(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 690 837**

(51) Int. CI.:

H04W 12/06 (2009.01)
H04N 1/00 (2006.01)
H04N 1/327 (2006.01)
G09C 5/00 (2006.01)
H04N 1/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **24.12.2012 PCT/EP2012/076885**

(87) Fecha y número de publicación internacional: **27.06.2013 WO13093120**

(96) Fecha de presentación y número de la solicitud europea: **24.12.2012 E 12808417 (5)**

(97) Fecha y número de publicación de la concesión europea: **11.07.2018 EP 2795947**

(54) Título: **Método de emparejamiento de equipos electrónicos**

(30) Prioridad:

23.12.2011 FR 1162408

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.11.2018

(73) Titular/es:

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

(72) Inventor/es:

MARSAUD, THIERRY y
MENARDAIS, MICHAEL

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Método de emparejamiento de equipos electrónicos

1. Dominio de la invención

La invención se refiere al dominio de la autentificación. La invención se refiera mas particularmente a la autentificación material de dispositivos entre si.

2. Estado de la técnica

Se conoce perfectamente del estado de la técnica numerosos protocolos que permiten a dos dispositivos autentificarse previamente a la transmisión o al intercambio de informaciones confidenciales. Tal es por ejemplo el caso de un terminal de comunicación inalámbrica que desea autentificarse en una red local de un usuario, por ejemplo, una red inalámbrica wifi. Para ello, previamente a cualquier intercambio de datos, el terminal debe autentificarse en la red de comunicación. Esta autentificación pasa generalmente por una fase de introducción de una clave, que es por ejemplo una clave WEP (del inglés “Wired Equivalent Privacy”, una clave WPA (“Wi-FI Protected Access”), PSK (“pre-shared key”) u otra. Uno de los problemas con este tipo de clave es la longitud de esta. Una clave WEP incluye 13 caracteres, mientras que una clave WPA-PSK es normalmente una frase secreta cuya introducción puede resultar larga.

Otros dominios precisan de una autentificación entro dispositivos inalámbricos. Tal es el caso por ejemplo de los dispositivos que comunican por medio de la tecnología Bluetooth. Bluetooth es una tecnología inalámbrica para crear redes personales inalámbricas que funcionan en la banda de frecuencia de 2,4 GHz no siendo necesaria autorización, con un alcance de alrededor de una decena de metros. Las redes están generalmente compuestas por periféricos nómadas como los teléfonos móviles, los asistentes personales y los ordenadores portátiles. Por defecto, una comunicación Bluetooth no está autentificada, y cualquier periférico puede intercambiar datos con cualquier otro periférico.

Un periférico Bluetooth (por ejemplo, un teléfono portátil) puede elegir solicitar una autentificación para suministrar un servicio en particular. La autentificación Bluetooth se efectúa generalmente mediante códigos PIN. Un código PIN Bluetooth es una cadena ASCII de una longitud máxima de 16 caracteres. Por defecto, el usuario debe introducir el mismo código PIN en los dos periféricos. Una vez que el usuario a introducido el código PIN, los dos periféricos generan una clave de emparejamiento (link key). Después esta clave de emparejamiento puede ser almacenada ya sea en los periféricos en si mismos o en un medio de almacenamiento externo. Durante el siguiente intercambio, los dos periféricos utilizarán la clave de emparejamiento anteriormente generada. Este procedimiento se llama emparejamiento. Cuando se pierde la clave de emparejamiento en uno de los dispositivos entonces debe repetirse la operación de emparejamiento para que se puede generar una nueva clave.

Cuando los datos que deben ser intercambiados entre los dos terminales Bluetooth son datos sensibles (como datos bancarios por ejemplo), los intercambios que suceden a la fase de emparejamiento están cifrados, por ejemplo con la ayuda del algoritmo E0. E0 es un algoritmo de cifrado de flujo utilizado para proteger la confidencialidad de los datos intercambiados por Bluetooth.

Sin embargo, el problema es el mismo que para la clave WEP o la clave WPA: es necesario que previamente a cualquier intercambio cifrado que el usuario introduzca en el terminal un código PIN cuya longitud varia de 4 a 16 caracteres, sabiendo que, para las aplicaciones con mayor seguridad, se prefiere el código PIN de 16 caracteres.

Ya sea mediante tecnología WIFI o mediante tecnología Bluetooth, la introducción de un código PIN o de una clave de una longitud excesiva conlleva al menos dos de los siguientes problemas:

- por una parte, un riesgo de error durante la introducción que es importante. En efecto, está casi asegurado que la introducción incluye al menos un error. Esto es particularmente cierto cuando la introducción se efectúa con caracteres ocultos (los caracteres introducidos no son mostrados, sino que en su lugar se muestran una serie de caracteres estrella);

- por otra parte, siendo manual la introducción, nada asegura que una persona malintencionada no espíe la introducción con el objetivo de apropiarse del código PIN o de la clave para un uso fraudulento.

