

Patente de invención

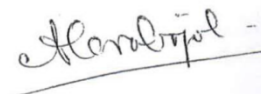
Certificado de utilidad

COPIA OFICIAL

El director general del Instituto Nacional de la Propiedad Industrial certifica que el documento adjunto a la presente es una copia certificada compulsada de una solicitud de título de propiedad industrial presentada en el Instituto.

Redactado en Lille, el **05 de febrero de 2020**

En nombre del director general del Instituto
Nacional de la Propiedad industrial La
directora del Departamento de Datos



Anne DUFOUR

Número de registro: FR1905521

Lugar de presentación: 92 INPI - Presentación electrónica

Fecha de solicitud: 24/05/2019

Referencia del cliente: B251336D39552MAO

Tipo de patente: Patente francesa

Apartado 1: NOMBRE Y DIRECCION DEL SOLICITANTE O DEL REPRESENTANTE A QUIEN DEBE IR DIRIGIDA LA CORRESPONDENCIA

Sociedad/Firma: REGIMBEAU

Apellido/Nombre: Señor CALLON DE LAMARCK Jean-Robert

Dirección:

20, rue de Chazelles
75847 PARIS CEDEX 17
FRANCIA

Apartado 2: TITULO DE LA INVENCION

Título: Procedimiento de autenticación fuerte de un individuo

Apartado 3: PRIORIDADES

Ninguna

Apartado 4 -1: SOLICITANTE (Persona jurídica)

Denominación social: IDEMIA IDENTITY & SECURITY FRANCE

Forma jurídica: Sociedad por acciones simplificada (SAS)

Núm. SIREN (Núm. de identificación fiscal francés):

440305282

Dirección:

2 place Samuel de Champlain
92400 COURBEVOIE
Francia

Sociedad/Firma: REGIMBEAU

Apellido/Nombre: Señor GALLON DE LAMARCK Jean-Robert

Tipo de relación: CPI patentes

Núm. CPI: 94-1102

Dirección:

20, rue de Chazelles
75847 PARIS CEDEX 17
Francia

Apartado 6: REMISIÓN A UNA SOLICITUD ANTERIOR

Remisión a una solicitud de patente ya presentada: No

Apartado 7: INFORME DE BÚSQUEDA EQUIVALENTE

Informe de búsqueda equivalente: No

Apartado 8: REDUCCIÓN DE TASAS

Beneficiario de la reducción de tasas: No

Apartado 9: DEPÓSITO DE MATERIAL BIOLÓGICO

Ninguna

Apartado 10: SECUENCIAS DE NUCLEÓTIDOS Y/O DE AMINOÁCIDOS

La solicitud contiene una lista de secuencias: No

Apartado 11: DOCUMENTOS Y ARCHIVOS ADJUNTOS

Núm.	Tipo de documento	Archivo electrónico	Detalles
1	Contenido de la solicitud DOCX	B251336 texte pour depot.docx	
2	Contenido de la solicitud PDF	B251336 texte pour depot.docx.pdf	
3	Contenido de la solicitud ZIP	B251336 texte pour depot.docx.zip	
4	Contenido de la solicitud XML	application-body.xml	

Apartado 12: SOLICITUD DE CONCESIÓN ACELERADA

Solicitud de concesión acelerada: No

Apartado 13: AMPLIACIÓN DE LA PROTECCIÓN

Ampliación de la protección a la Polinesia Francesa: No

Apartado 14: PAGO DE TASAS

Modo de pago: Adeudo en cuenta de cliente

Prestación	Tarifa	Cantidad	Total
Reivindicaciones, a partir de la núm. 11 (tarifa normal)	42	7	294
Presentación de una solicitud de patente / certificado de utilidad en formato electrónico	26	1	26
Informe de búsqueda	520	1	520
Total (EURO):			840

Apartado 15: FECHA Y FIRMA

Apellido/Nombre: Señor GALLON DE LAMARCK Jean-Robert

Tipo de relación: CPI

Núm. CPI: 94-1102

Fecha de firma: 24/05/2019

Este documento recapitula los datos de la solicitud que han sido declarados conformes por el firmante.



