(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 444 650**

(51) Int. CI.:

G06K 7/10 (2006.01)
G06K 7/00 (2006.01)
G06K 19/14 (2006.01)
G06K 19/073 (2006.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **13.04.2004 E 09005069 (1)**

(97) Fecha y número de publicación de la concesión europea: **18.12.2013 EP 2081135**

(54) Título: **Soporte de datos sin contacto.**

(30) Prioridad:

14.04.2003 DE 10317257

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
26.02.2014

(73) Titular/es:

GIESECKE & DEVRIENT GMBH (100.0%)
PRINZREGENTENSTRASSE 159
81677 MÜNCHEN, DE

(72) Inventor/es:

GRAF, HANS;
FINKENZELLER, KLAUS y
ROSSMADL, ALFRED

(74) Agente/Representante:

ARPE FERNÁNDEZ, Manuel

DESCRIPCIÓN

Soporte de datos sin contacto

La presente invención se refiere a un dispositivo y un procedimiento para la determinación segura de utilización voluntaria de un soporte de datos sin contacto.

Por el concepto "soporte de datos sin contacto" o "tarjeta sin contacto" utilizado en lo que sigue, se entienden todas las disposiciones que presentan un microchip y una antena conectada a éste que pueden intercambiar datos con un equipo lector adecuado. Entre éstas se incluyen, además de tarjetas inteligentes para aplicaciones de pago, también documentos de identificación legibles sin contacto, tales como pasaportes y documentos nacionales de identidad con microchip incorporado, así como además etiquetas RFID.

Hoy día, los soportes de datos sin contacto se emplean en el servicio de pagos exclusivamente en aplicaciones cerradas, como por ejemplo para el pago en un comedor colectivo, o en transportes públicos. El motivo de ello es que, en Alemania, hasta la fecha las tarjetas sin contacto no están permitidas para aplicaciones de pago, por ejemplo como monedero electrónico, por motivos de seguridad. Un factor decisivo para ello es el temor a la posibilidad de que terceras personas descarguen de manera inadvertida un monedero electrónico del titular de la tarjeta. Por ejemplo, sería concebible que, por medio de un terminal móvil para tarjetas sin contacto que se moviese a través de concentraciones de personas (por ejemplo ferias, conciertos, el metro, estaciones), fuese posible extraer inadvertidamente dinero "electrónico" de las carteras que se hallan en las proximidades. En el caso de las tarjetas con contacto no existe tal problema, ya que un proceso de pago por parte del titular de la tarjeta se realiza insertando la misma en el lector de tarjetas.

Además de la utilización como medios de pago, las tarjetas sin contacto pueden emplearse también como soportes de datos en documentos de valor, como por ejemplo pasaportes. En particular existe la posibilidad de utilizar tarjetas sin contacto como visados que pueden incluirse en el documento de viaje, por ejemplo pegados. Con este fin resulta adecuado por ejemplo el procedimiento Coil-on-Chip [bobina sobre chip] (CoC), en el que la antena está dispuesta en el chip. Sin embargo, también pueden utilizarse disposiciones sin contacto convencionales, como por ejemplo láminas con un chip dispuesto en las mismas y una bobina impresa en la lámina.

También en la utilización de tarjetas sin contacto en documentos de valor se presenta el problema de la necesidad de impedir una lectrura no voluntaria por terceros. Lo mismo es aplicable para la lectura no autorizada e inadvertida de transpondedores sin contacto empleados para la identificación de productos.

Un soporte de datos descrito en el documento FR 2770316 A1 comprende un elemento fotosensible, por ejemplo un fotodetector. El soporte de datos no está listo para utilizarse, por ejemplo para una transmisión de datos sin contacto basada en antena con un equipo lector, hasta que el elemento fotosensible detecta una incidencia de luz. Tal incidencia de luz puede darse por ejemplo cuando el usuario del soporte de datos saca éste de un bolsillo o similar en señal de una utilización voluntaria. También puede estar previsto que el elemento fotosensible detecte un rayo de luz emitido por un equipo lector y sólo entonces pase a un modo de disposición para el uso.

El documento US 2003/0057276 A1 describe un procedimiento para la detección automatizada de la corrección de la identidad de un objeto, que comprende una primera identificación legible por máquina, por ejemplo un código de barras, y una segunda identificación legible por máquina sin contacto. Para comprobar la identidad se leen y se comparan entre sí las dos identificaciones.

El objetivo de la presente invención es por lo tanto la puesta a disposición de un dispositivo y de un procedimiento para la determinación segura de utilización voluntaria de un soporte de datos sin contacto por parte del titular de una tarjeta.

El objetivo se logra mediante las características de las reivindicaciones independientes. En las reivindicaciones dependientes de éstas se indican configuraciones ventajosas y perfeccionamientos de la invención.

