad que no haya de ser extraída en general del soporte de datos. En un sentido adicional, el soporte de datos portátil es un teléfono móvil con el que puedan llevarse a cabo transacciones, por ejemplo mediante una comunicación de campo próximo con un equipo terminal. El teléfono móvil como soporte de datos portátil presenta en este caso una interfaz de comunicación de campo próximo.

[0016] Por equipo terminal debe entenderse todo tipo de equipo de comunicación con el que pueda comunicarse el soporte de datos portátil, en particular sin contacto. Una comunicación se realiza por ejemplo con un equipo lector, denominado también terminal, estandarizado según ISO/IEC 14443. El equipo terminal es por ejemplo un terminal punto de venta o una máquina expendedora de billetes con una interfaz de comunicación de campo próximo.

[0017] Una oscilación describe fundamentalmente el curso periódico de un cambio de estado de una magnitud física. Se entiende como un tipo de oscilación mecánica por ejemplo una vibración, una colocación abrupta o el frotamiento/el combado del soporte de datos.

[0018] Mediante el procedimiento según la invención se impide de un modo sencillo que un soporte de datos portátil lleve a cabo una transacción con un equipo terminal sin haberse autorizado antes la transacción. De este modo se impiden por ejemplo ataques de retransmisión (*relay-attacks*) o transacciones no deseadas por el usuario del soporte de datos portátil.

[0019] En una configuración ventajosa, el soporte de datos portátil se pone en oscilación propia mediante la excitación mecánica. A continuación se registra esta oscilación propia del soporte de datos en forma de aceleración mediante el sensor de aceleración y se evalúa la misma. La ventaja de esta configuración consiste en que con una excitación mínima puede ser bien evaluada una aceleración del soporte de datos.

[0020] La propiedad característica es ventajosamente la duración, la frecuencia y/o la amplitud de la oscilación mecánica. Por consiguiente, una transacción se autoriza sólo si se sobrepasa un valor nominal de la propiedad característica de la oscilación, y en caso contrario no se autoriza la transacción.

[0021] Según la invención, la excitación del soporte de datos la realiza el equipo terminal con una oscilación mecánica. Para ello se coloca el soporte de datos sobre el equipo terminal. En particular mediante un mecanismo, se hacen oscilar partes de la superficie del equipo terminal. También pueden concebirse procedimientos alternativos para hacer oscilar la superficie. Mediante esta oscilación mecánica se excita el soporte de datos portátil. El acelerómetro del soporte de datos registra estas oscilaciones mecánicas por el hecho de que el soporte de datos mismo es acelerado en al menos una dirección. Como oscilaciones mecánicas están previstas, ventajosamente, vibraciones con desviaciones en un intervalo milimétrico o sub-milimétrico. Con la colocación sobre el equipo terminal, el usuario del soporte de datos portátil participa activamente en el procedimiento de autorización de la transacción.

[0022] Se logra una configuración sencilla y por tanto ventajosa si el equipo terminal está equipado con una superficie parcial capaz de oscilar. Esta superficie parcial se hace oscilar mediante movimientos lineales o circulares, por ejemplo de un mecanismo del equipo terminal, y excita el soporte de datos portátil colocado sobre la misma. La antena del equipo terminal, que está prevista para emitir el campo electromagnético, se introduce preferentemente en o debajo de la superficie parcial capaz de oscilar del equipo terminal. De este modo no se reduce adicionalmente con el procedimiento según la invención la zona de todos modos pequeña para la comunicación entre el equipo terminal y el soporte de datos.

[0023] En una forma de realización preferida, las oscilaciones lineales o circulares del equipo terminal fluctúan en frecuencia. Como alternativa o adicionalmente están superpuestas varias oscilaciones mecánicas lineales o circulares. La fluctuación de las frecuencias y/o la superposición de oscilaciones se evalúa(n) como propiedad característica en el soporte de datos portátil. De este modo pueden realizarse distintos tipos de autorización para la comunicación entre el soporte de datos y el equipo terminal. Al mismo tiempo, también es posible una codificación correspondiente.

[0024] Mediante la emisión de oscilaciones lineales o circulares adicionales desde el equipo terminal durante la transacción pueden comunicarse diferentes mensajes de estado o informaciones de estado de la transacción, por ejemplo el final o el fallo de una transacción.

[0025] En una configuración alternativa de la invención, la excitación del soporte de datos con una oscilación mecánica se realiza depositando el soporte de datos de una manera abrupta sobre el equipo terminal. La colocación abrupta se evalúa como propiedad característica de las oscilaciones mecánicas. En particular se evalúa(n) aquí como propiedad(es) característica(s) de las oscilaciones mecánicas la aceleración propia del soporte de datos portátil antes de la colocación abrupta y/o una captación de ángulo tras la colocación abrupta.

[0026] En otra configuración alternativa, el soporte de datos portátil se excita mecánicamente moviéndolo o frotándolo contra una superficie exterior del equipo terminal. Las oscilaciones que se producen por el frotamiento se registran como aceleraciones en el soporte de datos portátil y se evalúan.

[0027] La introducción del soporte de datos portátil en un campo EM para el suministro de energía puede quedar suprimida con tal que el soporte de datos disponga de un suministro de energía propio, por ejemplo en forma de un acumulador, una batería y/o una célula fotovoltaica. En esta configuración, el campo EM para el suministro de energía es innecesario, pero la autorización de una transacción se desarrollará no obstante mediante el procedimiento según la invención para, por ejemplo, impedir la lectura de información relevante para la seguridad o de nivel crítico de seguridad del tipo descrito al principio.

[0028] También según la invención está previsto un soporte de datos portátil para la transmisión de datos con un equipo terminal, presentando el soporte de datos un dispositivo de autorización y comprendiendo el dispositivo de autorización un sensor de aceleración, que permite detectar oscilaciones mecánicas del soporte de datos, y una unidad de evaluación, que está prevista para evaluar las señales de salida del sensor de aceleración y que puede detectar oscilaciones mecánicas. Una transmisión de datos entre el soporte de datos portátil y el equipo terminal puede autorizarse en cuanto la unidad de evaluación genere una señal de autorización a partir de una característica de la oscilación mecánica necesaria para la autorización.

