(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 439 942**

(51) Int. CI.:

G06K 19/077 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **03.08.2006 E 06794305 (0)**

(97) Fecha y número de publicación de la concesión europea: **02.10.2013 EP 2047414**

(54) Título: **Documento securizado, especialmente pasaporte electrónico con seguridad reforzada**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.01.2014

(73) Titular/es:

SMART PACKAGING SOLUTIONS (SPS) (100.0%)
AVENUE OLIVIER PERROY - ZI DE ROUSSET
13106 ROUSSET, FR

(72) Inventor/es:

BRUNET, OLIVIER;
ARTIGUE, OLIVIER;
BOCCIA, HENRI;
PATRICE, PHILIPPE y
PEYTAVIN, IVAN

(74) Agente/Representante:

PÉREZ BARQUÍN, Eliana

DESCRIPCIÓN

Documento securizado, especialmente pasaporte electrónico con seguridad reforzada

La invención se refiere a un documento securizado, especialmente como un documento de identidad o un pasaporte electrónico, que incluye un dispositivo de identificación mediante radiofrecuencia. La invención se refiere asimismo a un sistema de identificación que emplea dichos documentos securizados.

Para mayor claridad y simplificación en el resto de la exposición y la descripción de la invención, se hará referencia al conjunto de documentos securizados, tanto si tienen como si no una función de identificación de una persona o un objeto, mediante la terminología "documento securizado", sin que esta expresión deba entenderse de manera restrictiva con relación al factor de forma del documento, que puede adoptar la forma clásica de un documento, especialmente de papel, o estar formado por un objeto portátil securizado de otro tipo como, por ejemplo, una tarjeta de memoria o una tarjeta con microprocesador.

Se conocen ya en el estado de la técnica documentos más o menos securizados que pueden servir para la identificación de personas u objetos. De este modo, se conocen documentos tales como documentos de identidad, pasaportes, permisos de circulación para la identificación de vehículos, y permisos de conducción, documentos que emplean ciertos artificios de seguridad, como impresiones del tipo "guilloqueado", bandas de firma previstas para recibir la firma del titular, o incluso hologramas fijados al soporte del documento.

Entre estos documentos securizados conocidos, existen por lo tanto aquellos que utilizan simplemente un artificio de seguridad visual, como el guilloqueado impreso en el documento y mencionados anteriormente. Aún es así hoy en día en la mayoría de los pasaportes en circulación en la mayoría de los países. Estas impresiones de guilloqueado son simples medios visuales y pasivos de identificación. Pero, al ser difíciles de reproducir, contribuyen sin duda a elevar el nivel de seguridad con relación a documentos sin dichos artificios de seguridad, incluso si el nivel de seguridad alcanzado ya no es de conformidad con las exigencias actuales.

Por ello, ocurre con frecuencia que redes criminales roben papel que sirve para fabricar documentos de identidad, y lo utilicen para fabricar documentos de identidad falsos. Ocurre asimismo que se roben documentos de identidad vírgenes tales como, por ejemplo, pasaportes aún no personalizados con los datos de su titular, y se pongan a continuación en circulación ilegalmente a petición de personas necesitadas de documentación falsa.

Debido a estas dificultades, ha empezado a aparecer otro tipo de documento de identidad. Se trata de documentos de identidad que incorporan, eventualmente además de los artificios de seguridad impresos mencionados anteriormente, medios de identificación activos en forma de un microprocesador o un microcircuito, que se solidariza con el documento de identidad y cuya memoria está cargada con información de identidad del titular del documento. La información almacenada en el microprocesador puede leerse por medio de un lector dedicado y comprobarse mediante conexión a bases de datos capaces de realizar una serie de cotejos. Además, los datos leídos por el lector pueden mostrarse en la pantalla de un sistema de lectura, a petición de una persona encargada del control, y deben corresponder entonces a los impresos en el documento.

Aunque no se puede negar que los documentos securizados dotados de medios de seguridad pasivos, tales como el guilloqueado, o de seguridad activos, como un microcircuito que almacena datos, presentan una mayor resistencia a la falsificación con relación a los documentos sin microprocesador electrónico, sigue siendo posible falsificarlos por parte de redes determinadas y dotadas de medios técnicos suficientes.

Efectivamente, algunos falsificadores son capaces de extraer el microcircuito de un documento auténtico robado, y reinsertarlo en un documento de identidad falso.

Por lo tanto, uno de los inconvenientes de los pasaportes electrónicos ya conocidos es que, en la práctica, es posible, procediendo con minucia y las herramientas adecuadas, extraer el microcircuito que permite la identificación mediante radiofrecuencia del titular del documento, y reinsertarlo en otro pasaporte o documento de identidad, que constituye entonces una falsificación. Basta para ello imprimir el pasaporte virgen (que incluye entre otras cosas el guilloqueado auténtico), con los datos de identificación de la persona, tal como están memorizados en el microprocesador.

Durante un control del documento por las autoridades, el documento de identidad pasará la prueba visual, ya que tendrá toda la apariencia de un documento de identidad válido, y pasará la prueba realizada mediante un lector, ya que este detectará la presencia de un microcircuito y eventualmente de la información cargada en la memoria. Además, habitualmente los datos de identificación almacenados en la memoria se corresponderán con los datos de identificación impresos en el soporte del documento, de manera que este tipo de falsificación es especialmente difícil de detectar por parte de las autoridades.