Se han propuesto soluciones de seguridad, principalmente para la ejecución de una conexión Wi-Fi. Consisten en la activación cuasi simultánea de los dos dispositivos que se quiere conectar conjuntamente. Una de estas soluciones se denomina “Wi-Fi Protected Setup (WPS)” Y es un estándar de red local inalámbrica simple y segura. Esta solución no soluciona sin embargo todos los problemas, ya que una de las variantes del WPS supone la introducción de un código PIN.

US2011/0081860 A1 y US2010/0012715 divulgan unos métodos que proponen el escaneo de códigos de barras con el fin de obtener el código PIN de emparejamiento Bluetooth.

En otros términos, es necesario suministrar una solución de conexión que sea a la vez simple y discreta con el fin de por una parte evitar los errores de introducción y por otra parte asegurar la confidencialidad de los datos necesarios para la conexión o para el emparejamiento.

3. Resumen de la invención

La invención no presenta estos inconvenientes del arte anterior.

La invención está definida en las reivindicaciones independientes 1, 2, 8 y 9. Unos modos de realización particulares están definidos en las reivindicaciones dependientes. La invención se refiere a un método de emparejamiento de un primer equipo, llamado equipo iniciador que desea transmitir y recibir datos con un segundo equipo, llamado equipo aceptador.

Según la invención, dicho método incluye:

- una etapa de generación de un código de emparejamiento;

- una etapa de restitución, con la forma de un primer símbolo, de dicho código de emparejamiento para dicho equipo aceptador;

- una etapa de adquisición de dicho primer símbolo por dicho equipo iniciador;

- una etapa de decodificación de dicho primer símbolo adquirido suministrando dicho código de emparejamiento.

Según la invención, el código de emparejamiento es aleatorio y volátil. No se almacena y no puede recuperarse posteriormente.

Según una característica particular dicho método de emparejamiento incluye, además:

- una etapa de obtención, para dicho equipo aceptador, de al menos un dato útil;

- una etapa de restitución, con la forma de un segundo símbolo, de al menos un dato útil.

Según una característica particular dicho método de emparejamiento incluye, además:

- una etapa de adquisición de dicho segundo símbolo por dicho equipo iniciador;

- una etapa de descodificación de dicho segundo símbolo que suministra dichos datos útiles.

Según una característica particular, dicho primer símbolo y dicho segundo símbolo forman un único y mismo símbolo.

Según un modo de realización particular un símbolo pertenece a un tipo de símbolo y porque dicho tipo de símbolo pertenece al grupo que incluye:

- un código de barras de una dimensión;

- un código de barras de dos dimensiones;

- una imagen de marca de agua;

- una secuencia sonora modulada;

Según una característica particular, dicho equipamiento iniciador es una PDA y porque dicho equipamiento aceptador es un terminal de pago.

Según una característica particular, dicha etapa de restitución de dicho código de emparejamiento con la forma de un primer símbolo incluye una etapa de impresión de dicho primer símbolo en una impresora de dicho equipo aceptador.

Según un modo de realización particular, dicha etapa de adquisición de dicho primer símbolo por dicho equipo iniciador incluye una etapa de adquisición de una imagen representativa de dicho primer símbolo.

La invención concierne igualmente un equipo iniciador que desea transmitir y recibir datos con un equipo aceptador.

Según la invención dicho equipo incluye:

- unos medios de adquisición de un primer símbolo representativo de un código de emparejamiento que permite el emparejamiento de dicho equipo aceptador y de dicho equipo iniciador, dicho primer símbolo está restituido por un equipo aceptador;

- unos medios de decodificación de dicho primer símbolo adquirido suministrando dicho código de emparejamiento;

La invención concierne igualmente un equipo aceptador que desea transmitir y recibir datos con un equipo iniciador. Según la invención dicho equipo incluye:

- Unos medios de generación de un código de emparejamiento que permita el emparejamiento de dicho equipo aceptador y de dicho equipo iniciador;

- Una etapa de restitución, con la forma de un primer símbolo, de dicho código de emparejamiento;

La invención tiene también como objetivo un soporte de informaciones que pueda leer un procesador de datos, e incluye unas instrucciones de un programa tal y como se menciona anteriormente.

El soporte de informaciones puede ser cualquier entidad o dispositivo capaz de almacenar el programa. Por ejemplo, el soporte puede incluir un medio de almacenamiento, tal como una ROM, por ejemplo un CD ROM o una ROM de circuito microelectrónico, o también un medio de almacenamiento magnético, por ejemplo un disquete (floppy disc) o un disco duro.

Por otra parte, el soporte de informaciones puede ser un soporte transmisible tal como una señal eléctrica u óptica, que puede ser conducida mediante un cable eléctrico u óptico, por radio o por otros medios. El programa según la invención puede ser en particular descargado en una red del tipo internet.

Alternativamente, el soporte de informaciones puede ser un circuito integrado en el que el programa es incorporado, estando el circuito adaptado para ejecutar o para ser utilizado en la ejecución del procedimiento en cuestión.

