(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 809 198**

(51) Int. CI.:

G06K 9/00 (2006.01)
G06Q 20/34 (2012.01)
G06Q 20/40 (2012.01)
G07F 7/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **09.04.2018 E 18166260 (2)**

(97) Fecha y número de publicación de la concesión europea: **27.05.2020 EP 3388974**

(54) Título: **Nuevo documento de identificación**

(30) Prioridad:

13.04.2017 IT 201700041158

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
03.03.2021

(73) Titular/es:

ISTITUTO POLIGRAFICO E ZECCA DELLO STATO S.P.A. (100.0%)
Via Salaria 691
00138 Roma (RM), IT

(72) Inventor/es:

GHISA, GIUSEPPE;
LUCIANI, LAURA;
INFORTUNA, FRANCESCO ANTONIO y
GUMIERO, ANDREA

(74) Agente/Representante:

DURAN-CORRETJER, S.L.P

DESCRIPCIÓN

Nuevo documento de identificación

Sector técnico de la invención

La presente invención se refiere a un dispositivo de identificación (literalmente, reconocimiento) portátil, específicamente una tarjeta de ID electrónica, que se puede utilizar en cualquier situación que requiera una identificación precisa del titular. Por ejemplo, el documento puede tener la forma de un cuaderno o una tarjeta, y es preferentemente de un tipo conforme al estándar ICAO 9303 (ISO 7810: 2003).

El dispositivo de reconocimiento, según la invención es de un tipo apropiado para memorizar una o varias características biométricas del titular, y ventajosamente comprende uno o varios sensores para detectar datos biométricos.

Estado de la técnica anterior

En el mercado están disponibles numerosas soluciones relativas a dicho documento, por ejemplo, en la forma de una *"tarjeta"*, que almacena los datos de identificación biométricos del titular. El proceso de reconocimiento asociado con estos documentos se basa en comparar los datos almacenados con un elemento biométrico y detectado en el momento de utilización o contenido en una memoria independiente, por ejemplo, una base de datos remota. Si esta comparación coincide, el proceso de autenticación termina con éxito y la actividad asociada con la utilización del documento, por ejemplo, una transacción financiera basada en tarjeta de crédito, se puede completar.

El documento de Patente WO200384124A1 describe un dispositivo y un procedimiento de utilización relacionado, tal que, cuando se hace funcionar tal como se describe anteriormente, se requiere la identificación biométrica del sujeto con el fin de llevar a cabo una transacción.

La Patente WO9913434A1 da a conocer un dispositivo portátil, por ejemplo, una *tarjeta*, que contiene un sensor capaz de producir un perfil digital del usuario basándose en un único rasgo biométrico, en particular su huella digital o ADN. Una copia de este perfil digital se almacena en el dispositivo y se utiliza como un modelo de comparación cada vez que se requiere la identificación del usuario.

La Patente WO2010/022129 da a conocer un sistema que comprende una tarjeta de transacción que tiene un sensor biométrico y un terminal configurado para leer la información de transacción.

La Patente EP1326196 da a conocer una tarjeta configurada para una autenticación de huella digital. Si la verificación proporciona un resultado positivo, la tarjeta transmite una señal de habilitación a un puesto de control de seguridad.

La Patente US6325285 se refiere a una tarjeta dotada de un procesador, una memoria y un lector de huellas digitales.

Los documentos de la técnica anterior a los que se hace referencia anteriormente y los procesos de identificación/autenticación asociados tienen algunas desventajas importantes.

En primer lugar, su fiabilidad está plagada de problemas relacionados con el *"envejecimiento"* (deterioro), al que todos los elementos biométricos están sujetos. De hecho, el proceso de autenticación puede fallar, incluso si se confronta con el titular real del documento, ya que las características biométricas de dicha persona experimentan variaciones con el tiempo. Dichas variaciones a lo largo del tiempo son menores para algunas características biométricas, tales como, por ejemplo, las huellas digitales, el iris y la retina, mientras que otras características, tales como la voz, la cara, los elementos de las manos y las firmas manuscritas pueden variar considerablemente. En general, la probabilidad de un fallo para identificar al titular real del documento depende, aparte de la sofisticación de la tecnología utilizada, de la característica biométrica seleccionada, en particular, de su alta o baja variabilidad, como se ha mencionado anteriormente, y del tiempo transcurrido desde la inicialización y la emisión del documento.

Otra desventaja es que numerosas configuraciones del documento de la técnica anterior están sujetas a manipulación mediante software malicioso, por ejemplo, las denominadas puertas traseras ("*backdoors*"), instaladas sin el conocimiento del titular y capaces de permitir un acceso incontrolado a los datos contenidos en

el documento y su utilización fraudulenta. Del mismo modo, algunas configuraciones conocidas son propicias para la manipulación debido a características biométricas falsas que se reproducen artificialmente, por ejemplo, mediante clonación.

Asimismo, los documentos de identificación de la técnica anterior requieren procesos de autenticación bastante complejos.

Además, los procesos implantados mediante dichos documentos de la técnica anterior están abiertos a mejoras con respecto a su capacidad de identificar al titular y de reducir el número de identificaciones (literalmente, reconocimientos) falsas, o no identificaciones.

Aún más, los dispositivos de la técnica anterior están configurados para comprender un número limitado de componentes, basándose en general, por ejemplo, en sensores externos para detectar uno o varios de los parámetros biométricos del sujeto.

Características de la invención

Por tanto, el problema técnico expuesto y solucionado por la presente invención es dar a conocer un dispositivo de reconocimiento portátil, en particular, un documento de identificación electrónico, que permita eliminar una o varias de las desventajas mencionadas anteriormente de la técnica anterior.

Este problema se soluciona mediante un dispositivo de reconocimiento, según la reivindicación 1.

Las características preferentes de la presente invención representan la materia objeto de las reivindicaciones dependientes.

En este contexto, el término “documento electrónico” se debe entender en su sentido más amplio para incluir cualquier documento portátil, por ejemplo, en la forma de una tarjeta o cuaderno, preferentemente conforme al estándar ICAO 9303/ISO 7810:2003, que transporte los datos de identificación del sujeto y comprenda medios de funcionamiento electrónicos.

Del mismo modo, los términos “identificación”, “reconocimiento” o palabras similares pretenden significar cualquier proceso de autenticación anterior a la habilitación de características o actividades adicionales, independientemente de cómo se produzca dicha habilitación.

Además, términos tales como “datos biométricos” o “parámetros biométricos” se refieren a cualquier magnitud relacionada o asociada con la identificación del titular del documento, en particular huellas digitales, características oculares o somáticas, firma manuscrita, o similares.

Del mismo modo, el término “sensores” o expresiones similares se refiere a cualquier medio de detección y/o transducción.

El documento de reconocimiento y el sistema inventivo requieren que uno o varios parámetros biométricos de referencia del titular, que se pueden definir también como modelos o *plantillas*, se almacenen en el propio documento durante su fase de inicialización. Por tanto, la invención da a conocer un proceso diacrónico (o cronológico) para actualizar estas características biométricas de referencia, y hace posible evitar eficazmente los incidentes de *“envejecimiento”* de los perfiles biométricos del sujeto, garantizando así el correcto funcionamiento del documento a lo largo de su vida útil.

El documento de identificación preferentemente se configura para almacenar dos parámetros biométricos diferentes utilizando una característica de detección incorporada en un único sensor o en sensores independientes. Esta dualidad paramétrica minimiza el riesgo de que falsas características biométricas se utilicen con éxito. Asimismo, es posible (incluso con dicho sensor, transductor o detector) determinar dos magnitudes biométricas correlacionadas, por ejemplo, la resistencia digital de la piel (por medio del denominado procedimiento capacitivo) y las diferencias de temperatura entre las crestas y los valles de la huella digital (por medio del denominado procedimiento térmico). Esta detección de dos o, en cualquier caso, de múltiples parámetros hace posible un proceso de autenticación y/o una actualización cruzada de dichos parámetros.

El documento de identificación incluye asimismo un sistema de protección de datos basado en dividir dicho documento en dos partes, separadas eléctricamente en los modos de no utilización, conteniendo una el(los) parámetro(s) biométrico(s), y la otra, diversos datos de identificación o habilitación del sujeto para la interacción

con un dispositivo de lectura. Ventajosamente, la primera parte permite el funcionamiento de la segunda por medio de un elemento “desconector”, que, por ejemplo, activa o comparte una antena de radiofrecuencia, pero solo cuando el proceso de identificación biométrica se ha completado con éxito.

La configuración del dispositivo de reconocimiento y el sistema, que es la materia objeto de la presente invención, es por lo tanto tal que, si una persona distinta del titular utiliza dicho dispositivo, dará como resultado un fallo de reconocimiento de las características biométricas. En consecuencia, la parte del dispositivo de reconocimiento configurada para interactuar con un lector remoto permanecerá aislada físicamente, y, por lo tanto, será imposible utilizar el dispositivo para la actividad para la que estaba destinado. Esta característica ha demostrado ser particularmente ventajosa, ya que hace que sea imposible introducir software malicioso en el documento, y permitir que se ejecute allí, incluyendo en ausencia del titular. Además, esta configuración particular impide el acceso no autorizado a los datos almacenados en el documento.

Otras ventajas, características y procedimientos de aplicación de la presente invención serán evidentes a partir de la siguiente descripción detallada de algunas de sus realizaciones, presentadas a modo de ejemplos no limitativos.