15 rue des Minimes - CS 50001 - 92677 Courbevoie Cedex
INPI Direct: 0820 210 211 (Servicio 0,10 €/min + coste de llamada)
Para presentaciones por fax: 33(0)1 56 65 86 00

Sus referencias para este expediente: B251336D39552MAO
núm. de presentación: FR1905521

EL/LOS SOLICITANTE(S)

Apartado -1: EL SOLICITANTE (Persona jurídica)

Denominación social: IDEMIA IDENTITY & SECURITY FRANCE

Forma jurídica: Sociedad por acciones simplificada (SAS)

Núm. SIREN (Núm. de identificación fiscal francés):

440305282

Dirección:

2 place Samuel de Champlain
92400 COURBEVOIE
Francia

DESIGNA(N) COMO INVENTOR(ES)

Apartado -1: INVENTOR

Apellido/Nombre: Señor BAHLOUL Sébastien

Dirección:

c/o Idemia Identity & Security France 2 place Samuel de Champlain
92400 COURBEVOIE
Francia

Apartado -1: FECHA Y FIRMA

Apellido/Nombre: Señor CALLON DE LAMARCK Jean-Robert

Tipo de relación: CPI

Núm. CPI: 94-1102

Fecha de firma: 24/05/2019

DESCRIPCIÓN

TÍTULO: PROCEDIMIENTO DE AUTENTICACIÓN FUERTE DE UN

INDIVIDUO

5

CAMPO DE LA INVENCION

La invención se refiere a un procedimiento de autenticación fuerte de un individuo portador de un documento de identidad.

10

ESTADO DE LA TÉCNICA

Hoy en día, se conocen procedimientos de autenticación fuerte (es decir, con varios factores de autenticación) muy robustos, particularmente tales como los definidos por las especificaciones de la alianza FIDO.

15

Por ejemplo, se combina un autenticador que posee el usuario (típicamente su terminal móvil, una tarjeta inteligente, etc.) y algo que el usuario “sabe” o “es” (un código, un rasgo biométrico, etc.).

20

Estos procedimientos son completamente satisfactorios, pero presentan una deficiencia a través de sus mecanismos de “recuperación” implementados en caso de olvido del código o pérdida de su autenticador.

25

Más precisamente, bien estos mecanismos de recuperación solamente utilizan un único factor de autenticación (típicamente se envía un enlace a una dirección de correo electrónico de recuperación) y
5 entonces se pierde todo el beneficio de la autenticación fuerte, o bien se debe conservar información personal confidencial de tipo “respuesta a una pregunta secreta” o una foto de identidad.

Se observa, por un lado, que esta solución no es
10 fiable (si la información solicitada es demasiado secreta, el usuario puede perderla/olvidarla, y si es demasiado común, determinados hackers pueden encontrarla mediante ingeniería social) y, por otro lado, la posesión de tal información plantea problemas en términos de respeto de la
15 privacidad de los usuarios.

Se ha propuesto en la solicitud núm. EP2656321 utilizar como factor de autenticación una imagen de un objeto cualquiera elegido secretamente por el individuo, tal como una joya o un documento de identidad. Este método
20 mejora la fiabilidad, pero sigue siendo problemático en términos de gestión de la privacidad.

Por tanto, sería deseable disponer de una solución simple, fiable, segura y completamente respetuosa de la privacidad, para la autenticación de un individuo,
25 en particular con fines de recuperación.

DESCRIPCIÓN DE LA INVENCION

De acuerdo con un primer aspecto, la invención se refiere a un procedimiento de autenticación fuerte de un individuo implementado por un servidor y un equipo cliente conectados; el equipo cliente dispone de un dato biométrico candidato del individuo y de una imagen adquirida de un documento de identidad que representa al menos una fotografía de dicho individuo y un dato de lectura óptica visibles en dicho documento de identidad, y el servidor de una huella digital criptográfica dispone de una primera concatenación de dicho dato de lectura óptica de dicho documento de identidad y de un primer dato aleatorio, denominada primera huella digital criptográfica;

el procedimiento está caracterizado por que comprende la implementación mediante medios de procesamiento de datos del servidor y/o del equipo cliente de las etapas de;

(b) extracción, mediante un análisis de dicha imagen adquirida de dicho documento de identidad de:

- una información candidata representativa de la apariencia de dicha fotografía tal como se representa en la imagen adquirida;

- dicho dato de lectura óptica tal como se representa en la imagen adquirida;

(c) cálculo de un primer dato decodificado mediante la aplicación de un procedimiento de decodificación a dicha información candidata representativa de la apariencia de dicha fotografía y a un primer dato codificado, de manera que dicho primer dato decodificado corresponda al primer dato aleatorio si dicha información candidata representativa de la apariencia de dicha fotografía coincide con una información de referencia representativa de la apariencia de dicha fotografía;

(d) verificación de que:

- una huella digital criptográfica de una primera concatenación del dato de lectura óptica extraído y del dato decodificado coincide con dicha primera huella digital criptográfica de la que dispone el servidor; y
- un dato biométrico de referencia y el dato biométrico candidato del individuo coinciden.