Según un modo de realización, la invención es ejecutada por medio de componentes de software y/o materiales. En esta óptica, el termino “modulo” puede corresponder en este documento tanto a un componente de software, como a un componente de material o a un conjunto de componentes materiales y de software.

Un componente de software corresponde a unos o varios programas de ordenador, a uno o varios sub-programas de un programa, o de forma mas general a cualquier elemento de un programa o de un software apto para llevar a cabo una función o un conjunto de funciones, según lo que está descrito mas adelante para el modulo en cuestión. Dicho componente de software es ejecutado por un procesador de datos de una entidad física (terminal. Servidor, etc.) y es susceptible de acceder a los medios materiales de esta entidad física (memorias, soportes de grabación, bus de comunicación, tarjetas electrónicas de entradas/salidas, interfaces de usuario, etc…).

Del mismo modo, un componente material corresponde a cualquier elemento de un conjunto material (o hardware) apto para ejecutar una función o un conjunto de funciones, según lo que está descrito mas adelante para el modulo en cuestión. Puede tratarse de un componente material programable o un procesador integrado para la ejecución de software, por ejemplo un circuito integrado, una tarjeta inteligente, una tarjeta de memoria, una tarjeta electrónica para la ejecución de un microcodigo (firmware), etc..

4. Figuras

Otras características y ventajas de la invención aparecerán con mas claridad con la lectura de la siguiente descripción de un modo de realización preferente, dado a titulo de simple ejemplo ilustrativo y no limitativo, y unos dibujos adjuntos, de entre los cuales:

- la figura 1 describe el principio general de la invención;

- la figura 2 describe las etapas necesarias para el emparejamiento de una PDA con un terminal de pago;

- la figura 3 simboliza un equipo aceptador según la invención;

- la figura 4 simboliza un equipo iniciador según la invención.

5. Descripción de un modo de realización

5.1 Recordatorio del principio de la invención

Tal y como se ha explicitado anteriormente, la invención ofrece un nuevo método de introducción del código de emparejamiento (por ejemplo, un código PIN) para el emparejamiento de dos dispositivos. La invención se aplica principalmente a la tecnología de emparejamiento Bluetooth, pero es igualmente posible aplicarla a otros protocolos que incluyen una introducción, por el usuario, de un código PIN o de una clave o de una “passphase” (frase secreta utilizada para una mejor seguridad que una simple palabra clave).

En un modo de realización particular, que se describirá a continuación, la solución de la invención lleva a cabo dos equipos Bluetooth, uno que inicia el proceso de emparejamiento y el otro que lo acepta.

En lo que sigue, se hace referencia respectivamente al iniciador y al aceptador para designar respectivamente estos equipos.

El procedimiento de la invención se describe en relación con la figura 1. En el marco del invento, el equipamiento iniciador E_{init} dispone de un captador electrónico de imagen (como por ejemplo: lector de código, lector de código de barras, periférico que permite la lectura y la decodificación de imágenes tales como los aparatos de fotografía integrados en los teléfonos inteligentes u otros equipos electrónicos), y el equipo aceptador E_{ACC} dispone de una impresora o de una pantalla y debe ser capaz de imprimir o mostrar los símbolos (el equipo aceptador dispone generalmente de un medio de restitución visual o sonoro).

El termino símbolo utilizado aquí se extiende como cualquier representación de un datos numérico o alfanumérico con la forma de un símbolo grafico o de audio (ejemplo: código de barras de una, dos o tres dimensiones, pulsaciones sonoras, etc. Según la invención, el símbolo incluye un conjunto de datos que pueden ser restituidos por el equipo aceptador y adquiridos por el equipo iniciador. Según la invención, el símbolo no es interpretable por un humano (no se puede leer directamente y comprensible o audible y comprensible). En un modo de realización especifico de la invención, el símbolo está incrustado en una imagen según un método de watermarking (marca de agua). En este modo de realización, el equipo iniciador adquiere la imagen y obtiene la marca oculta en la imagen adquirida. A partir de esta marca recrea el símbolo y lo decodifica para obtener el código PIN. Hay por tanto una doble codificación del código PIN. Esto es ventajoso desde varios puntos de vista. Por una parte, el hecho de que el símbolo esté escondido en una imagen de marca de agua impide al que quiere realizar el fraude percibir que la imagen mostrada contiene un código. Por otra parte, para obtener la marca oculta, es necesario ejecutar un método de descubrimiento (de decodificación) del símbolo, lo que constituye en realidad una doble codificación y aumenta la seguridad. Ventajosamente, la imagen utilizada para insertar el símbolo es por ejemplo el logo de la tienda o del banco o de la entidad que utiliza los terminales. Así, el descubrimiento del hecho de que se emite un símbolo es todavía mas complejo. En el caso de una secuencia sonora, las ventajas producidas son similares. Por una parte por el hecho de que la secuencia es producida a iniciativa del primer terminal y que el que quiere realizar el fraude no sabe cuando se producirá. Por otra parte, como para la imagen de la marca de agua, por el hecho de la secuencia sonora representa de nuevo una codificación del símbolo y que es por tanto necesario realizar una doble decodificación para obtener la información. En tercer lugar, la secuencia sonora modulada puede ser emitida en frecuencias imperceptibles para un defraudador de manera que es incapaz de saber cuando se emite el código. En función de los modos de realización, la secuencia sonora podrá por ejemplo ser una secuenciua DTMF. Así, en el marco de la invención, hay varios tipos de símbolos utilizables. Tal y como se presentará posteriormente, los diferentes tipos de símbolos pueden ser utilizados conjuntamente o sucesivamente,

