

19



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 717 159**

51 Int. Cl.:

**G06K 19/073** (2006.01)

**G07C 9/00** (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **10.12.2008 PCT/EP2008/067171**

87 Fecha y número de publicación internacional: **25.06.2009 WO09077398**

96 Fecha de presentación y número de la solicitud europea: **10.12.2008 E 08862675 (9)**

97 Fecha y número de publicación de la concesión europea: **24.10.2018 EP 2225703**

54 Título: **Método para autorizar una comunicación con un dispositivo electrónico portátil, tal como un acceso a un área de memoria, dispositivo y sistema electrónicos correspondientes**

30 Prioridad:

**18.12.2007 EP 07301688**

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

**19.06.2019**

73 Titular/es:

**GEMALTO SA (100.0%)  
6, rue de la Verrerie  
92190 Meudon, FR**

72 Inventor/es:

**BANCHELIN, XAVIER**

74 Agente/Representante:

**CASANOVAS CASSÁ, Buenaventura**

ES 2 717 159 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

## DESCRIPCION

Método para autorizar una comunicación con un dispositivo electrónico portátil, tal como un acceso a un área de memoria, dispositivo y sistema electrónicos correspondientes

Campo técnico de la invención.

La invención se refiere a un método para autorizar una comunicación con un dispositivo electrónico portátil, tal como un acceso a al menos un área de memoria del dispositivo.

La invención también incluye en un dispositivo electrónico portátil de este tipo al menos un área de memoria.

Además, la invención se refiere a un sistema electrónico que comprende al menos un dispositivo de comunicación electrónico, particularmente de lectura, que coopera con un dispositivo electrónico portátil de este tipo.

La invención encuentra aplicación en el control del funcionamiento de un dispositivo en general, preferiblemente portátil. El dispositivo autoriza o prohíbe una operación. La operación puede ser total o parcial y comprender, en particular, una autorización en el acceso a la memoria para leer o escribir, una comunicación del dispositivo con el exterior a través de medios de comunicación, etc.

Por dispositivo electrónico portátil, debe comprenderse cualquier dispositivo que comprenda medios de control y procesamiento de informaciones y medios de almacenamiento de datos. Estos datos pueden ser accesibles desde el exterior, en particular de lectura o comunicados desde el exterior. De preferencia, el objeto portátil se guarda en un bolsillo, una bolsa.

Típicamente, un dispositivo electrónico portátil puede tener la forma de un objeto integrado portátil (o "token", en inglés), tal como una tarjeta inteligente, que comprende al menos una unidad lógica de procesamiento o al menos un microprocesador, al menos una memoria, y al menos una interfaz de comunicación. La interfaz de comunicación está a cargo de la comunicación con el exterior del dispositivo electrónico portátil.

El dispositivo electrónico portátil puede cooperar con un dispositivo electrónico de comunicación o lectura, para poder explotar, al menos en parte, una o más aplicaciones compatibles con el dispositivo electrónico portátil a través del dispositivo electrónico de comunicación o lectura.

El documento WO 97/36264 revela un sistema electrónico de control del acceso de este tipo.

Estado de la técnica:

Se conoce, como dispositivo electrónico portátil, un pasaporte electrónico que comprende una página de datos (llamada "data page" en inglés) propios de su titular. El pasaporte está equipado con un chip de módulo de comunicación sin contacto de tipo PICC (acrónimo en inglés de "Tarjeta de Circuito Integrado de Proximidad"). El chip está integrado dentro del pasaporte que constituye un documento de viaje legible por una máquina (o MRTD, acrónimo de "Máquina Lectora de Documento de Viaje"). La página de datos reserva un área en la que se ve la información específica del titular. Dicha área define un área legible por una máquina (o "Zona Legible por Máquina") destinada a ser leída, ya sea a simple vista o por una máquina, pasando el área de información visible frente a un lector óptico. El chip conoce la información visible, por lo que puede utilizarse especialmente para autorizar o prohibir el acceso a un área de memoria del chip.

El lector óptico lee la información visible. El lector óptico transmite la información leída a un lector sin contacto, al que está conectado el lector óptico. El lector sin contacto utiliza la información leída al implementar un mecanismo de control de acceso básico (o "Basic Access Control" o BAC, en inglés) de acuerdo con las especificaciones de la OACI (acrónimo de "Organización de Aviación Civil Internacional", o el acrónimo inglés ICAO "International Civil Aviation Organisation") para comunicarse con el chip.

El lector sin contacto posteriormente intercambia con el chip, a través de un enlace de comunicación sin contacto, por ejemplo de tipo ISO (acrónimo en inglés de "Organización Internacional de Estandarización") 14 443. El intercambio de información permite el acceso al área de memoria del chip.

Sin embargo, tal solución conocida presente un inconveniente importante. De hecho, la información visible constituye la única información a conocer para acceder al área de memoria del chip, por lo que esta solución tiene una baja entropía. En otras palabras, la cantidad de información a ser conocida es reducida, ya que se reduce sólo a la información visible. El mecanismo de control de acceso básico es entonces particularmente sensible a un ataque llamado de tipo exhaustivo, mediante el cual se trata de intentar toda la información posible, alguna de las cuales puede ser predecible.

Así, una persona malintencionada puede acceder, sin el conocimiento de su titular, al área de memoria del chip, haciendo una simple copia de la información visible o encontrándola.

Presentación de la invención:

5 La invención supera el principal inconveniente anteriormente enunciado al proporcionar, en una realización preferida, un método para acceder a al menos a un área de memoria de un dispositivo electrónico portátil. Sin embargo, puede ser un método para establecer una comunicación, transmitiendo datos el objeto portátil, estando permitida la comunicación en función del procesamiento de la información visible efectuada por el exterior.