[0029] En el alcance de la invención se incluye además un módulo para autorizar una transacción con un equipo terminal. El módulo comprende un sensor de aceleración para registrar una oscilación mecánica, una unidad de evaluación para evaluar la oscilación mecánica registrada, evaluándose la oscilación mecánica con respecto a propiedades características, una unidad de comparación para comparar las propiedades características de la oscilación mecánica de la unidad de evaluación con un valor nominal de las propiedades características, autorizando la unidad de comparación la transacción si se sobrepasa el valor nominal de la propiedad característica y no autorizando la unidad comparación la transacción si no se alcanza el valor nominal de la propiedad característica.

[0030] El valor nominal podría estar almacenado en una memoria de datos del soporte de datos y llamarse durante la evaluación de la propiedad característica de la oscilación.

[0031] Por último, según la invención está previsto un sistema para autorizar una transacción. El sistema comprende un soporte de datos portátil, que contiene un módulo como el anteriormente descrito para autorizar una transacción con un equipo terminal, y el equipo terminal mismo, pudiendo el soporte de datos portátil excitarse con una oscilación mecánica y autorizando la unidad de comparación del módulo la transacción si se sobrepasa un valor nominal de una propiedad característica de la oscilación mecánica.

[0032] En el procedimiento según la invención resulta ventajosa la utilización de la tarjeta en la forma acostumbrada por el usuario. Para ello se utilizan componentes semiconductores, que pueden integrarse fácilmente en un módulo de hardware, por ejemplo en un módulo de chip de una tarjeta chip como soporte de datos portátil.

[0033] Se muestran:

- Figura 1, un diagrama de bloques de un soporte de datos portátil según la invención con un dispositivo de autorización para autorizar una transacción, en una vista desde arriba,
- Figura 2, un diagrama de bloques de un soporte de datos portátil según la invención de acuerdo con la figura 1, en una vista en sección,
- Figura 3, un diagrama de bloques de un sistema según la invención para autorizar una transacción,
- Figura 4, una representación a modo de croquis de una superficie parcial capaz de oscilar según la invención perteneciente a un equipo terminal con un dispositivo generador de oscilaciones,
- Figura 5, un diagrama de bloques detallado de un dispositivo de autorización según la invención para su introducción en un soporte de datos portátil según la figura 1 o 2,
- Figura 6, un diagrama tensión-tiempo, a modo de ejemplo, de las señales de salida del sensor de aceleración en las direcciones X, Y y Z al excitar el soporte de datos mediante oscilaciones mecánicas generadas por el equipo terminal,
- Figura 7, un diagrama tensión-tiempo, a modo de ejemplo, de las señales de salida del sensor de aceleración en las direcciones X, Y y Z al excitar el soporte de datos mediante una colocación abrupta del soporte de datos,
- Figura 8, señales de salida del sensor de aceleración en las direcciones X, Y y Z, a modo de ejemplo, al colocar el soporte de datos sobre una superficie inclinada 30°,
- Figura 9, diagrama amplitud-frecuencia, a modo de ejemplo, de las señales de salida del sensor de aceleración en las direcciones X, Y y Z mediante un análisis FFT (transformada rápida de Fourier) del diagrama mostrado en la figura 6,
- Figura 10, un organigrama de un procedimiento según la invención para autorizar una transacción entre un soporte de datos portátil y un equipo terminal.

[0034] En la figura 1 está representado, en una vista desde arriba, un diagrama de bloques de un soporte de datos portátil 1 según la invención, con un dispositivo de autorización 7 para autorizar una transacción. El soporte de datos portátil 1 está representado aquí en forma de una tarjeta chip, o *smartcard (tarjeta inteligente)* en inglés. Para la comunicación con un equipo terminal (aquí no representado), se ha introducido en el cuerpo del soporte de datos 1 una antena 2 para la comunicación de campo próximo, o *near field communication* (NFC) en inglés. La antena 2 está acoplada eléctricamente con unas conexiones de antena a un circuito integrado 3. Mediante el campo EM y la antena 2 se suministra energía al circuito integrado 3 y se activa éste. El circuito integrado 3 presenta el dispositivo de autorización 7. El soporte de datos portátil 1 tiene incorporados además unos sensores de aceleración 4, 5, 6. El sensor de aceleración 4 registra aquí aceleraciones en la dirección X, el sensor 5 aceleraciones en la dirección Y y el sensor de aceleración 6 en la dirección Z. Las señales de salida 4a, 5a y 6a de los sensores de aceleración 4, 5, 6 se alimentan al circuito integrado 3.

[0035] En la figura 2 está representado un diagrama de bloques del soporte de datos portátil 1 de la figura 1, en una vista en sección.

[0036] Si el soporte de datos portátil 1 según la figura 1 o 2 se introduce en un campo electromagnético o, abreviado, campo EM generado por un equipo terminal, la antena 2 toma energía del campo EM generado y pone esta energía a disposición del circuito integrado 3. Según la invención está previsto, en el caso de la entrada y permanencia del soporte de datos 1, evaluar las señales de salida 4a, 5a, 6a de los sensores de aceleración 4, 5, 6 con respecto a una propiedad característica y derivar a partir de esta evaluación la decisión de si se autoriza o no una transacción sin contacto. Por lo tanto, el circuito integrado 3 no autoriza una transacción con el equipo terminal hasta que los sensores de aceleración 4, 5, 6 registren aceleraciones en la forma y las alimenten como señales de salida 4a, 5a, 6a al circuito integrado 3, de tal manera que se haya detectado una propiedad característica de una oscilación mecánica.

[0037] Como propiedad característica que pueda llevar a la autorización de una transacción entre el equipo terminal y el soporte de datos 1, puede considerarse por ejemplo una duración T, un nivel de amplitud de las señales de salida 4a, 5a, 6a, una secuencia de una fluctuación de intensidad o una frecuencia especial de las aceleraciones registradas. Estas propiedades características pueden también combinarse a voluntad para una autorización necesaria.