Según la invención, el proceso de emparejamiento se efectúa globalmente en dos etapas para el usuario:

- el equipo aceptador E_{ACC} restituye 10 (imprime o muestra o emite un sonido) los símbolos SYMB del código PIN; como complemento, otros parámetros pueden igualmente ser restituidos (dirección del equipo aceptador por ejemplo, este aspecto se detalla a continuación)

- el equipo iniciador E_{init} adquiere 20 (mediante lectura, escáner o reconocimiento de audio) el código PIN con la ayuda del detector de símbolos. Cuando se utilizan otros parámetros (dirección del equipo aceptador por ejemplo, esta dirección es igualmente adquirida).

No hay por tanto introducción manual por el usuario, lo que simplifica le proceso y evita los errores.

El mecanismo de emparejamiento estándar con autentificación se inicia entonces 30 y los dos equipos se conectan en algunos segundos (en función del entorno de radio).

El código PIN es generado 10-1 de forma aleatoria en el equipo aceptador y esto compuesto por el máximo de caracteres posible, lo que asegura un nivel de seguridad elevado en la unión entre los dos equipos. En el caso de una aplicación que utilice la tecnología Bluetooth por ejmplo, el código PIN incluye 16 caracteres.

Además, el código PIN se genera de forma asíncrona, anterior o posteriormente a la decisión 10-0 de emparejamiento del equipo iniciador E_{init}, con el equipo aceptador E_{ACC}. La decisión 10-0 se toma por un usuario que decide emparejar los dos equipos. El código PIN es aleatorio y volátil.

Cuando dos equipos ya están emparejados, se puede igualmente establecer un segundo emparejamiento con un nuevo código PIN aleatorio, lo que permite modificar las claves de cifrado de forra periódica y permite por tanto aumentar mas la seguridad de este enlace.

Como se ha explicitado anteriormente, es igualmente posible suministrar al equipo iniciador E_{init}, además del código PIN, otros datos útiles que puedan tenerse en cuenta para aumentar el nivel de seguridad del método propuesto. En función de los modos de realización, estos datos útiles pueden ser obligatorios para poder validar el proceso de emparejamiento.

De entre estos datos útiles, se puede por ejemplo mencionar la dirección (por ejemplo, la dirección Bluetooth) del dispositivo aceptador E_{ACC}. En función de los modos de realización de la invención, el suministro de estos datos útiles se puede llevar a cabo de distinta forma.

En un primer modo de realización, el suministro de datos útiles está separado del suministro del código PIN. Esto significa que, posteriormente a la adquisición del símbolo que representa el código PIN por el equipo iniciador E_{init}, tiene lugar una segunda etapa de adquisición. Esta separación en dos etapas permite asegurar el respeto del procedimiento y por tanto ofrece una seguridad suplementaria. Por supuesto, estos datos útiles están igualmente presentados bajo la forma de símbolo, que puede ser de un tipo diferente del del primer símbolo. Asi, por ejemplo, el primer símbolo puede ser un código de barras de una dimensión mientras que el segundo símbolo puede presentarse con la forma de un código de barras de dos dimensiones.

En un segundo modo de realización, el suministro de datos útiles se realiza conjuntamente con el suministro del código PIN con la forma de símbolo. Este suministro conjunto puede ser realizado en un único y mismo símbolo, por ejemplo un código de barras de una o dos dimensiones o entonces utilizando dos tipos de símbolo diferentes (el primer símbolo puede ser un código de barras de una dimensión mientras que el segundo símbolo se puede presentar con la forma de un código de barras de dos dimensiones). La diferencia entre este segundo modo de realización y el primer modo de realización se realiza en el momento de la adquisición de símbolos. En el caso donde los datos útiles son presentados conjuntamente con el código PIN, pero con un símbolo distinto del símbolo de código PIN, se beneficia de la capacidad de los nuevos escaners de escanear varios códigos simultáneamente.

5.2 Descripción de un modo de realización particular

Se describe, en este modo de realización, la ejecución del invento para el emparejamiento de dos dispositivos por medio de la tecnología Bluetooth: se trata de realizar un emparejamiento de una PDA y de un terminal de pago. En este modo de realización, la PDA es el equipo iniciador y el terminal de pago es el equipo aceptador.