10 Más particularmente, la invención es un método para autorizar la comunicación con un dispositivo electrónico portátil, según la reivindicación 1.

15 Según la invención, el método comprende una etapa de variación de la información, según la cual la información varía al menos en parte.

20 El principio general de la invención se basa, por lo tanto, en un nuevo enfoque en el que la información visible presentada al exterior no se encuentra fijada como en la solución del arte anterior explicada anteriormente, sino que es modificable. Como tal, la información puede cambiar, particularmente de una sesión de presentación a una sesión de presentación posterior o, principalmente, por iniciativa del titular del dispositivo.

En consecuencia, dicha posibilidad de cambiar la información aumenta la cantidad de información a conocer para acceder al área de memoria del dispositivo electrónico portátil.

25 La naturaleza de la información no es limitada, es suficiente que sea visible desde el exterior. Por lo tanto, puede tratarse de, por ejemplo, un pictograma, un signo, una imagen, uno o más caracteres alfanuméricos, un código de barras en dos o tres dimensiones, un patrón legible por láser, y/o toda combinación de dichos elementos u otros.

30 Se entiende que el resultado de dicho aumento de la cantidad de información es una mejora en la entropía en comparación con la inherente a la solución conocida descrita anteriormente. La mejora de la entropía provoca una disminución en la probabilidad de robo de la información visible utilizada para acceder al área de memoria del dispositivo electrónico portátil.

35 En cuanto a la lectura óptica de la información visible, ésta es efectuada por el ojo humano o por un dispositivo de lectura óptica.

Cabe señalar que por la expresión "información visible" se ha de entender que se trata de una información perceptible, especialmente, por un lector óptico.

40 Así, la información visible se puede leer en cualquier presentación externa. En particular, se puede citar una presentación de la información visible en un mismo plano o en varios planos, para información en relieve.

45 Debido a la variabilidad de la información, el acceso al área de memoria del dispositivo electrónico portátil se hace más complejo.

Según otro aspecto, la invención es un dispositivo electrónico portátil que incluye un área de memoria.

50 Más particularmente, el dispositivo electrónico portátil comprende, además, medios para presentar una información visible al exterior y medios de comunicación con el exterior. Además, el dispositivo electrónico portátil comprende medios para tener en cuenta, al menos en parte, la información visible para permitir o prohibir el acceso, desde el exterior del dispositivo electrónico portátil, al área de memoria.

55 Según la invención, el dispositivo electrónico portátil comprende medios de variación de información que hace variar, al menos en parte, la información.

60 Como dispositivo electrónico portátil, constituye un objeto integrado portátil (o "token" en inglés) que puede adoptar diversas formas. Puede, por ejemplo, ser una memoria de tipo USB (acrónimo inglés de "Universal Serial Bus"), un dongle (que no necesita un lector específico para comunicar con un ordenador personal (o el acrónimo inglés PC "Personal Computer") o una tarjeta SIM (acrónimo inglés de "Subscriber Identity Module") provisto de al menos una interfaz de comunicación, como, por ejemplo, una interfaz de comunicación sin contacto de tipo ISO 14 443.

Por último, la invención incluye un sistema electrónico que comprende un dispositivo electrónico de comunicación o lectura que coopera con el dispositivo electrónico portátil como se mencionó anteriormente.

65 Más específicamente, la invención es un sistema para autorizar una comunicación tal como el acceso a al menos un área de memoria de un dispositivo electrónico portátil; El dispositivo electrónico portátil comprende medios para presentar información visible al exterior, medios de comunicación con el exterior del dispositivo electrónico portátil y

medios para tener en cuenta, al menos en parte, la información para autorizar o prohibir la comunicación, como el acceso a dicha, al menos una, área de memoria; El sistema que comprende el dispositivo electrónico portátil y un dispositivo electrónico de comunicación o lectura permite particularmente el acceso a dicha, al menos una, área de memoria.

Según la invención, el dispositivo electrónico portátil comprende medios para variar la información, modificando los medios de variación, al menos en parte, la información, denominada información variable. Además, el dispositivo electrónico de comunicación o lectura está adaptado para leer o recuperar la información variable y comunicar al dispositivo electrónico portátil una información basada, al menos en parte, en la información variable.

Debe tenerse en cuenta que la información visible y variable es mostrada al exterior por el dispositivo electrónico portátil o por cualquier otro dispositivo electrónico que coopere con el dispositivo electrónico portátil, tal como un dispositivo huésped. El dispositivo huésped está conectado al dispositivo electrónico portátil. El dispositivo huésped puede ser un teléfono móvil, un asistente numérico personal (o el acrónimo inglés PDA "Personal Digital Assistant") o un PC. El dispositivo huésped puede, además, estar él mismo conectado a una red de comunicaciones, por ejemplo del tipo de telecomunicación móvil, y/o de tipo alámbrico, como Internet.

Como dispositivo de lectura electrónico, puede ser, por ejemplo, un PC provisto de medios de reconocimiento óptico de caracteres (o el acrónimo inglés OCR "Optical Character Recognition") y de al menos una interfaz de comunicación con contacto y/o sin contacto (de tipo radiofrecuencia o infrarrojos).

Como dispositivo electrónico portátil, puede ser, por ejemplo, un "dongle" provisto de una interfaz de comunicación de contacto, por ejemplo de tipo USB, SD (acrónimo inglés de "Secure Digital") o MMC (acrónimo inglés de "Multi-Media Card") y de una interfaz de comunicación sin contacto (de tipo de radiofrecuencia, por ejemplo, de tipo Bluetooth o infrarrojos).