[0038] En las figuras 1 y 2, los sensores de aceleración 4, 5, 6 se han incorporado al cuerpo del soporte de datos portátil 1 separados del circuito integrado 3. Como alternativa y preferentemente, los sensores de aceleración 4, 5, 6 están incorporados al circuito integrado 3. Como alternativa puede estar previsto sólo un sensor de aceleración o al menos un sensor de rotación (no representado en los dibujos), en lugar de los tres sensores de aceleración 4, 5, 6.

[0039] El soporte de datos 1 está constituido de tal manera que, al excitarlo mediante una oscilación mecánica, lleva a cabo una aceleración suficientemente detectable en el interior del cuerpo del soporte de datos.

[0040] En la figura 3 está representado un sistema según la invención para autorizar una transacción entre un soporte de datos portátil 1 y un equipo terminal 8. El soporte de datos 1 corresponde aquí al soporte de datos 1 descrito en las figuras 1 y 2. El equipo terminal 8, o *terminal* en inglés, no está limitado en cuanto a su función y es por ejemplo un equipo lector. El equipo terminal 8 presenta una antena 12. Así pues, mediante las antenas 2 y 12 tiene lugar una comunicación de campo próximo 9. Adicionalmente, el equipo terminal 8 presenta una superficie parcial capaz de oscilar 10. Con esta superficie parcial 10 se realizan oscilaciones mecánicas 13. La oscilación mecánica 13a la activa el equipo terminal 8 mismo. La antena 12 del equipo lector está alojada preferentemente en o debajo de la superficie parcial capaz de oscilar, por ejemplo en una disposición coaxial.

[0041] En la figura 3, la oscilación mecánica que excita el soporte de datos portátil 1 la genera el equipo terminal 8 y puede ser por ejemplo lineal o circular.

[0042] La figura 4 muestra un ejemplo para la generación de una oscilación circular de la superficie parcial 10. Con este fin, la superficie parcial 10 está suspendida de manera concéntrica en un volante de inercia 11. Un movimiento de giro 13a del volante de inercia 11 lleva a un movimiento circular de la superficie parcial 10. En la práctica, las oscilaciones tienen una amplitud en un intervalo milimétrico o sub-milimétrico. Las frecuencias de oscilación pueden estar dentro de un intervalo de unos pocos hercios hasta algunas decenas de hercios. Tales oscilaciones mecánicas son percibidas por los humanos como una vibración, similar a la alarma por vibración de un equipo de radiotelefonía móvil.

[0043] Para llevar a cabo una transacción, por ejemplo una transacción de pago o la lectura de información de nivel crítico de seguridad, está previsto que el soporte de datos 1 según la invención se deposite sobre la superficie 10 de un equipo terminal 8 según la invención. Para autorizar el intercambio de datos o la comunicación con el soporte de datos 1, está previsto generar en primer lugar una vibración en un determinado momento antes de la transacción. Esta vibración se transmite al soporte de datos 1 y se registra mediante los sensores de movimiento 4, 5, 6. El tipo de vibración, la amplitud y la frecuencia de la vibración pueden registrarse fácilmente mediante las señales de salida de sensor 4a, 5a, 6a.

[0044] En la figura 6 está representado un ejemplo de los valores de medición de sensor de una vibración circular pulsada. Las tres curvas de medición representan aquí los ejes de oscilación X, Y, Z, correspondientes a las señales 4a, 5a, 6a de los sensores de aceleración 4, 5, 6. Según la invención, está previsto que el soporte de datos 1 analice y evalúe los patrones de oscilación de las oscilaciones registradas con respecto a, al menos, una propiedad característica. Si los valores de medición se hallan dentro de un margen de tolerancia de un intervalo esperado, está previsto que se autorice la transacción prevista con el soporte de datos 1. Como alternativa, también puede autorizarse el acceso a un área de memoria seleccionada del soporte de datos 1 y/o la posterior comunicación entre el equipo terminal 8 y el soporte de datos 1. El margen de tolerancia también puede ser un umbral de valor nominal de una de las propiedades características de la oscilación, que haya de sobrepasarse para la autorización.

[0045] Una posible opción consiste en que la señal de vibración se emita también para señalar estados de funcionamiento al usuario del soporte de datos 1. Si el soporte de datos 1 se sujeta con la mano sobre un equipo terminal 8 correspondiente, las vibraciones son fáciles de percibir. Esto es ventajoso, dado que es fácil no oír una "señal de zumbido" en un entorno ruidoso, o dado que las personas ciegas no pueden ver una "señal parpadeante". Así, a la primera vibración, que lleva a la autorización de una transacción, etc., puede seguirle una segunda vibración para señalar al usuario una transacción realizada con éxito. También puede señalar al usuario que una transacción se ha realizado con éxito una especie de codificación de la vibración, por ejemplo una fluctuación de la intensidad de la vibración (rrr---rrr) en caso de una transacción realizada con éxito y una vibración más larga y de intensidad uniforme (rrrrrrrrrrrrrr) en caso de aparecer un error. La interpretación, el cálculo y la evaluación de las oscilaciones mecánicas se efectúan por ejemplo mediante un software en el circuito integrado 3.

[0046] Otra opción consiste en que el soporte de datos 1 analice del equipo terminal 8 determinados parámetros de la oscilación, en particular la frecuencia. Otra posibilidad consiste también en superponer varias frecuencias de oscilación. Tal oscilación superpuesta puede generarse muy fácilmente, por ejemplo con un sistema oscilante electromagnético.

[0047] Por medio de una FFT puede comprobarse fácilmente la aparición de las diferentes frecuencias de oscilación. En la figura 9 está representado esto a modo de ejemplo mediante las señales FFT calculadas 4c, 5c, 6c. Mediante la FFT realizada, el espectro de las señales de salida de sensor evaluadas 4b, 5b, 6b muestra, tras un análisis FFT, las distintas partes de frecuencia en las señales.