La solicitud internacional de patente WO 2004/008386 A1 se refiere a un documento de identidad o tarjeta con microprocesador que incluye un sustrato, por ejemplo de papel. Una antena está impresa en el sustrato, así como

dos primeros armazones de dos condensadores. El contra-electrodo, es decir el otro armazón de los dos condensadores, está formado por una banda conductora que constituye asimismo una característica de seguridad del documento de identidad, como un guilloqueado o un holograma.

Un objeto de la invención es, en consecuencia, proponer un documento securizado, especialmente un pasaporte electrónico, que sea aún más seguro que los documentos securizados conocidos en el estado de la técnica.

Otro objeto de la invención es proponer un documento securizado dotado de un microcircuito electrónico, que sea capaz de resistir la extracción abusiva del microcircuito, o que sea tal que la extracción del microcircuito a partir del documento de origen convierta el documento en totalmente inutilizable.

Otro objeto de la invención es proponer un documento securizado con microcircuito con funcionamiento con contacto y/o sin contacto, especialmente mediante radiofrecuencia en este último caso, y que solo pueda funcionar, a efectos del lector de contacto o de radiofrecuencia susceptible de interactuar con él, solo cuando el documento securizado incluye el microcircuito electrónico de origen, así como medios de seguridad pasivos de origen, de manera que la alteración de uno de los dos tipos de medios de seguridad convierta el conjunto del documento en inoperante, es decir que no pueda ser detectado como válido por los lectores previstos.

A tal efecto, el principio de la invención prevé unir estrecha y funcionalmente los medios de seguridad visuales o pasivos del documento securizado, tales como el guilloqueado y otros, y las características de seguridad activas incorporadas en un circuito microelectrónico incluido en el documento. Los medios de seguridad pasivos están diseñados para ser capaces de interactuar con los medios de seguridad activos, de manera a hacerlos funcionales cuando el documento securizado se sitúa en el campo electromagnético de un lector sin contacto. De esta forma, la componente de seguridad basada en los medios de seguridad gráficos del documento y la componente de seguridad basada en la información almacenada en el procesador microelectrónico forman un conjunto indivisible capaz de aumentar considerablemente el nivel de seguridad de los documentos securizados, especialmente de los documentos de identidad securizados.

Para poner en aplicación este nuevo principio, la invención tiene por objeto un documento securizado según la reivindicación 1.

Preferentemente, se filtra la respuesta electromagnética de los medios de seguridad activos, de manera que la señal amplificada, especialmente la corriente inducida en los medios de seguridad activos, lo sea en una horquilla de frecuencia característica del soporte securizado.

Preferentemente, la antena de los medios de seguridad activos se calcula y dispone para no permitir el reconocimiento del documento securizado por parte de un lector, en la ausencia de dichos medios de seguridad pasivos. Es decir que en la ausencia de los medios de seguridad pasivos asociados (tales como guilloqueado específico), la señal obtenida en los bornes de los medios de seguridad activos en respuesta a la señal de interrogación del lector nunca puede ser suficiente, cualquiera que sea especialmente la proximidad del lector, para leer los datos de identidad contenidos en el microprocesador. En consecuencia, fuera de la asociación específica en el mismo soporte del microprocesador de origen y de los medios de seguridad pasiva de origen, el lector nunca podrá dar por válido el documento securizado.

En un primer modo de realización de la invención, los medios de seguridad pasivos incluyen una red de guilloqueado conductor impreso en el soporte, especialmente mediante tintas conductoras, elegidas de manera que el circuito (R,L,C) que forma amplifique la corriente inducida en la antena de los medios de seguridad activos cuando se sitúa el documento en el campo de un lector sin contacto, para conducir la corriente inducida más allá de un umbral necesario para garantizar el funcionamiento del microcircuito de los medios de seguridad activos.

En una variante de realización de la invención, los medios de seguridad pasivos incluyen una banda de firma realizada en el soporte, incluyendo asimismo esta banda de firma características eléctricas (R,L,C) y electromagnéticas específicas. Otra variante de realización de la invención prevé, en lugar del guilloqueado conductor o la banda de firma, un holograma realizado en el soporte. Una variante aún más sofisticada puede incluir para los medios de seguridad pasivos, cualquier combinación de guilloqueado, una banda de firma y/o un holograma, sabiendo que el conjunto tendrá, también en este caso, características R,L,C y electromagnéticas específicas.

En el caso en que el documento de firma se realiza de la manera clásica de los pasaportes que incluyen un libro con una pluralidad de páginas con eventualmente una tapa más gruesa que las páginas internas para recibir el microprocesador, se puede prever que los medios de seguridad activos estén insertados en una primera página o en la tapa, y que los medios de seguridad pasivos estén dispuestos en otra página, pero también es posible la disposición inversa.

Esta disposición impide especialmente un técnica de fraude clásica, que consiste en colocar en el interior de una tapa del pasaporte electrónico robado (y dotado de un microprocesador) un conjunto de páginas con guilloqueado

recuperadas de otra parte. Gracias a la invención, un pasaporte con guilloqueado que no presente las características R.L.C específicas que permiten el funcionamiento del microprocesador no podrá ser leído por el lector y será considerado como un pasaporte falso.

En un modo de realización ventajoso y compacto del documento securizado según la invención, este se presenta en forma de una tarjeta con microprocesador, teniendo los medios de seguridad activos la forma de un módulo microelectrónico con un microprocesador unido a una antena e incorporado al cuerpo de la tarjeta con microprocesador, y estando los medios de seguridad pasivos dispuestos en una capa interna o en el grosor de la tarjeta con microprocesador, de manera a amplificar el campo electromagnético que atraviesa el módulo microelectrónico cuando la tarjeta con microprocesador se sitúa en el campo de un lector.