Descripción de los dibujos:

Otras características y ventajas de la invención aparecerán al leer la descripción de una única forma de realización preferida de la invención, dada a título de simple ejemplo indicativo no limitativo y los dibujos adjuntos, en los cuales:

- la figura 1 muestra un sistema, según la invención, que comprende un pasaporte electrónico o chip, como un dispositivo electrónico portátil, que interactúa con un dispositivo electrónico de lectura;
- la figura 2 ilustra un diagrama detallado del chip del pasaporte electrónico del sistema de la figura 1;
- la figura 3 muestra un organigrama simplificado de un ejemplo de un método implementado por el sistema de la figura 1 para acceder a un área de memoria del chip del pasaporte electrónico.

Descripción de una realización:

La realización explicada en relación con las figuras adjuntas no pretende reducir el alcance de la invención, se pueden realizar numerosas modificaciones sin apartarse del alcance de la misma.

Se observará, en particular, que el dispositivo electrónico portátil de la invención puede adoptar diferentes formas.

Puede tratarse, particularmente, de un dispositivo electrónico portátil autónomo o no autónomo.

En el presente documento de patente, el dispositivo electrónico portátil es autónomo, es decir que aparte del dispositivo de lectura, no necesita otro dispositivo electrónico para funcionar.

Como dispositivo electrónico portátil autónomo, puede tratarse principalmente de una tarjeta inteligente para pago electrónico, una tarjeta inteligente para validación de un título de transporte, una tarjeta inteligente para la identificación de un objeto o una persona.

Como dispositivo eléctrico portátil no autónomo, es decir que necesita, además del dispositivo de lectura, otro dispositivo electrónico tal como un dispositivo huésped, a continuación se describe un ejemplo de un sistema que comprende un módulo de identificación de suscriptor provisto de una interfaz sin contacto.

De una manera conocida per se, un sistema comprende una tarjeta SIM (acrónimo inglés de "Subscriber Identity Module") provista de una interfaz de tipo de comunicación de campo cercano NFC (acrónimo inglés de "Near Field Communication") que coopera con un teléfono móvil. Dicha tarjeta SIM-NFC admite al menos dos aplicaciones. La tarjeta dispone de una primera interfaz de contacto de tipo ISO 7816 para implementar una aplicación de identificación de suscriptor, y de una segunda interfaz sin contacto de tipo NFC para implementar una aplicación de pago electrónico, una aplicación de pago y/o validación de un título de transporte, y/o de control de acceso.

Según una primera realización particular, la invención se implementa mediante un sistema que incluye la tarjeta SIM-NFC, como dispositivo electrónico portátil, que coopera con el teléfono móvil, como dispositivo huésped, y un lector

sin contacto, como dispositivo electrónico de lectura. La tarjeta SIM-NFC presenta, utilizando en particular la pantalla del teléfono móvil, una información variable. La información variable es leída, a simple vista, por una persona. La persona transmite al lector sin contacto la información variable mostrada, ingresándola, por ejemplo con la ayuda de un teclado que incorpora el lector sin contacto. El lector sin contacto procesa la información variable recibida y envía, a través de una comunicación por radiofrecuencia, una información basada en la información variable mostrada en la tarjeta multi-aplicación SIM-NFC.

Según una segunda realización, la invención se implementa mediante un sistema que incluye la tarjeta SIM-NFC, como dispositivo electrónico portátil, que coopera con el teléfono móvil, como dispositivo huésped, y un lector sin contacto dotado de medios de reconocimiento óptico, como dispositivo electrónico de lectura. La tarjeta multi-aplicación SIM-NFC presenta, utilizando en particular la pantalla del teléfono móvil, una información variable alrededor del lector sin contacto, efectuando además una función de lectura óptica, a fin de leer toda o parte de la información variable. El lector óptico y sin contacto lee la información variable mostrada, la procesa y envía, a través de una comunicación por radiofrecuencia, una información basada en la información variable mostrada en la tarjeta SIM-NFC.

El primer modo de realización, que involucra a una persona, y la segunda realización del sistema, enteramente automática, permiten asegurar, debido a la presentación de una información variable en la pantalla del teléfono, una transacción del modo "sin contacto" deseado por un usuario del equipo del teléfono móvil-tarjeta SIM-NFC.

Está claro que la invención no impone ninguna restricción en cuanto a la aplicación comprometida dentro del dispositivo electrónico portátil. Puede tratarse de, al menos, una aplicación perteneciente al siguiente grupo:

- una aplicación de identificación del titular,
- una aplicación de autenticación de un interlocutor externo;
- una aplicación de fidelización de un titular;
- una aplicación de control de acceso a un área de acceso restringido o a un servicio de transporte;
- una aplicación de pago electrónico;
- una aplicación de identificación de abonado.

Como se muestra a modo de ejemplo en la figura 1, un sistema electrónico comprende un documento de identificación de un objeto o de una persona, tal como un pasaporte electrónico, como dispositivo electrónico portátil y un dispositivo electrónico de lectura.

Cabe señalar que el pasaporte 11 es solo una forma particular de un documento al que se le puede aplicar la invención.

La invención se puede aplicar a cualquier otro documento de identificación de un objeto o de una persona, incluido el documento llamado MRTD.

Puede mencionarse una lista de elementos de chip, a los que se le puede aplicar la invención, tales como:

- un permiso de conducción;
- una tarjeta de identidad;
- una tarjeta gris;
- una tarjeta de inmigración;
- una tarjeta de residencia;
- un permiso de residencia;
- una tarjeta de inmigración;
- un mapa de la vida cotidiana;
- un visado;

Por supuesto, tal lista no es exhaustiva.

