(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 635 328**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 12/12 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **18.06.2014 PCT/EP2014/001694**

(87) Fecha y número de publicación internacional: **31.12.2014 WO14206545**

(96) Fecha de presentación y número de la solicitud europea: **18.06.2014 E 14734393 (3)**

(97) Fecha y número de publicación de la concesión europea: **17.05.2017 EP 3014838**

(54) Título: **Protección de una transacción de campo cercano entre un terminal y un módulo de seguridad**

(30) Prioridad:

24.06.2013 DE 102013010627

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
03.10.2017

(73) Titular/es:

GIESECKE+DEVRIENT MOBILE SECURITY GMBH (100.0%)
Prinzregentenstraße 159
81677 München, DE

(72) Inventor/es:

DAHMOUNI, YOUSSEF

(74) Agente/Representante:

ARPE FERNÁNDEZ, Manuel

DESCRIPCIÓN

Protección de una transacción de campo cercano entre un terminal y un módulo de seguridad

[0001] La invención se refiere a un procedimiento para la protección de una transacción entre un terminal y un módulo de seguridad.

[0002] En la realización de transacciones entre un terminal y un módulo de seguridad a través de una interfaz sin contacto, como por ejemplo una interfaz NFC, existe el peligro de los, así llamados, ataques de retransmisión. En este contexto, un atacante posiciona un terminal manipulado (denominado *leech* - parásito) dentro del alcance de comunicación de la interfaz sin contacto del módulo de seguridad de un usuario (por ejemplo una tarjeta inteligente). Sin que el usuario lo sepa, se establece una comunicación a través de la interfaz sin contacto. A continuación, interponiendo un módulo del atacante (denominado ghost - fantasma), que está en comunicación sin contacto con otro terminal, se lleva a cabo una transacción en este otro terminal a través del módulo de seguridad del usuario. Para evitar los ataques de retransmisión, actualmente se conocen mediciones de duración que determinan la duración de señales entre el módulo de seguridad y el terminal, interrumpiéndose la transacción en caso de duraciones demasiado largas.

[0003] Del ensayo "Enhancing RFID Privacy via Antenna Engery Analysis" de Kenneth P. Fishkin et al. se deriva un procedimiento con el que se puede calcular a qué distancia se encuentra una etiqueta RFID de un terminal o aparato lector.

[0004] Del documento EP 2592584 A1 se deriva un procedimiento con el que se puede proteger una transacción con un soporte de datos portátil. En este contexto, una transacción solo se realiza si el equipo terminal de transacción y el soporte de datos con el que se realiza la transacción se encuentran en un campo cercano del campo de comunicación inalámbrico.

[0005] El objetivo de la invención consiste en crear un procedimiento para la protección de una transacción entre un terminal y un módulo de seguridad, que posibilite de forma sencilla el reconocimiento de un ataque de retransmisión sin mediciones de duración.

[0006] Este objetivo se resuelve mediante el objeto de las reivindicaciones independientes. En las reivindicaciones subordinadas se definen perfeccionamientos de la invención.

[0007] El procedimiento según la invención sirve para proteger una transacción, como por ejemplo una transacción de pago o transacción de tique, entre un terminal y un módulo de seguridad que se comunican en el marco de la transacción a través del campo alternante (magnético o electromagnético) de una primera interfaz sin contacto. Durante la realización de la transacción, en el emplazamiento del módulo de seguridad se registra una intensidad de acoplamiento que representa un acoplamiento, en particular un acoplamiento inductivo entre el terminal y el módulo de seguridad a través del campo alternante de la primera interfaz y/o un acoplamiento entre el terminal y el módulo de seguridad a través de un campo alternante de una segunda interfaz sin contacto. Si la intensidad de acoplamiento cumple un criterio de interrupción en relación con su magnitud y/o su variación temporal, la transacción se interrumpe.

[0008] De acuerdo con la invención se aprovecha el conocimiento de que el usuario, al realizar una transacción sin ataque de retransmisión, posiciona su módulo de seguridad con la mayor exactitud posible junto al terminal, mientras que, en caso de un ataque de retransmisión, el atacante no puede mantener su *leech* con esta precisión junto al módulo de seguridad. Esto se manifiesta en una magnitud o una variación de la intensidad de acoplamiento diferente a las de un caso normal.

[0009] El concepto arriba indicado del módulo de seguridad se ha de entender aquí y en adelante en un sentido amplio. El módulo de seguridad consiste en particular en un soporte de datos portátil, o en caso dado también en un equipo terminal (por ejemplo un equipo terminal móvil) con soporte de datos portátil conectado con el mismo, pudiendo el soporte de datos portátil estar instalado en el equipo terminal o en caso dado también estar integrado de forma fija en el equipo terminal, por ejemplo en forma de un módulo TPM o un SIM incorporado o un módulo NFC. El soporte de datos portátil consiste preferiblemente en una tarjeta inteligente, por ejemplo una tarjeta SIM/USIM, y/o un elemento de seguridad y/o un testigo y/o un transpondedor RFID y/o un módulo NFC.