De acuerdo con otras características ventajosas

y no limitativas:

el procedimiento comprende una etapa (a) de adquisición previa de dicha imagen de dicho documento de identidad que representa al menos una fotografía de un individuo y un dato de lectura óptica visibles en dicho documento de identidad mediante medios de adquisición óptica del equipo cliente y la generación del dato biométrico candidato a partir de un rasgo biométrico proporcionado por medios de adquisición biométrica;

los medios de adquisición biométrica son los medios de adquisición óptica del equipo cliente, el equipo cliente es un equipo electrónico personal para dicho individuo, en particular de tipo terminal móvil o tarjeta inteligente:

el servidor o el equipo dispone de un cifrado del dato de referencia biométrico de dicho individuo con una huella digital criptográfica de una segunda concatenación del dato de lectura óptica del documento de identidad y del primer dato aleatorio, diferente de la primera concatenación; la etapa (c) comprende el desciframiento de al menos un dato biométrico de referencia de dicho individuo cifrado, por medio de la huella digital criptográfica de una segunda

concatenación del dato de lectura óptica
extraído y del primer dato decodificado;

el servidor dispone de una huella digital
criptográfica construida a partir de un segundo
5 dato aleatorio, denominada tercera huella digital
criptográfica; la etapa (c) comprende el cálculo
por los medios de procesamiento de datos del
servidor o del equipo cliente de un segundo dato
decodificado mediante la aplicación de un
10 procedimiento de decodificación a dicho dato
biométrico candidato y a un segundo dato
codificado, de manera que dicho segundo dato
decodificado corresponda al segundo dato
aleatorio si dicho dato biométrico candidato
15 coincide con el dato biométrico de referencia;
dicha verificación de la etapa (d) de que el dato
biométrico de referencia y el dato biométrico
candidato del individuo coinciden comprende la
verificación de que una huella digital
20 criptográfica construida a partir del segundo
dato decodificado de la misma manera que la
tercera huella digital criptográfica se construye
a partir del segundo dato aleatorio coincide con
dicha tercera huella digital criptográfica de la
25 que dispone el servidor;

la etapa (a) comprende la recepción por parte del servidor de la imagen adquirida de dicho documento de identidad y del dato biométrico candidato desde el equipo cliente, las etapas (b) a (d) son implementadas por los medios de procesamiento de datos del servidor;

el procedimiento comprende las etapas (b) y (c) que son implementadas por los medios de procesamiento de datos del equipo cliente, la etapa (c) comprende el cálculo de la huella digital criptográfica de una primera concatenación del dato de lectura óptica extraído y del primer dato decodificado, y la generación de una prueba de divulgación nula de conocimientos del cálculo de dicha huella digital criptográfica a partir de la primera concatenación del dato de lectura óptica extraído y del primer dato decodificado; la verificación de la etapa (d) de que la huella digital criptográfica de una primera concatenación del dato de lectura óptica extraído y del dato decodificado coincide con la primera huella digital criptográfica comprende la verificación de que:

- la prueba de divulgación nula de conocimiento del cálculo de dicha huella

digital criptográfica a partir de la primera concatenación del dato de lectura óptica extraído y del primer dato decodificado es válida, y

- 5 - la huella digital criptográfica recibida coincide con dicha primera huella digital criptográfica de la que dispone el servidor;
- las etapas (b) y (c) son implementadas por los medios de procesamiento de datos del equipo
- 10 cliente, la etapa (c) comprende la generación de una prueba de divulgación nula de conocimientos del hecho de que el dato biométrico de referencia y el dato biométrico candidato del individuo coinciden; dicha verificación de la etapa (d) de
- 15 que el dato biométrico de referencia y el dato biométrico candidato del individuo coinciden comprende la verificación por los medios de procesamiento de datos del servidor de que la prueba de divulgación nula de conocimiento del
- 20 hecho de que el dato biométrico de referencia y el dato biométrico candidato del individuo coinciden es válida.