El pasaporte 11 electrónico, de una manera conocida per se, comprende una página de datos (llamada "data page" en inglés), constituido por un soporte 13 dotado de un circuito 14 integrado o chip electrónico.

Según una realización alternativa, el chip 14 está integrado dentro de una página del pasaporte 11 diferente de la de la página de datos, tal como, por ejemplo, la de la cubierta del pasaporte 11.

El chip 14 (detallado en relación con la figura 2) comprende una antena para comunicarse, por ondas de radiofrecuencia, con el exterior. Típicamente, el chip 14 es un chip denominado sin contacto de tipo PICC.

Dos líneas de información aparecen abajo en el soporte 13. Las líneas de información se proporcionan visibles desde el exterior del soporte 13. Una parte de la información visible es fija. La parte fija de la información visible es fijada durante una impresión de la página 13 en el curso de la fabricación, durante su fase de personalización antes

de la entrega a su titular. La parte fija incluye información específica de la identidad del titular del pasaporte, tal como el nombre, apellido, fecha y lugar de nacimiento e información específica del pasaporte, como es su número de serie y fecha de caducidad.

5 La persona poseedora del pasaporte 11 se supone que es su titular.

De acuerdo con una realización de la invención, el pasaporte 11 electrónico comprende medios para modificar, en todo o parte, la información presentada en el soporte 13 visible desde el exterior.

10 Para hacer esto, el soporte 13 incluye un botón pulsador (no mostrado), como medio de activación para generar una información a presentar total o parcialmente al exterior. Así, el titular del pasaporte 11 activa, al presionar el botón pulsador, la generación de una información presentada, por ejemplo, en forma de caracteres.

15 Según una variante, los medios de activación para generar una información consisten en una tecla o combinación de teclas a las que puede acceder el titular del pasaporte 11. Por ejemplo, puede tratarse de una tecla o varias teclas de un teclado conectado por medio de una interfaz de contacto utilizada dentro del lector 12 óptico, tras la introducción de la página dotada del chip 14 en una ranura del lector 12 óptico previsto para este propósito.

20 Según otra realización, el chip 14 detecta la sola presencia de ondas electromagnéticas, sonoras, o de uno o más rayos luminosos, o también de un campo eléctrico en su entorno cercano, para activar la generación de la información variable.

25 Toda o parte de la información visible, con al menos en parte, una parte variable comprende al menos un área legible por una máquina llamada MRZ.

30 Para hacer esto, el soporte 13 incluye una pantalla 15 de cristal líquido o pantalla LCD (acrónimo inglés de "Liquid Crystal Display") provista en un área predefinida, para presentar toda o parte de la información visible. Por ejemplo, la pantalla 15 LCD se encuentra situada en el extremo derecho de la primera de las dos líneas de información presente y muestra ocho caracteres "12345678".

35 De esta manera, la información que incluye una parte fija y una parte variable se presenta fuera del soporte 13 en la presente realización. La información puede ser modificada. Con una simple acción voluntaria del titular del pasaporte 11, se cambia la información visible.

40 Según otra realización, el chip está adaptado para presentar, toda o parte de la información visible, a través de una pantalla separada, incluida en otro dispositivo electrónico con el que puede cooperar el dispositivo electrónico portátil a través de otra interfaz de comunicación, por ejemplo de contacto (físico).

45 La información visible en particular desde el lector 12 óptico, como dispositivo de lectura electrónico, puede cambiar de forma dinámica. El conjunto o, según una variante de realización, solamente una parte de la información presentada en la pantalla 15 LCD es necesario para iniciar una aplicación de autenticación soportado por el chip 14.

50 La aplicación de autenticación iniciada es entonces ejecutada por el chip 14 y termina exitosamente cuando la información proporcionada por el chip 14, por un lado, a la pantalla 15 LCD, y por otro lado al chip 14, a través de un canal 16 externo de comunicación de radiofrecuencia, coinciden.

Toda o parte de la información visible, incluida toda o parte de la información variable, es utilizada por el chip 14, por ejemplo, para autenticar a un interlocutor externo.

55 La información visible desde el dispositivo 12 electrónico de lectura puede cambiar de manera dinámica.

Dicha variabilidad de la información visible aumenta el número de posibles combinaciones de informaciones presentables.

60 Un potencial usurpador se ve obligado, para encontrar la información correcta utilizada para el acceso, desde el exterior, al chip 14, a probar un número muy elevado de combinaciones de datos con respecto a una información que consiste únicamente en datos fijos.

De esta manera, el riesgo de usurpación de la información variable es menor en comparación con el riesgo de usurpación de la única información fija relacionada con la solución conocida explicada anteriormente.

El dispositivo 12 electrónico de lectura, que incluye un dispositivo de reconocimiento de caracteres óptico u OCR, está adaptado y diseñado para interactuar con el pasaporte 11.

El lector 12 óptico, como interlocutor externo, comprende un microprocesador 17, memorias de diferentes tipos, simbolizadas por un único módulo 18 de memoria, un dispositivo 19 de reconocimiento óptico u OCR, y una antena 110, como Interfaz de comunicación con el exterior.

5 Cabe señalar que el dispositivo 12 electrónico de lectura se puede proporcionar en el interior de una sola carcasa o en dos carcasas separadas. En este último caso, el dispositivo 19 OCR se encuentra en una primera carcasa, y el lector sin contacto dentro de una segunda carcasa conectada a la primera carcasa para recuperar la información leída por el dispositivo OCR.

10 Típicamente, el lector 12 óptico es un lector de tipo PCD (acrónimo inglés de "Proximity Coupling Device") al cual se agrega un OCR interno.