A través del canal de transmisión de datos adicional se intercambian por medios ópticos, entre el equipo lector y el soporte de datos, datos que son adecuados para realizar una autentificación entre el equipo lector y la tarjeta sin contacto. La autentificación a través del canal de transmisión de datos adicional, impide un accionamiento no voluntario de la tarjeta sin contacto, dado que la información óptica deja de estar disponible cuando el soporte de datos ya no es ópticamente visible para el equipo lector, o sea por ejemplo cuando se lleva el mismo en un bolsillo/monedero.

Según una primera forma de realización de la invención, el soporte de datos presenta información ópticamente legible, como por ejemplo un código de barras o un código matricial. Cuando se presenta la tarjeta al equipo lector, esta información se lee mediante un dispositivo lector óptico, por ejemplo un escáner de código de barras, y se evalúa. A continuación, la información leída por medios ópticos puede ser utilizada por el soporte de datos sin contacto para la autentificación con el equipo lector sin contacto, con el fin de presentar así la autorización para una transacción subsiguiente.

Una ampliación de esta primera configuración consiste en emitir a través del chip la información indicada ópticamente en un dispositivo de presentación, por ejemplo una pantalla LCD. De este modo, ya no resulta fácil copiar la información, dado que ésta puede contener también estructuras de datos generadas de manera aleatoria.

Según otra configuración de la invención, el soporte de datos sin contacto está equipado con medios ópticos luminosos, por ejemplo un diodo emisor de luz IR o una lámina luminiscente. Al mismo tiempo, los medios luminosos puede disponer de una conexión eléctrica con el chip o ser parte integrante de dicho chip. En cuanto un equipo lector sin contacto se propone efectuar una transacción con el soporte de datos, se utilizan los medios luminosos para enviar al equipo lector por medios ópticos datos adicionales del chip. Estos datos pueden formar parte de una autentificación recíproca y, según la invención, se utilizan para autorizar una transacción subsiguiente. Si en el equipo lector no se conocen los datos transmitidos ópticamente no puede efectuarse una transacción con el soporte de datos.

Adicionalmente pueden detectarse en el soporte de datos variaciones de las condiciones ambientales, en cuanto éste es sacado del bolsillo para un proceso de pago. Así, por ejemplo mediante un componente óptico fotosensible (14), puede determinarse si la tarjeta se halla en un bolsillo o fuera del mismo. Al mismo tiempo, el componente fotosensible puede disponer de una conexión eléctrica con el chip o ser parte integrante de dicho chip. En cuanto el componente fotosensible está expuesto a una luminosidad mínima, se genera una señal de autorización que permite una transacción del chip con el equipo lector sin contacto.

Un perfeccionamiento de esta idea consiste en que el propio equipo lector genere una señal óptica. Para autorizar una transacción con el chip es concebible el dotar a la señal óptica de una modulación marcada, por ejemplo una señal de 1 kHz, o transmitir al chip mediante la señal óptica datos que se utilicen para la autentificación entre el soporte de datos y el equipo lector.

Una combinación de las formas de realización antes mencionadas consiste en poner a disposición en la tarjeta tanto medios ópticos luminosos como medios receptores ópticos y conectarlos al chip o poner a disposición estos medios como parte integrante del chip. En este caso, además de una transmisión bidireccional de datos sin contacto, podría realizarse una transmisión bidireccional de datos óptica entre la tarjeta y un equipo lector. Según la invención, está previsto al mismo tiempo cambiar entre los distintos canales de transmisión, pudiendo utilizarse preferentemente cada canal de transmisión, al menos, una vez para la transmisión de datos.

Otra ventaja de esta disposición consiste en que la energía para el funcionamiento de los medios ópticos de comunicación se obtiene del canal de transmisión sin contacto (por ejemplo acoplamiento magnético o capacitivo). Se sobrentiende que para la comunicación óptica puede utilizarse, además de luz visible, también IR, UV o una mezcla (uplink vs. downlink [enlace ascendente frente a enlace descendente]) de estos intervalos.

Análogamente a la información óptica podría utilizarse también adicionalmente información acústica, por ejemplo en forma de la transmisión de una señal acústica codificada, que puede generarse por ejemplo con un altavoz (por ejemplo un altavoz piezoeléctrico) integrado en la tarjeta.

Además, un altavoz dispuesto en la tarjeta es adecuado también para acusar recibo de cada transacción de pago con una señal, que indique al titular de la tarjeta que en ese momento se está realizando un proceso de pago con su tarjeta. Cierto es que en esta configuración de la invención aún sería posible extraer dinero de la tarjeta de manera no autorizada con un terminal sin contacto móvil, pero la transacción no pasaría inadvertida.

En lugar de un altavoz puede estar previsto también como alternativa o adicionalmente dotar al soporte de datos de una alarma por vibración.

A continuación se explica la invención más detalladamente por medio de los ejemplos de realización representados en los dibujos.