Respecto de las dificultades y los problemas previamente expuestos, el emparejamiento de un terminal de pago presenta además otras dificultades, de entre las cuales la obligación de asegurar un nivel de confidencialidad absoluto de los datos que son transmitidos al terminal.

En efecto, una de las funciones que conlleva el emparejamiento de un terminal de pago con una PDA es la función de pago. Esta función está brevemente descrita en relación con la figura 2. Una vez que han sido emparejados (método objeto de la invención), es decir posteriormente a la etapa 30 de la figura 1, el terminal de pago y la PDA van a intercambiar datos cifrados, por ejemplo, según el siguiente proceso:

Un cliente C realiza unas compras en una tienda con la ayuda de una PDA. Puede o bien utilizar únicamente la PDA para ello, o bien es el vendedor el que tiene la PDA. LA PDA es utilizada para escanear 40 los artículos comprados por el cliente. Para ello, la PDA ejecuta una aplicación llamada “trabajo” que es ejecutada en la PDA. Esta fase de “escaneo” debe entenderse en su sentido mas amplio. Se puede tratar de un escaneo de un código de barras, como de un escaneo a partir de un captador óptico de cámara o de una selección sobre una lista de productos presentada en la pantalla de la PDA. Esta frase de “escaneo” se repite 40-1 tantas veces como el cliente desee comprar productos o servicios.

Cuando el cliente ha terminado sus compras, la aplicación trabajo de la PDA requiere el pago de las compras del cliente C mediante el terminal de pata TP. Esta petición Rq se transmite 50 por la PDA al terminal de pago TP por medio de la unión Bluetooth que ha sido previamente configurada por el método objeto de la invención. Esta solicitud cifrada R_q incluye principalmente el importe de la transacción (de entre otros parámetros). Este importe se recupera por el terminal de pago TP que lo utiliza para iniciar una transacción. Generalmente, esta transacción es efectuada mediante una tarjeta de pago CP propiedad del usuario. Durante la inicialización de la transacción 60, el terminal de pago TP toma el relevo: esto significa que la aplicación trabajo que es lanzada en la PDA se ha situado en modo “espera”. El terminal de pago TP es por si solo maestro del desarrollo de la transacción de pago. El cliente C efectúa así el pago por medio del terminal de pago TP. Cuando el pago ha sido validado por el terminal de pago TP (o que la transacción ha fracasado), el terminal de pago TP transmite 70 a la PDA el resultado RES de la transacción (o bien una confirmación del pago, o bien una notificación del fallo de la transacción), y la aplicación trabajo instalada en la PDA toma el relevo para finalizar la compra. Esta finalización puede consistir, en función de la aplicación trabajo, desde acreditar los puntos de fidelidad en una cuenta del cliente hasta verificar el estado de los stocks etc..

En la descripción que se acaba de realizar, se comprende fácilmente que las amenazas que recaen sobre los intercambios de datos entre la PDA y el terminal deben controlarse al máximo. Es por tanto indispensable garantizar un nivel de seguridad elevado del proceso de emparejamiento entre la PDA y el terminal de pago. Se comprende en efecto que, si desde el principio un atacante llega a conseguir el código PIN transmitido del terminal de pago hacia la PDA, la seguridad posterior de los intercambios entre estos dos aparatos está fuertemente comprometida.

En este modo de realización, los inventores han tenido la ingeniosa idea de utilizar las funcionalidades que están integradas tanto en el terminal de pago como en la PDA. Mas particularmente, en este modo de realización, el terminal de pago dispone de una impresora y la PDA de un escáner óptico de códigos de barras. Por tanto mas que ser necesaria la introducción de un código PIN por el comerciante, los inventores han propuesto, en este modo de realización, generar aleatoriamente un código PIN a nivel del terminal de pago, e imprimir el símbolo que representa este código PIN con la forma de un código de barras gracias a la impresora del terminal de pago. Una vez impreso, este símbolo con forma de código de barras es después escaneado por la PDA, con la ayuda de una aplicación de

escaneo adecuada e interpretada por la PDA. El resultado de esta interpretación (que es el código PIN generado por el terminal de pago) es después suministrado al modulo Bluetooth de la PDA con el fin de que pueda finalizar el procedimiento de emparejamiento.

En un modo de realización, igualmente, se imprime un segundo símbolo con la forma de un código de barras. Corresponde a la dirección Bluetooth del terminal de pago. Este segundo código de barras es igualmente escaneado por la PDA en una segunda fase y se obtiene la dirección Bluetooth del terminal de pago. Esto permite autentificar de forma única el terminal al que debe emparejarse la PDA.

Así, gracias a este método de la invención, se resuelven los dos problemas anteriormente citados, a saber, por una parte el problema ligado a los errores de introducción de cadenas de caracteres de gran longitud y el problema ligado a la necesaria confidencialidad que debe estar alrededor del código PIN obtenido.