El documento securizado según la invención puede ser tal que los medios de seguridad activos incluyen un microcircuito sin contactos externos, estando los bornes del microcircuito unidos únicamente a una antena, lo que lo hace capaz de interactuar únicamente con los lectores sin contacto.

Alternativamente, los medios de seguridad activos incluyen un microcircuito provisto de contactos, a la vez que está unido a una antena, lo que hace el documento securizado capaz de interactuar tanto en modo contacto con lectores con contacto, como en modo sin contacto con lectores sin contacto.

Además, en el caso de recurrir a medios de seguridad pasivos en forma de guilloqueado, es teóricamente posible que el conjunto de la red de guilloqueado sea conductor. Sin embargo, las tintas conductoras que sirven para la impresión del guilloqueado son relativamente caras. Además, la resistencia eléctrica de una red de guilloqueado totalmente conductora sería muy elevada, lo que haría más difícil la elección de los demás parámetros (L.C) para obtener un funcionamiento satisfactorio. Una alternativa ventajosa consiste en seleccionar únicamente, en la red de guilloqueado, alguno de ellos a realizar en tinta conductora. Esta solución presenta la doble ventaja de ser menos cara, pero también de incrementar aún más la seguridad, ya que será aún más difícil para un defraudador determinar las características de la red de guilloqueado conductor a reproducir, ya que no bastará con reproducir el conjunto del guilloqueado que aparece visualmente en el pasaporte electrónico.

Otra variante de la invención consiste en sustituir el guilloqueado conductor por una antena integrada en la red de guilloqueado lo más discretamente posible, desde el punto de vista visual, realizándose entonces la red de guilloqueado de manera clásica con tinta no conductora.

La invención tiene asimismo por objeto un sistema de comprobación de identidad según la reivindicación 13.

Otras características y ventajas de la invención aparecerán mediante la lectura de la descripción detallada y los dibujos adjuntos, en los cuales:

- la figura 1 ilustra un documento securizado con microcircuito y sin guilloqueado, según el estado de la técnica;

- la figura 2 ilustra un documento securizado con microcircuito idéntico al de la figura 1, visto en plano para mostrar el guilloqueado, con un reventado parcial para mostrar los medios de seguridad activos;

- la figura 3 ilustra un primer modo de realización de un documento securizado según la invención;

- la figura 4 ilustra un esquema eléctrico de un sistema compuesto por un lector de documentos securizados, y de un documento securizado según la invención;

- la figura 5 representa, en forma de gráfico, la potencia electromagnética reflejada por el sistema de la figura 4.

Se hace referencia a figura 1. Se ha representado en esta figura un esquema de principio en plano de un documento securizado 1 conocido en el estado actual de la técnica, habiéndose realizado este documento al tamaño de una tarjeta con microprocesador. La representación incluye un reventado parcial 3 para mostrar la capa del cuerpo de tarjeta que incluye la antena 5. El documento securizado 1 incluye un módulo microelectrónico 7 que incluye un microprocesador (no representado), cuyos bornes están unidos a los bornes de una pequeña antena 9. Dado el escaso tamaño de la antena 9, el flujo magnético que se puede recuperar mediante la antena 9 durante el paso por el campo magnético de un lector es relativamente débil, lo que limita el alcance de funcionamiento del documento de identidad. Para remediar esto, se conoce la opción de añadir al cuerpo de tarjeta una antena 5 de mayor tamaño cuyo efecto, conocido en sí, será amplificar considerablemente, mediante mutua inductancia, el flujo captado por la pequeña antena 9 cuando la tarjeta pasa por el campo del lector.

Sin embargo, se observa en esta realización conocida, que es bastante fácil de falsificar, ya que incluye una única componente de seguridad activa. Para obtener un documento de identidad funcional, basta con trasladar el micromódulo 7 extraído de otro pasaporte a una tarjeta falsa, es decir a un cuerpo de tarjeta personalizado con los datos relativos al falso portador.

Para remediar esto y aumentar un poco la seguridad del documento, se conoce asimismo, como se muestra en la figura 2, la opción de revestir el cuerpo de tarjeta 1 con una serie de medios de seguridad pasivos visuales, tales como un guilloqueado 11. La impresión de guilloqueado se realiza mediante tintas no conductoras, y recurre, en lo que se refiere a su forma y reparto, a funciones matemáticas aleatorias, como ya es conocido en sí. No todos los falsificadores potenciales controlan este tipo de impresión, lo que reduce un poco el riesgo de fraude. Sin embargo, sigue sin existir, en esta segunda variante del estado de la técnica, una asociación estrecha entre los medios de seguridad pasivos que constituye el guilloqueado, y los medios de seguridad activos que constituye el módulo microeléctrico 7. Se trata en realidad de una simple yuxtaposición de medios, sin interacción entre ellos.

A continuación, se hace referencia a la figura 3, que representa esquemáticamente el principio de la invención, en asociación con guilloqueado 11 no conductor, entendiéndose que este ejemplo no es en absoluto limitativo, ya que el principio de la invención puede llevarse a cabo con otros tipos de medios de seguridad pasivos, especialmente como las bandas de firma, los hologramas u otros, o una combinación de dichos medios de seguridad pasivos. El documento securizado 13 representado en forma de un pasaporte electrónico con las dimensiones de una tarjeta con microprocesador (tanto si es conforme a la norma ISO 7816 como si no), incluye siempre un módulo electrónico 7 dotado de un microprocesador y de una pequeña antena 9, así como de guilloqueado clásico 11 impreso en el cuerpo de tarjeta.