Muestran:

- Figura 1 una forma de realización de la presente invención, en la que en el soporte de datos está aplicada una información óptica,

- Figura 2 otra forma de realización de la invención, con medios luminosos dispuesto en el soporte de datos,

- Figura 3 otra forma de realización de la invención, con medios de recepción óptica dispuestos en el soporte de datos,

- Figura 4 otra forma de realización de la invención, con un componente óptico dispuesto en el soporte de datos,

- Figura 5 un ejemplo de realización de un procedimiento para la derivación de una clave criptográfica y

- Figura 6 un ejemplo de realización de un procedimiento de autentificación.

La figura 1 muestra un soporte de datos sin contacto 1a, con una antena 2 dispuesta en éste y un chip 3 conectado de manera eléctrica al mismo. Una zona del soporte de datos presenta información óptica 4, por ejemplo un código de barras o también un código matricial, adecuado para ser transmitido al equipo lector 1 a través de un canal de transmisión de datos óptico 5. El canal de transmisión de datos ópticos 5 se pone a disposición adicionalmente al canal de transmisión de datos sin contacto basado en antena 15.

En la figura 2 se representa un soporte de datos sin contacto en el que está dispuesto medios ópticos luminosos 6. Los medios luminosos 6, que puede configurarse como LED, OLED o también como diodo emisor de luz infrarroja (IR-LED), que está eléctricamente conectado al chip 3, como se indica con la flecha 7, y es activado por éste. También en este caso se realiza una transmisión óptica de datos a través del canal de transmisión de datos 8.

En la figura 3 está representada otra forma de realización en la que en el soporte de datos 1a está dispuesto medios de recepción óptica 9, que están eléctricamente conectados al chip 3 que permiten una transmisión de datos bidireccional óptica entre el equipo lector 1 y el soporte de datos 1a. Aquí, el chip 3 puede encargarse del control tanto de la transmisión de datos sin contacto 15 como de la transmisión de datos óptica 10. Ambos canales de transmisión pueden hacerse funcionar alternativa o también simultáneamente. Además, los canales de transmisión pueden hacerse funcionar de manera equilibrada o de manera jerárquica (Master-Slave [maestro-esclavo]).

Por medio del componente óptico 14 representado en la figura 4, que presenta una conexión galvánica 11 con el chip 3, puede autorizarse la transmisión de datos (indicada mediante la flecha 12) a través de la interfaz sin contacto basada en antena si se produce una incidencia de luz 13 suficiente.

El procedimiento para el desbloqueo de información secreta almacenada en el soporte de datos 1a puede desarrollarse como se explica a continuación. Como está representado en la figura 5, la memoria 21 del chip 3 presenta varias zonas de memoria 24 o 22, que en parte son libremente legibles y en parte tienen su contenido protegido contra una lectura no autorizada por medio de unas claves adecuadas. La zona de memoria protegida 22 contiene, al menos, un juego de datos 23 que consiste en información que ha de mantenerse en secreto, como por ejemplo datos biométricos, PIN, etc. La zona de memoria libremente legible 24 contiene, al menos, un juego de datos 25 que está asignado de forma unívoca al juego de datos respectivo 23 y representa un valor de compresión, por ejemplo un CRC, un troceo [*hash]*, una suma de comprobación criptográfica, etc. Queda excluida la posibilidad de deducir el contenido del juego de datos secreto 23, a partir del contenido del juego de datos libremente legible 25.

Para la lectura de uno de los juegos de datos 23 está previsto, según la invención, leer en una primera etapa de procedimiento el juego de datos 25 asignado al mismo, a través del canal de transmisión de datos basado en antena 15, y leer la información ópticamente legible 20, por ejemplo un código de barras o una MRZ (machine readable zone [zona legible por máquina]), del soporte de datos 1a por medio del equipo lector 1.

En una segunda etapa de procedimiento a partir del juego de datos 25 y de la información ópticamente legible 20, se deriva una clave criptográfica 26. Para ello pueden emplearse cualesquiera métodos de derivación de claves, suficientemente conocidos en el estado actual de la técnica, como por ejemplo una derivación de clave mediante el uso de una clave maestra, etc. La clave criptográfica individual para el soporte de datos, derivada a partir de la clave maestra secreta, está almacenada ya en el soporte de datos. La clave maestra está depositada en el equipo lector para la derivación de la clave criptográfica 26, mediante la información leída ópticamente 20 y el juego de datos leído sin contacto 25.

Una tercera etapa de procedimiento prevé realizar una autentificación 27 entre el equipo lector 1 y el chip 3 del soporte de datos 1a mediante la clave criptográfica derivada. De este modo se comprueba si la clave en cuestión conocida por el equipo lector 1 y la clave depositada en el soporte de datos 1a son idénticas. Un procedimiento de autentificación ya conocido en el estado actual de la técnica funciona según el principio "*Challenge-Response* [pregunta-respuesta] ", que se ha extendido ampliamente en el campo de las tarjetas chip. Mediante una instrucción "GetChallenge", el equipo lector 1 recibe un número aleatorio del chip 3, para a continuación autentificarse frente al chip a través de los datos de una instrucción "External Authenticate [autenticación externa]", derivada del número aleatorio y la clave. Por supuesto, pueden utilizarse etapas de autentificación adicionales, por ejemplo para la autenticación recíproca, y otros procedimientos de autenticación.