La invención ha sido descrita en un modo de realización particular. Se entiende que la invención no se limita únicamente a este modo de realización. La invención se refiere igualmente a los equipos que son empleados para permitir el emparejamiento tal y como ha sido anteriormente descrito. Mas concretamente, la invención se refiere a un equipo aceptador. El equipo aceptador incluye, según la invención: unos medios de generación de un código de emparejamiento en respuesta a esta decisión de emparejamiento, unos medios de restitución, con la forma de un símbolo, del código de emparejamiento. Estos medios de restitución pueden, tal y como se ha indicado, consistir en una impresora, una pantalla o un medio de restitución sonora.

El conjunto de estos medios están controlados por un programa de ordenador específicamente adaptado, en función de un protocolo de emparejado inicial, para generar un código de emparejado, transformarlo en un símbolo y restituir este símbolo. El programa de ordenador incluye además una fase de suspensión del emparejado mientras que el procedimiento de emparejado no se haya completado a nivel del equipo iniciador.

La invención se refiere igualmente a un equipo iniciador. El equipo iniciador incluye, según la invención: unos medios de obtención de un símbolo de un código de emparejamiento en respuesta a esta decisión de emparejamiento, unos medios de decodificación del símbolo adquirido suministrando un código de emparejamiento u otros datos útiles en función del símbolo y de su tipo. Estos medios de obtención pueden, tal y como se ha indicado, consistir en un captador óptico, una cámara, un micro.

El conjunto de estos medios son controlados por un programa de ordenador específicamente adaptado, en función de un protocolo de emparejamiento inicial, para obtener uno o varios símbolos, decodificarlo en un código de emparejamiento y llevar a cabo el consiguiente emparejamiento. El programa de ordenador incluye además una fase de suspensión del emparejamiento mientras que el procedimiento de emparejamiento no haya sido completado a nivel del equipamiento aceptador.

Se presenta, en relación con la figura 3, un modo de realización de un equipo aceptador según la invención.

Dicho equipo aceptador incluye una memoria 31 constituida por una memoria intermedia, una unidad de tratamiento 32 , equipada por ejemplo con un microprocesador P, y controlada por el programa de ordenador 33, llevando a cabo el procedimiento de modificación según la invención.

Al iniciarse, las instrucciones de código del programa de ordenador 33 están por ejemplo cargadas en una memoria RAM antes de ser ejecutadas por el procesador de la unidad de tratamiento 32. La unidad de tratamiento 32 recibe en la entrada al menos una información I, tal como una decisión de emparejamiento. El microprocesador de la unidad de tratamiento 32 lleva a cabo las etapas del procedimiento de emparejamiento descrito anteriormente, según las instrucciones del programa de ordenador 33, para suministrar una información tratada T, tal como el o los símbolos necesarios para el emparejamiento del equipo. Para ello, el equipo incluye, además de la memoria intermedia 31, los medios anteriormente descritos. Estos medios son controlados por el microprocesador de la unidad de tratamiento 32.

Se presenta, en relación con la figura 4, un modo de realización de un equipo iniciador según la invención.

Dicho dispositivo incluye una memoria 41 constituida por una memoria intermedia, una unidad de tratamiento 42, equipada por ejemplo con un microprocesador P, y controlada por el programa de ordenador 43, llevando a cabo el procedimiento de emparejamiento según la invención.

Al inicio, las instrucciones del código del programa de ordenador 43 están por ejemplo cargadas en una memoria RAM antes de ser ejecutadas por el procesador de la unidad de tratamiento 42. La unidad de tratamiento 42 recibe en la entrada al menos la información I, tal como un símbolo que proviene de un equipo aceptador. El microprocesador de la unidad de tratamiento 42 lleva a cabo las etapas del procedimiento de modificación descrito anteriormente, según las instrucciones del programa de ordenador 43, para suministrar una información tratada T, tal como el código de emparejamiento. Para ello, el dispositivo incluye, además de la memoria intermedia 41, los medios anteriormente descritos. Estos medios están controlados por el microprocesador de la unidad de tratamiento 42.

Tal y como se ha comprendido perfectamente, el procedimiento de emparejamiento tal y como ha sido descrito incluye de hecho un primer sub procedimiento de emparejamiento que es llevado a cabo en el terminal iniciador y un segundo sub procedimiento de emparejamiento que es llevado a cabo en el terminal aceptador.

REIVINDICACIONES

1- Método de emparejamiento de un primer equipo, llamado equipo iniciador que desea transmitir y recibir unos datos con un segundo equipo, llamado equipo aceptador, dicho método incluye

- una etapa de generación asíncrona de un código de emparejamiento, que incluye un código PIN aleatorio;

- una etapa de restitución, con la forma de una imagen de marca de agua en la que un primer símbolo está oculto, dicho primer símbolo incluye dicho código de emparejamiento;

- una etapa de obtención, por dicho equipo aceptador, de al menos un dato útil para la transmisión y para la recepción con dicho equipo iniciador;

- una etapa de restitución, con la forma de un segundo símbolo, de dicho al menos un dato útil.