[0048] En la figura 5 está representado un diagrama de bloques detallado de un circuito integrado 3 de las figuras anteriores incorporado al soporte de datos portátil 1. En este caso, los sensores 4, 5, 6 están dispuestos también dentro del circuito integrado 3. Las señales de salida 4a, 5a, 6a de los sensores 4, 5, 6 se alimentan a la unidad de evaluación 7a. Una evaluación de las señales puede ser por ejemplo el nivel de amplitud, la duración, etc. En principio, estas señales evaluadas pueden alimentarse directamente a la unidad de comparación 7c, para, en esta última, compararlas en caso dado con un valor nominal almacenado en una memoria de valor nominal 7d del soporte de datos 1. Si se sobrepasa el valor nominal, se autoriza la transacción mediante una señal de autorización 7e. Como alternativa, tal y como está representado en la figura 6, las señales evaluadas se alimentan en primer lugar a una unidad de cálculo 7b. Esta unidad de cálculo 7b calculas las señales 4c, 5c, 6c. Como cálculo está previsto por ejemplo un análisis FFT o el cálculo del ángulo estático del soporte de datos a partir de las señales evaluadas 4b, 5b, 6b.

[0049] En una segunda forma de realización de la invención está previsto que la excitación del soporte de datos 1 no se realice mediante oscilaciones mecánicas generadas por el equipo terminal. El soporte de datos 1 puede excitarse por ejemplo colocándolo de manera abrupta sobre una superficie, por ejemplo una superficie cerca de la antena 12, del equipo terminal 8 y dejándolo en la misma durante la transacción. Al colocar, sobreponer o hacer chocar de manera abrupta el soporte de datos 1 se producen grandes valores de aceleración 21, como está representado en la figura 7. En la figura 7 puede verse también bien la aceleración propia 20 del soporte de datos 1 antes de la colocación abrupta. Mediante la unidad de cálculo 7b es posible, por ejemplo, evaluar qué ángulo estático presenta en ese momento el soporte de datos 1. La figura 8 muestra los valores de medición de un soporte de datos 1 en posición de reposo sobre una superficie inclinada 30°.

[0050] Por consiguiente, según la invención está previsto que, al entrar en la zona de comunicación de un equipo terminal 8, el soporte de datos 1 mida la aceleración y analice y evalúe los valores de medición. Tras la colocación abrupta del soporte de datos 1 sobre la superficie del equipo lector, se determina la posición estática, por ejemplo el ángulo, del soporte de datos 1, que por regla general descansa en plano sobre la superficie del equipo terminal 8. Si los valores de medición se hallan dentro de un margen de tolerancia de un intervalo esperado, está previsto que se autorice(n) la(s) transacción(es) prevista(s) con el soporte de datos 1, el acceso a un área de memoria seleccionada del soporte de datos y/o la posterior comunicación entre el equipo terminal 8 y el soporte de datos 1.

[0051] Una opción consiste en disponer la superficie de apoyo (superficie de la antena) del equipo lector en un ángulo definido, por ejemplo 30° véase la figura 8. Una vez colocado sobre la superficie del equipo terminal 8, el soporte de datos 1 puede comprobar si se cumple este ángulo dentro de unos márgenes de tolerancia definidos.

[0052] Una alternativa para la excitación del soporte de datos 1 consiste en que un usuario frote el soporte de datos 1 de un lado a otro en una superficie del equipo terminal 8. Las oscilaciones mecánicas o la aceleración propia del soporte de datos 1 que con ello se producen se registran mediante los sensores de aceleración 4, 5, 6 y se evalúan.

[0053] En la figura 10 está representado, a modo de ejemplo, un organigrama de un procedimiento según la invención para autorizar una transacción entre el equipo terminal 8 y un soporte de datos portátil 1. Mediante la puesta a disposición 14 de un campo EM por parte del equipo terminal 8 se activa eléctricamente 15 el soporte de datos portátil 1. A través de una excitación mecánica 16 mediante una oscilación mecánica, por ejemplo una vibración, una colocación abrupta con grandes valores de aceleración 20, 21 resultantes o un frotamiento mutuo de las superficies del soporte de datos 1 y el equipo terminal 8, y un subsiguiente registro 17 de la aceleración en la dirección X, Y, Z por medio de los sensores 4, 5, 6, pueden determinarse las aceleraciones a través de una evaluación y/o un cálculo 18 de las señales de salida 4a, 5a, 6a de los sensores de aceleración. En la etapa 19 se realiza la comparación de los valores de señal con respecto a propiedades características, como por ejemplo frecuencia, amplitud, duración, ángulo estático, fluctuación de frecuencia, superposición de frecuencias, partes de frecuencia u otras similares. En la etapa 22 del procedimiento se autoriza finalmente la transacción si se sobrepasa un valor nominal o si se observa un margen de tolerancia definido. Los valores nominales y el margen de tolerancia están depositados preferentemente en un área de memoria del soporte de datos 1.

[0054] El procedimiento según la invención está preferentemente implementado, al menos parcialmente, en forma de un software en el circuito integrado 3. El circuito integrado 3 ejecuta entonces las correspondientes etapas del procedimiento como etapas de programa implementadas.

[0055] Como otro caso de aplicación de la invención está prevista la realización de una transacción con un teléfono móvil apto para NFC como soporte de datos portátil. Un usuario que por ejemplo desee llevar a cabo una transacción de pago ya no tiene que confirmar ésta con el teclado de su teléfono móvil, sino que la autorización de la transacción se realiza según los objetos de la invención descritos. Excitando el teléfono móvil como soporte de datos portátil mediante una oscilación mecánica, la autorización de la transacción se realiza en cuanto se hayan registrado y evaluado propiedades características de las oscilaciones en el teléfono móvil. En esta solicitud se utilizan como sinónimos los conceptos "teléfono móvil", "PDA", "equipo de comunicación", "agenda electrónica", "calendario electrónico" y similares.

[0056] La ventaja decisiva de ambas formas de realización consiste en que los patrones de movimiento esperados del soporte de datos 1 no pueden ser aplicados de forma inadvertida por un atacante que no tenga acceso mecánico a la tarjeta, como por ejemplo en el caso de un típico *relay-attack* (ataque de retransmisión). Un atacante tampoco puede modificar de forma inadvertida la posición absoluta de la tarjeta.