[0010] En una realización especialmente preferente, la primera interfaz, a través de la cual el terminal y el módulo de seguridad realizan la transacción, consiste en una interfaz RFID, en particular una interfaz NFC o en caso dado también una interfaz UHF-RFID. En cambio, la segunda interfaz consiste preferiblemente en una interfaz para la transferencia de energía por inducción, en particular una interfaz Qi, que se basa en el estándar Qi para la transferencia de energía por inducción a través de distancias cortas. La utilización de la intensidad de acoplamiento de una interfaz de transferencia de energía para determinar un ataque de retransmisión presenta la ventaja de que, a diferencia de un enlace de datos NFC, una transferencia de energía presenta un coeficiente de acoplamiento lo más alto posible, de modo que a través de este medio se puede constatar con mucha fiabilidad un ataque de retransmisión. En otra forma de realización preferente, la primera interfaz está asegurada criptográficamente, lo que por regla general siempre ocurre en el caso de las interfaces NFC.

[0011] En una configuración especialmente preferente, la intensidad de acoplamiento registrada durante la realización de la transacción es suministrada al terminal, que comprueba el criterio de interrupción y, si se cumple el mismo, interrumpe la transacción. Por consiguiente, la protección de la transacción es vigilada centralmente por el terminal.

[0012] Preferiblemente, el terminal también registra una intensidad de acoplamiento. La comprobación del criterio de interrupción tiene lugar mediante una comparación de una intensidad de acoplamiento medida localmente con una intensidad de acoplamiento transmitida.

[0013] En una configuración preferente, la intensidad de acoplamiento registrada en el terminal es suministrada al módulo de seguridad, que comprueba el criterio de interrupción y, si se cumple el mismo, interrumpe la transacción. Por consiguiente, la protección de la transacción es vigilada individualmente por el módulo de seguridad.

[0014] En una variante especialmente preferente del procedimiento según la invención, el módulo de seguridad registra la intensidad de acoplamiento que representa el acoplamiento entre el terminal y el módulo de seguridad a través del campo alternante de la segunda interfaz. Después, la intensidad de acoplamiento registrada es transmitida a través de la primera interfaz al terminal, que comprueba el criterio de interrupción y, si se cumple el mismo, interrumpe la transacción. Tal como se ha mencionado más arriba, la utilización de la intensidad de acoplamiento de una interfaz para la transferencia de energía posibilita un registro especialmente fiable de ataques de retransmisión, ya que las intensidades de acoplamiento en estas interfaces son por regla general considerablemente más grandes que en el caso de las interfaces meramente para comunicación. Además, si la primera interfaz está asegurada criptográficamente, se evita que un atacante pueda interceptar o manipular la intensidad de acoplamiento transmitida.

[0015] La intensidad de acoplamiento registrada en el procedimiento según la invención se representa preferiblemente mediante un valor que es mayor cuanto mayor es la intensidad de señal del campo alternante de la primera y/o de la segunda interfaz en el emplazamiento del módulo de seguridad. En particular, la intensidad de acoplamiento puede ser la propia intensidad de señal. Del mismo modo, la intensidad de acoplamiento puede estar representada por ejemplo por un coeficiente de acoplamiento que representa la relación entre la energía recibida en el módulo de seguridad y la energía emitida por el terminal.

[0016] En otra forma de realización preferente de la invención, para que se cumpla el criterio de interrupción es necesario que durante la realización de la transacción la intensidad de acoplamiento esté al menos temporalmente y en particular durante un tiempo mayor que un intervalo de tiempo predeterminado (preferiblemente continuo) fuera de una gama de valores predeterminada, en particular por debajo de un valor umbral predeterminado, y/o que la variación temporal de la intensidad de acoplamiento sobrepase un umbral predeterminado al menos temporalmente y en particular durante un tiempo mayor que un intervalo de tiempo predeterminado (preferiblemente continuo). En otra configuración, para que se cumpla el criterio de interrupción es necesario que durante la realización de una transacción la intensidad de acoplamiento esté dentro de una gama de valores predeterminada durante un tiempo menor que un período de tiempo predeterminado.

[0017] En otra configuración, el cumplimiento del criterio de interrupción está asociado con un límite de tiempo, cumpliéndose el criterio de interrupción cuando un período de tiempo (preferiblemente continuo) en el que la intensidad de acoplamiento durante la realización de la transacción está fuera de una gama de valores predeterminada, en particular por debajo de un valor umbral predeterminado, sobrepasa dicho límite de tiempo.

[0018] En otra forma de realización, una transacción se interrumpe cuando, durante la realización de la transacción, una distorsión de una señal temporalmente variable del terminal, que es recibida en el módulo de seguridad a través de la primera y/o la segunda interfaz, sobrepasa un umbral predeterminado.

[0019] En otra variante, durante la transacción se registran eventos en los que la intensidad de acoplamiento abandona una gama de valores predeterminada y/o fluctúa más allá de una medida predeterminada. Si se produce un evento, el módulo de seguridad emite un mensaje perceptible por un usuario. El mensaje puede indicar al usuario en particular que mantenga su módulo de seguridad con más precisión con respecto al terminal o más cerca de éste. De este modo se puede evitar una detección errónea de un ataque de retransmisión no existente.