2- Método de emparejamiento de un primer equipo, dicho equipo iniciador desea transmitir y recibir datos con un segundo equipo, llamado equipo aceptador, dicho método incluye

- una etapa de adquisición de una imagen de marca de agua en la que está oculto un primer símbolo, por dicho equipo iniciador;

- una etapa de obtención de dicho primer símbolo;

- una etapa de decodificación de dicho primer símbolo adquirido suministrando un código de emparejamiento asíncrono incluyendo un código PIN aleatorio;

- una etapa de adquisición de un segundo símbolo por dicho equipo iniciador;

- una etapa de decodificación de dicho segundo símbolo que entrega datos útiles para la transmisión y la recepción con dicho equipo iniciador.

3- Método de emparejamiento según una de las reivindicaciones 1 y 2 en el que dicho segundo símbolo pertenece a un tipo de símbolo y dicho tipo de símbolo pertenece al grupo que incluye:

- un código de barras de una dimensión;

- un código de barras de dos dimensiones;

- una imagen de marca de agua;

- una secuencia sonora modulada.

4- Método de emparejamiento según la reivindicación 2, en el que dicho equipo iniciador es una PDA

5- Método de emparejamiento según la reivindicación 1, en el que dicho equipo aceptador es un terminal de pago.

6- Método según la reivindicación 1, en el que dicha etapa de restitución de dicho código de emparejamiento con la forma de una imagen con una marca de agua incluye una etapa de impresión de dicha imagen de marca de agua en una impresora de dicho equipo aceptador.

7- Método según la reivindicación 2, en el que dicha etapa de adquisición de dicha imagen de marca de agua por dicho equipo iniciador incluye una etapa de adquisición de una imagen representativa de dicha imagen de marca de agua.

8- Equipo iniciador que desea transmitir y recibir datos con un equipo aceptador que incluye:

- unos medios de adquisición de una imagen de marca de agua en la que un primer símbolo está oculto, dicho primer símbolo es representativo de un código de emparejamiento asíncrono que incluye un código PIN aleatorio, permitiendo el emparejamiento de dicho equipo aceptador y de dicho equipo iniciador, dicha imagen de marca de agua está restituida por un equipo aceptador;

- unos medios de obtención de dicho primer símbolo;

- unos medios de decodificación de dicho primer símbolo adquirido suministrando dicho código de emparejamiento.

- unos medios de adquisición de un segundo símbolo representativo de datos útiles para la transmisión y la recepción con dicho equipo aceptador;

- unos medios de decodificación de dicho segundo símbolo que suministra dichos datos útiles.

9- Equipo aceptador que desea transmitir y recibir datos con un equipo iniciador, que incluye:

- unos medios de generación de un código de emparejamiento asíncrono que incluye un código PIN aleatorio que permite el emparejamiento de dicho equipo aceptador y de dicho equipo iniciador;

- unos medios de generación de una imagen de marca de agua en la que está oculto un primer símbolo, dicho símbolo incluye dicho código de emparejamiento;

- unos medios de restitución, de dicha imagen de marca de agua.

- unos medios de obtención de al menos un dato útil para la transmisión y la recepción con dicho equipo iniciador;

- unos medios de restitución, con la forma de un segundo símbolo, de al menos dicho dato útil.

10- Método de emparejamiento según la reivindicación 5, en el que dicha imagen de marca de agua es un logo de marca de agua de una entidad que utiliza dicho terminal de pago.