El procedimiento también comprende una etapa anterior (a0) de registro de datos de dicho documento de

25 identidad que incluye las subetapas de:

(A) obtención de la fotografía de dicho individuo visible en dicho documento de identidad y del dato de lectura óptica del documento de identidad;

5 (B) extracción, mediante análisis de dicha fotografía, de la información de referencia representativa de la apariencia de dicha fotografía;

(C) generación del primer dato aleatorio; cálculo

10 del primer dato codificado mediante la aplicación de un procedimiento de codificación a dicha información de referencia representativa de la apariencia de dicha fotografía y a dicho primer dato aleatorio, y

15 de la primera huella digital criptográfica;

durante la etapa (a0), la subetapa (A) o la subetapa (B) comprende la obtención de dicho dato biométrico de referencia; y la subetapa (C) comprende, además, la generación del segundo dato

20 aleatorio y el cálculo del segundo dato codificado mediante la aplicación de dicho procedimiento de codificación a dicho dato biométrico de referencia y a dicho segundo dato aleatorio, y de la tercera huella digital criptográfica;

el procedimiento de decodificación es un procedimiento complementario a un procedimiento de bosquejo de un algoritmo de tipo “secure sketch”; el dato de lectura óptica del documento de identidad es un dato de tipo MRZ, código QR o PDF417;

el procedimiento también comprende una etapa (e) de registro de un autenticador, en particular, de la alianza Fast IDentity Online, FIDO;

la información de referencia representativa de una apariencia esperada de dicha fotografía es un dato de seguridad de tipo Digital Photo Seal.

De acuerdo con un segundo aspecto, la invención se refiere a un conjunto de autenticación fuerte que comprende un servidor y un equipo cliente conectados, caracterizado por que el equipo cliente y/o el servidor comprenden unos medios de procesamiento de datos configurados para:

extraer, mediante análisis de una imagen adquirida de un documento de identidad que representa al menos una fotografía de un individuo y un dato de lectura óptica visibles en dicho documento de identidad:

- una información candidata representativa de la apariencia de dicha fotografía tal como se representa en la imagen adquirida;

- dicho dato de lectura óptica tal como se representa en la imagen adquirida; calcular un primer dato decodificado mediante la aplicación de un procedimiento de decodificación a dicha información candidata representativa de la apariencia de dicha fotografía y al primer dato codificados, de manera que dicho primer dato decodificado corresponda a un primer dato aleatorio si dicha información candidata representativa de la apariencia de dicha fotografía coincide con una información de referencia representativa de la apariencia de dicha fotografía, el servidor dispone de una huella digital criptográfica de una primera concatenación de dicho dato de lectura óptica de dicho documento de identidad y dicho primer dato aleatorio, denominada primera huella digital criptográfica;

verificar que:

- una huella digital criptográfica de una primera concatenación del dato de lectura óptica extraído y del dato decodificado coincide con dicha primera huella digital criptográfica de la que dispone el servidor;

y

- un dato biométrico de referencia y el dato biométrico candidato del individuo coinciden.

De acuerdo con un tercer y un cuarto aspecto, la invención se refiere a un producto de programa informático que comprende instrucciones de código para la ejecución de un procedimiento según el primer aspecto de autenticación fuerte de un individuo, cuando dicho procedimiento se ejecuta en una computadora; y un medio de almacenamiento legible por un equipo informático en el que un producto de programa informático comprende instrucciones de código para la ejecución de un procedimiento según el primer aspecto de autenticación fuerte de un individuo.

DESCRIPCIÓN DE LAS FIGURAS

15

Otras características, objetivos y ventajas de la presente invención aparecerán con la lectura de la siguiente descripción detallada, con referencia a las figuras adjuntas, aportadas de manera ilustrativa no limitativa y en las que:

20

[Fig. 1] La Figura 1 representa esquemáticamente un sistema para la implementación de los procedimientos de acuerdo con la invención.

DESCRIPCIÓN DETALLADA

Arquitectura

La presente invención se refiere a un
5 procedimiento de autenticación fuerte de un individuo
portador de un documento de identidad, es decir, permite
verificar que este individuo es realmente aquel cuya
identidad es presentada por el documento 1, incluyendo
posiblemente un procedimiento de registro de información
10 de este documento de identidad 1.

El presente procedimiento se denomina
autenticación fuerte porque combina “algo que el individuo
posee”, es decir, su documento de identidad 1, y “algo que
el individuo es/sabe”, en este caso un rasgo biométrico.
15 De hecho, hay dos niveles de posible fraude:

- el primero es la falsificación del documento
de identidad, por ejemplo, el cambio de la
fotografía,
- el segundo es la usurpación de identidad, por
20 ejemplo, la utilización de un documento de
identidad 1 válido por un ladrón como si fuera
el suyo.

El presente procedimiento permite detectar los dos
niveles de fraude gracias al carácter fuerte de la
25 autenticación.