En un procedimiento simplificado, el equipo lector debe autenticarse en la tercera etapa de procedimiento sólo como tal equipo lector que utiliza ambos canales de transmisión de datos, sin probar al mismo tiempo el conocimiento de una clave secreta. En este caso, en la segunda etapa de procedimiento 26 se deriva, por ejemplo, un valor que, si bien se utiliza como clave para la tercera etapa 27, no es secreto ni ha sido derivado a partir de una clave maestra.

En una última etapa opcional del procedimiento, a partir del juego de datos 23 leído se forma un valor de compresión y se compara este último con el contenido del juego de datos libremente legible 25 (véase la figura 5, comprobación 28). Si los dos valores de compresión son diferentes, ha de suponerse que el juego de datos 23 ha sido modificado de forma no autorizada. Si la autenticación se realiza con éxito puede leerse el juego de datos 23.

El procedimiento descrito en la figura 6 prevé también permitir el acceso, al menos, a una parte, de los datos almacenados en el transpondedor, sólo después de haberse realizado con éxito la autenticación. El procedimiento funciona también según el principio "Challenge-Response [pregunta-respuesta]".

En una primera etapa 30, el equipo lector 1 pide un número aleatorio al soporte de datos 1a mediante el canal de transmisión de datos basado en antena 15. En este procedimiento, un número aleatorio generado por el soporte de datos 1a se transmite al equipo lector 1 (etapa 31: "response [respuesta]") mediante el canal de transmisión de datos óptico 5, por ejemplo un LED (infrarrojo/UV). Otra posibilidad consiste en dar salida al número aleatorio en una pantalla 4 del soporte de datos sin contacto 1a en forma de un código de barras, un código de píxeles, una MRZ (machine readable zone [área legible por máquina]). Simultáneamente puede enviarse también mediante el canal de transmisión de datos basado en antena 15 una respuesta que se diferencie en su contenido de los datos sin contacto transmitidos por medios ópticos, pero que evite un *timeout* (vencimiento) en el canal de transmisión, o sea en particular en el equipo lector. Por una parte, un posible atacante no puede sacar conclusiones sobre el contenido escuchando en paralelo el canal de transmisión basado en antena 15, y por otra parte tampoco es necesario un tratamiento especial de distintas instrucciones de aplicación, de manera que no es necesario modificar el software del equipo lector 1. Existe por ejemplo la posibilidad de enviar el código "90 00" (instrucción ejecutada con éxito). Para desorientar a eventuales atacantes pueden transmitirse también datos falsos.

También es concebible pedir el número aleatorio a través del canal de transmisión de datos óptico y transmitirlo a través del canal de transmisión de datos basado en antena.

El algoritmo de autentificación se desarrolla a continuación según el procedimiento ya conocido para la autenticación unilateral o recíproca ("external authenticate [autenticación externa]", 32). Si la autenticación concluye con éxito puede comenzar la comunicación propiamente dicha 33 y leerse el juego de datos 23.

El procedimiento descrito con referencia a la figura 6 puede aplicarse en combinación con o independientemente del procedimiento descrito en la figura 5.

Una ventaja de los procedimientos descritos consiste en que mediante la utilización de dos canales de transmisión de datos distintos – el óptico 5 y el basado en antena 15 – se dificulta considerablemente una falsificación o un intercambio de datos. Por lo tanto, resultan especialmente adecuados para el intercambio de datos delicados, como por ejemplo datos personales. Mediante el empleo unido de ambos canales de transmisión de datos se mejoran tanto la autenticación unilateral como la autenticación recíproca.

Sin embargo, dependiendo de los datos a transmitir, también es concebible utilizar opcionalmente sólo un canal de transmisión de datos. La pérdida de seguridad que esto implica va unida por regla general a una ganancia en velocidad de procesamiento y, si los datos son por ejemplo como los que se requieren para el campo de la logística, el transporte de mercancías y la gestión de mercancías, puede tolerarse en determinadas circunstancias. Si han de procesarse también datos delicados por medio del mismo soporte de datos 1a, puede estar prevista para ello de manera forzosa la utilización de ambos canales de transmisión de datos en la lectura por parte del equipo lector. La conmutación entre uno o dos canales de transmisión puede realizarse aquí de manera automatizada una vez colocado un señalizador o similar.