Según la figura 3, una antena 15 está prevista e integrada visualmente en la red de guilloqueado 11 para ocultarse en la misma. No está conectada eléctricamente a ningún otro componente, pero se utilizan sus características R.L.C como se explicará con mayor detalle más adelante. Cabe subrayar que esta antena 15 puede asimismo estar constituida ventajosamente, para cumplir la misma función, por algún guilloqueado (también con referencia 15) con las mismas características electromagnéticas.

La antena o el guilloqueado 15 están impresos con tinta conductora, de colores que no permiten distinguirlos del otro guilloqueado 11, no conductor, de la red de guilloqueado. Poseen características eléctricas de resistencia R, inductancia L y capacidad C específicas, que hacen de ellos un circuito R.L.C distinto entre una tarjeta y otra, o entre un tipo de tarjeta y otro tipo de tarjeta. En la práctica, se puede tener por ejemplo la misma red de guilloqueado para un mismo cliente para todas las tarjetas emitidas entre dos fechas dadas. Se podría obtener asimismo un grado de distinción más o menos grande, en función de la aplicación y de las necesidades de seguridad expresadas por el emisor de tarjetas.

Se hace referencia a las figuras 4 y 5 para explicar con mayor detalle el funcionamiento eléctrico y electromagnético de un sistema que utiliza un lector de documentos securizados, y documentos securizados conformes a la invención.

En la figura 4, se ha representado en la parte izquierda el esquema eléctrico de principio de un lector 17 con funcionamiento sin contacto. Incluye de manera conocida un amplificador 19 que emite hacia un circuito (R,L,C) 21, una señal destinada a un documento electrónico securizado. La señal puede ser en principio una señal que comanda la lectura de información almacenada en la memoria del documento securizado, o una señal de escritura, entendiéndose sin embargo que, en una aplicación de seguridad clásica, el lector 17 enviará una señal de lectura al documento securizado 13 para comprobar su autenticidad y la correcta correspondencia con el portador del documento. En la parte derecha, se ha representado el esquema eléctrico de principio de un documento securizado 13 según la invención. Incluye medios de seguridad activos, en forma de un procesador microelectrónico 23 que incluye por lo menos una memoria en la que se almacenan los datos que debe leer el lector, teniendo dicho procesador por lo menos uno de sus circuitos, típicamente su circuito de alimentación, conectado a un circuito R_m,L_m,C_m que hace oficio de antena. Las características R_m,L_m,C_m se eligen de tal manera que, cualquiera que sea la distancia del documento securizado 13 con relación al lector 17, es decir incluso si esta distancia es nula o casi nula, la corriente inducida por el lector en el circuito de alimentación del microprocesador 23 es insuficiente para despertar el microprocesador y para hacerlo funcionar en lectura o en escritura.

A estos medios de seguridad activos (23, 25) se asocian medios de seguridad pasivos 27, en forma de un amplificador de campo magnético, cuyas características eléctricas R_a,L_a,C_a se eligen para amplificar de manera considerable, mediante mutua inductancia con referencia M2, la señal electromagnética de lectura o de escritura procedente del lector 17 mediante el acoplamiento M1. De esta forma, circula por el circuito de alimentación 25 del microprocesador 23 una corriente superior a la corriente mínima para hacer funcionar el microprocesador.

Cabe subrayar que debido a las características de funcionamiento de los circuitos R_a,L_a,C_a, la amplificación mediante el amplificador de campo 27 se acompaña de un filtrado de frecuencia, de manera que es posible ajustar en una horquilla de frecuencia característica el pico de amplitud de campo o de corriente inducida, debido al acoplamiento con los medios de seguridad pasivos. Por lo tanto, el único acoplamiento electromagnético de medios de seguridad activos (23, 25) y pasivos (27) correctamente emparejados será susceptible de llevar la corriente inducida a los medios de seguridad pasivos más allá de su umbral de funcionamiento y, por ello, podrá hacer funcionar un documento de seguridad dado.

La figura 5 representa una curva representativa de la potencia electromagnética reflejada por el documento securizado 13, por ejemplo la curva de la intensidad de la corriente inducida en el circuito de alimentación del

microprocesador 23, en función de la distancia con el lector 17, medida en unidades arbitrarias. La representación se ha realizado en la ausencia de amplificación de campo magnético (curva A), y con amplificación de campo magnético (curva B). Se observa en la curva A que, cualquiera que sea la proximidad del documento securizado con relación al lector, la intensidad de la corriente inducida permanecerá siempre inferior al umbral S que permite hacer funcionar el microprocesador 23. Por el contrario, se observa en la curva B que, gracias a la amplificación, existen zonas (en el ejemplo representado, aquellas para las que la distancia entre el lector y el documento securizado es inferior a dos unidades de distancia) en las que la corriente inducida es superior al umbral mínimo S, lo que permite despertar el microprocesador y hacerlo funcionar.