Lista de números de referencia

[0057]

1	Soporte de datos portátil
2	Antena de campo próximo soporte de datos portátil
3	Circuito integrado
4	Sensor de aceleración dirección X
4a	Señal de salida de sensor de aceleración
4b	Señal de aceleración evaluada dirección X
4c	Señal de aceleración calculada dirección X
5	Sensor de aceleración dirección Y
5a	Señal de salida de sensor de aceleración
5b	Señal de aceleración evaluada dirección Y
5c	Señal de aceleración calculada dirección Y
6	Sensor de aceleración dirección Z
6a	Señal de salida de sensor de aceleración
6b	Señal de aceleración evaluada dirección Z
6c	Señal de aceleración calculada dirección Z
7	Dispositivo de autorización
7a	Unidad de evaluación
7b	Unidad de cálculo
7c	Unidad de comparación
7d	Memoria de valor nominal
7e	Señal de autorización
8	Equipo terminal, terminal
9	Comunicación de campo próximo
10	Superficie parcial capaz de oscilar
11	Volante de inercia, oscilación mecánica circular
12	Antena de campo próximo equipo terminal
13a	Oscilación mecánica equipo terminal
13b	Oscilación mecánica soporte de datos portátil
14	Puesta a disposición de campo EM por parte del equipo terminal
15	Activación eléctrica del soporte de datos portátil
16	Excitación mecánica mediante oscilación mecánica
17	Registro de la aceleración en dirección X, Y, Z
18	Evaluación de las señales de salida de sensor de aceleración
19	Comparación con respecto a propiedades características
20	Aceleración propia del soporte de datos
21	Gran aceleración del soporte de datos causada por una colocación abrupta
22	Autorización de la transacción al sobrepasarse un valor nominal

REIVINDICACIONES

1. Procedimiento para autorizar una transacción entre un soporte de datos portátil (1) y un equipo terminal (8), con las etapas de procedimiento:
a) introducción del soporte de datos portátil (1) en un campo electromagnético, generando el equipo terminal (8) el campo electromagnético y tomando el soporte de datos (1) energía del campo electromagnético para el suministro de energía del soporte de datos (1),
b) excitación del soporte de datos portátil (1) mediante una oscilación mecánica (13),
c) registro de la oscilación mecánica (13) en el soporte de datos portátil (1) mediante un sensor de aceleración (4, 5, 6),
d) evaluación de una señal de salida (4a, 5a, 6a) del sensor de aceleración (4, 5, 6) con respecto a propiedades características de la oscilación mecánica (13),
e) autorización de la transacción (7e) por parte del soporte de datos portátil (1) en cuanto se detecta una propiedad característica de la oscilación (13) mediante la evaluación de la señal de salida (4a, 5a, 6a),
caracterizado porque:
- la excitación del soporte de datos portátil (1) con una oscilación mecánica la realiza el equipo terminal (8).

2. Procedimiento según la reivindicación 1, en el que el soporte de datos portátil (1) se pone en oscilación propia mediante la excitación mecánica y esta oscilación propia se registra y se evalúa.

3. Procedimiento según la reivindicación 1 o 2, en el que como propiedad característica se evalúa la duración, la frecuencia o la amplitud de la oscilación mecánica.

4. Procedimiento según una de las reivindicaciones precedentes, en el que el equipo terminal (8) genera oscilaciones mecánicas lineales o circulares (13a) y excita mecánicamente el soporte de datos portátil (1) mediante estas oscilaciones mecánicas lineales o circulares (13a) a través de una superficie parcial capaz de oscilar (10) del equipo terminal (8).

5. Procedimiento según la reivindicación 4, en el que las oscilaciones mecánicas lineales o circulares (13a) del equipo terminal (8) fluctúan en frecuencia y la fluctuación de la frecuencia se evalúa como propiedad característica en el soporte de datos portátil (1).

6. Procedimiento según la reivindicación 4 o 5, en el que están superpuestas varias oscilaciones mecánicas lineales o circulares (13a) del equipo terminal (8) y esta superposición de oscilaciones se evalúa como propiedad característica en el soporte de datos portátil (1).

7. Procedimiento según una de las reivindicaciones 4 a 6, en el que durante la transacción se emiten oscilaciones lineales o circulares (13a) adicionales.

8. Procedimiento según una de las reivindicaciones 4 a 7, en el que la antena (12) del equipo terminal (8), para emitir el campo electromagnético, se introduce en o debajo de la superficie parcial capaz de oscilar (10) del equipo terminal (8).

9. Procedimiento según una de las reivindicaciones 4 a 8, en el que el equipo terminal (8) vibra.

10. Procedimiento para autorizar una transacción entre un soporte de datos portátil (1) y un equipo terminal (8), con las etapas de procedimiento: a) introducción del soporte de datos portátil (1) en un campo electromagnético, generando el equipo terminal (8) el campo electromagnético y tomando el soporte de datos (1) energía del campo electromagnético para el suministro de energía del soporte de datos (1), b) excitación del soporte de datos portátil (1) mediante una oscilación mecánica (13), c) registro de la oscilación mecánica (13) en el soporte de datos portátil (1) mediante un sensor de aceleración (4, 5, 6), d) evaluación de una señal de salida (4a, 5a, 6a) del sensor de aceleración (4, 5, 6) con respecto a propiedades características de la oscilación mecánica (13), e) autorización de la transacción (7e) por parte del soporte de datos portátil (1) en cuanto se detecta una propiedad característica de la oscilación (13) mediante la evaluación de la señal de salida (4a, 5a, 6a), caracterizado porque: la excitación del soporte de datos portátil se realiza con una oscilación mecánica, excitándose mecánicamente el soporte de datos portátil (1) por el método de colocarlo de manera abrupta sobre el equipo terminal (8) y evaluándose la colocación abrupta como propiedad característica de las oscilaciones mecánicas.

11. Procedimiento según la reivindicación 10, en el que como propiedad(es) característica(s) de las oscilaciones mecánicas se evalúa(n):
- la aceleración propia (20) y/o grandes valores de aceleración (21) antes de la colocación abrupta y/o
- una captación de ángulo tras la colocación abrupta.