El equipo lector 1 se trata de un equipo inteligente, que dispone tanto de medios de lectura sin contacto basados en antena 2 como de medios de lectura ópticos. En una forma de realización preferida, el equipo lector 1 está configurado como un equipo terminal móvil, por ejemplo un teléfono móvil, un PDA, un ordenador portátil o similar, y presenta una interfaz para la comunicación sin contacto, por ejemplo NFC (Near Field Communication [comunicación de campo cercano]). Como medio de comunicación óptico puede emplearse la interfaz IRDA presente en la mayoría de los equipos. Como medio lector óptico puede estar prevista una cámara. Los datos ópticamente legibles, como por ejemplo el número de serie del chip 3 del soporte de datos 1a, se representan en una forma legible por máquina (código de barras, datos OCR). Un equipo lector 1 de este tipo resulta especialmente adecuado para el control de documentos de viaje por parte de la policía o la guardia fronteriza, pudiendo realizarse otras consultas a través de una conexión en línea adicional eventualmente existente.

Para aumentar la seguridad puede estar previsto que el chip 3 del soporte de datos 1a genere adicionalmente un número aleatorio como número de serie y lo transmita al equipo lector 1 mediante el canal de transmisión de datos basado en antena. La utilización de tales números de serie aleatorios se describe por ejemplo en ISO 14443 (Chapter 6.4.4, "UID contents and cascade levels"). El número de serie del soporte de datos 1a necesario para el desarrollo del algoritmo anticolisión no consiste aquí como es habitual en una cifra inequívoca e inconfundible, sino en un número aleatorio generado en cada transacción. Gracias a esta medida, ya no es posible deducir a partir del número de serie utilizado la identidad del soporte de datos. De este modo es posible impedir con gran eficacia un eventual ataque efectuado mediante la repetición de una comunicación captada una vez entre el soporte de datos y el terminal.

Los datos ópticamente legibles pueden también estar disponibles de manera no estática en el soporte de datos 1a y por ejemplo modificarse dinámicamente por medio de una pantalla o similar. De este modo pueden generarse y presentarse también contraseñas de un solo uso, números de serie aleatorios, etc. Además, también es concebible cualquier combinación de los datos generados dinámicamente y los datos transmitidos bien por medio de la antena o bien por medios ópticos.

Según la presente invención, un soporte de datos sin contacto presenta una antena y un chip, presentando el soporte de datos medios para la transmisión de datos a través de un canal de transmisión de datos óptico y medios para la transmisión de datos a través de un canal de transmisión de datos basado en antena. En el soporte de datos están dispuestos datos que pueden transmitirse a un equipo lector mediante el canal de transmisión de datos óptico y/o el canal de transmisión de datos basado en antena.

REIVINDICACIONES

1. Soporte de datos sin contacto (1a) con una antena (2) y un chip (3), en el que el chip (3) comprende una memoria (21) con varias zonas de memoria (22, 24),

en el que, al menos, una de las zonas de memoria (24) es libremente legible y al menos una de las zonas de memoria (22) está protegida contra una lectura no autorizada por medio de una clave criptográfica,

en el que la zona de memoria protegida (22) comprende, al menos, un primer juego de datos (23) mientras que la zona de memoria libremente legible (24), comprende, al menos, un segundo juego de datos (25), estando el segundo juego de datos (25) asignado de forma unívoca al primer juego de datos (23) y formando el segundo juego de datos (25) un valor de compresión, y

en el que el primer juego de datos (23) y el segundo juego de datos (25) pueden transmitirse a un equipo lector (1) mediante un canal de transmisión de datos basado en antena (15),

estando dispuestos además en el soporte de datos (1a) datos ópticamente legibles (20) que pueden transmitirse al equipo lector (1) mediante un canal de transmisión de datos óptico, y

estando el soporte de datos (1a) adaptado para permitir al equipo lector (1) una lectura del primer juego de datos (23) después de haberse realizado con éxito una autentificación entre el soporte de datos (1a) y el equipo lector (1) por medio de una clave criptográfica derivada del segundo juego de datos (25) y los datos ópticamente legibles (20).

2. Soporte de datos según la reivindicación 1, caracterizado porque los juegos de datos almacenados se almacenan como juegos de datos codificados con una clave criptográfica.

3. Soporte de datos según una de las reivindicaciones 1 a 2, caracterizado porque en el soporte de datos está dispuesto un componente fotosensible, que controla el funcionamiento del chip dependiendo de la luminosidad.

4. Soporte de datos según una de las reivindicaciones 1 a 3, caracterizado porque en el soporte de datos está aplicado un código matricial.

5. Soporte de datos según una de las reivindicaciones 1 a 3, caracterizado porque en el soporte de datos está aplicado un código de barras.

6. Soporte de datos según una de las reivindicaciones precedentes, caracterizado porque en el soporte de datos está dispuesto una pantalla para la presentación de datos ópticos.

7. Soporte de datos según una de las reivindicaciones precedentes, caracterizado porque en el soporte de datos está dispuesto medios luminosos para enviar señales ópticas.

8. Soporte de datos según una de las reivindicaciones precedentes, caracterizado porque en el soporte de datos está dispuesto un medio receptor óptico para recibir señales ópticas.

9. Soporte de datos según una de las reivindicaciones precedentes, caracterizado porque en el soporte de datos está dispuesto un altavoz.

10. Soporte de datos según una de las reivindicaciones precedentes, caracterizado porque en el soporte de datos está dispuesto un avisador por vibración.