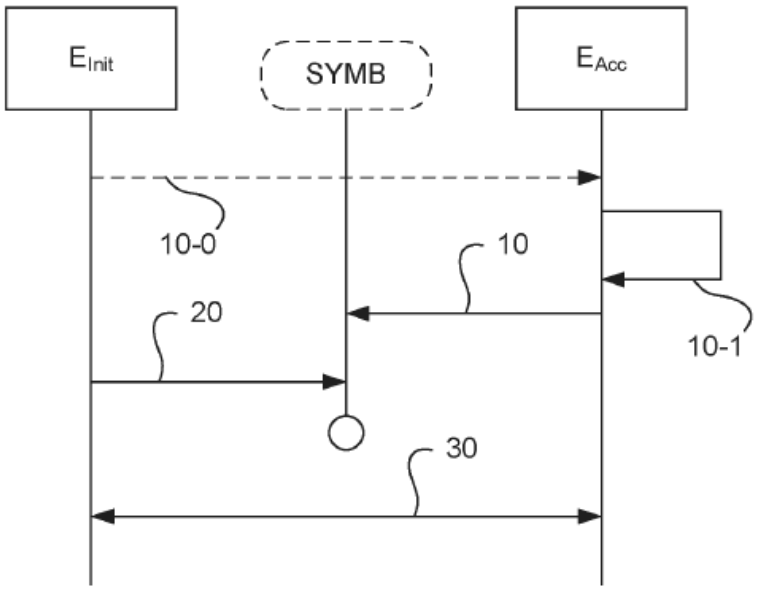

Figura 1

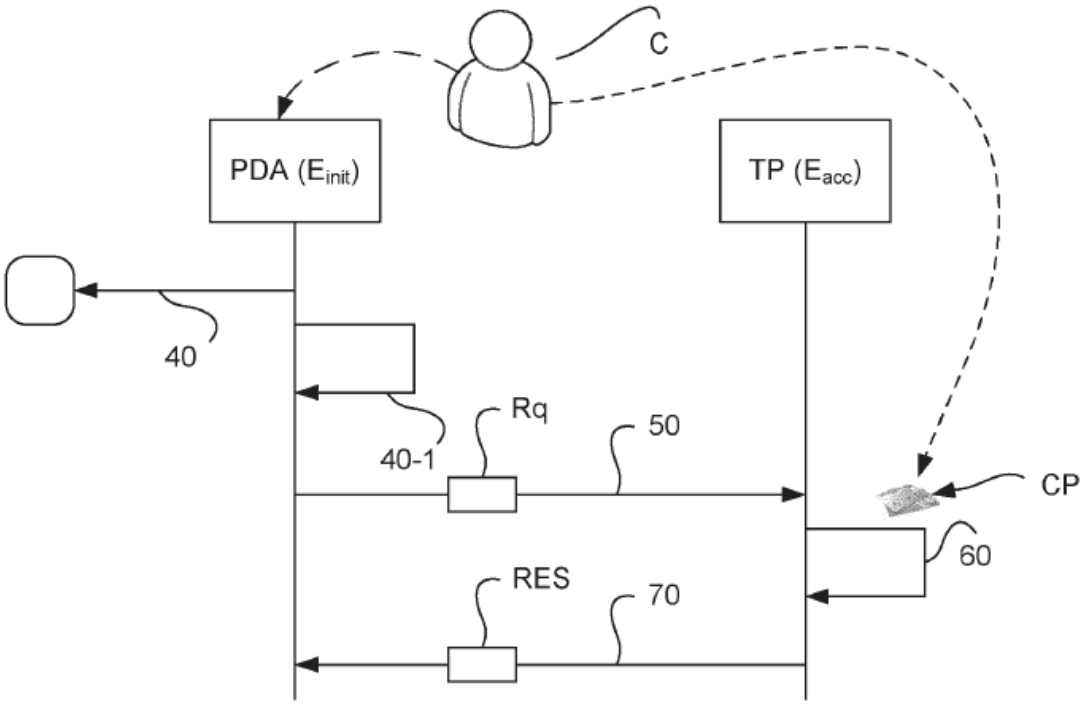

Figura 2

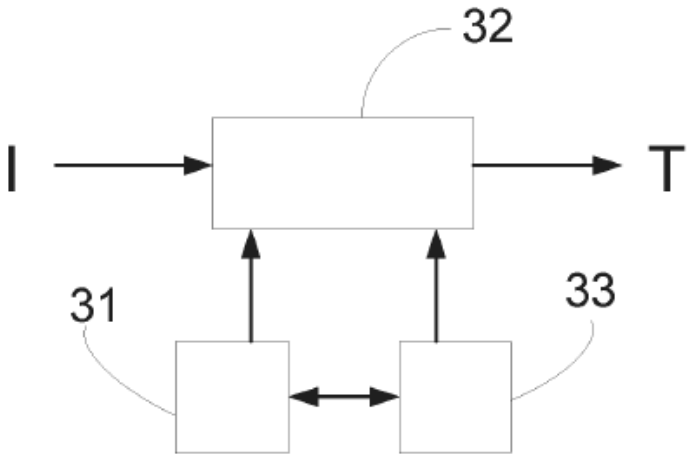

Figura 3

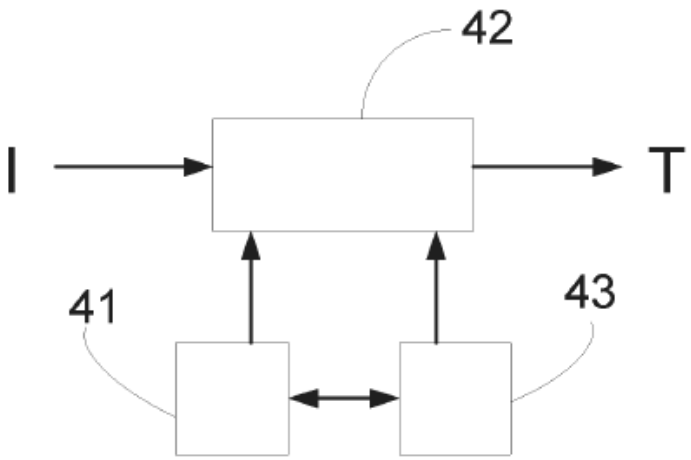

Figura 4