12. Procedimiento para autorizar una transacción entre un soporte de datos portátil (1) y un equipo terminal (8), con las etapas de procedimiento: a) introducción del soporte de datos portátil (1) en un campo electromagnético, generando el equipo terminal (8) el campo electromagnético y tomando el soporte de datos (1) energía del campo

electromagnético para el suministro de energía del soporte de datos (1), b) excitación del soporte de datos portátil (1) mediante una oscilación mecánica (13), c) registro de la oscilación mecánica (13) en el soporte de datos portátil (1) mediante un sensor de aceleración (4, 5, 6), d) evaluación de una señal de salida (4a, 5a, 6a) del sensor de aceleración (4, 5, 6) con respecto a propiedades características de la oscilación mecánica (13), e) autorización de la transacción (7e) por parte del soporte de datos portátil (1) en cuanto se detecta una propiedad característica de la oscilación (13) mediante la evaluación de la señal de salida (4a, 5a, 6a), caracterizado porque: la excitación del soporte de datos portátil se realiza con una oscilación mecánica (8), excitándose mecánicamente el soporte de datos portátil (1) por el método de frotar el soporte de datos portátil (1) en una superficie exterior del equipo terminal (8).

13. Soporte de datos portátil previsto para la transmisión de datos con un equipo terminal, presentando el soporte de datos un dispositivo de autorización y comprendiendo el dispositivo de autorización:
- un sensor de aceleración, estando unas oscilaciones mecánicas del equipo terminal configuradas para excitar el soporte de datos y pudiendo el sensor de aceleración detectar las oscilaciones mecánicas, y
- una unidad de evaluación, estando la unidad de evaluación prevista para evaluar las señales de salida del sensor de aceleración y pudiendo la unidad de evaluación detectar las oscilaciones mecánicas,
pudiendo autorizarse una transmisión de datos entre el soporte de datos portátil y el equipo terminal en cuanto la unidad de evaluación genera una señal de autorización sobre la base de una característica de la oscilación mecánica necesaria para la autorización.

14. Módulo para autorizar una transacción con un equipo terminal, que comprende:
- un sensor de aceleración para registrar una oscilación mecánica, realizándose la excitación del módulo con la oscilación mecánica mediante el equipo terminal,
- una unidad de evaluación para evaluar la oscilación mecánica registrada, evaluándose la oscilación mecánica con respecto a propiedades características,
- una unidad de comparación para comparar las propiedades características de la oscilación mecánica de la unidad de evaluación con un valor nominal de las propiedades características,
autorizando la unidad de comparación la transacción si se sobrepasa el valor nominal de la propiedad característica y
no autorizando la unidad de comparación la transacción si no se alcanza el valor nominal de la propiedad característica.

15. Sistema para autorizar una transacción, que comprende:
- un soporte de datos portátil que contiene un módulo según la reivindicación 14 y
- un equipo terminal,
pudiendo el soporte de datos portátil excitarse con una oscilación mecánica y autorizando la unidad de comparación del módulo para la autorización la transacción si se sobrepasa un valor nominal de una propiedad característica de la oscilación mecánica.