11. Procedimiento para la determinación segura de utilización voluntaria de un soporte de datos sin contacto con una antena (2) y un chip (3),

en el que el chip (3) comprende una memoria (21) con varias zonas de memoria (22, 24),

en el que, al menos, una de las zonas de memoria (24) es libremente legible y, al menos, una de las zonas de memoria (22) está protegida contra una lectura no autorizada por medio de una clave criptográfica,

en el que la zona de memoria protegida (22) comprende, al menos, un primer juego de datos (23) y la zona de memoria libremente legible (24) comprende, al menos, un segundo juego de datos (25), estando el segundo juego de datos (25) asignado de forma unívoca al primer juego de datos (23) y formando el segundo juego de datos (25) un valor de compresión, y

en el que el primer juego de datos (23) y el segundo juego de datos (25) pueden transmitirse a un equipo lector (1) mediante un canal de transmisión de datos basado en antena (15),

estando dispuestos además en el soporte de datos (1a) datos ópticamente legibles (20) que pueden transmitirse al equipo lector (1) mediante un canal de transmisión de datos óptico (5),

procedimiento en el que, para leer el primer juego de datos (23),

en una primera etapa de procedimiento, el equipo lector (1) lee el segundo juego de datos (25), asignado de forma unívoca al primer juego de datos (23), mediante el canal de transmisión de datos basado en antena (15) y lee los datos ópticamente legibles (20) mediante el canal de transmisión de datos óptico (5),

en una segunda etapa de procedimiento el equipo lector (1) deriva del segundo juego de datos (25) y de los datos ópticamente legibles (20) una clave criptográfica,

en una tercera etapa de procedimiento se realiza una autentificación entre el soporte de datos (1a) y el equipo lector (1) mediante la clave criptográfica derivada, y

en una cuarta etapa de procedimiento el equipo lector (1), una vez realizada con éxito la autentificación, lee el primer juego de datos (23).

12. Procedimiento según la reivindicación 11, caracterizado porque la transmisión de datos se realiza de forma bidireccional.

13. Procedimiento según una de las reivindicaciones 11 a 12, caracterizado porque se realiza una autentificación (27, 32) al menos unilateral entre el equipo lector y el soporte de datos.

14. Procedimiento según la reivindicación 13, caracterizado porque la autentificación (27, 32) se realiza de tal manera que requiere la utilización de ambos canales de transmisión de datos.

15. Procedimiento según una de las reivindicaciones 11 a 14, caracterizado porque en una quinta etapa de procedimiento se forma un valor de compresión a partir del primer juego de datos y en una etapa adicional de procedimiento se realiza una comparación del valor de compresión así formado con el segundo juego de datos.

16. Procedimiento según una de las reivindicaciones 13 a 15, caracterizado porque la autentificación (27, 32) se realiza a modo de un procedimiento cuestión-respuesta (*challenge-response)*.

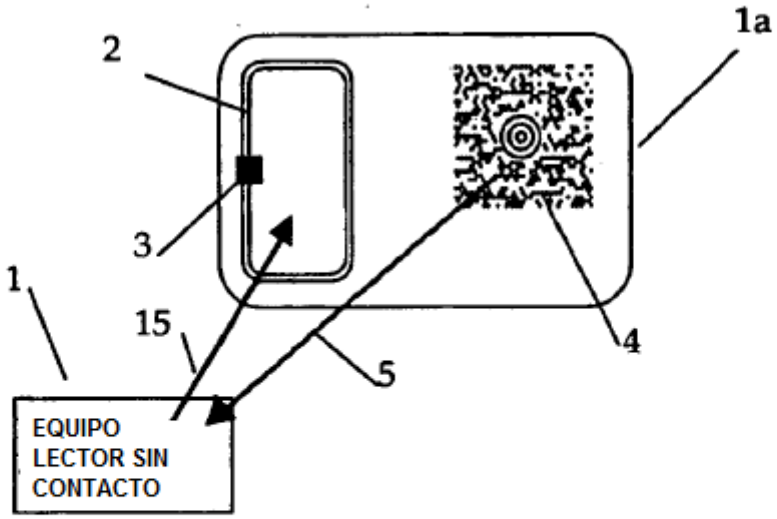
2
1a
3
1
15
5
4
EQUIPO
LECTOR SIN
CONTACTO

Fig. 1

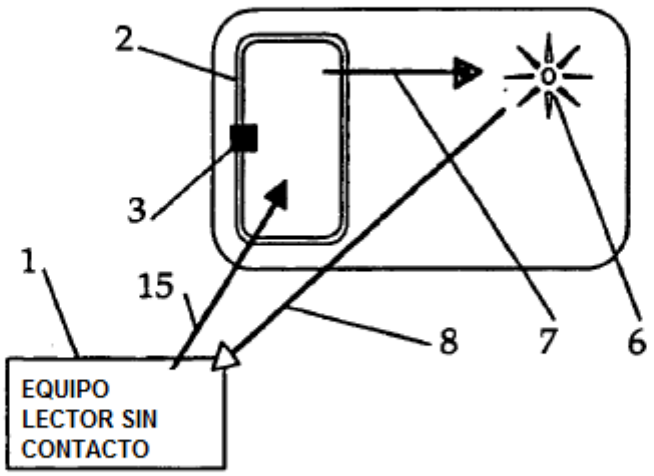
2
3
1
15
8
7
6
EQUIPO
LECTOR SIN
CONTACTO