[0020] Además del procedimiento arriba descrito, la invención se refiere además a un dispositivo para la protección de una transacción entre un terminal y un módulo de seguridad que se comunican en el marco de la transacción a través del campo alternante de una primera interfaz sin contacto. El dispositivo está configurado de tal modo que durante la realización de la transacción registra una intensidad de acoplamiento en el emplazamiento del módulo de seguridad o recibe una intensidad de acoplamiento registrada, representando la intensidad de acoplamiento un acoplamiento entre el terminal y el módulo de seguridad a través del campo alternante de la primera interfaz o un acoplamiento entre el terminal y el módulo de seguridad a través de un campo alternante de una segunda interfaz sin contacto, y, si la intensidad de acoplamiento cumple un criterio de interrupción con respecto a su magnitud y/o su variación temporal, el dispositivo interrumpe la transacción.

[0021] El dispositivo arriba descrito está adaptado preferiblemente para la realización de una o más variantes preferentes del procedimiento según la invención. Además, el dispositivo preferiblemente forma parte del terminal, pero en caso dado también puede estar integrado en el módulo de seguridad.

[0022] A continuación se describen detalladamente ejemplos de realización de la invención con referencia a las figuras adjuntas.

[0023] Se muestran:

- la figura 1, una representación esquemática de una comunicación usual entre un terminal y un equipo terminal móvil a través de una interfaz sin contacto;
- la figura 2, el escenario de un ataque de retransmisión sobre la comunicación según la figura 1;
- la figura 3, los componentes de un terminal y un equipo terminal con los que se puede proteger una transacción sobre la base de una forma de realización del procedimiento según la invención; y
- la figura 4 un diagrama de flujo que reproduce la ejecución de una forma de realización del procedimiento según la invención.

[0024] La figura 1 muestra un escenario de una comunicación usual entre un terminal TE (por ejemplo un terminal de pago) y un equipo terminal MD móvil (por ejemplo un teléfono móvil). La comunicación tiene lugar a través de una interfaz IF sin contacto, que en la forma de realización aquí descrita consiste en una interfaz de comunicación NFC de corto alcance. El equipo terminal MD es un ejemplo de realización de un módulo de seguridad e incluye un

elemento de seguridad SE (véase la figura 3) que lleva a cabo la comunicación NFC a través de una bobina o antena con una bobina o antena correspondiente del terminal TE. Entre el terminal TE y el equipo terminal MD se realiza una transacción a través de la interfaz IF, como por ejemplo una transacción de pago, en la que el usuario paga con su equipo terminal en el terminal TE.

[0025] En el estado actual de la técnica se conocen los, así llamados, ataques de retransmisión, en los que un atacante realiza una transacción sin autorización a través del equipo terminal MD. La Figura 2 muestra uno de estos ataques de retransmisión. El atacante utiliza para ello un terminal manipulado LE, también designado como *leech*. El atacante pone el *leech* LE dentro del alcance de la interfaz IF de comunicación y establece una comunicación con el equipo terminal MD, sin que el usuario del equipo terminal tenga conocimiento de ello. Después, la comunicación entre el equipo terminal MD y el *leech* LE se dirige a través de un canal de datos DC a un módulo de seguridad ficticio GH (también designado como *ghost*) del atacante, que se hace pasar por el equipo terminal MD y realiza sin autorización una transacción con el terminal TE a través de la interfaz IF" sin contacto.

[0026] Para evitar estos ataques de retransmisión, de acuerdo con la invención se aprovecha el conocimiento de que, en caso de un ataque de retransmisión, el *leech* LE solo se puede posicionar de modo impreciso para el establecimiento de la comunicación sin contacto con el equipo terminal MD, lo que se manifiesta en que la intensidad de un acoplamiento inductivo entre el *leech* LE y el equipo terminal MD está fuera de una gama de valores usuales o fluctúa mucho. En este contexto, en la forma de realización aquí descrita no se considera el acoplamiento inductivo de la interfaz NFC IF de la figura 1 o la figura 2, sino el acoplamiento inductivo de otra interfaz sin contacto para la transferencia de energía, con la que el terminal TE suministra energía eléctrica al equipo terminal MD para la carga de éste. Preferiblemente, la interfaz para la transferencia de energía se basa en el estándar Qi y en adelante también se designa como interfaz Qi. Esta interfaz representa un ejemplo de realización de una segunda interfaz en el sentido de las reivindicaciones, mientras que la interfaz IF sin contacto mostrada en la figura 1 o la figura 2 es un ejemplo de realización de una primera interfaz en el sentido de las reivindicaciones.

[0027] Tal como se describe con mayor detalle más abajo, un ataque de retransmisión sobre el equipo terminal MD siempre se reconoce cuando se sobrepasa o no se llega a la intensidad de acoplamiento del campo alternante de la interfaz Qi. El motivo para ello es que para un usuario es muy fácil sujetar su equipo terminal MD correctamente junto al terminal TE para la realización de una transacción reglamentaria. En cambio, un atacante no puede llevar su *leech* con la misma precisión ni mucho menos a las proximidades del equipo terminal del usuario para el ataque de retransmisión. Esto se debe a que el atacante desconoce o solo conoce aproximadamente el emplazamiento del equipo terminal (por ejemplo el bolsillo del usuario).