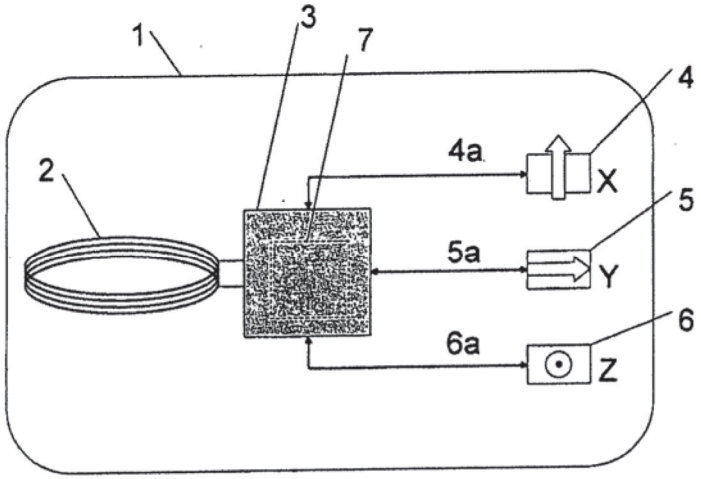


Figura 1

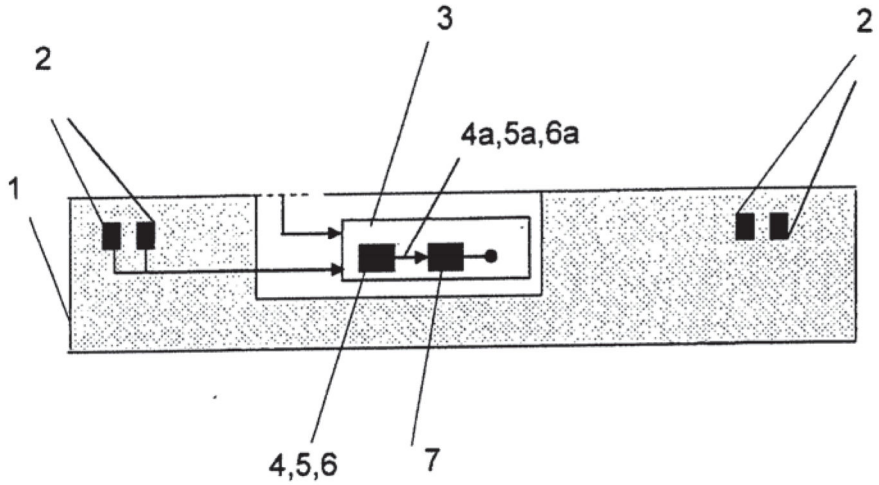


Figura 2

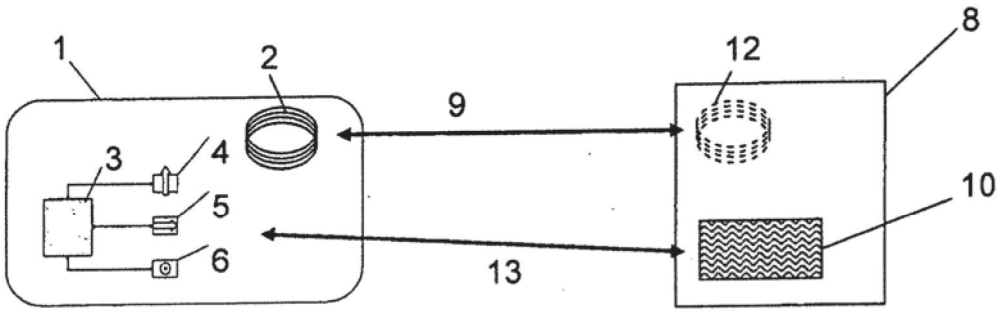


Figura 3

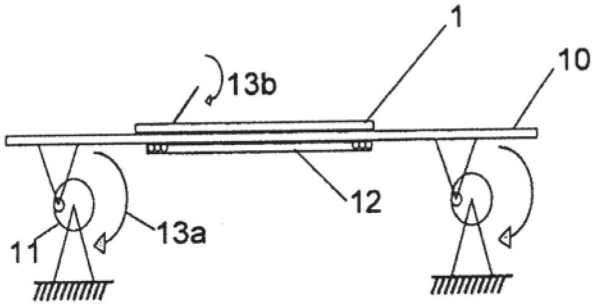


Figura 4

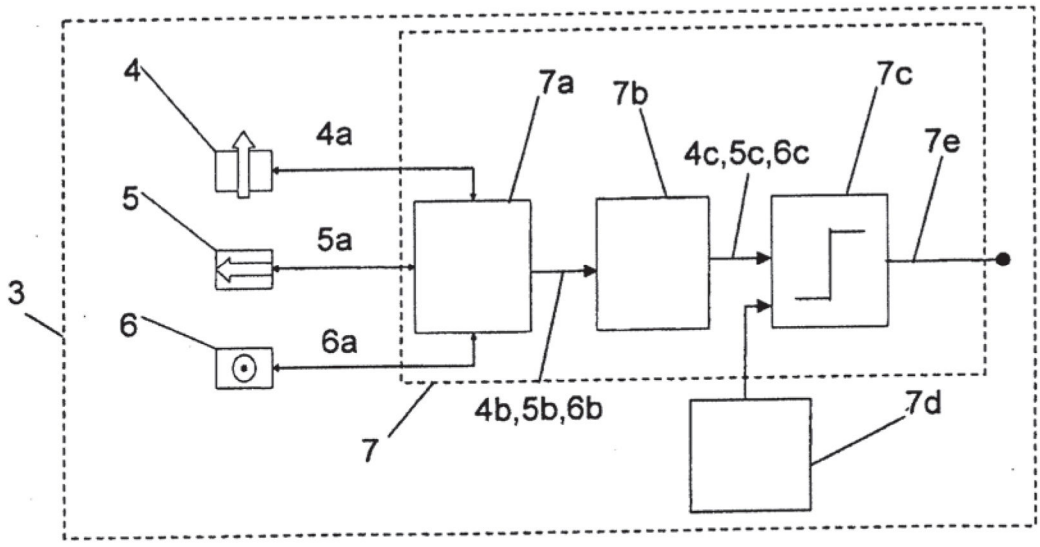
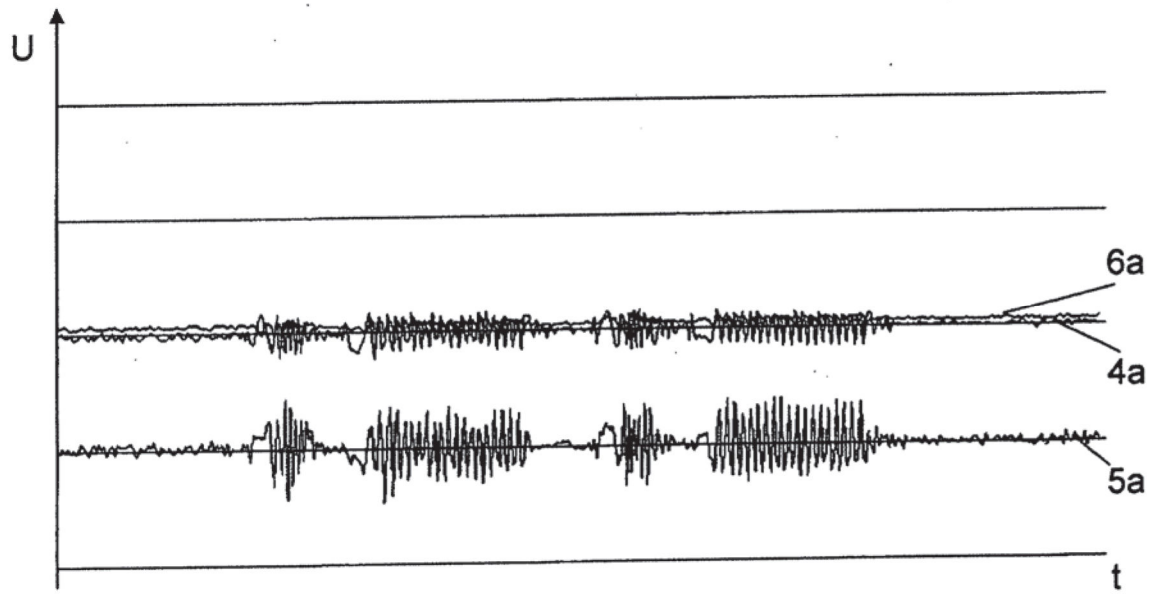
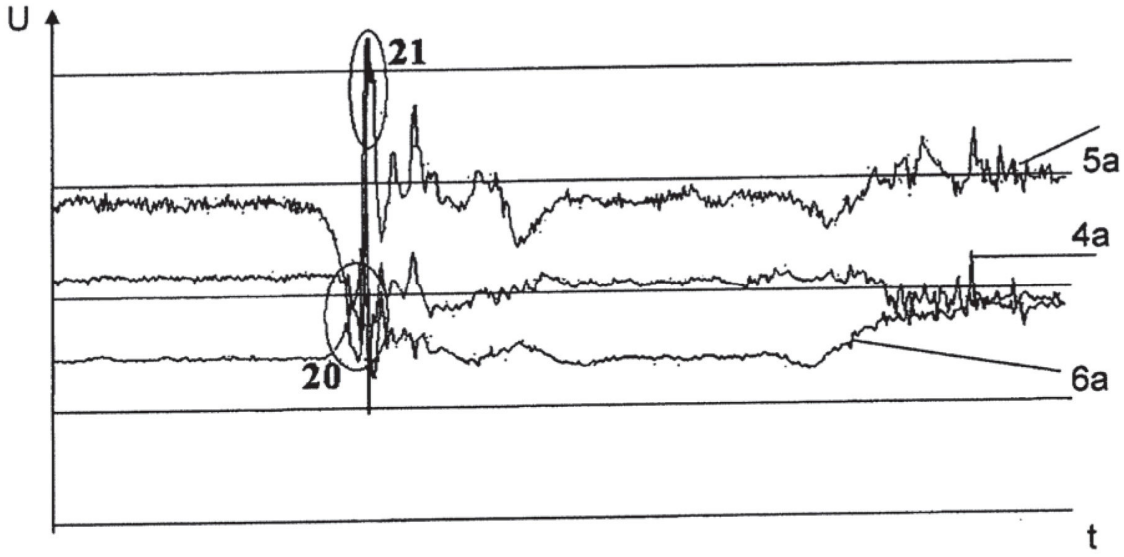