Ventajosamente, el presente procedimiento es un procedimiento “de registro de un factor de autenticación”, es decir, de adición o de modificación de un medio de autenticación (que se puede elegir de entre una contraseña, un equipo físico de autenticación y en particular un “autenticador FIDO”, una dirección de correo electrónico, etc.) que seguidamente se podrá utilizar repetidamente para la autenticación diaria. Por tanto, el procedimiento anterior se implementa así típicamente en la primera utilización de dicho factor de autenticación y, particularmente, en caso de pérdida de un factor de autenticación anterior (se habla entonces de procedimiento de recuperación: es el caso en el que el usuario desea autenticarse de nuevo a pesar de esta pérdida)

Por autenticador FIDO, se entiende un equipo de seguridad de la alianza FIDO (Fast IDentity Online), particularmente, conforme a un estándar de autenticación tal como U2F (Universal 2nd Factor), FIDO2, Client to Authenticator Protocol (CTAP), etc.; por ejemplo, un terminal móvil (tal como el equipo 3, ver más adelante), una memoria USB, una tarjeta inteligente, cada uno de los cuales almacena un secreto (un par de clave privada/clave pública). Por tanto, el presente procedimiento generalmente se inscribe así en el caso de pérdida de un autenticador FIDO, pero se entenderá que es perfectamente adecuado para cualquier tipo de factor de identificación,

e incluso podría implementarse en cada autenticación de acceso a un servicio para el que se solicita un nivel máximo de seguridad (por ejemplo, para realizar una transferencia bancaria, una compra inmobiliaria, etc.)

5 De manera particularmente preferida, dicho autenticador a registrar es el equipo cliente 3, lo que permite un procedimiento de registro simple y transparente, el equipo 3 proporciona al pasar todos los datos de identificación necesarios, como, por ejemplo, una dirección
10 MAC, y puede enviar al finalizar este procedimiento un secreto (por ejemplo, un par de claves) que le permite actuar posteriormente como autenticador del individuo.

 Con referencia a la **Figura 1**, se ha representado esquemáticamente una arquitectura de sistema de
15 autenticación para la implementación del presente procedimiento. Este sistema comprende al menos un documento de identidad 1, un servidor 2 y un equipo cliente 3 conectado al servidor 2 a través de una red 20 tal como la Internet.

20 El documento de identidad 1 es un objeto personal de un individuo (muchos individuos pueden tener, cada uno, un documento de identidad de este tipo), y preferentemente constituye un título oficial, emitido ventajosamente por un organismo gubernamental. Este documento puede adoptar muchas
25 formas, tales como una cédula de identidad o un pasaporte, y eventualmente puede ser electrónico. Como alternativa, puede

ser cualquier documento elegido por el individuo o por un proveedor de servicios que tenga un valor probatorio para autenticarlo, es decir, un documento representativo de la identidad del individuo, este podría ser, por ejemplo, una
5 tarjeta de transporte, una tarjeta profesional, una credencial de empresa, una licencia o incluso un documento creado a medida por una organización de gestión de autenticadores que sería necesario para registrar un nuevo autenticador, por analogía con los documentos provistos con
10 cerraduras de seguridad que son necesarios para hacer un duplicado de claves.

De acuerdo con un modo de realización, adopta la forma de una tarjeta inteligente (del tipo “smart card”) con dimensiones estándar y generalmente de PVC o policarbonato.

15 En cualquier caso, el documento de identidad 1 consta de una superficie sólida en la que se imprime cierta cantidad de información y, en particular:

- una fotografía del individuo en posesión de la tarjeta (y eventualmente otro dato “gráfico”
20 tal como una firma del individuo);
- un dato de lectura óptica (es decir, legible automáticamente, destinado a computadoras), de tipo MRZ, código QR o PDF417 (en lo sucesivo en el documento se tomará el ejemplo
25 de la MRZ, pero se entenderá que no está

limitado a este tipo de dato de lectura óptica);

- datos alfanuméricos variados, denominados “datos visuales”, elegidos particularmente de entre:

5

- o número completo del documento de identidad 1;

- o fecha de vencimiento;

- o fecha de emisión;

10

- o apellidos;

- o nombre(s);

- o nacionalidad;

- o fecha de nacimiento;

- o lugar de nacimiento;

15

- o sexo;

- o estatura;

- o dirección;

- o etc.

El servidor 2 es un equipo remoto y seguro, típicamente de una autoridad o un proveedor de soluciones de seguridad. Comprende medios de procesamiento de datos 21 (de tipo procesador) y medios de almacenamiento de datos 22 (una memoria, por ejemplo, un disco duro).