Breve descripción de las figuras

Se hará referencia a las figuras de los dibujos adjuntos, en los que:

- la figura 1 muestra un diagrama esquemático de una realización preferente de un documento de identificación, según la presente invención;
- la figura 1A muestra un diagrama esquemático de una realización alternativa del documento de identificación de la figura 1;
- la figura 2 muestra un diagrama esquemático relativo a la interacción sin contacto entre el documento de la figura 1 o 1A y un dispositivo de lectura y/o escritura;
- la figura 3 muestra un diagrama de flujo esquemático de una secuencia de inicialización preferente del documento de la figura 1 o 1A;
- la figura 3A muestra un diagrama de flujo esquemático relativo a un modo de inicialización preferente de un soporte externo del documento de la figura 1 o 1A;
- la figura 3B muestra un diagrama de flujo esquemático relativo a un modo de inicialización preferente de una primera parte del documento de la figura 1 o 1A;
- la figura 3C muestra un diagrama de flujo esquemático relativo a un modo de inicialización preferente de una segunda parte del documento de la figura 1 o 1A;
- la figura 4 muestra un diagrama de flujo esquemático relativo a un modo de funcionamiento preferente del documento de la figura 1 o 1A;
- la figura 5A muestra un diagrama de flujo esquemático relativo a las realizaciones preferentes de un proceso diacrónico asociado con el documento de la figura 1 o 1A;
- la figura 5B muestra un diagrama de flujo esquemático relativo a las realizaciones preferentes de un proceso diacrónico llevado a cabo por medio de una certificación mutua;
- cada una de las figuras 6A a 6D es una representación esquemática de una realización alternativa correspondiente del documento de la figura 1, con referencia específica al posicionamiento de los biosensores, es decir, sensores para detectar uno o varios parámetros biométricos. En particular, en la imagen (I), las figuras 6A y 6B representan una vista frontal de un documento de reconocimiento en formato de cuaderno, y, en la imagen (II), el mismo documento durante un proceso de identificación, refiriéndose dichas figuras a dos configuraciones preferentes diferentes; la figura 6C, en las imágenes (I) y (II), muestra vistas planas de dos superficies principales opuestas correspondientes de un documento de reconocimiento en formato de tarjeta, y, en la imagen (III), el mismo documento durante un proceso de identificación; la figura 6D, en la imagen (I), muestra una vista plana de un documento de identificación en formato de tarjeta y, en la imagen (II), el mismo documento durante un proceso de identificación.

Descripción detallada de las realizaciones preferentes

Con referencia inicial a la figura 1, un dispositivo de reconocimiento portátil, según una realización preferente de la invención se indica, en general, con el numeral de referencia 100. En el presente ejemplo, el dispositivo 100 representa un documento de identificación electrónico en el denominado formato de *tarjeta* o en la forma de un cuaderno.

El documento 100 comprende un soporte o sustrato físico indicado por el numeral de referencia 10, sobre o dentro del cual se incorporan los otros componentes que se describen a continuación.

Preferentemente, el documento 100 comprende dos partes, o elementos, independientes, indicados mediante A y B. En particular, el primer elemento A se puede definir como un elemento de reconocimiento biométrico, y es responsable de identificar al titular y de habilitar el elemento B que, cuando está en el modo de no utilización, está eléctricamente desconectado del elemento A.

El elemento B se puede definir como un elemento para el almacenamiento electrónico de los datos del titular y para la interacción con los medios externos con el fin de llevar a cabo el funcionamiento para el cual está destinado el documento.

Es evidente que las dos partes A y B pueden corresponder a una división física del dispositivo 100, en particular de su soporte 10, o ser independientes desde un aspecto puramente funcional y/o de activación.

El elemento de reconocimiento biométrico A puede comprender uno o varios sensores biométricos 101, o biosensores, configurados para detectar uno o varios parámetros biométricos, que se pueden indicar mediante P_c, o una o varias magnitudes asociadas con los mismos. En el presente ejemplo, el(los) parámetro(s) biométrico(s) Pc pueden representar uno o varios de los siguientes elementos de identificación del titular del documento 100: huella digital, iris, retina, voz, imagen facial, elementos de las manos, firma manuscrita.

En una realización particularmente preferente, los sensores 101 están configurados para detectar características biométricas asociadas con las denominadas magnitudes físicas de primer y segundo nivel, por ejemplo, para medir la resistencia de la piel de un dedo (con el denominado procedimiento capacitivo) y las diferencias de temperatura entre las crestas y los valles de la huella digital (con el denominado procedimiento térmico). Estas magnitudes de primer y segundo nivel se pueden detectar mediante medios de sensor convencionales.

En el presente ejemplo, el elemento de reconocimiento biométrico A comprende, además, medios de comunicación 102 con un dispositivo remoto de lectura o de lectura/escritura 301, mediante el cual el último se muestra esquemáticamente en la figura 2. En el presente ejemplo, los medios 102 comprenden un circuito o antena de radiofrecuencia (RF), que permite al elemento A funcionar con tecnologías de RFID.

En la presente realización, la antena 102 alimenta el(los) sensor(es) 101, utilizando la energía de RF generada por una fuente externa, en particular el dispositivo de lectura/escritura anterior 301.

La antena mencionada anteriormente proporciona también comunicación entre un *controlador* 103, que se presentará a continuación, y el dispositivo de lectura/escritura 301. La comunicación se puede implementar utilizando tecnologías de cifrado de datos.

Las realizaciones alternativas pueden requerir que los medios de comunicación 102 comprendan diferentes elementos o antenas para una implementación independiente de las características de comunicación anteriores relacionadas con el dispositivo remoto 301, la alimentación de los componentes internos del documento 100, etc.

El elemento de reconocimiento biométrico A preferentemente comprende asimismo una unidad de energía 104, en comunicación con los medios de comunicación 102 y configurada para la conversión y la gestión de la energía de RF. En particular, la unidad 104 está configurada para convertir la energía de RF en energía eléctrica, y para controlar el almacenamiento y la distribución de esta energía eléctrica a los otros componentes del documento 100.

Por lo tanto, el elemento de reconocimiento biométrico A comprende medios de proceso, o una unidad de control 103, en particular, un *controlador*/microprocesador, por ejemplo, el tipo de chip ASIC *("Application*

Specific Integrated Circuit", *Circuito integrado específico de la aplicación*). Los medios de proceso 103 están en comunicación con y controlan los otros componentes del elemento A presentados hasta ahora. En el presente ejemplo, los medios de proceso 103 incorporan también medios para almacenar, como mínimo, un parámetro biométrico de referencia, que se indicará mediante P_R, del titular del documento 100, según modalidades, que se ilustrarán a continuación.

En la presente realización, el elemento B para el almacenamiento electrónico de los datos del titular comprende un procesador o un microprocesador 201, u otros medios de proceso, almacenamiento y/o comunicación configurados para interactuar con el dispositivo 301.

En el ejemplo actual, el microprocesador 201 está configurado para almacenar los datos personales del titular y/o las claves de acceso para la interacción con el dispositivo 301, dependiendo de la utilización a la que está destinado del documento 100. El microprocesador 201 se comunica con los medios de proceso 103, y está configurado particularmente para activarse mediante los últimos. En el presente ejemplo, esta activación implica compartir la antena 102 con propósitos de suministro de energía, así como, preferentemente, la comunicación bidireccional entre los dispositivos 100 y 301.

Con referencia a la figura 1A, en una realización alternativa, el elemento B comprende, asimismo, una antena dedicada 202 para el microprocesador 201.

Además, basándose en otra realización alternativa, mostrada también en la figura 1A, el elemento A comprende asimismo una pila 107, un panel solar y/o una fuente de energía independiente para alimentar, como mínimo, a los medios de proceso 103.

Asimismo, según posibles realizaciones alternativas, el dispositivo 100, por ejemplo, en correspondencia con el elemento A, puede incluir una pantalla 105, configurada particularmente para proporcionar información sobre el estado del dispositivo 100 o de un procedimiento de identificación asociado.

De igual modo, el dispositivo 100 puede incluir medios de entrada 106, en particular uno o varios botones (pulsadores) que permiten a un operador llevar a cabo selecciones.

En un modo de funcionamiento preferente, la pantalla 105 puede proporcionar información relacionada con el resultado de la autenticación o una actividad particular realizada por el dispositivo 100, posiblemente interactuando con los botones 106.

Los botones 106 pueden interactuar con los otros componentes del dispositivo 100, habitualmente mediante los medios 103, para proporcionar comandos relacionados con las actividades realizadas por el dispositivo 100. Por ejemplo, pueden activar la visualización de la información por medio de la pantalla 105.

La figura 2 muestra un ejemplo de interacción, en particular una interacción *sin contacto*, entre el dispositivo 100 y el dispositivo de lectura anterior 301.

En realizaciones alternativas, el dispositivo 301 puede ser efectivamente un dispositivo de lectura y/o de escritura, y/o un dispositivo de suministro de energía. En el ejemplo actual, el dispositivo 301 está configurado para:

- Proporcionar energía de radiofrecuencia a la antena 102 con el fin de activar el(los) biosensor(es) 101 del elemento A generando un campo de RF;

- Establecer una conexión del elemento B con el microprocesador 201 (por ejemplo, mediante comunicación bidireccional) con el fin de intercambiar datos/información;

- Llevar a cabo otras posibles operaciones de lectura/escritura en la memoria de los medios de proceso 103 y/o en los medios de almacenamiento adicionales proporcionados en el microprocesador 201.

A continuación, se describirán los modos de funcionamiento preferentes del dispositivo 100 con referencia a los procedimientos de inicialización preliminares, así como al funcionamiento del dispositivo 100 en un proceso de identificación. En el siguiente ejemplo, el dispositivo 100 está configurado para funcionar con parámetros biométricos que consisten en dos de las huellas biométricas del titular de la tarjeta, en particular una huella digital detectada mediante dos metodologías diferentes (por ejemplo, el procedimiento capacitivo y el procedimiento térmico).

Con referencia a la figura 3, se proporciona un procedimiento de inicialización para cada uno de los tres elementos del documento al mismo tiempo que se emite el documento. Los tres procedimientos de inicialización, relativos al soporte físico 10, al elemento de reconocimiento biométrico A y al elemento para almacenar electrónicamente los datos del titular B, respectivamente, se pueden llevar a cabo secuencialmente, simultáneamente o sin ningún orden en particular. Estos procedimientos de inicialización están destinados principalmente a asociar el documento 100 con su propietario.