[0028] En la variante aquí descrita, como intensidad de acoplamiento de la interfaz Qi se registra la intensidad de señal del campo alternante de la interfaz Qi en el emplazamiento del equipo terminal MD. Alternativamente, la intensidad de acoplamiento también se puede representar mediante un coeficiente de acoplamiento que representa la relación entre la energía recibida a través de la interfaz Qi y la energía emitida por el terminal. La intensidad de acoplamiento basada en la intensidad de señal o en el coeficiente de acoplamiento depende de muchos factores. En particular, la intensidad de acoplamiento es menor cuanto mayor es la distancia entre el terminal y el equipo terminal. Además, la intensidad de acoplamiento es menor cuanto mayor es el ángulo de las bobinas del equipo terminal y del terminal, utilizados para la transferencia de energía sin contacto, siendo la intensidad de acoplamiento máxima en caso de una orientación paralela de las bobinas. También influye en la intensidad de acoplamiento el desplazamiento lateral entre sí de las bobinas que intervienen en la transferencia de energía sin contacto, siendo la intensidad de acoplamiento máxima cuando no hay desplazamiento lateral de las bobinas.

[0029] Para llevar a cabo un proceso de carga sin contacto a través de una interfaz Qi con la mayor eficiencia energética posible, en la interfaz Qi del equipo terminal MD está prevista una unidad de medición correspondiente para la intensidad de señal del campo alternante utilizado para la carga. Esta intensidad de señal se designa en el estándar Qi como "*signal strength*" y se transmite en un, así llamado, *signal strength packet* (0x01). Esta intensidad de señal se utiliza ahora para reconocer ataques de retransmisión.

[0030] La figura 3 muestra la estructura de un terminal TE y un equipo terminal MD con los que se puede lograr una protección de una transacción basada en la intensidad de señal de una interfaz Qi. El terminal TE y el equipo terminal MD móvil disponen de la interfaz NFC IF sin contacto, a través de la cual se realiza la transacción. Para ello, en el terminal TE está prevista una unidad de transmisión de datos DT (DT = *data transmitter*) y en el equipo terminal MD está prevista una unidad de recepción de datos DR (DR = *data receiver*). La comunicación sin contacto basada en la interfaz IF tiene lugar a través de un intercambio de datos entre una antena de alta frecuencia AN1 de la unidad de transmisión de datos DT y una antena de alta frecuencia AN2 de la unidad de recepción de datos DR. En la figura 3, un intercambio de información ente componentes correspondientes está indicado siempre mediante flechas con el símbolo de referencia I. Para la transmisión de datos a través de una interfaz NFC IF están previstos además un procesador de terminal TP en la unidad de transmisión de datos DT así como un elemento de seguridad SE y un procesador móvil MP en la unidad de recepción de datos DR. El procesador de terminal TP se comunica con la antena AN1. Correspondientemente, el elemento de seguridad SE o el procesador móvil MP con interposición del elemento de seguridad se comunican con la antena AN2.

[0031] Entre el terminal TE y el equipo terminal MD está prevista además la interfaz Qi IF', que está realizada por el lado del terminal TE por una estación de carga PT (PT = *power transmitter*) y por el lado del equipo terminal MD por una unidad de carga PR (PR = *power receiver*). Para la transferencia de energía por inducción mediante un campo alternante magnético, en la estación de carga PT está prevista una bobina primaria CO1 y en la unidad de carga PR está prevista una bobina secundaria CO2. En este contexto, la transferencia de energía de la bobina CO1 a la bobina CO2 está indicada mediante la flecha E. También es posible un intercambio de información entre las bobinas, tal como está indicado mediante flechas I. La estación de carga PT dispone además de una unidad de

comunicación y control CU1, que se comunica por un lado con la bobina CO1 y por otro lado con el procesador de terminal TP de la unidad de transmisión de datos DT. Análogamente, en la unidad de carga PR también está prevista una unidad de comunicación y control CU2, que se comunica tanto con la bobina CO2 como con el procesador móvil MP de la unidad de recepción de datos DR.

[0032] En el diagrama de flujo de la figura 4 se muestra una variante del procedimiento según la invención para la protección de una transacción realizada a través de la interfaz IF de la figura 3. En el paso S1 se inicia la transacción a través de la interfaz NFC IF por medio de un intercambio de datos entre la unidad de transmisión de datos DT y la unidad de recepción de datos DR. A continuación, en un paso S2 comienza una transferencia de energía mediante una instrucción correspondiente de la unidad de transmisión de datos DT a la estación de carga PT. Después, en el paso S3 tiene lugar la transferencia de energía a través de la interfaz IF' entre la estación de carga PT del terminal TE y la unidad de carga PR del equipo terminal MD. En el paso S4 se transmite una respuesta a través de la interfaz IF' (en particular los, así llamados, paquetes "*end power transfer*" de acuerdo con el estándar Qi) desde la unidad de carga PR a la estación de carga PT. En el paso S5, la estación de carga PT transmite a la unidad de transmisión de datos DT la información de que la transferencia de energía está establecida. Además se transmite a la unidad de transmisión de datos DT una intensidad de acoplamiento KS' medida por la estación de carga PT.