El microprocesador 17 controla y procesa los datos, como el órgano central del lector 12 óptico. El microprocesador 17 está conectado a través de un bus 111 de datos a cada elemento que compone el lector 12 óptico. El  
15 microprocesador 17 controla los intercambios de datos para la comunicación interna y externa al lector óptico 12.

El módulo 18 de memoria almacena una o más aplicaciones para ser ejecutadas por el microprocesador 17, incluida una aplicación de autenticación de un interlocutor externo.

20 Al presentar el pasaporte 11 cerca del lector 12, el OCR 19 puede leer el conjunto de las dos líneas de información visibles en el soporte 13, incluidos los ocho caracteres que se muestran "12345678", o solo una parte, en la pantalla 15 LCD.

25 El lector 12 óptico realiza la adquisición óptica, en particular, de la totalidad o parte de los ocho caracteres de la información variable mediante escaneo óptico. El lector 12 óptico selecciona la totalidad o parte de los ocho caracteres. La adquisición óptica de la totalidad o parte de los ocho caracteres de la información variable es necesaria para acceder a al menos una aplicación admitida por el pasaporte 11 electrónico. El lector 12 almacena los caracteres seleccionados dentro del módulo 18 de memoria.

30 El microprocesador 17 ejecuta una aplicación utilizando al menos parte de los ocho caracteres de la información variable. El microprocesador 17 aplica una función predeterminada F a los caracteres seleccionados almacenados. El microprocesador 17 obtiene, como resultado, una información basada en la información variable. El microprocesador 17 almacena el resultado de la aplicación basada en la información variable adquirida ópticamente.

35 El lector 12 óptico transmite, mediante ondas de radiofrecuencia, al pasaporte 11 un mensaje con, como datos, particularmente el resultado de la aplicación basada en la información variable adquirida ópticamente.

Opcionalmente, el lector 12 óptico utiliza el resultado para cifrar los datos a transmitir al pasaporte 11 para acceder, por ejemplo, a los datos relacionados con su titular almacenados en la memoria.

40 El pasaporte 11 y el lector 12 óptico utilizan al menos una parte de la información variable para un mecanismo de control de acceso, por ejemplo, el BAC modificado y adaptado en consecuencia.

45 Se recuerda que el mecanismo de control de acceso BAC conocido permite, a partir de la información visible, tal como el número de pasaporte, la fecha de nacimiento y la fecha de caducidad, al lector y al pasaporte, como MRTD, calcular las claves de cifrado y descifrado, para acceder a los datos almacenados en el chip.

50 Gracias a la invención, el mecanismo de control de acceso BAC se modifica para tener en cuenta también toda o parte de la información variable mostrada en la pantalla 15 LCD.

55 La figura 2 muestra, de manera detallada, el chip 14 de la página de datos del pasaporte 11. El chip 14 comprende un microprocesador 21, una antena 22, como interfaz de comunicación con el exterior, una o más memorias de diferentes tipos representadas por un solo módulo 23 de memoria, y medios de alimentación 24 internos, conectados juntos a través de un bus 25 de datos.

El microprocesador 21 o un microcontrolador controla y procesa los datos del chip 14. El microprocesador 21 constituye la unidad central del chip 14 de control de los elementos del chip 14.

60 Según una variante de realización, una unidad lógica controla y procesa los datos del chip y sustituye a un microprocesador o un microcontrolador.

65 Ventajosamente, el chip 14 proporciona la información variable a mostrar en la pantalla 15 LCD. Para hacer esto, el microprocesador 21 ejecuta una aplicación de generación de información variable, por ejemplo, con la ayuda de una función para generar un número aleatorio predeterminado G, o de una lectura secuencial o no secuencial de una tabla de datos variables previstos para este fin.

Según una variante, la información variable es proporcionada por una entidad externa al pasaporte 11, como un dispositivo electrónico portátil. La entidad externa encargada de proporcionar la información variable a mostrar está, por ejemplo, conectada a través de una interfaz de contacto al dispositivo electrónico portátil. La entidad externa está en contacto físico a nivel de sus interfaces correspondientes con el dispositivo electrónico portátil.

5 El módulo 23 de memoria almacena una o más aplicaciones, incluida la aplicación de autenticación de un interlocutor externo al dispositivo electrónico portátil. El módulo 23 almacena una aplicación basada en la función predeterminada F compartida con el lector 12. Además, el módulo 23 almacena toda o parte de la información variable a mostrar en la pantalla 15 LCD. Además, el módulo 23 almacena la información específica de las características biométricas, tales como una foto de la cara, una huella de uno o más dedos, y/o el iris de un ojo u ojos del titular en cuestión.

10 El microprocesador 21 decide autorizar o prohibir el acceso a su módulo 23 de memoria, desde el exterior del pasaporte 11. La decisión se toma a partir de una comparación de la información recibida del exterior, por el canal 15 de radiofrecuencia, y de una información de comparación. La información de comparación se basa en la totalidad o parte de la información variable mostrada en la pantalla 15 LCD.

15 Para tomar la decisión, el microprocesador 21 aplica la función F a toda o parte de la información variable, para determinar la información de comparación. La función F aplicada a la totalidad o parte de los ocho caracteres a ambos lados, es decir, por el pasaporte 11 y por el lector óptico 12, es idéntica.

20 El chip 14 es capaz de detectar la presencia de un campo electromagnético emitido por un lector sin contacto.

25 La antena 22 recibe un mensaje acompañado de datos en que al menos algunos de los cuales deben corresponder a la aplicación de la función F a la totalidad o parte de los ocho caracteres de la información variable.