En el ejemplo actual y con referencia a la figura 3A, la inicialización del soporte físico 10 proporciona la personalización de la información del titular, por ejemplo, aplicada de forma gráfica por medio de impresión, en particular impresión termográfica, *grabado por láser*, *colores embebidos*, etc.

Con referencia a la figura 3B, durante la fase de registro o *inscripción* del usuario, la inicialización del elemento A (un componente biométrico) requiere obtener un muestreo de cada una de las huellas digitales biométricas del titular, por ejemplo, utilizando un dispositivo de adquisición dedicado [1].

Esta fase de *inscripción* se puede realizar, por ejemplo, utilizando las cuatro etapas que se explican a continuación.

(i) Adquisición de datos: utilizando el(los) sensor(es) 101 de un aparato de detección dedicado, se adquiere un muestreo suficiente para cada huella digital biométrica de interés para constituir un conjunto de datos estadísticamente válido [1].

(ii) *Extracción de características*: cada detección adquirida se somete a un tratamiento de preproceso utilizando:

- un algoritmo de “mejora de calidad” [2] con el fin de mejorar la calidad de las muestras y reducir el ruido;

- un algoritmo de “extracción de características” [3] para la extracción de las características más significativas (“conjunto de características”) de las muestras discriminativas para el reconocimiento y la transformación de estas características en una representación digital (plantilla), por ejemplo, las características más significativas se extraen de las huellas digitales, es decir, las discontinuidades de la estructura de crestas/valles (“detalles minuciosos”), y se representan digitalmente como un código binario.

(iii) Definición de las *“Plantillas de referencia”*, es decir, el(los) parámetro(s) biométrico(s) de referencia P_R: para cada parámetro biométrico, el conjunto de *“Plantillas”* producido por las detecciones constituirá la *“Plantilla de referencia”*. Las “Plantillas de referencia” se utilizarán como elementos de comparación durante la fase de identificación del titular.

(iv) Almacenamiento de la(s) *“Plantilla(s) de referencia”*: las *“Plantillas de referencia”* se almacenan de forma cifrada en la memoria no volátil de los medios de proceso 103 utilizando algoritmos de cifrado [4] [5] [6] (por ejemplo, algoritmos de cifrado simétrico AES de 192 o 256 bits con función hash SHA-256 o 3DES de 112 bits con función hash SHA-1).

Con referencia a la figura 3C, la inicialización del elemento B (un dispositivo de almacenamiento electrónico) se realiza almacenando los datos del titular en la memoria no volátil del microprocesador 201, junto con toda la información necesaria para el que documento 100 funcione.

Como se ha mencionado anteriormente, las tres fases de inicialización explicadas anteriormente se pueden llevar a cabo simultáneamente o en momentos independientes.

Después de la inicialización, el documento 100 está preparado para utilizarse. A continuación, se explica, con referencia a la figura 4, un procedimiento preferente para su utilización en un proceso de identificación.

Activación del (de los) biosensor(es) 101

La parte A del dispositivo 100 obtiene la energía requerida a través de la unidad de energía 104, tan pronto como dicho dispositivo 100, y, en particular, su antena 102, se coloca en las cercanías del dispositivo 301, que genera un campo de RF. El(los) sensor(es) 101 (cuando están) alimentado(s), se activan y están preparados para la detección biométrica. Alternativamente, la energía se puede proporcionar mediante la pila 107, si está presente.

Creación de la *"Plantilla nueva"* o del parámetro biométrico actual P_C

El titular procede con la adquisición de sus huellas biométricas utilizando el sensor 101 del dispositivo 100. Las huellas recién detectadas se someten a un *preproceso* y se digitalizan, y constituyen las *Plantillas nuevas* (una para cada tipo de huella) o parámetros biométricos actuales P_C. Las *Plantillas nuevas* se almacenan en la memoria del dispositivo de proceso 103 y quedan disponibles para posteriores actividades de identificación.

Identificación/reconocimiento

A través de un algoritmo de búsqueda de similitud (que se puede definir como *Coincidencia de plantillas*) [7], se realiza una comparación para cada tipo de huella entre la *Plantilla nueva* P_c y la *Plantilla de referencia* P_R, con lo cual se determina un índice de simulación S_i, que se puede definir también como una puntuación global o *puntuación de coincidencia*, y que indica la similitud global.

Como, en general, los sistemas biométricos no proporcionan una *coincidencia* del 100 %, el índice de simulación Si se compara con un umbral prefijado T_S. Si el índice de similitud S_I para cada tipo de huella es mayor que (el valor de) el umbral predeterminado pertinente T_S, se considera que la autenticación se ha completado con éxito. (El valor de) Este umbral T_S se establece de tal manera que limita la tasa de falsos rechazos o "falsos negativos" y reduce a cero las falsas aceptaciones o "falsos positivos".

En el caso de una autenticación positiva, los medios de proceso 103 activan el funcionamiento de la antena 102, que incluye el microprocesador 201, que de otro modo está desactivado con respecto a la última. La antena 102 alimenta el microprocesador 201 del elemento B del dispositivo 100, con lo que puede comenzar la comunicación con el dispositivo de lectura 301. Por lo tanto, el documento 100 se puede utilizar, según su propósito.

Cuando se completa la actividad de solicitud, el documento 100 se retira del dispositivo 301 y la funcionalidad (funcionamiento) de la antena 102 vuelve a su estado inicial desactivado. Por tanto, los datos del procesador 201 ya no están disponibles de ninguna forma hasta otra utilización.

Además, en el caso de una autenticación positiva, siempre se puede activar un proceso diacrónico dentro del dispositivo para una posible actualización de la *Plantilla de referencia* P_R. A continuación, se describirá este proceso.

En el caso de una autenticación negativa, es decir, si el índice de similitud S_I es menor que el valor prefijado T_S para, como mínimo, uno de los parámetros biométricos detectados, se considera que la autenticación no se ha completado con éxito, y, por lo tanto, el documento no se puede utilizar para su propósito (destinado), ya que la parte, parte B (error tipográfico), del documento (procesador 201) es inaccesible. El usuario debe retirar el documento 100 del dispositivo 301 con el fin de desactivar dicho documento 100, y, posiblemente, reiniciar el proceso de autenticación.

A continuación, se describe el proceso diacrónico para actualizar la *Plantilla de referencia* P_R.

Como se ha mencionado anteriormente, los elementos biométricos del titular pueden experimentar un proceso de envejecimiento durante la vida útil del documento 100. Una *Plantilla de referencia* estática P_R no tiene en cuenta estas variaciones, y, a lo largo del tiempo, es posible que ya no represente completamente (~refleje) al titular del documento 100. En consecuencia, a lo largo del tiempo, esto podría dar lugar a errores durante la fase de reconocimiento del titular del documento 100 y afectar a su utilización.

Para garantizar que la *Plantilla de referencia* P_R continúa siendo completamente representativa del usuario, la utilización de algoritmos que son capaces de actualizarla continuamente, mientras se utiliza el documento, es ventajosa.

El proceso diacrónico se puede activar cada vez que el usuario se identifica positivamente, y sigue las etapas principales que se describen a continuación.

Verificación de la fiabilidad de las adquisiciones

La *Plantilla nueva* P_C para cada uno de los parámetros biométricos detectados se considera fiable para el proceso diacrónico solo si la comparación con la Plantilla de referencia P_R pertinente genera un índice de

similitud que supera un segundo umbral prefijado T_{Sbis}, que, en general, es mayor que el umbral T_S utilizado para identificar al titular (figura 5A). Este umbral se puede elegir lo suficientemente alto de manera que se excluyan los "falsos negativos", es decir, las falsas aceptaciones, y lo suficientemente bajo para poder identificar las variaciones de las características biométricas detectadas.

Actualización de la *Plantilla de referencia* P_R

Si el documento 100 requiere dos o más detecciones biométricas, la actualización de la *Plantilla de referencia* P_R solo se realiza si la fiabilidad de, como mínimo, una de las *Plantillas nuevas* P_C está verificada, es decir, si, como mínimo, una de las plantillas supera el umbral T_{Sbis} pertinente y el resto han superado el umbral T_S. A continuación, se muestran algunos criterios útiles por medio de algunos ejemplos no limitativos que se pueden utilizar basándose en la variabilidad relativamente alta de las huellas biométricas aplicadas, el grado de seguridad que se desea conseguir, y las circunstancias concretas.

(i) Actualización independiente de cada *Plantilla de referencia* P_R correspondiente a la *Plantilla nueva* P_C, cuya fiabilidad se ha verificado.

(ii) Actualización a través de la certificación mutua, es decir, si la fiabilidad de la primera *Plantilla nueva* P_C está verificada, (y) la *Plantilla de referencia* P_R está actualizada con respecto a la(s) otra(s) huella(s) biométrica(s), y viceversa, como se muestra en la figura 5B.

(iii) Actualización de todas las *Plantillas de referencia* P_R solo (se realiza) si la fiabilidad de todas las *Plantillas nuevas* P_C está verificada.

(iv) Actualización de la *Plantilla de referencia* P_R solo (se realiza) si la fiabilidad de las *Plantillas nuevas* P_C se ha verificado y se verifican simultáneamente otras condiciones de límite, posiblemente de tipo estadístico.

La actualización de la(s) *Plantilla(s) de referencia* se puede realizar mediante los medios de proceso 103 utilizando algoritmos seleccionados, según los tipos de huellas biométricas aplicadas. Dichos algoritmos pueden ser, por ejemplo, del (de los) siguiente(s) tipo(s): *"Sustitución aleatoria"*, es decir, sustitución aleatoria de una de las *"Plantillas"* que constituyen la *Plantilla de referencia* P_R por la *Plantilla nueva* P_C; *"Sustitución FIFO"*, mediante la cual se sustituye la *"Plantilla"* antigua, que constituye la *Plantilla de referencia* P_R; *"Sustitución NAIVE"*, en la que la *Plantilla nueva* P_C sustituye a la más parecida en la *Plantilla de referencia* P_R [7] [8] [9].