Figura 5


U
6a
4a
5a
t


U
21
5a
4a
20
6a
t

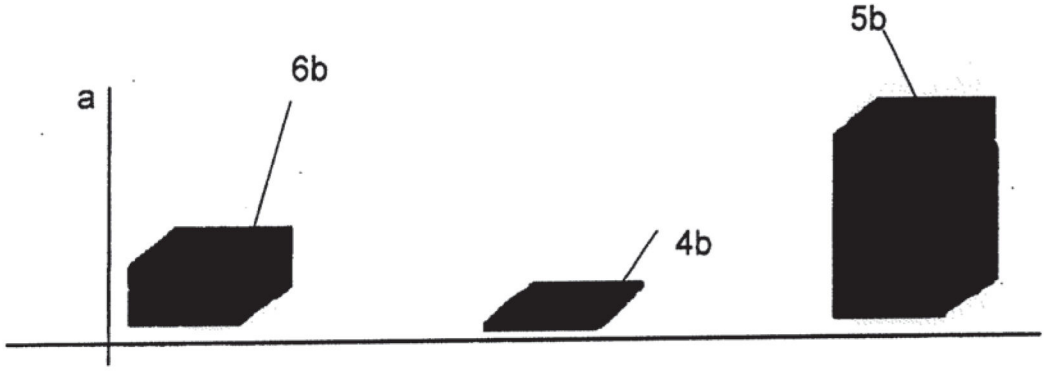


Figura 8

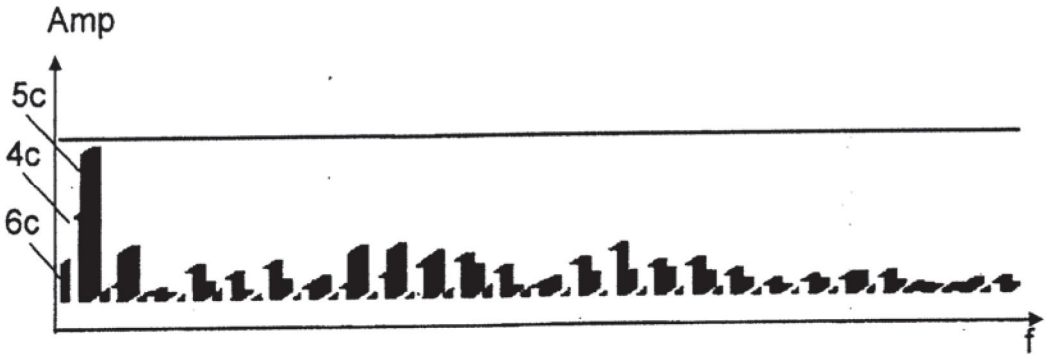


Figura 9

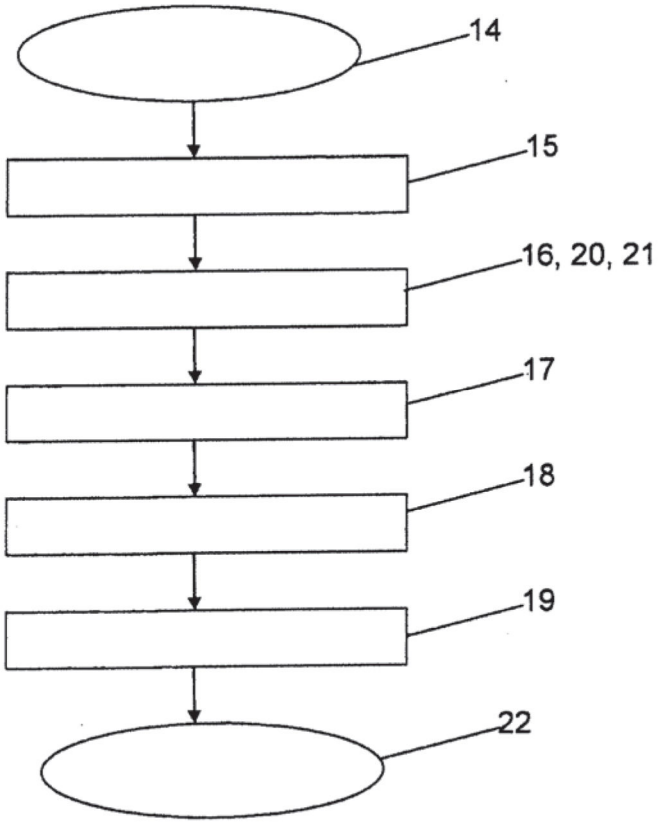


Figura 10

REFERENCIAS CITADAS EN LA DESCRIPCIÓN

La lista de referencias citada por el solicitante lo es solamente para utilidad del lector, no formando parte de los documentos de patente europeos. Aún cuando las referencias han sido cuidadosamente recopiladas, no pueden excluirse errores u omisiones y la OEP rechaza toda responsabilidad a este respecto.

Documentos de patente citado en la descripción

- DE 10248389 **[0003]**
- EP 1745420 B1 **[0008]**
- WO 2008092527 A1 **[0009]**
- US 2009065575 A1 **[0010]**

Bibliografía no de patentes citada en la descripción

- RFIDs and Secret Handshakes: Defending Against Ghost-and-Leech Attacks and Unauthorized Reads with Context-Aware Communications. *ACM Conference of Computer and Communications Security,* 2008, 479-490 **[0006]**