30 El microprocesador 21 recupera y procesa el mensaje acompañado de datos. El microprocesador 21 extrae los datos, y selecciona aquellos relacionados con la información que se va a comparar con la información de comparación. Si la información comparada coincide, entonces el microprocesador 21 proporciona acceso a los datos almacenados en el módulo 23 de memoria. Dichos datos se relacionan con una solicitud solicitada y/o con la información específica de los datos biométricos relacionados con su titular.

35 Los medios 24 de alimentación internos consisten en una batería. La batería 24 alimenta todos los componentes del pasaporte 11 electrónico para su funcionamiento.

De manera ventajosa, la batería 24 es, al menos parcialmente, recargable. Para recargar la batería 24, el chip 14 está equipado con sensores de energía de un campo electromagnético externo generado por el lector 12 óptico, de sensores de energía solar y/o sensores de energía luminosa.

40 Según una realización alternativa, no se proporcionan medios de alimentación internos dentro del pasaporte 11. Según una variante de realización de este tipo, la energía se recupera de un campo electromagnético externo.

45 La figura 3 muestra un diagrama de flujo de una realización particular del método 30 según la invención implementado para acceder a una zona de memoria del pasaporte 11.

En primer lugar, el chip 14 del pasaporte 11 inicializa un contador 31 de ratificación, asignándole el valor nulo.

50 Luego, durante una etapa 32 de prueba, el chip 14 prueba 32 si se ha presionado el botón pulsador. Mientras el chip 14 no detecte ninguna pulsación, se realiza un bucle a la etapa 32 de prueba.

Según una variante, se trata de una detección de la presencia de un campo electromagnético durante una introducción del pasaporte 11 en el campo electromagnético generado por el lector 12 provisto de una antena radiante.

55 Una vez que el chip detecta una presión en el botón pulsador, el chip 14 genera una información 34 variable.

Una vez generada, toda o parte de la información variable se presenta 36 al exterior del pasaporte 11, a través de la pantalla 15 LCD.

60 Durante un pasaje suficientemente cercano al OCR 19, el OCR 19 lee la totalidad o parte de la información visible, incluida la totalidad o parte de la información variable mostrada en la pantalla 15 LCD.

65 De manera opcional, la información variable se presenta al exterior durante un lapso de tiempo predefinido que permite al lector óptico acceder a la información variable, por ejemplo, 3 segundos.

Según una alternativa, una acción del titular, como presionar un botón, bloquea la alimentación de la pantalla LCD, para invalidar la información variable mostrada.

5 El chip 14 determina 310, por su parte, un primer valor de autenticación mediante la aplicación de una función F o un algoritmo predeterminado, utilizando especialmente la entrada de toda o parte de la información variable leída.

10 De manera similar, el lector 12 óptico determina 310 un segundo valor de autenticación mediante la aplicación de la misma función o algoritmo predeterminado, utilizando también especialmente la entrada de toda o parte de la información variable leída.

El lector 12 óptico transmite 312 al pasaporte 11 un mensaje acompañado del segundo valor de autenticación.

15 Una vez recibido el mensaje, el chip 14 compara 314 el primer y el segundo valor de autenticación para decidir si hay una coincidencia.

20 En caso afirmativo, es decir, si el primer y el segundo valor de autenticación coinciden, el chip 14 autoriza 316 el acceso a un área de memoria del módulo 23 de memoria, por ejemplo, los datos biométricos específicos de su titular. Luego, seguidamente al éxito de la comparación entre los dos valores de autenticación generados por cada una de las dos partes involucradas, se realiza un bucle en la etapa 31 de inicialización del valor del contador a cero.

En caso negativo, es decir, cuando los valores de autenticación primero y segundo no coinciden, entonces el chip 14 prohíbe 318 todo acceso a un área de memoria del módulo 23 de memoria.

25 Como consecuencia de un fallo en la comparación entre los dos valores de autenticación, se incrementa 320, el valor de un contador de ratificación.

Luego, el chip 14 prueba 322 si el contador de ratificación ha alcanzado un valor de ratificación máximo predeterminado, por ejemplo 10.

30 Siempre que el valor del contador de ratificaciones sea estrictamente inferior al valor de ratificaciones máximo, entonces se vuelve a la etapa 34 de generación de una nueva información variable destinada a ser leída, al menos en parte.

35 De lo contrario, tan pronto como el contador de ratificación haya alcanzado el valor de ratificación máximo, entonces se vuelve a la etapa 31 de inicialización del valor del contador a cero.

40 Aunque la invención se ha descrito principalmente con respecto a un acceso a la memoria, es aplicable al control del funcionamiento de un dispositivo en general, preferiblemente portátil. El dispositivo que autoriza o prohíbe una operación según el resultado de una prueba que comprende una lectura de proximidad de una información variable conocida del dispositivo y luego la transformación con la ayuda de un algoritmo o un método compartido, preferiblemente criptográfico y comparación en el dispositivo del resultado devuelto para autorizar su funcionamiento o cooperación. La operación puede ser total o parcial e incluye, en particular, una autorización en el acceso a la memoria para su lectura o escritura, una comunicación del dispositivo con el exterior a través de medios de comunicación, etc.