Fig. 2

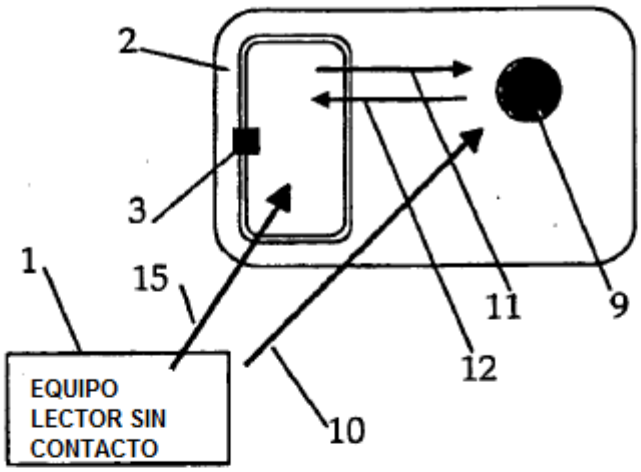
2
3
1
15
11
9
12
EQUIPO
LECTOR SIN
CONTACTO
10

Fig. 3

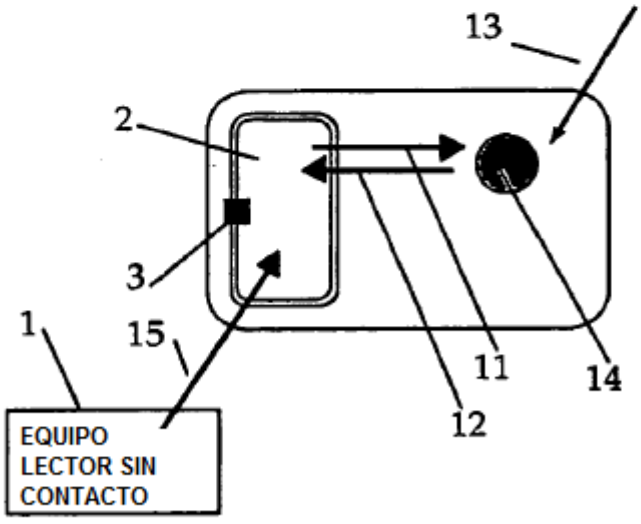
13
2
3
1
15
11
14
12
EQUIPO
LECTOR SIN
CONTACTO

Fig. 4

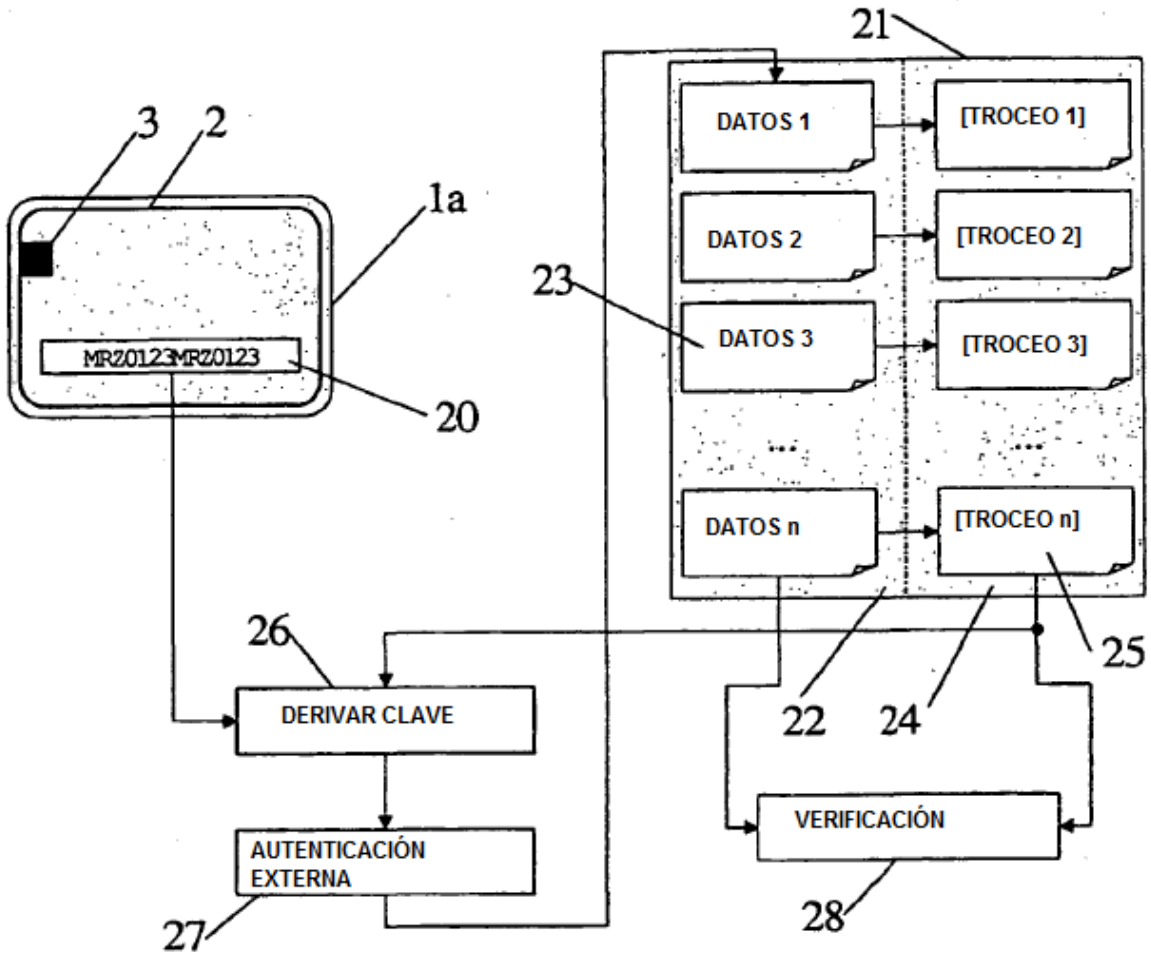
21
3
2
1a
MRZ0123MRZ0123
20
23
DATOS 1
[TROCEO 1]
DATOS 2
[TROCEO 2]
DATOS 3
[TROCEO 3]
DATOS n
[TROCEO n]
26
DERIVAR CLAVE
AUTENTICACIÓN EXTERNA
27
22
24
25
VERIFICACIÓN
28