Cada conjunto de guilloqueado específico 15 se calcula de manera a amplificar el campo electromagnético del lector 17 de un sistema de identificación, en una horquilla de frecuencia determinada, lo que tiene como efecto amplificar y filtrar el flujo de que se beneficia la antena 9 del micromódulo 7. Preferentemente, el circuito de antena 9 del módulo 7 se calcula de tal manera que el flujo procedente solo de la corriente inducida en la antena 9 en la ausencia del guilloqueado conductor 15 no permite “despertar” el microprocesador del micromódulo 7 y leerlo. Por el contrario, el guilloqueado 15 se calcula, por parte del especialista en la materia, desde el punto de vista de su tamaño y de su disposición, para constituir un circuito electrónico que es tal que el campo que recuperan permite, mediante mutua inductancia M2, amplificar considerablemente la corriente inducida en la antena 9, en una horquilla de frecuencia determinada. Esta amplificación permite llevar el campo y, por lo tanto, la corriente inducida, más allá de un umbral que permite “despertar” el microprocesador del micromódulo 7 en su horquilla de frecuencia de funcionamiento asociada y, por lo tanto, comunicarse con el microprocesador en lectura y/o en escritura.

A continuación, se describe con mayor detalle el papel y el funcionamiento de concentrador o de amplificador de campo magnético desempeñado por el circuito pasivo R,L,C que constituye los medios de seguridad pasivos 27.

El amplificador de campo magnético está definido para tener una frecuencia de resonancia muy próxima o igual a la frecuencia de resonancia del sistema RFID (Radio Frequency Identification Device, en terminología anglosajona) que le será acoplado.

La siguiente fórmula permite definir el valor R,L,C:

$$Fr = 1/(2*Pi*\sqrt{(L.C)}$$

en la que Fr designa la frecuencia de resonancia, L la inductancia y C la capacidad del circuito pasivo constituido por el guilloqueado 15 en este ejemplo.

Más concretamente, estos valores R,L,C se calculan de manera conocida por el especialista en la materia, para que el par formado por el amplificador de campo magnético 27 y el módulo microelectrónico 7 con su antena 9 sea resonante en la frecuencia de trabajo de los emisores de radiofrecuencia del lector sin contacto que permiten hacer funcionar el sistema, o en una frecuencia próxima de la misma. Este sistema de amplificador de campo magnético genera en su proximidad una concentración muy fuerte de flujo electromagnético en la frecuencia de trabajo. El módulo microelectrónico 7 (aún llamado en ocasiones la “pastilla”) situado a proximidad de este amplificador de campo podrá activarse mediante un campo más fuerte que si estuviera solo y, por lo tanto, el sistema en su conjunto es más eficiente en términos de distancia de funcionamiento, o bien puede trabajar en un campo emitido por el lector más débil.

A continuación, se describe con mayor detalle un modo de realización del circuito pasivo R.L.C una vez calculado. Se toma a modo de ejemplo el caso en que el circuito pasivo 27 contiene el guilloqueado 15 de tinta electroconductora, entendiéndose que el modo de realización sería fácil de transponer, por el especialista en la materia, a otros modos de realización en los que los elementos de seguridad pasivos no son el guilloqueado.

La capacidad eléctrica C está ventajosamente realizada con tres capas de material superpuestas, es decir una capa conductora que realiza el guilloqueado que hace oficio de antena, una capa aislante realizada de un material de permitividad conocida, y una capa conductora que permite conectar los distintos guilloqueados entre ellos.

Un cálculo sencillo permite, en función de la superficie de las capas conductoras enfrentadas, del grosor del aislante que las separa y de la permitividad del aislante, definir las características R,L,C proporcionadas por dicha realización.

En una variante de esta invención en la que el documento securizado es una tarjeta con doble interfaz de comunicación con contacto y sin contacto, el módulo electrónico 7 incluye en su cara superior una bornera de conexión con contacto y, en su cara inferior, una antena conectada al microprocesador 23, localizándose el medio de seguridad pasivo 27 en el interior del cuerpo de tarjeta y constituyendo un circuito dedicado a concentrar o amplificar el flujo electromagnético procedente del lector y a dirigirlo hacia el módulo microelectrónico 7 que incluye las dos interfaces de comunicación. En esta variante, el medio de seguridad pasivo 27 está localizado en frente del módulo con doble interfaz y rodea por lo menos tres de los lados de dicho módulo.

Además, el posicionamiento de la pastilla que forma el módulo microelectrónico se define en función de las tensiones mecánicas aplicadas al documento de identidad, como ya se conoce en sí. Preferentemente, se posiciona el módulo microelectrónico 7 lejos de los ejes de tensiones mecánicas que experimenta el producto acabado. Además, para realizar la pastilla en sí, se puede proceder de manera conocida, o preferentemente como se describe en la solicitud de patente FR 05-01378 (FR 2882174 A1) del mismo depositante.

En el modo de realización en que los medios de seguridad pasivos 27 incluyen una antena 15 integrada de manera tan discreta como sea posible, incluso de forma invisible, en una red de guilloqueado 11 realizado en tinta no conductora, se procede de la siguiente manera. Como ya se conoce, se genera mediante un programa de generación de guilloqueado, el fichero PAO que permite una visualización de dicho guilloqueado. A continuación, a partir de los cálculos del amplificador magnético que proporciona especialmente el valor de inductancia L de la antena del amplificador magnético, se define una geometría de antena, utilizando una anchura de espira idéntica a la anchura del guilloqueado con objeto de que la antena sea invisible o casi invisible en la red de guilloqueado. Por medio de un programa de creación de imagen, esta antena se diseña a continuación para que se integre perfectamente en la red de guilloqueado, desde el punto de vista visual.

Se definen a continuación las superficies de las capas que permiten la creación del elemento capacitivo de los medios de seguridad pasivos, y se diseña como anteriormente, para que se integre visualmente con la antena y el guilloqueado.