## REIVINDICACIONES

1. Un método (30) para permitir la comunicación con un dispositivo (11) electrónico portátil y un dispositivo de comunicación externo (12), comprendiendo el dispositivo electrónico portátil medios (14, 15) para presentar una primera información visible al exterior y medios (22) de comunicación, siendo la información, al menos en parte, tomada en cuenta por el dispositivo electrónico portátil para permitir la comunicación con el dispositivo (21) de comunicación externo, comprendiendo el método una etapa (38) de lectura óptica de la información por el dispositivo de comunicación externo (12) que proporciona al dispositivo electrónico portátil una segunda información basada, al menos en parte, en dicha primera información y efectuando el dispositivo electrónico portátil una etapa de comparación (314) con relación a dicha segunda información para autorizar dicha comunicación, **caracterizado porque** el método comprende una etapa (34) de variación que modifica dicha primera información por el dispositivo portátil, siendo dicha primera información una información variable.
2. Un método según la reivindicación 1, **caracterizado porque** la información variable es proporcionada en respuesta a la recepción desde el exterior, por el dispositivo electrónico portátil, de al menos una información representativa de un éxito en la comparación relacionada con una lectura anterior de una información variable.
3. Un método según la reivindicación 2, el suministro de una información variable comprende la recepción desde el exterior, por el dispositivo electrónico portátil, de un número predeterminado de ratificaciones relacionadas con la lectura anterior de una información variable.
4. Método según una de las reivindicaciones 1 a 3, en el que la etapa de lectura óptica permite el acceso a al menos una aplicación soportada por el dispositivo electrónico portátil.
5. El método según la reivindicación 4, en el que la aplicación está comprendida en la siguiente lista:
- una solicitud de identificación de un portador;
  - una aplicación de autenticación de un interlocutor del dispositivo electrónico portátil;
  - una solicitud de fidelización de un portador;
  - una aplicación de control de acceso a un área de acceso restringido o a un servicio de transporte;
  - una aplicación de pago electrónico; y/o
  - una aplicación de identificación de abonado.
6. Aplicación del método según una de las reivindicaciones 1 a 5 para una identificación del portador del dispositivo electrónico portátil, en el que el método comprende las siguientes etapas:
- lectura óptica, por un dispositivo electrónico de lectura, de la información variable;
  - determinación, por el dispositivo electrónico de lectura, de un primer valor de autenticación según un algoritmo de autenticación predeterminado y de la información variable;
  - recepción por el dispositivo electrónico portátil, por un enlace de radiofrecuencia desde el dispositivo electrónico de lectura, del primer valor de autenticación;
  - comparación, por el dispositivo electrónico portátil, del primer valor de autenticación con un segundo valor de autenticación, el segundo valor de autenticación dependiendo de la información variable;
  - en el supuesto de que el primer y el segundo valor de autenticación se correspondan, autorización del acceso, por el dispositivo electrónico portátil, a dicha, al menos una, zona de memoria.
7. Dispositivo electrónico portátil (11) para autorizar una comunicación con dispositivo de comunicación externo (12), comprendiendo dicho dispositivo electrónico portátil (11) comprendiendo medios (12) de comunicación y medios (14, 15) para presentar una primera información visible al exterior, estando dicha primera información, la menos en parte, tomada en cuenta por el dispositivo electrónico portátil para autorizar la comunicación con el dispositivo (12) de comunicación externo, estando dicha primera información destinada para ser leída ópticamente por el dispositivo de comunicación externo, siendo el dispositivo electrónico portátil capaz de efectuar una etapa de comparación (314) con relación a una segunda información basada al menos en parte en dicha primera información, para autorizar dicha comunicación, estando dicha segunda información proporcionada por el dispositivo electrónico portátil, **caracterizado porque** comprende medios (14) de variación que modifican dicha primera información, siendo dicha primera información una información variable.
8. Dispositivo según la reivindicación 7, en el que el dispositivo electrónico portátil comprende medios de activación del suministro de la información variable.
9. Dispositivo según la reivindicación 8, en el que los medios de activación del suministro de la información variable comprenden medios de detección de una introducción del dispositivo electrónico portátil en un campo eléctrico, electromagnético, luminoso y/o sonoro.
10. Dispositivo según la reivindicación 9, en el que los medios de activación del suministro de la información

variable comprenden al menos una tecla accionable desde el exterior del dispositivo electrónico portátil.

11. Dispositivo según una de las reivindicaciones 7 a 10, en el que el dispositivo electrónico portátil es una tarjeta inteligente incluido en la lista que comprende:

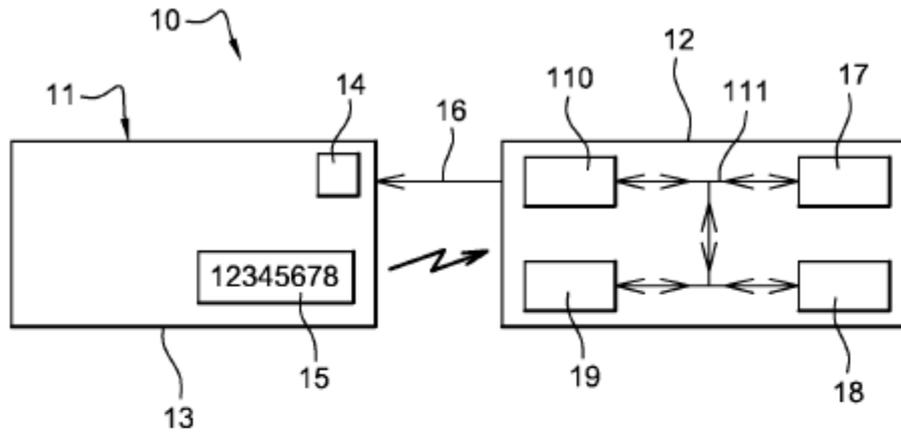
- 5
- identificación electrónica de un objeto y/o de una persona;
  - pasaporte electrónico;
  - tarjeta sanitaria;
  - pago electrónico;
  - 10 - billete de transporte electrónico; y/o
  - módulo de identificación de abonado provisto de medios de comunicación por radiofrecuencia con el exterior de la tarjeta inteligente.