Las realizaciones alternativas pueden requerir que el almacenamiento del (de los) parámetro(s) de la P_C actual y/o su comparación con el(los) parámetro(s) de referencia P_R se lleve a cabo al nivel de un dispositivo independiente del documento 100, posiblemente un dispositivo remoto o el mismo dispositivo 301, tal como se describe anteriormente, en lugar de utilizar componentes que estén incorporados en el documento 100.

Las figuras 6A a 6D se refieren a realizaciones alternativas del documento de reconocimiento considerado hasta ahora, que se describirán a continuación (pero) solo con relación a las características adicionales y a lo que se ha descrito hasta ahora. En todas las realizaciones alternativas descritas, el documento de reconocimiento se configura para detectar múltiples parámetros biométricos, por ejemplo, una serie de las huellas digitales del titular, para hacer posible que dicho documento interactúe con un dispositivo de lectura remoto.

La imagen (I) de las figuras 6A y 6B muestra un documento de identificación electrónico en la forma de un cuaderno, por ejemplo, un pasaporte. Como medios de sensor, el documento lleva cuatro biosensores 1011 a 1014 dispuestos en la contraportada del cuaderno. En particular, los sensores se posicionan en zonas externas de dicho documento en el momento de la autenticación automática (por ejemplo, en una puerta electrónica).

El documento, incluido en la imagen (II) que ilustra sus procedimientos de utilización, se muestra en una configuración abierta, lo que permite la lectura automática de una de sus *"Zonas legibles por máquina"* asociada con una página de datos interna, en un punto de cruce de fronteras. Con este fin, el documento se sujeta firmemente contra un dispositivo de lectura, correspondiente al dispositivo remoto presentado anteriormente, y en las yemas de los dedos de la mano. Los cuatro biosensores 1011 a 1014 posicionados en las yemas de los dedos adquieren las huellas digitales que autentican al titular del documento con el fin de activar la operación de verificación, es decir, la interacción con el dispositivo de lectura.

Las imágenes (I) y (II) de la figura 6C muestran un documento de identificación electrónico en la forma de una tarjeta, es decir, una tarjeta de ID o un permiso de conducir. Como medios de sensor, el documento tiene dos detectores de huellas digitales 1015 y 1016, uno para cada superficie principal opuesta F1 y F2 de la *tarjeta*. Por tanto, el documento se puede sujetar eficazmente entre el pulgar y el dedo índice, cuando se lleva a cabo la autenticación del titular como se representa en la imagen (III), es decir, cuando interactúa con un dispositivo de lectura remoto.

La imagen (I) de la figura 6C muestra un documento de identificación electrónico alternativo en la forma de una *tarjeta*, es decir, una tarjeta de ID o un permiso de conducir. El documento está configurado con un detector de huellas digitales 1017 y un detector de firma 1018, dispuestos de modo que permiten la operación de autenticación. De hecho, el titular puede firmar digitalmente el documento con una mano mientras sujeta firmemente la *tarjeta* con el dedo índice de la otra mano.

La presente invención se ha descrito hasta ahora con referencia a las realizaciones preferentes. Se debe entender que pueden existir otras realizaciones que pertenecen al mismo núcleo inventivo, tal como se define mediante el alcance de las reivindicaciones expuestas a continuación.

Literatura:

[1] D Maltoni, D Maio, AK Jain, and S Prabhakar, Handbook of Fingerprint: Recognition (2nd Edition), Springer, 2009

[2] L Hong, Y Wan, AK Jain, "Fingerprint Image Enhancement Algorithms and Performance Evaluation", IEEE Transactions on Pattern Analysis: and Machine Intelligence, vol. 20, no. 8, pp. 777-789, 1998.

[3] NK Ratha, SY Chen, AK Jain, "Adaptive Flow Orientation-based Feature Extraction in Fingerprint Images", Pattern Recognition, vol. 28, No. 11, pp.1657-1672, 1995.

[4] ICAO 9303 2015

[5] Advanced Encryption Standard, searchsecurity.techtarget.com

[6] Crittografia a chiave simmetrica [Symmetric Key Cryptography], cs.cornell.edu.

[7] Kumar, D Ashok, and T Ummal Sariba Begum. "A Comparative Study on Fingerprint Matching Algorithms for EVM." Journal of Computer Sciences and Applications 1.4 (2013): 55-60.

[8] T Scheidat, A Makrushin, and C Vielhauer, Automatic Template Update Strategies for Biometrics, Tech. Rep., Otto-von-Guericke University Magdeburg, 2007. [cired ar p. 48, 53]

[9] Strategies for Biometrics, Tech. Rep., Otto-von-Guericke University Magdeburg,2007.

REIVINDICACIONES

1. Documento de identificación electrónico (100) en la forma de una tarjeta o cuaderno, que comprende:

- un soporte físico (10);

- una unidad de control (103) que incorpora medios para almacenar, como mínimo, un parámetro biométrico de referencia (P_R) de un titular del documento de identificación electrónico (100);

- medios de sensor (101), configurados para detectar, como mínimo, un parámetro biométrico actual (P_C);

- medios de comunicación (102);

- una unidad de energía (104);

- un procesador (201) configurado para interactuar con un dispositivo remoto (301), leer datos de, escribir datos en y/o alimentar dicho documento de identificación electrónico (100) y almacenar los datos personales del titular para la interacción con el dispositivo remoto (301);

en el que la unidad de control (103) está programada para:

a) comparar dicho parámetro biométrico de referencia (P_R) con dicho parámetro biométrico actual (P_C) y calcular un índice de similitud (I_S);

b) comparar dicho índice de similitud (I_S) con un primer umbral predeterminado (T_S), y, en caso de que dicho índice de similitud (I_S) sea mayor que dicho primer umbral predeterminado (T_S), permitir que dicho procesador (201) interactúe con el dispositivo remoto (301);

y está **caracterizada por que**:

c) en el caso de que dicho índice de similitud (I_S) sea mayor que un segundo umbral predeterminado (T_{Sbis}) mayor que dicho primer umbral predeterminado (T_S), actualizar dicho parámetro biométrico de referencia (P_R) con dicho parámetro biométrico actual (P_C) en dichos medios de almacenamiento;

cuyo documento de identificación electrónico (100) presenta una división en una primera (A) y una segunda (B) partes, en el que dicha primera parte (A) transporta dichos medios de sensor (101), dichos medios de comunicación (102), dicha unidad de control (103) y dicha unidad de energía (104), y dicha segunda parte (B) transporta dicho procesador (201),

en el que dicha segunda parte (B) transporta medios de almacenamiento adicionales de datos de identificación del titular del propio documento y/o claves de acceso para la interacción con el dispositivo remoto (301),

y en el que dicha unidad de control (103) está configurada para permitir una habilitación de dichos medios de comunicación (102) entre dicha primera parte (A) y dicha segunda parte (B) y/o entre dicha segunda parte (B) y el dispositivo remoto (301) en dicha etapa (b).

2. Documento de identificación electrónico (100), según la reivindicación 1, en el que dichos medios de comunicación (102) comprenden, como mínimo, una antena o circuito de radiofrecuencia.

3. Documento de identificación electrónico (100), según las reivindicaciones 1 o 2, en el que dichos medios de comunicación (102) están configurados para alimentar dichos medios de proceso (103) y/o dichos medios de sensor (101).

4. Documento de identificación electrónico (100), según cualquiera de las reivindicaciones anteriores, en el que dicho parámetro biométrico de referencia (P_R) y dicho parámetro biométrico actual (P_C) son representativos de uno o varios de los siguientes elementos: huella digital, iris, retina, voz, imagen facial, resistencia de la piel, firma manuscrita.

5. Documento de identificación electrónico (100), según cualquiera de las reivindicaciones anteriores, en el que dichos medios de almacenamiento (103) están configurados para almacenar, como mínimo, un par de parámetros biométricos de referencia distintos (P_R), y en el que dichas etapas desde la (a) hasta la (c) se

realizan con respecto a cada uno de dichos parámetros biométricos de referencia (P_R) y a un par respectivo de parámetros biométricos actuales (P_C).

6. Dispositivo de identificación electrónico (100), según cualquiera de las reivindicaciones anteriores, en el que dichos medios de sensor comprenden medios de detección de dos parámetros biométricos actuales correlacionados, por ejemplo, la resistencia digital de la piel y una diferencia de temperatura entre crestas y valles de una huella digital correspondiente.

7. Dispositivo de identificación electrónico (100), según la reivindicación anterior, en el que dichos medios de proceso (103) están configurados para ejecutar una autenticación cruzada de dichos parámetros biométricos actuales correlacionados.

8. Documento de identificación electrónico (100), según cualquiera de las reivindicaciones anteriores, que está en forma de tarjeta y en el que dichos medios de sensor (101) comprenden un primer (1015) y un segundo (1016) detectores de huellas digitales colocados en lados opuestos.

9. Documento de identificación electrónico (100), según cualquiera de las reivindicaciones anteriores, que está en forma de tarjeta y en el que dichos medios de sensor (101) comprenden un detector de huellas digitales (1017) y un detector de firma manuscrita (1018), preferentemente colocados en el mismo lado.

10. Documento de identificación electrónico (100), según cualquiera de las reivindicaciones 1 a 9, que está en forma de cuaderno y en el que dichos medios de sensor (101) comprenden una serie de detectores de huellas digitales (1011 a 1014) colocados en la contraportada.