Siempre utilizando un programa de creación gráfica, esta imagen se separa a continuación en función de las capas por imprimir:

- una capa para el guilloqueado que se imprimirá en tinta estándar,

- una capa para la primera capa de tinta conductora del amplificador magnético,

- una capa para el depósito aislante del elemento capacitivo del amplificador magnético y, finalmente,

- una capa para el segundo depósito conductor del amplificador magnético.

Estas distintas capas o máscaras del fichero de imagen creadas permitirán fabricar las formas impresoras utilizadas para la fabricación (película “offset”, pantalla de serigrafía... según la elección efectuada).

La última operación antes de la fabricación es la elección de los colores de las tintas. Se elegirán preferentemente para las tintas conductoras de los elementos de seguridad pasivos 27, colores similares a los de las tintas utilizadas para el guilloqueado no conductor 11.

Un procedimiento que suele emplearse para la impresión del guilloqueado en offset, es el uso de tintas de distintos colores colocadas en distintos lugares de un mismo tintero de la prensa de impresión. Esto permite una mezcla parcial en algunos lugares del tintero y, por lo tanto, en el documento, de lo que resulta un efecto de difuminado entre dos o tres tonos. En el caso del uso de este modo de impresión, los colores utilizados para las tintas conductoras y no conductoras se elegirán idénticos y se colocarán de manera idéntica en los dos tinteros.

Con objeto de no perturbar los efectos gráficos, la tinta aislante se elegirá ventajosamente transparente.

Con objeto de incrementar aún más la dificultad para localizar visualmente los elementos de seguridad pasivos 27, estos podrán realizarse por medio de una tinta conductora transparente, a base de polímero intrínsecamente conductor.

Las ventajas de la presente invención con relación a los documentos de identidad existentes son numerosas. La invención permite aumentar considerablemente la resistencia de los documentos securizados existentes, como documentos de identidad, a los intentos de falsificación. En particular, si el documento securizado es abierto o desensamblado, el módulo electrónico 23 no puede funcionar solo, ya que estará privado de los medios de seguridad pasivos 27 que lleva asociados. Efectivamente, los medios de seguridad pasivos están estrecha y funcionalmente ligados al funcionamiento eléctrico de los medios de seguridad activos del documento. Por ejemplo, si se extrae el micromódulo activo del campo del guilloqueado, deja de emitir, incluso si se sitúa en el campo del lector. Dado que el guilloqueado y el campo magnético que emiten son específicos de cada documento de identidad o de cada tipo de documento de identidad, se llega al resultado de que cada dispositivo de identificación radiofrecuencia no puede separarse de su documento de identidad, o se vuelve inactivo, lo que constituye un elevado grado de seguridad.

Además, la seguridad física o gráfica está estrechamente unida a la seguridad electrónica del documento. La falsificación de este tipo de documento es aún más difícilmente posible. Sería necesario reproducir el circuito de acoplamiento específico de un documento, lo que consistiría en emular el efecto electromagnético de los medios de seguridad pasivos tales como el guilloqueado conductor.

A las anteriores ventajas de seguridad, se añade una ventaja durante la personalización de los documentos securizados, ya que los sitios de personalización gráfica y eléctrica, a menudo separados, pueden ser objetivo de robos. Si se diera el caso, es inútil querer ensamblar módulos activos robados y cuerpos de tarjeta con los medios de seguridad pasivos según la invención, ya que el ensamblaje de tales componentes no previstos para ser emparejados, no podrá funcionar.

REIVINDICACIONES

1. Documento securizado (13), especialmente pasaporte electrónico, que incluye un soporte provisto, por una parte, de medios de seguridad activos (23, 25) susceptibles de producir una respuesta electromagnética cuando el documento securizado atraviesa el campo electromagnético de un lector sin contacto (17) previsto para obtener datos de dicho documento, estando provisto dicho soporte, por otra parte, de medios de seguridad pasivos (15, 27) capaces de interactuar con los medios de seguridad activos (23, 25) de manera a convertirlos en eléctricamente funcionales cuando el documento (13) se sitúa en el campo electromagnético del lector sin contacto, caracterizado porque dichos medios de seguridad pasivos (15, 27) se eligen de manera a presentar características eléctricas R,L,C (Ra, La, Ca) que los hacen capaces de amplificar la respuesta electromagnética de los medios de seguridad activos (23, 25), mediante acoplamiento electromagnético de los medios de seguridad activos y pasivos, más allá de un umbral que permite la identificación del documento de identidad (13) cuando este se sitúa en el campo electromagnético del lector sin contacto.

2. Documento securizado (13) según la reivindicación 1, caracterizado porque los medios de seguridad activos (23, 25) incluyen un microcircuito (23) conectado a una antena (25) susceptible de producir una respuesta electromagnética cuando atraviesa el campo electromagnético de un lector sin contacto (17), y porque dicha antena (25) está dispuesta para no permitir el reconocimiento del documento securizado (13) mediante un lector, en la ausencia de dichos medios de seguridad pasivos (27).

3. Documento securizado (13) según una de las reivindicaciones anteriores, caracterizado porque dichos medios de seguridad pasivos (27) incluyen una red de guilloqueado conductor (15) impresa en el soporte y elegida de manera que el circuito (R,L,C) que forma amplifique la corriente inducida en la antena (25) de los medios de seguridad activos cuando el documento securizado se sitúa en el campo de un lector sin contacto (17), más allá de un umbral (S) necesario para garantizar el funcionamiento del microcircuito (23) de los medios de seguridad activos.