El equipo cliente 3 es un terminal local que comprende o está conectado a unos medios de adquisición óptica 30 (típicamente una cámara fotográfica o un

escáner), y adecuado para adquirir una imagen (del documento 1, como se verá). Además, comprende medios de procesamiento de datos 31 y medios de almacenamiento de datos 32. El equipo cliente 3 y el servidor 2 comprenden
5 ventajosamente interfaces de comunicaciones que les permiten dialogar remotamente. Preferentemente, el cliente 3 es un equipo personal del individuo portador del documento de identidad 1, por ejemplo, un terminal móvil del individuo (en particular de tipo smartphone).

10 De manera preferida, el equipo cliente 3 es capaz de generar un dato biométrico a partir de un rasgo biométrico del individuo. El rasgo biométrico puede ser, por ejemplo, la forma del rostro, una huella digital, una huella de la palma, el iris del individuo, etc. La extracción del dato
15 biométrico se implementa mediante un procesamiento de la imagen del rasgo biométrico que depende de la naturaleza del rasgo biométrico. El experto en la técnica conoce varios procesamientos de imágenes para extraer datos biométricos. A título ilustrativo no limitativo, la extracción del dato
20 biométrico puede comprender una extracción de puntos particulares o de una forma del rostro en el caso en el que la imagen sea una imagen del rostro del individuo.

El equipo cliente 3 comprende o está conectado por ese motivo a unos medios de adquisición biométrica,
25 típicamente un sensor de imagen y de una manera particularmente preferida estos medios de adquisición

biométrica son los medios de adquisición óptica 30, por ejemplo, una cámara fotográfica adecuada para adquirir una fotografía del rostro en modo “selfie” (se observa que, como alternativa, se pueden utilizar medios de adquisición
5 distintos, como un sensor de huellas digitales).

En cualquier caso, un dato de referencia biométrico utilizado para la autenticación del individuo es ventajosamente un dato pregrabado en presencia de una autoridad (ver más adelante), o un dato proveniente del
10 documento de identidad 1, tal como la fotografía.

Se observa que el equipo 3 puede adoptar muchos modos de realización. Más precisamente y como se verá, basta para la implementación de la invención que el equipo cliente 3 pueda obtener una imagen adquirida del documento de
15 identidad 1 de una manera u otra, incluido indirectamente, y procesar esta imagen.

En cualquier caso, como se ha explicado, el equipo cliente 3 puede adquirir una imagen de una imagen del documento de identidad 1, es decir, fotografiar una fotocopia
20 en lugar del documento 1 directamente, o incluso una fotocopia de una fotocopia, etc. Como se verá, bastará con que la imagen adquirida represente el documento 1. Se entenderá que el presente procedimiento no está limitado a ninguna manera de obtener esta imagen ni a ninguna naturaleza
25 en particular (la imagen adquirida puede estar en negro y blanco, distorsionada, etc.). Se observa que es muy posible

que otras entidades estén conectadas al servidor 2 y al equipo 3, en particular servidores que implementan servicios que consumen las afirmaciones producidas por el equipo 3, es decir, servicios que desean la autenticación del individuo, por ejemplo, un servidor de un banco, de un hotel, etc. Particularmente, se puede imaginar que tal servidor dispone de una solución de autenticación convencional (por ejemplo, con un autenticador FIDO) e iniciará el presente procedimiento (contactando con el equipo 3) cuando el usuario desee registrar un nuevo factor de autenticación. Este servidor de servicio puede, por ejemplo, implementar una API dedicada a interrogar al servidor 2 para la implementación del presente procedimiento.

Como se verá, el presente procedimiento permite que este servidor de servicio no almacene ninguna información personal del individuo.

Digital Photo Seal

En el resto de la presente descripción, el experto en la técnica podrá consultar las solicitudes núms. FR1904375 y FR1904406 que describen mecanismos que pueden utilizarse independientemente o en combinación en el contexto de la invención.

De manera conocida, el presente procedimiento utiliza información representativa de la apariencia de una fotografía (u otro elemento gráfico del documento 1), es

decir un dato descriptivo de al menos un fragmento de esta fotografía, tal como aparece, es decir una “firma”, que permitirá comparaciones.

Se denomina información de “referencia” a la
5 información representativa de la apariencia “teórica” de la fotografía, es decir, como se esperaba. En contraste, se denomina información “candidata” a la información representativa de la apariencia constatada de la fotografía, es decir, tal como se representa en una imagen adquirida del
10 documento 1. Se entiende que esta apariencia constatada generalmente no es perfectamente idéntica a la apariencia esperada, debido a las condiciones de los defectos inherentes a la adquisición de una imagen y a la variabilidad de las condiciones de toma de imágenes (iluminación, movimiento,
15 distancia, etc.).