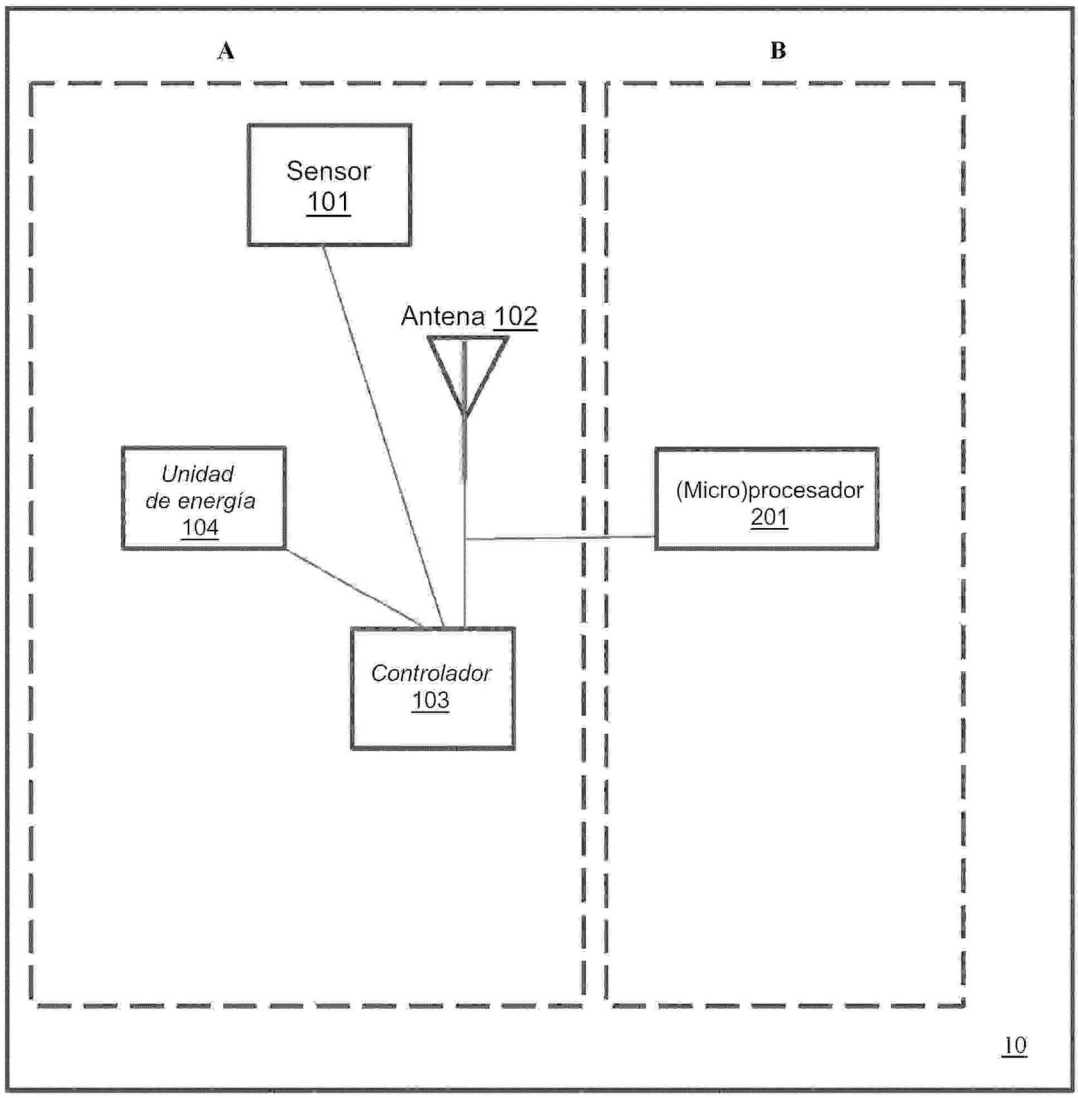
11. Sistema de identificación, que comprende:

- un documento de identificación electrónico (100), según cualquiera de las reivindicaciones anteriores; y
- un dispositivo remoto (301), configurado para leer datos de, escribir datos en y/o alimentar dicho documento de identificación electrónico (100).

12. Sistema de identificación, según la reivindicación anterior, en el que el dispositivo remoto está configurado para:

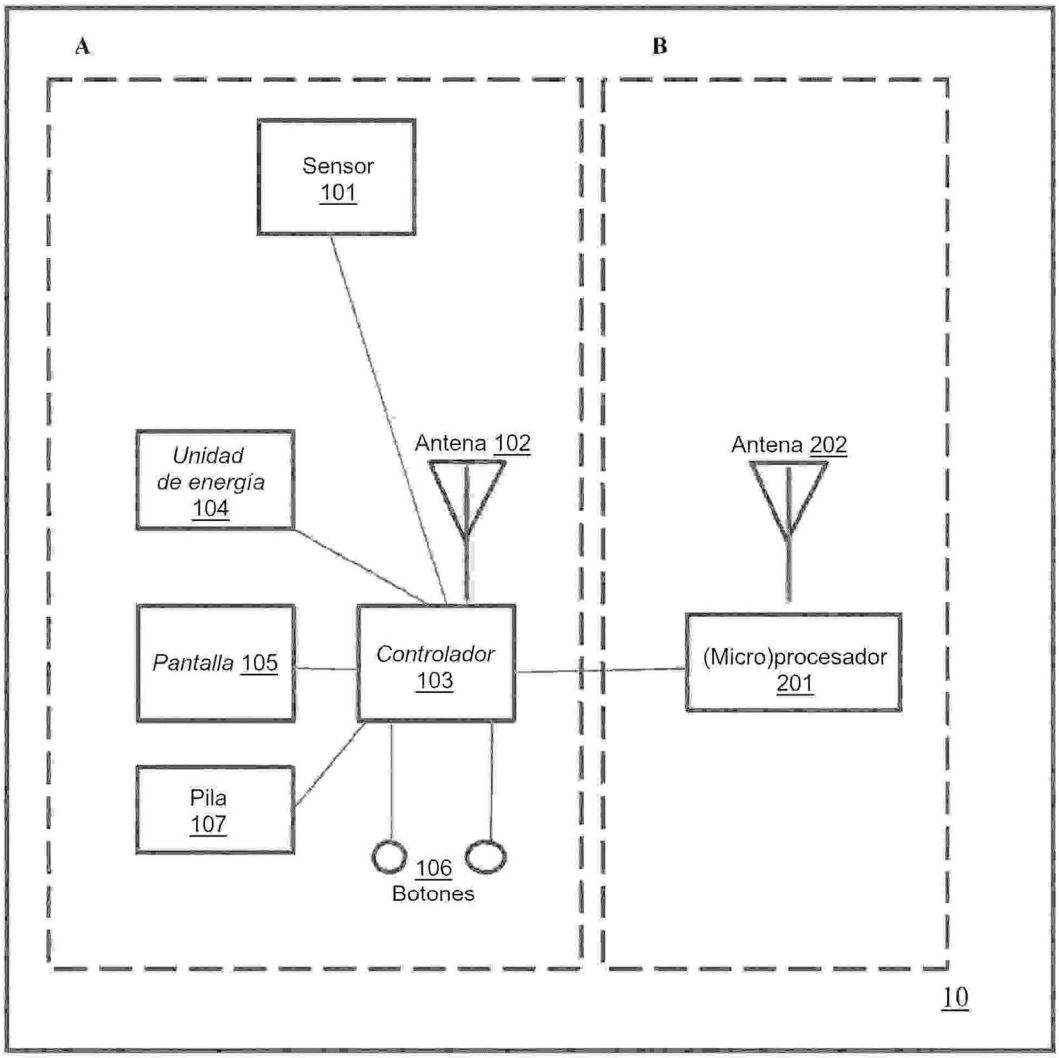
- proporcionar energía de radiofrecuencia a los medios de comunicación (102) de dicho documento de identificación electrónico (100) con el fin de activar dichos medios de sensor (101);
- establecer una conexión con dicho procesador con el fin de intercambiar datos y/o información; y
- llevar a cabo operaciones de lectura/escritura en dichos medios de comunicación (102) y/o dicha unidad de control (103) y/o dicho procesador (201).

FIG. 1


A
B
Sensor
101
Antena 102
Unidad
de energía
104
(Micro)procesador
201
Controlador
103
10

100

FIG. 1A


A
B
Sensor
101
Antena 102
Antena 202
Unidad
de energía
104
Pantalla 105
Controlador
103
(Micro)procesador
201
Pila
107
106
Botones
10