4. Documento securizado (13) según una de las reivindicaciones 1 a 3, caracterizado porque los medios de seguridad pasivos (27) incluyen una antena cuyas espiras están integradas de manera invisible en una red de guilloqueado (11) realizada en tinta no conductora.

5. Documento securizado (13) según una de las reivindicaciones 1 a 3, caracterizado porque dichos medios de seguridad pasivos (27) incluyen una banda de firma realizada en el soporte.

6. Documento securizado (13) según una de las reivindicaciones 1 a 3, caracterizado porque dichos medios de seguridad pasivos (27) incluyen un holograma realizado en el soporte.

7. Documento securizado (13) según una de las reivindicaciones 4 a 6, caracterizado porque los medios de seguridad pasivos (27) incluyen una antena y/o guilloqueado conductor y/o una banda de firma y/o un holograma combinados.

8. Documento securizado (13) según una cualquiera de las reivindicaciones anteriores, caracterizado porque se presenta en forma de un libro de pasaporte con una pluralidad de páginas, y porque los medios de seguridad activos (23, 25) están insertados en una primera página o tapa, con los medios de seguridad pasivos (27) dispuestos en otra página.

9. Documento securizado (13) según una cualquiera de las reivindicaciones anteriores, caracterizado porque se presenta en forma de una tarjeta con microprocesador, teniendo los medios de seguridad activos, la forma de un módulo microelectrónico (7) que incluye un microprocesador (23) conectado a una antena (25) e incorporado al cuerpo de la tarjeta con microprocesador, y estando los medios de seguridad pasivos (27) dispuestos en el grosor de la tarjeta con microprocesador de manera a amplificar sensiblemente el campo electromagnético que atraviesa el módulo microelectrónico cuando la tarjeta con microprocesador se sitúa en el campo de un lector (17).

10. Documento securizado (13) según una cualquiera de las reivindicaciones anteriores, caracterizado porque los medios de seguridad activos (23, 25) incluyen un microcircuito (23) sin contactos externos pero conectado a una antena (25), que lo hace capaz de interactuar únicamente con lectores sin contacto (17).

11. Documento securizado (13) según una cualquiera de las reivindicaciones 1 a 10, caracterizado porque los medios de seguridad activos (23, 25) incluyen un microcircuito (23) provisto de contactos a la vez que está conectado a una antena (25), y permiten que el documento securizado sea capaz de interactuar tanto en modo con contacto con lectores con contacto, como en modo sin contacto con lectores sin contacto.

12. Documento securizado según la reivindicación 3 o la reivindicación 7, caracterizado porque solo algún guilloqueado específico (15) de la red de guilloqueado (11) es conductor y participa en los medios de seguridad pasivos.

13. Sistema de comprobación de identidad que incluye una pluralidad de documentos de identidad y por lo menos un

lector (17) con funcionamiento con contacto o sin contacto, capaz de interactuar con dicha pluralidad de documentos de identidad, incluyendo dicho lector medios de software para enviar una señal de interrogación hacia cada documento de identidad con fines de comprobación de los datos de identidad almacenados en el documento de identidad, caracterizado porque cada documento de identidad es un documento securizado (13) conforme a una cualquiera de las reivindicaciones 1 a 12.