Fig. 5

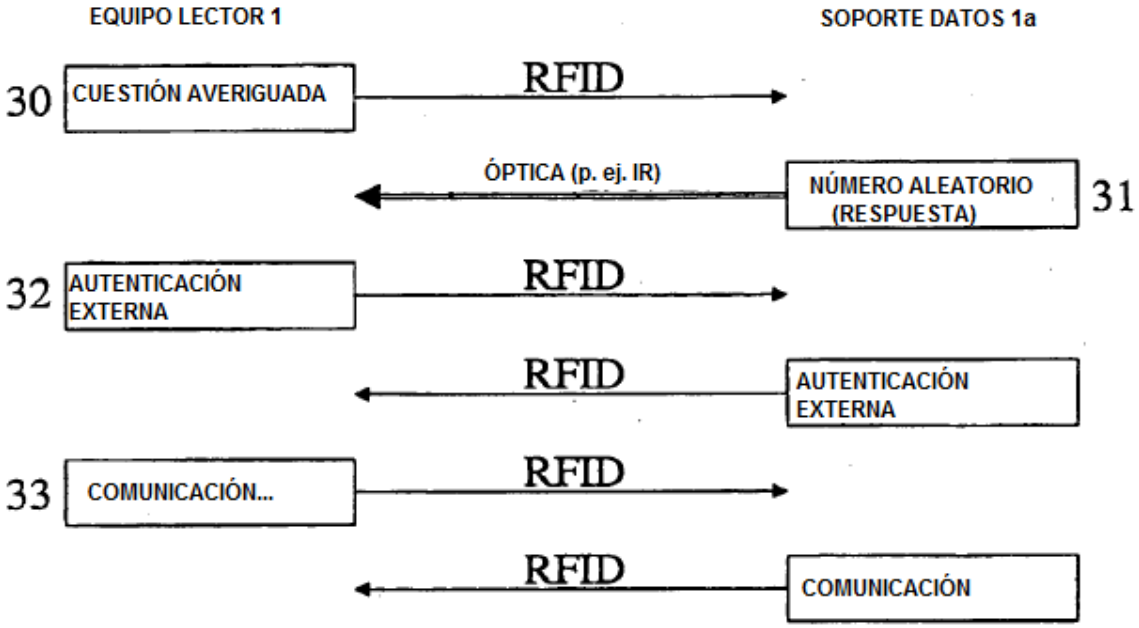
EQUIPO LECTOR 1
SOPORTE DATOS 1a
30
CUESTIÓN AVERIGUADA
RFID
ÓPTICA (p. ej. IR)
NÚMERO ALEATORIO (RESPUESTA)
31
32
AUTENTICACIÓN EXTERNA
RFID
RFID
AUTENTICACIÓN EXTERNA
33
COMUNICACIÓN...
RFID
RFID
COMUNICACIÓN

Fig. 6

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 citados en la descripción

- FR 2770316 A1 **[0006]**
- US 20030057276 A1 **[0007]**