100

FIG. 2

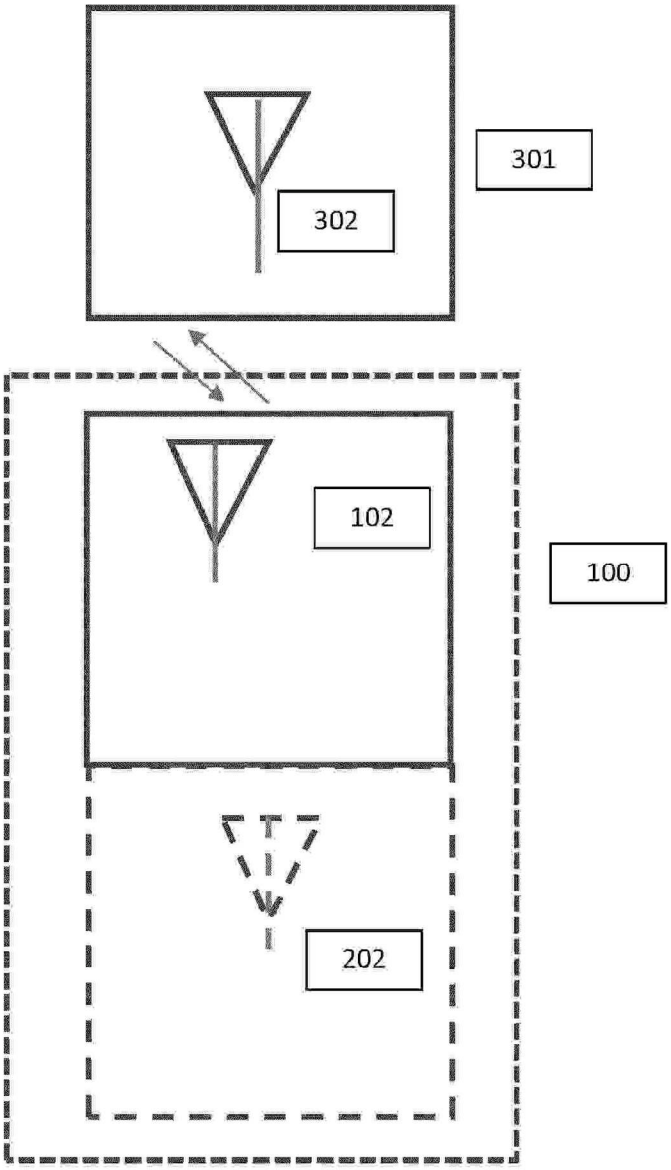


FIG. 3

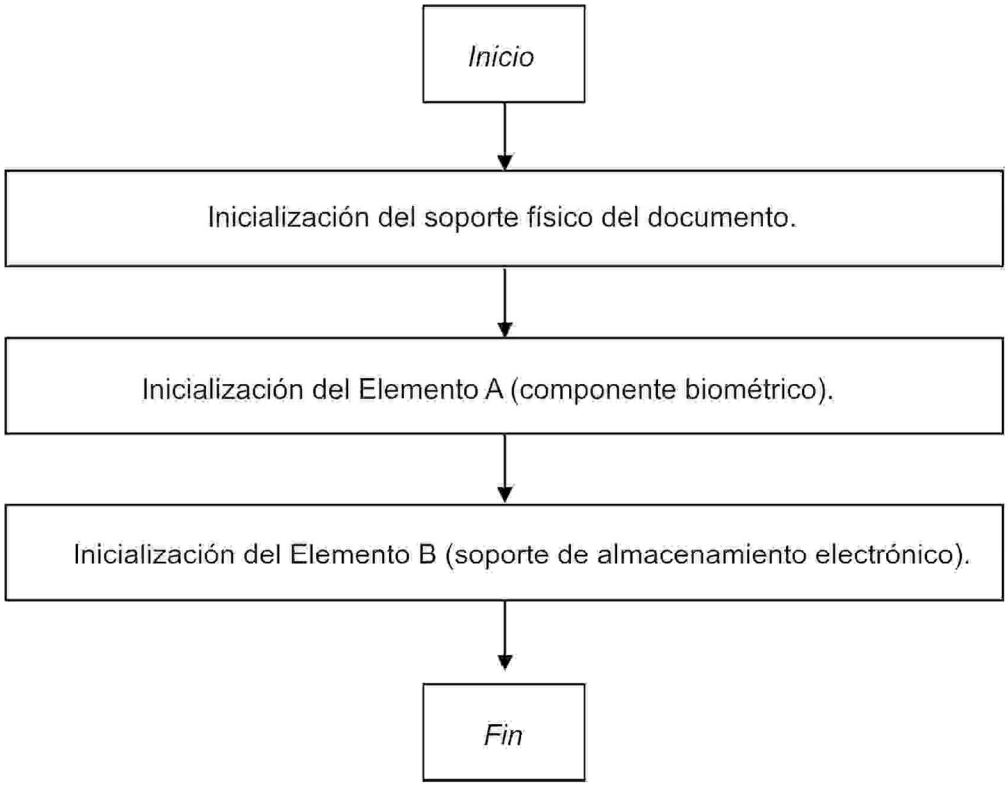

Inicio
Inicialización del soporte físico del documento.
Inicialización del Elemento A (componente biométrico).
Inicialización del Elemento B (soporte de almacenamiento electrónico).
Fin

FIG. 3A

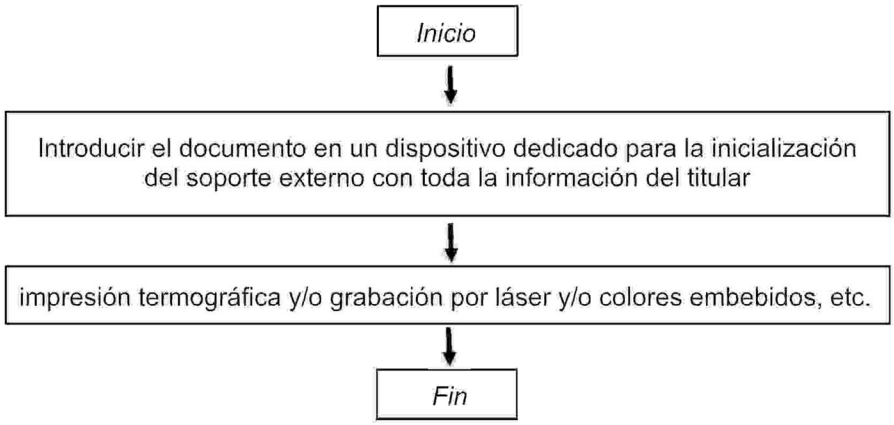

Inicio
Introducir el documento en un dispositivo dedicado para la inicialización del soporte externo con toda la información del titular
impresión termográfica y/o grabación por láser y/o colores embebidos, etc.
Fin

FIG. 3B

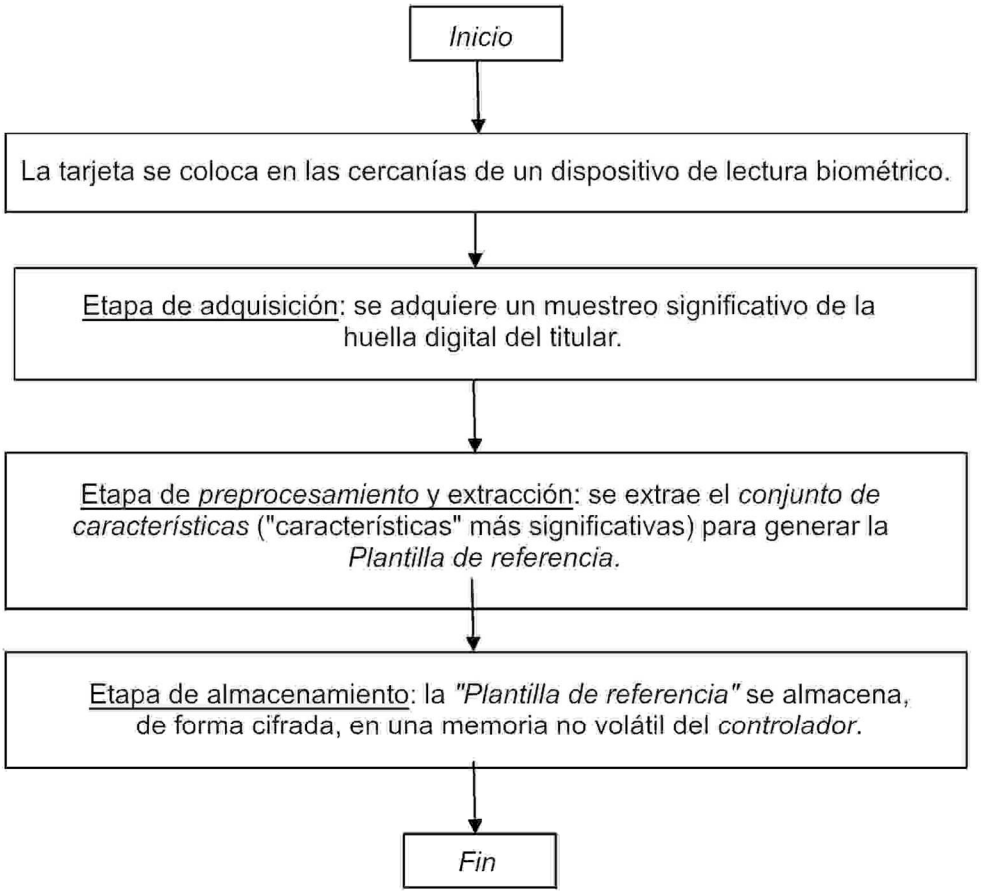

Inicio
La tarjeta se coloca en las cercanías de un dispositivo de lectura biométrico.
Etapa de adquisición: se adquiere un muestreo significativo de la huella digital del titular.
Etapa de preprocesamiento y extracción: se extrae el conjunto de características ("características" más significativas) para generar la Plantilla de referencia.
Etapa de almacenamiento: la "Plantilla de referencia" se almacena, de forma cifrada, en una memoria no volátil del controlador.
Fin

FIG. 3C

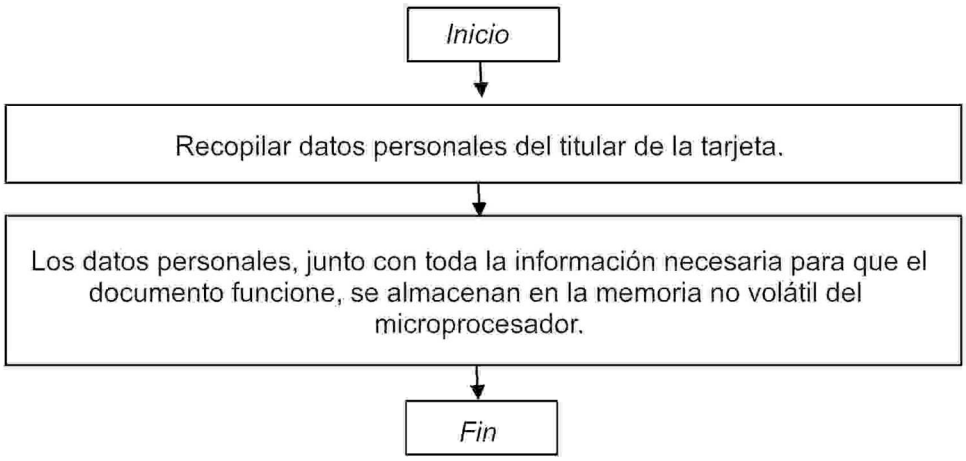

Inicio
Recopilar datos personales del titular de la tarjeta.
Los datos personales, junto con toda la información necesaria para que el documento funcione, se almacenan en la memoria no volátil del microprocesador.
Fin