Sin embargo, dicha información representativa de la apariencia se elige de modo que si dos fotografías tienen apariencias coincidentes (es decir, es la misma fotografía incluso si las condiciones de toma de imágenes no son
20 idénticas), entonces sus informaciones representativas también coinciden (es decir, presentan una distancia de acuerdo con una métrica dada inferior a un umbral).

Por tanto, la información de referencia y la información candidata coinciden si y solo si la apariencia
25 constatada y la apariencia esperada de la fotografía coinciden, es decir, que de hecho sea la misma fotografía,

en otras palabras, que la fotografía impresa en el documento de identidad 1 no haya sido alterada fraudulentamente. Esta verificación se puede hacer para cada elemento gráfico, tal como una firma.

5 Se podrá utilizar como información representativa de la apariencia de la fotografía el “Digital Photo Seal” (DPS) que se tomará como ejemplo en lo sucesivo en la presente solicitud, es decir, el dato de seguridad tal como se describe en las solicitudes citadas en la introducción
10 o de manera más precisa la solicitud núm. EP3206192, basada en la posición de puntos singulares del elemento gráfico, o cualquier otra “firma” de un objeto gráfico tal como una fotografía.

 El DPS de una fotografía es una característica de
15 esta imagen que no es un modelo biométrico y puede comprender, por ejemplo, un histograma de gradiente orientado (se habla entonces de algoritmo con descriptor HOG). Como alternativa, se puede utilizar un algoritmo de clasificación del tipo que emplea una red neuronal convolucional, también conocido por
20 el acrónimo CNN (del inglés Convolutional Neural Network).

Registro

 En el lanzamiento del procedimiento, se supone que el equipo cliente 3 dispone al menos de una imagen
25 adquirida de dicho documento de identidad 1 que representa al menos una fotografía de un individuo y un dato de lectura

óptica visibles en dicho documento de identidad 1 (en la que son legibles los datos personales del individuo) y de un dato biométrico candidato.

El equipo cliente 3 o el servidor 2 también
5 necesita disponer de un primer “dato codificado” (denominado SSKD) obtenido mediante la aplicación de un procedimiento de codificación a la información DPS de referencia representativa de la apariencia de la fotografía de dicho individuo visible en dicho documento de identidad 1 y a un
10 primer dato aleatorio (denominado RNGD). En la práctica, este primer dato codificado generalmente es almacenado (al menos inicialmente) por el servidor 2.

El servidor 2, por su parte, solo necesita disponer de una huella digital criptográfica de una primera
15 concatenación del dato de lectura óptica del documento de identidad 1 y el primer dato aleatorio RNGD.

Eventualmente, el equipo cliente 3 o el servidor 2 pueden disponer de un cifrado con una huella digital criptográfica de una segunda concatenación del dato de
20 lectura óptica del documento de identidad 1 y del primer dato aleatorio RNGD, diferente de la primera concatenación, del dato biométrico de referencia de dicho individuo, y posiblemente de otros datos personales (de nuevo, el cifrado a menudo es almacenado por el servidor 2).

Se entiende que ninguno de estos datos es aprovechable por sí mismo (en particular si están todos almacenados en el servidor 2) porque:

- dicho primer dato codificado SSKD solo no
5 permite recuperar la información DPS de referencia ni el primer dato aleatorio RNGD;
- la huella digital criptográfica de una primera concatenación del dato de lectura óptica del documento de identidad 1 y del primer dato
10 aleatorio RNGD es una huella digital simple que no aporta ninguna información;
- el eventual cifrado del dato biométrico no es legible por nadie sin la clave.

En un modo de realización preferido, el
15 procedimiento comprende una etapa previa “de registro” (a0) que permite integrar a un individuo y su documento de identidad 1 y generar los datos de los que debe disponer el servidor 2 y/o el equipo cliente 3. Aquí es necesario marcar la diferencia con el registro de un factor de
20 autenticación que puede ser el resultado del presente procedimiento.

Esta etapa (a0) se puede implementar mucho antes que el resto del procedimiento, y no es necesario repetirla cada vez que se produce el procedimiento (debe observarse
25 que se puede prever repetirla de vez en cuando por seguridad y para actualizar los datos personales, pero

esto es opcional). Por tanto, puede considerarse que dichos datos mencionados anteriormente están predefinidos para la implementación del procedimiento.

Este procedimiento de registro de datos del documento de identidad 1 del individuo puede ser llevado a cabo por el servidor 2 o por el servidor de una autoridad gubernamental, y entonces los datos obtenidos se transmiten al servidor 2 y/o al equipo cliente 3.