[0033] En el paso S6, en la unidad de carga PR se calcula de forma conocida en sí una intensidad de acoplamiento KS en forma de la intensidad de señal del campo alternante de la interfaz IF', y dicha intensidad de acoplamiento KS es transmitida a la unidad de recepción de datos DR. Ésta transmite la intensidad de acoplamiento KS a la unidad de transmisión de datos DT en el paso S7.

[0034] A continuación, la unidad de transmisión de datos DT evalúa la intensidad de acoplamiento KS transmitida. En este contexto se comprueba si la intensidad de señal está dentro de un intervalo predeterminado, estando fijado dicho intervalo predeterminado de tal modo que representa valores de intensidades de señal cuando el equipo terminal está posicionado correctamente en el terminal TE en caso de una transacción reglamentaria sin ataque de retransmisión. Si en este contexto se comprueba que la intensidad de señal no está dentro del intervalo predeterminado, en un paso S8 la unidad de transmisión de datos DT rechaza la intensidad de acoplamiento KS y la transacción a través de la interfaz IF se interrumpe. En cambio, si la intensidad de acoplamiento KS está dentro del intervalo predeterminado, la unidad de transmisión de datos DT acepta dicha intensidad de acoplamiento en el paso S9 y la transacción se concluye reglamentariamente en el paso S10.

[0035] El intervalo dentro del cual se debería encontrar la intensidad de acoplamiento KS transmitida está determinado principalmente por la intensidad de acoplamiento KS' medida localmente. Por lo tanto, la evaluación incluye por ejemplo una comparación de la intensidad de acoplamiento KS' medida localmente con la intensidad de acoplamiento KS transmitida.

[0036] En una variante del procedimiento arriba descrito, la intensidad de acoplamiento debe estar además dentro del intervalo predeterminado durante un período de tiempo determinado (por ejemplo 20 ms) para que no se constate un ataque de retransmisión. En este caso, el equipo terminal registra a intervalos regulares la intensidad de acoplamiento KS y la transmite a la unidad de transmisión de datos DT. Se pueden transmitir valores de medición individuales de la intensidad de acoplamiento, o una curva de medición correspondiente a un período de tiempo. La transacción se concluye únicamente si la intensidad de acoplamiento está dentro del intervalo predeterminado durante el período de tiempo determinado. De lo contrario, la transacción se interrumpe. Precisamente la comparación de la intensidad de acoplamiento KS' medida localmente con la intensidad de acoplamiento KS transmitida ofrece una seguridad especialmente alta, ya que existen muchísimas posibilidades de que los ataques de retransmisión sean reconocidos. En caso dado también se puede comprobar si una señal variable transmitida por la estación de carga PT a través de la interfaz IF' es reproducida con la menor distorsión posible (es decir, medición de una señal a lo largo del tiempo). Si no es este el caso, la transacción también se interrumpe.

[0037] Igualmente es posible transmitir la intensidad de acoplamiento KS' a la unidad de recepción de datos DR y comparar la misma en el equipo terminal MD con la intensidad de acoplamiento medida localmente en éste. En este caso, la interrupción también tiene lugar análogamente a través del equipo terminal MD.

[0038] Preferiblemente, una intensidad de acoplamiento KS, KS' transmitida se transmite asegurada criptográficamente, es decir, cifrada y/o firmada. Por lo tanto, un atacante no puede utilizar ningún valor de medición posiblemente registrado por el mismo.

[0039] En las variantes arriba descritas del procedimiento según la invención, la intensidad de acoplamiento KS se transmite al terminal TE a través del enlace de datos NFC cifrado y no a través del enlace de datos de la interfaz Qi. Esto tiene la ventaja de que un atacante no puede manipular ni interceptar la intensidad de acoplamiento. De este modo se evita que el *ghost* del atacante transmita una intensidad de señal manipulada al terminal y de este modo simule un posicionamiento reglamentario del equipo terminal MD al terminal TE. Además se evita que el atacante, en respuesta a una intensidad de señal interceptada, adapte el posicionamiento de su *leech* con respecto al equipo terminal y de este modo logre que el ataque de retransmisión no sea reconocido.

[0040] Las formas de realización de la invención anteriormente descritas presentan una serie de ventajas. En particular, los ataques de retransmisión se reconocen de un modo sencillo a través del cálculo de una intensidad de acoplamiento de una interfaz sin contacto entre un equipo terminal y un terminal. Para ello se pueden utilizar medios existentes en el terminal y el equipo terminal, en particular una interfaz para la transferencia inalámbrica de energía. El procedimiento no solo se puede utilizar con equipos terminales, sino también con tarjetas inteligentes o testigos, ya que la transferencia inalámbrica de energía no requiere ningún acumulador de energía en el lado del receptor.