FIG. 4

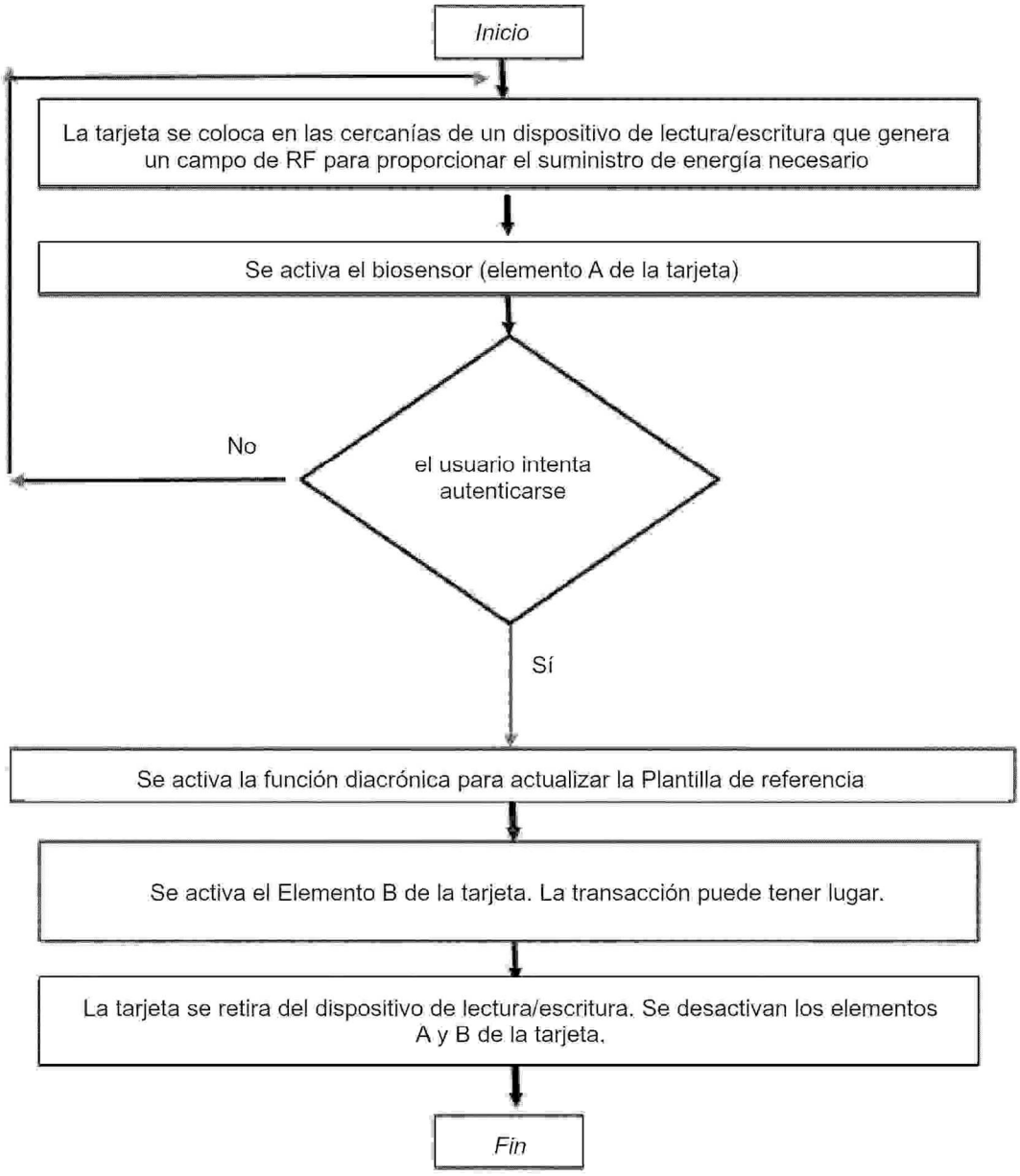

Inicio
La tarjeta se coloca en las cercanías de un dispositivo de lectura/escritura que genera un campo de RF para proporcionar el suministro de energía necesario
Se activa el biosensor (elemento A de la tarjeta)
el usuario intenta autenticarse
No
Sí
Se activa la función diacrónica para actualizar la Plantilla de referencia
Se activa el Elemento B de la tarjeta. La transacción puede tener lugar.
La tarjeta se retira del dispositivo de lectura/escritura. Se desactivan los elementos A y B de la tarjeta.
Fin

FIG. 5A

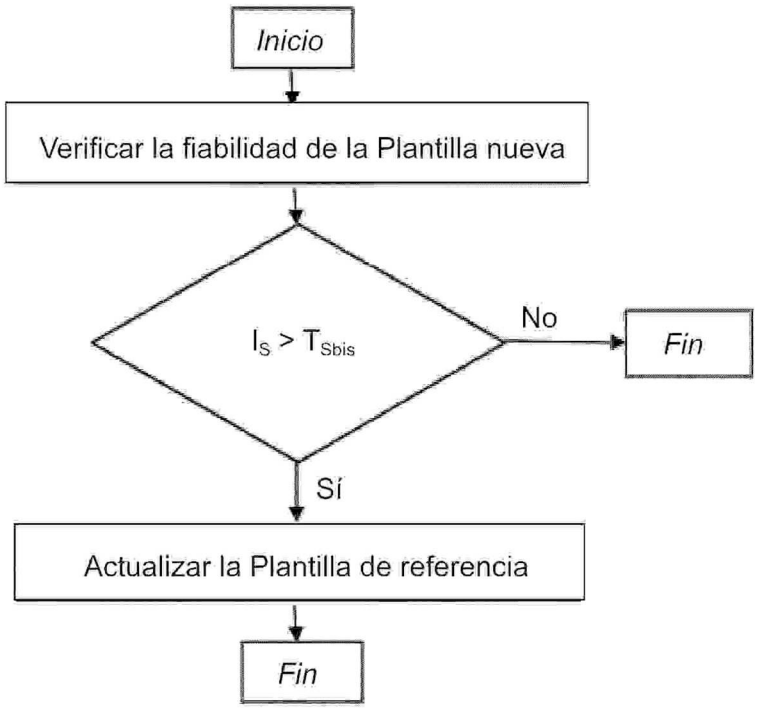

Inicio
Verificar la fiabilidad de la Plantilla nueva
$I_S > T_{Sbis}$
No
Fin
Sí
Actualizar la Plantilla de referencia
Fin

FIG. 5B

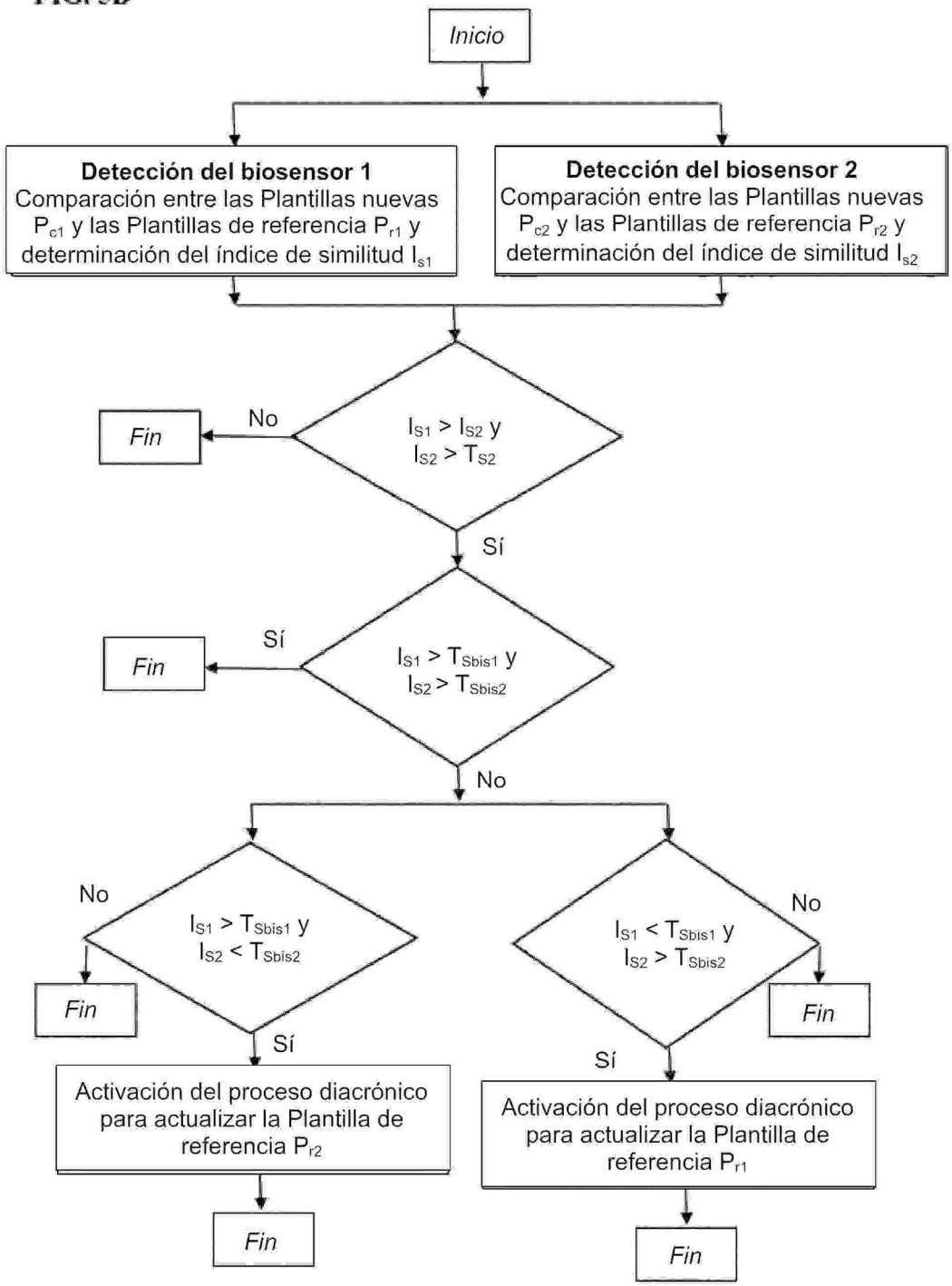

Inicio
Detección del biosensor 1
Comparación entre las Plantillas nuevas P_{c1} y las Plantillas de referencia P_{r1} y determinación del índice de similitud I_{s1}
Detección del biosensor 2
Comparación entre las Plantillas nuevas P_{c2} y las Plantillas de referencia P_{r2} y determinación del índice de similitud I_{s2}
$I_{S1} > I_{S2}$ y $I_{S2} > T_{S2}$
No
Fin
Sí
$I_{S1} > T_{Sbis1}$ y $I_{S2} > T_{Sbis2}$
Sí
Fin
No
$I_{S1} > T_{Sbis1}$ y $I_{S2} < T_{Sbis2}$
No
Fin
Sí
Activación del proceso diacrónico para actualizar la Plantilla de referencia P_{r2}
Fin
$I_{S1} < T_{Sbis1}$ y $I_{S2} > T_{Sbis2}$
No
Fin
Sí
Activación del proceso diacrónico para actualizar la Plantilla de referencia P_{r1}
Fin