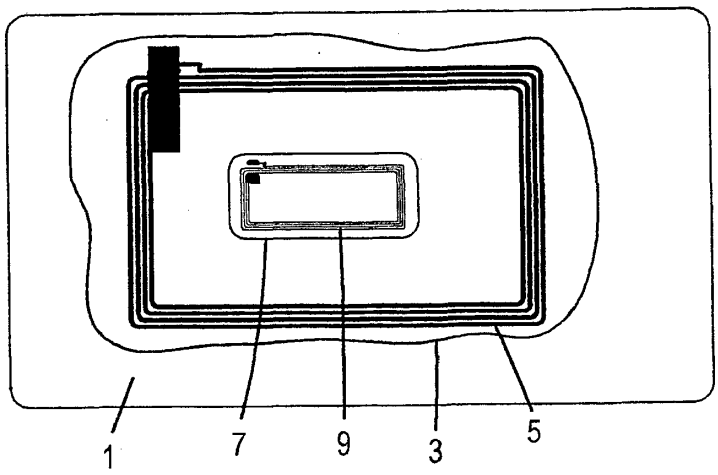

Fig.1

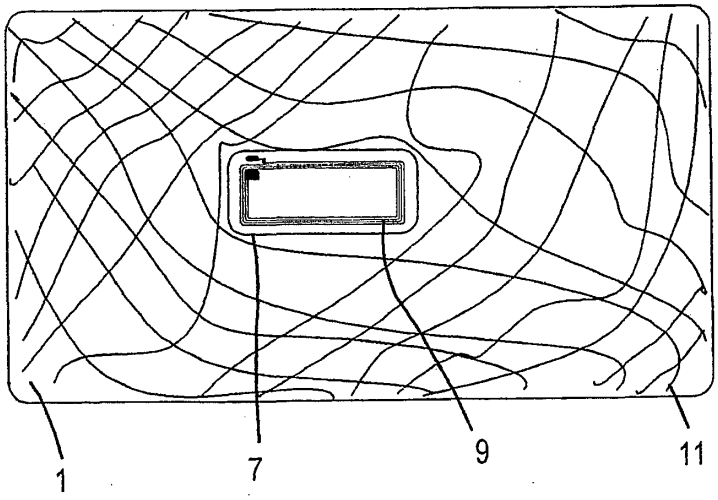

Fig.2

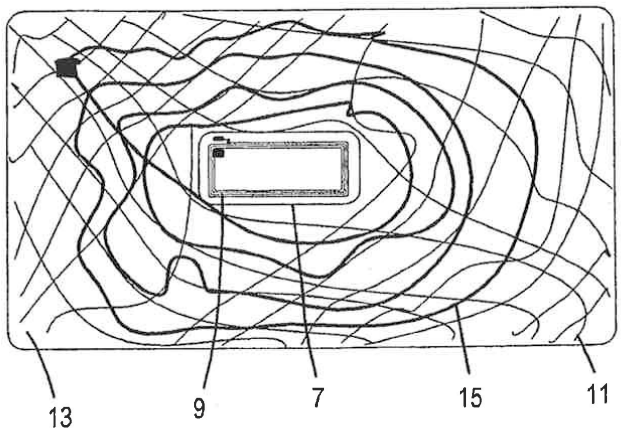
13
9
7
15
11

Fig.3

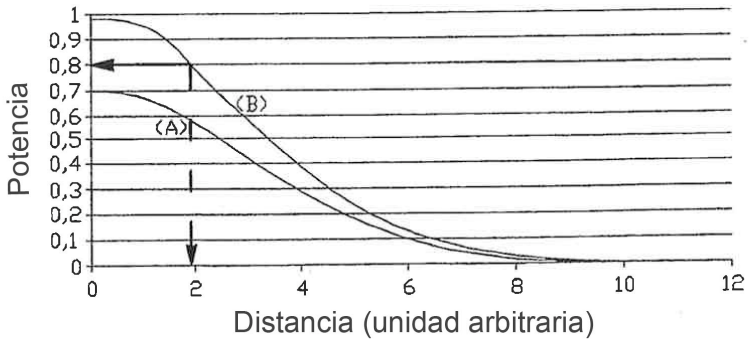
Potencia
1
0,9
0,8
0,7
0,6
0,5
0,4
0,3
0,2
0,1
0
(B)
(A)
0
2
4
6
8
10
12
Distancia (unidad arbitraria)

Fig. 5

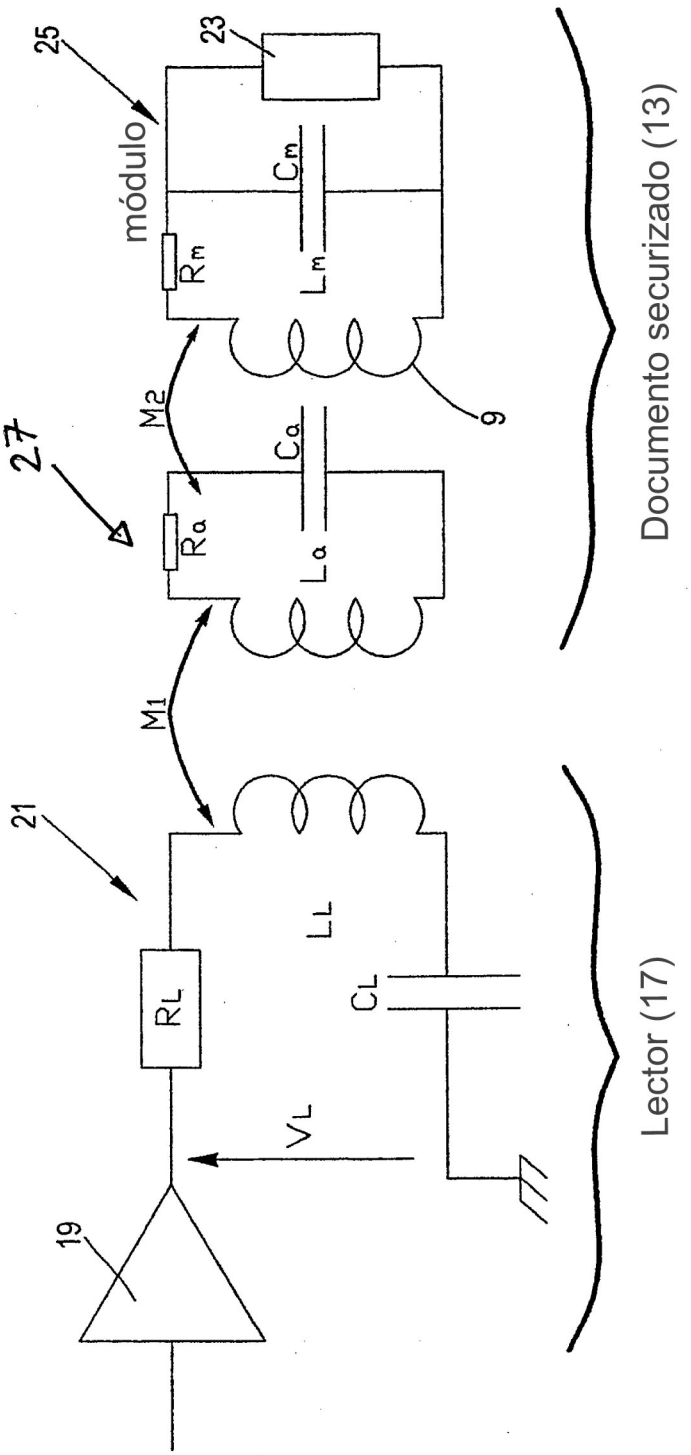
25
módulo
23
Cm
Rm
Lm
M2
27
Ca
Ra
La
9
M1
21
LL
RL
CL
VL
19
Documento securizado (13)
Lector (17)

Fig. 4