REIVINDICACIONES

1. Procedimiento para proteger una transacción entre un terminal (TE) y un módulo de seguridad (MD) que se comunican en el marco de la transacción a través del campo alternante de una primera interfaz (IF) sin contacto, registrándose durante la realización de la transacción en el emplazamiento del módulo de seguridad (MD) una intensidad de acoplamiento (KS) que representa un acoplamiento entre el terminal (TE) y el módulo de seguridad (MD) a través de un campo alternante de una segunda interfaz (IF') sin contacto, e interrumpiéndose la transacción si la intensidad de acoplamiento (KS) cumple un criterio de interrupción en relación con su magnitud y/o su variación temporal.

2. Procedimiento según la reivindicación 1, caracterizado por que el módulo de seguridad (MD) consiste en un soporte de datos portátil o en un equipo terminal con soporte de datos portátil conectado con el mismo, siendo el soporte de datos portátil preferiblemente una tarjeta inteligente y/o un elemento de seguridad y/o un testigo y/o un transpondedor RFID y/o un módulo NFC.

3. Procedimiento según la reivindicación 1 o 2, caracterizado por que la primera interfaz (IF) consiste en una interfaz RFID, en particular una interfaz NFC o una interfaz UHF-RFID, y/o la segunda interfaz (IF') consiste en una interfaz para la transferencia de energía por inducción, en particular una interfaz Qi.

4. Procedimiento según una de las reivindicaciones anteriores, caracterizado por que la primera interfaz (IF) está asegurada criptográficamente.

5. Procedimiento según una de las reivindicaciones anteriores, caracterizado por que, durante la realización de la transacción, en el terminal (TE) se registra una intensidad de acoplamiento (KS') de terminal.

6. Procedimiento según una de las reivindicaciones anteriores, caracterizado por que la intensidad de acoplamiento (KS) registrada durante la realización de la transacción es transmitida al terminal (TE), que comprueba el criterio de interrupción y, si se cumple el mismo, interrumpe la transacción.

7. Procedimiento según una de las reivindicaciones 5 o 6, caracterizado por que la intensidad de acoplamiento (KS) de terminal registrada durante la realización de la transacción es transmitida al módulo de seguridad (MD), que comprueba el criterio de interrupción y, si se cumple el mismo, interrumpe la transacción.

8. Procedimiento según una de las reivindicaciones anteriores, caracterizado por que la comprobación del criterio de interrupción incluye una comparación de una intensidad de acoplamiento (KS'; KS) medida localmente con una intensidad de acoplamiento (KS; KS') transmitida a través de la primera interfaz (IF).

9. Procedimiento según una de las reivindicaciones anteriores, caracterizado por que el módulo de seguridad (MD) registra la intensidad de acoplamiento (KS) que representa el acoplamiento entre el terminal (TE) y el módulo de seguridad (MD) a través del campo alternante de la segunda interfaz (IF'), y transmite la intensidad de acoplamiento (KS) registrada a través de la primera interfaz (IF) al terminal (TE), que comprueba el criterio de interrupción y, si se cumple el mismo, interrumpe la transacción.

10. Procedimiento según una de las reivindicaciones anteriores, caracterizado por que la intensidad de acoplamiento (KS) se representa mediante un valor que es mayor cuanto mayor es la intensidad de señal del campo alternante de la primera y/o la segunda interfaz (IF, IF') en el emplazamiento del módulo de seguridad (MD).

11. Procedimiento según una de las reivindicaciones anteriores, caracterizado por que para que se cumpla el criterio de interrupción es necesario que durante la realización de la transacción la intensidad de acoplamiento (KS) esté al menos temporalmente y en particular durante un tiempo mayor que un intervalo de tiempo predeterminado fuera de una gama de valores predeterminada, en particular por debajo de un valor umbral predeterminado, y/o que la variación temporal de la intensidad de acoplamiento (KS) sobrepase un umbral predeterminado al menos temporalmente y en particular durante un tiempo mayor que un intervalo de tiempo predeterminado.

12. Procedimiento según una de las reivindicaciones anteriores, caracterizado por que para que se cumpla el criterio de interrupción es necesario que durante la realización de una transacción la intensidad de acoplamiento (KS) esté dentro de una gama de valores predeterminada durante un tiempo menor que un período de tiempo predeterminado.

13. Procedimiento según una de las reivindicaciones anteriores, caracterizado por que el cumplimiento del criterio de interrupción está asociado con un límite de tiempo, cumpliéndose el criterio de interrupción cuando un período de tiempo, en el que la intensidad de acoplamiento (KS) durante la realización de la transacción está fuera de una gama de valores predeterminada, sobrepasa dicho límite de tiempo.