15 comprendiendo el procedimiento una etapa (38) de lectura óptica de la información por el dispositivo de comunicación externo.

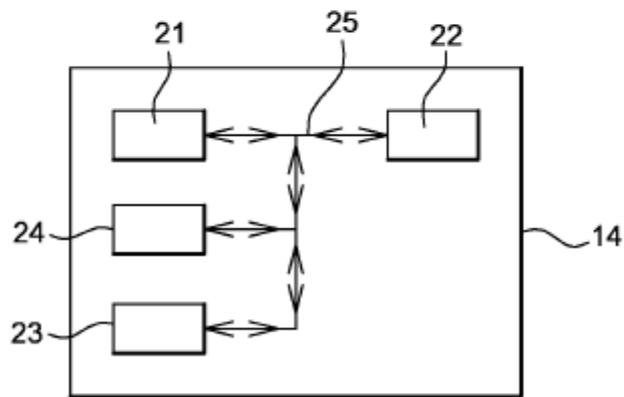
12. Sistema (10) para autorizar una comunicación entre un dispositivo (11) electrónico portátil y un dispositivo de comunicación externo (12),

- 20
- estando configurado el dispositivo de comunicación externo (12) para efectuar una lectura óptica de una primera información presentada por el dispositivo electrónico portátil y suministrar al dispositivo electrónico portátil una segunda información basada, al menos en parte, en dicha primera información,
  - comprendiendo el dispositivo electrónico portátil, medios (22) de comunicación con el exterior y medios (14, 25 15) para presentar una primera información visible al exterior, estando dicha primera información, al menos en parte, tenida en cuenta por el dispositivo electrónico portátil para autorizar la comunicación con el dispositivo (12) de comunicación externo, efectuando una etapa de comparación (314) en relación a dicha segunda información basada, al menos en parte, en dicha primera información para autorizar dicha comunicación,

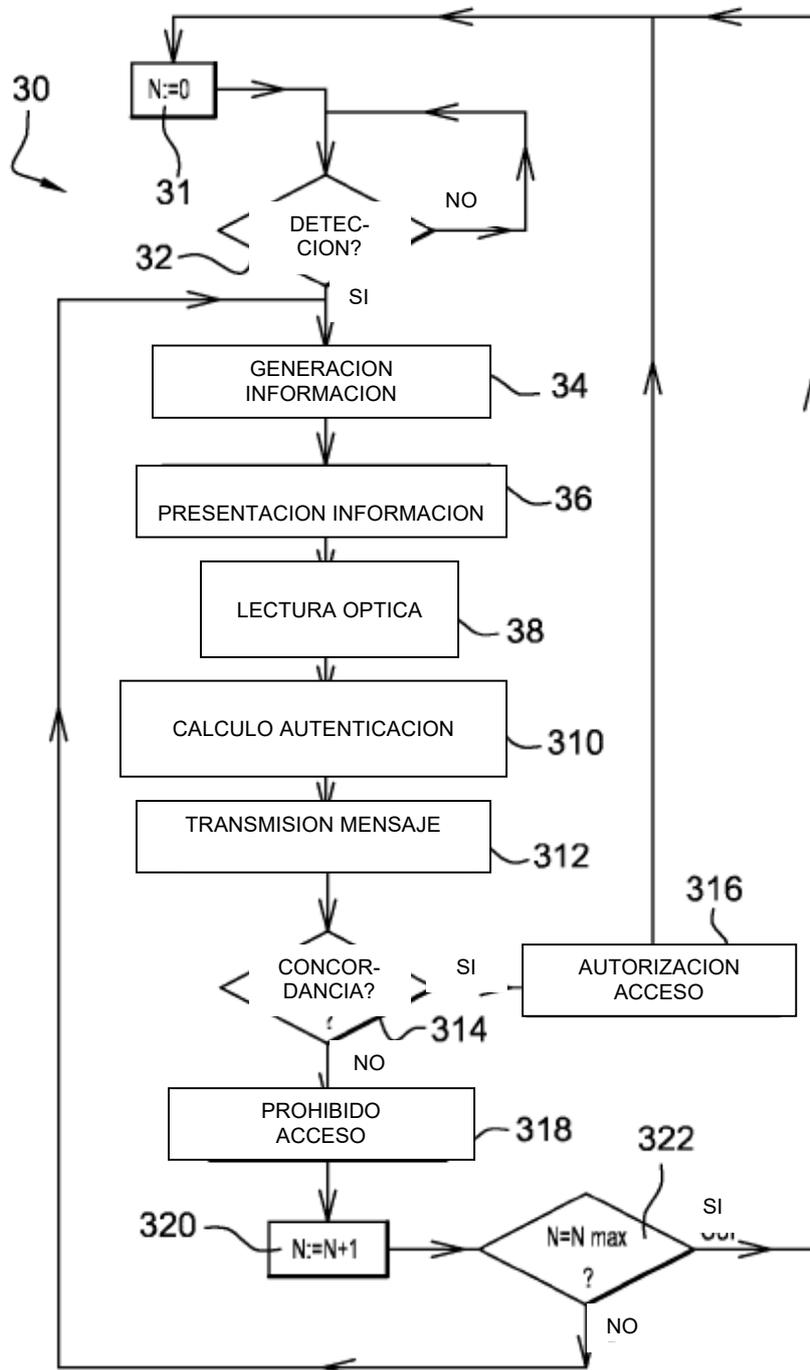
30 **caracterizado porque** el dispositivo electrónico portátil comprende medios (14) de variación que modifican dicha primera información, siendo dicha primera información una información variable.



**Fig. 1**



**Fig. 2**



**Fig. 3**