FIG. 6A

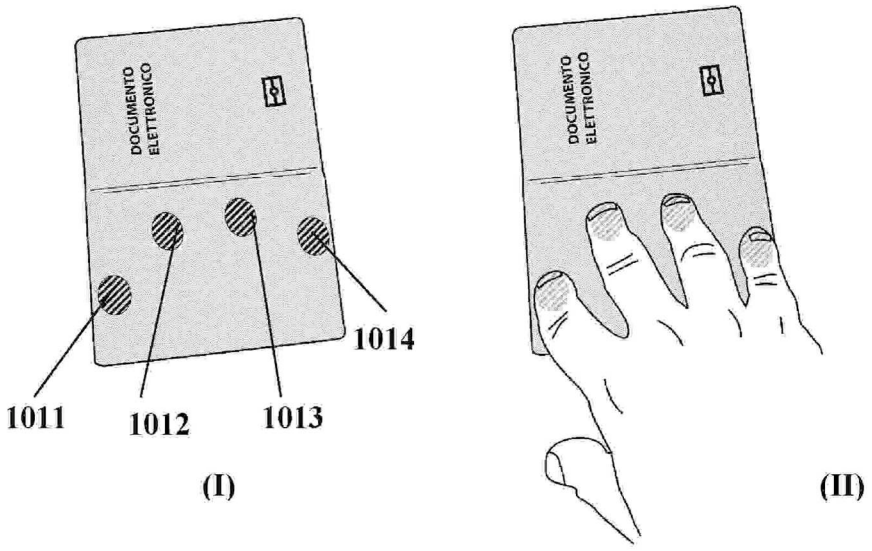
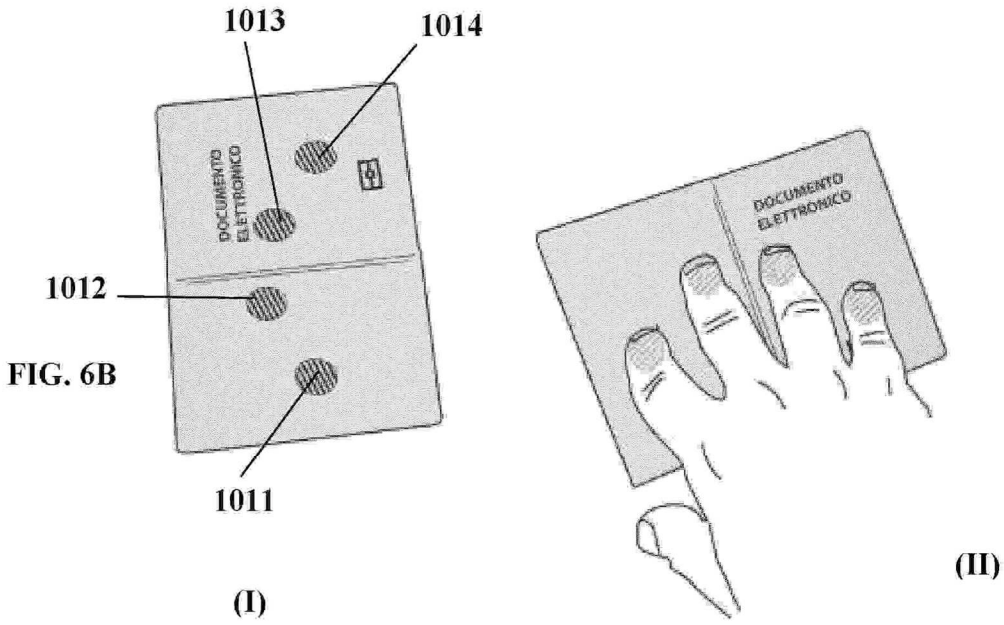

DOCUMENTO ELETTRONICO
1011
1012
1013
1014
(I)
DOCUMENTO ELETTRONICO
(II)

FIG. 6B


1013
1014
DOCUMENTO ELETTRONICO
1012
1011
(I)
DOCUMENTO ELETTRONICO
(II)

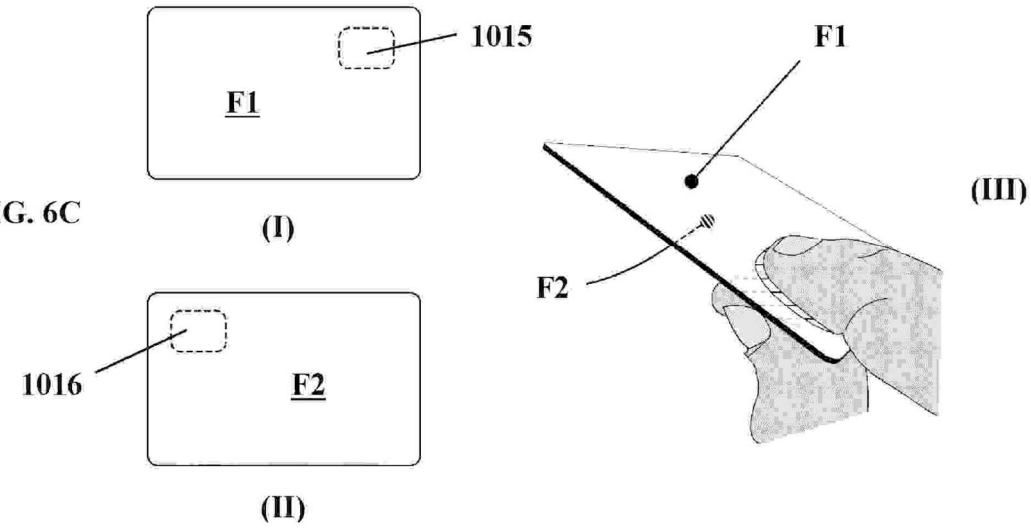


FIG. 6C

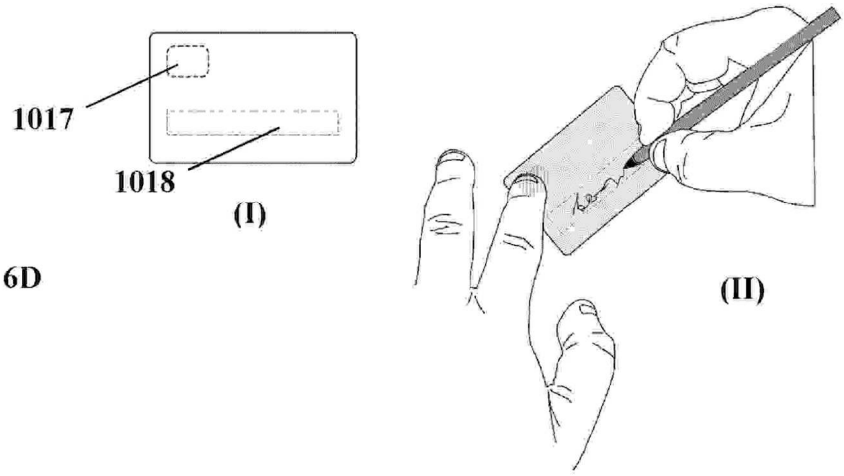


FIG. 6D

REFERENCIAS CITADAS EN LA DESCRIPCIÓN

Esta lista de referencias citada por el solicitante es únicamente para mayor comodidad del lector. No forman parte del documento de la Patente Europea. Incluso teniendo en cuenta que la compilación de las referencias se ha efectuado con gran cuidado, los errores u omisiones no pueden descartarse; la EPO se exime de toda responsabilidad al respecto.

Documentos de patentes citados en la descripción

- WO 200384124 A1
- WO 9913434 A1
- WO 2010022129 A
- EP 1326196 A
- US 6325285 B

Literatura no patente citada en la descripción

- **D MALTONI ; D MAIO ; AK JAIN ; S PRABHAKAR.** Handbook of Fingerprint: Recognition. Springer, 2009
- **L HONG ; Y WAN ; AK JAIN.** Fingerprint Image Enhancement Algorithms and Performance Evaluation. *IEEE Transactions on Pattern Analysis: and Machine Intelligence*, 1998, vol. 20 (8), 777-789
- **NK RATHA ; SY CHEN ; AK JAIN.** Adaptive Flow Orientation-based Feature Extraction in Fingerprint Images. *Pattern Recognition*, 1995, vol. 28 (11), 1657-1672
- **KUMAR, D ASHOK ; T UMMAL SARIBA BEGUM.** A Comparative Study on Fingerprint Matching Algorithms for EVM. *Journal of Computer Sciences and Applications*, 2013, vol. 1.4, 55-60
- Automatic Template Update Strategies for Biometrics. **T SCHEIDAT ; A MAKRUSHIN ; C VIELHAUER.** Tech. Rep. Otto-von-Guericke University Magdeburg, 2007, 48, , 53
- Strategies for Biometrics, Tech. Rep. Otto-von-Guericke University Magdeburg, 2007