14. Dispositivo para la protección de una transacción entre un terminal (TE) y un módulo de seguridad (MD) que se comunican en el marco de la transacción a través del campo alternante de una primera interfaz (IF) sin contacto, estando configurado el dispositivo de tal modo que durante la realización de la transacción registra una intensidad de

acoplamiento (KS) en el emplazamiento del módulo de seguridad (MD) o recibe una intensidad de acoplamiento (KS) registrada, representando la intensidad de acoplamiento (KS) un acoplamiento entre el terminal (TE) y el módulo de seguridad (MD) a través de un campo alternante de una segunda interfaz (IF') sin contacto, y, si la intensidad de acoplamiento (KS) cumple un criterio de interrupción con respecto a su magnitud y/o su variación temporal, el dispositivo interrumpe la transacción.

15. Dispositivo según la reivindicación 14, caracterizado por que el dispositivo está adaptado para la realización de un procedimiento según una de las reivindicaciones 2 a 13.

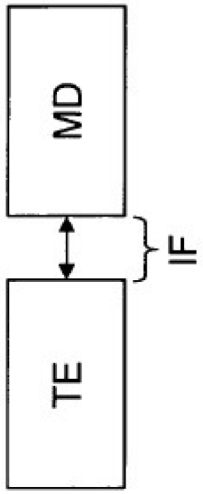

Fig. 1

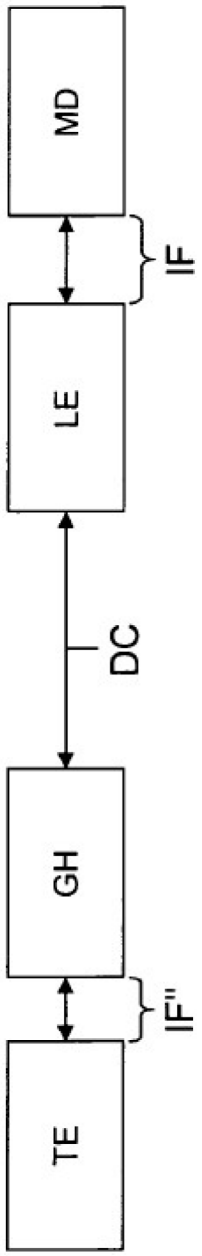

Fig. 2

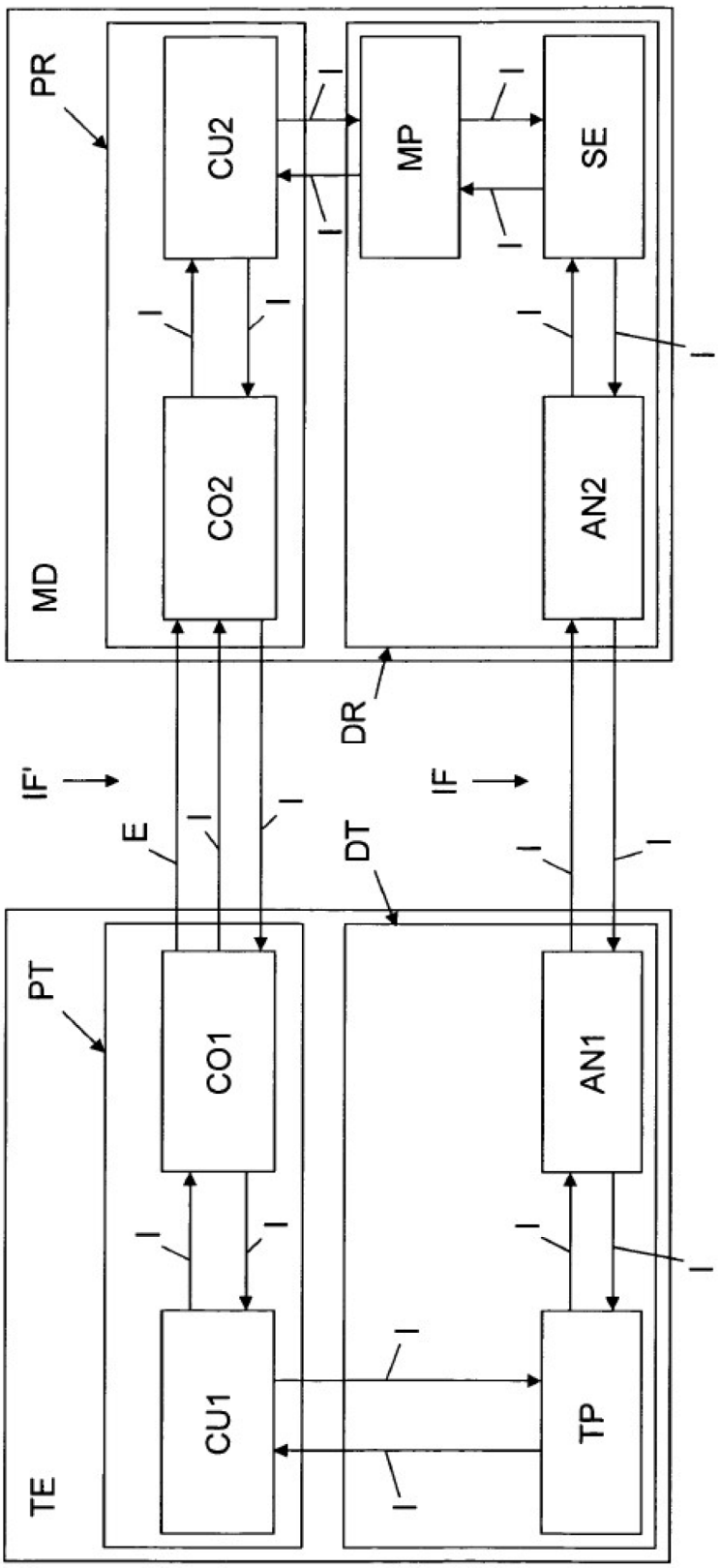

Fig. 3

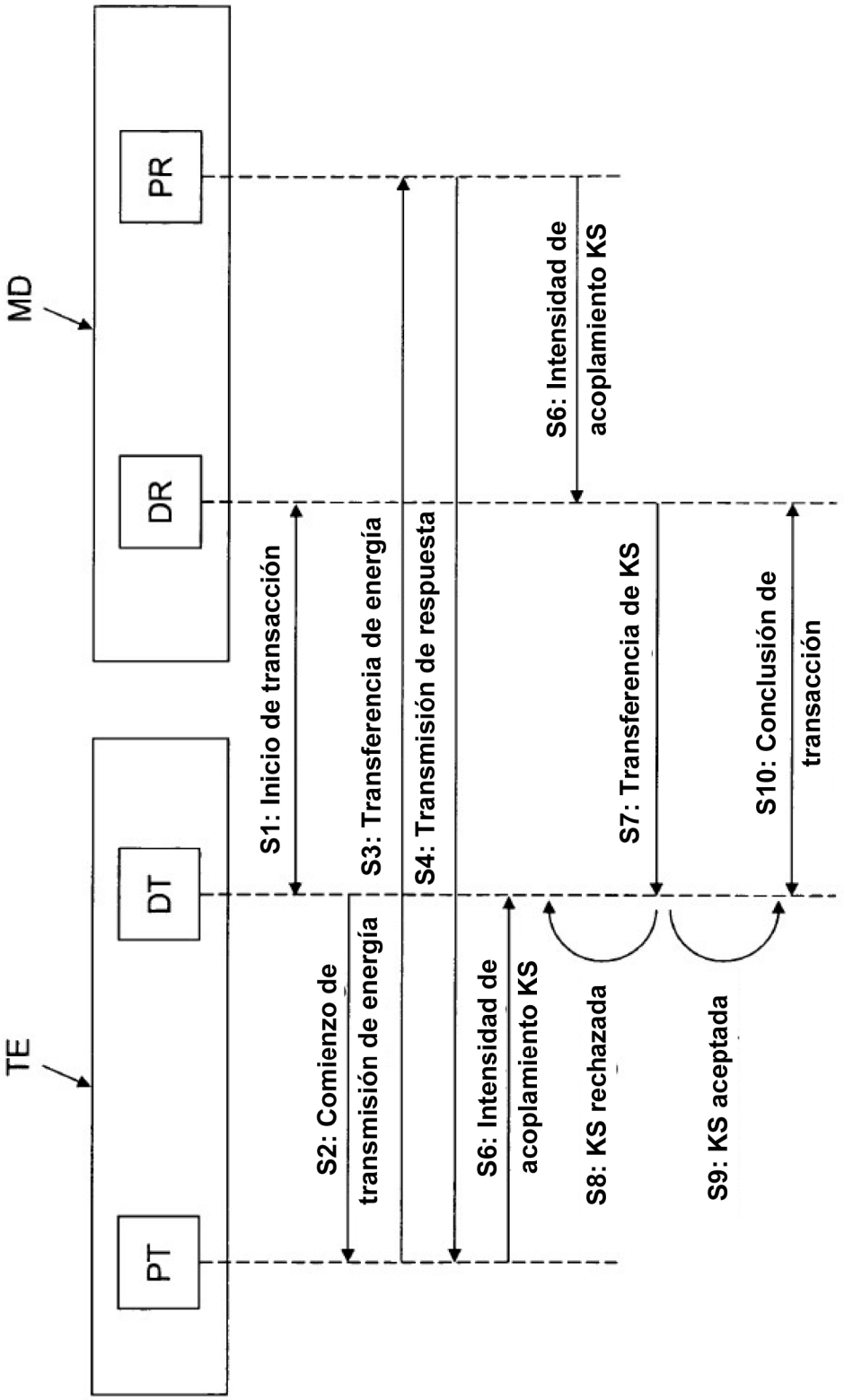
MD
PR
DR
TE
DT
PT
S1: Inicio de transacción
S2: Comienzo de transmisión de energía
S3: Transferencia de energía
S4: Transmisión de respuesta
S6: Intensidad de acoplamiento KS
S6: Intensidad de acoplamiento KS
S7: Transferencia de KS
S8: KS rechazada
S9: KS aceptada
S10: Conclusión de transacción

Fig. 4

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

• EP 2592584 A1 **[0004]**

Bibliografía no de patentes citada en la descripción

• **KENNETH P. FISHKIN.** *Enhancing RFID Privacy via Antenna Engery Analysis* **[0003]**