El registro comienza con una etapa (A) de obtención de una fotografía de dicho individuo visible en dicho documento de identidad 1, de un dato de lectura óptica del documento de identidad 1 y, llegado el caso, del dato biométrico de referencia de dicho individuo.

Esta etapa (A) puede implementarse, a su vez, mediante una imagen del documento de identidad 1 (como se explicará para el procedimiento de autenticación), pero preferentemente, para evitar los problemas de digitalización y pérdida de calidad, estos datos (es decir, la fotografía, el dato de lectura óptica y/o el dato biométrico de referencia) son manipulados directamente, en particular si el registro es realizado por una autoridad gubernamental. Esto permite además una eventual actualización de los datos, ver más adelante.

En una etapa (B), como se explica, se implementa la extracción por análisis de dicha fotografía de la información (denominada DPS por conveniencia, aunque como

se ha explicado, el presente procedimiento no se limita al Digital Photo Seal) de referencia representativa de la apariencia de dicha fotografía, por medio de un algoritmo conocido.

5 A continuación, en una etapa (C), se genera el primer dato aleatorio RNGD, para calcular el primer dato codificado (denominado SSKD de SSK-DATA por conveniencia, aunque, como se ha explicado, el presente procedimiento no se limita al secure sketch) mediante la aplicación de un
10 procedimiento de codificación a dicha información DPS de referencia representativa de la apariencia de dicha fotografía y a dicho primer dato aleatorio RNGD, es decir, $SSKD = \text{enc}(DPS, \text{RNGD})$.

El primer dato aleatorio RNGD es, como su nombre
15 indica, un dato de valor aleatorio que aporta aleatoriedad, lo cual es importante porque su conocimiento permitirá probar que se dispone del documento de identidad 1.

Preferentemente, el procedimiento de codificación es un procedimiento de bosquejo de un
20 algoritmo de tipo “secure sketch”. Este procedimiento de bosquejo es conocido por el experto en la técnica. Se describe particularmente en el documento “Fuzzy extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data”, de Dodis y col. (ver la definición
25 3 aportada en la página 11 de este documento).

Sin embargo, la unidad de procesamiento 4 puede utilizar otros procedimientos de codificación en lugar de un procedimiento de bosquejo (por ejemplo, procedimientos de algoritmos de tipo “fuzzy extractor” y, de manera general, la
5 lógica difusa).

Se debe observar que el procedimiento de codificación se puede aplicar directamente a dicha información de referencia representativa de la apariencia de dicha fotografía, pero también indirectamente, es decir,
10 a datos derivados de esta información de referencia para añadir más entropía. Por ejemplo, se puede utilizar como dato derivado una combinación de la información de referencia con el dato de lectura óptica, particularmente, un cierto número de los primeros bits de su huella digital
15 criptográfica (ver más adelante). En particular, esta combinación puede ser “o exclusiva”, es decir, $XOR(DPS; HMRZ)$, HMRZ es los primeros n bits de la huella digital criptográfica del dato de lectura óptica (en el ejemplo donde es MRZ) donde n es el número de bits de la información
20 de referencia (el mismo número de bits es necesario para XOR).

En cualquier caso, el procedimiento de codificación permite “enmascarar” el primer dato aleatorio RNGD mediante el resultado del procesamiento DPS de la
25 fotografía, pero de manera recuperable mediante un

procedimiento de decodificación complementario al procedimiento de codificación.

Cuando el procedimiento de codificación utilizado para el registro es un procedimiento de bosquejo para un
5 algoritmo de tipo “secure sketch”, el procedimiento de decodificación es el procedimiento de recuperación (“recovery” en inglés) del mismo algoritmo de tipo “secure sketch”. Tal procedimiento de recuperación también es conocido por el experto en la técnica (ver la definición 3
10 aportada en la página 11 del documento “Fuzzy extractors: How to Generate...” mencionado anteriormente).

De manera más precisa, si se denomina $DpsRef$ a la información de referencia y $DpsCand$ a una información candidata (con $SSKD = enc(RNGD, DpsRef)$), entonces los
15 procedimientos de codificación y decodificación son tales que si $DpsCand$ está suficientemente cerca de $DpsRef$ (es decir, diferente de menos de un umbral, lo que normalmente es el caso si se extrae la información representativa de la misma fotografía a partir de la cual se generó la información
20 de referencia, incluso si se observa que sigue siendo imposible que los dos valores coincidan, seguiremos teniendo $IDpsCand - DpsRef > 0$), entonces el primer dato decodificado es igual al primer dato aleatorio $RNGD$.

Si, por el contrario, $DpsCand$ no está lo
25 suficientemente cerca de $DpsRef$, entonces el primer dato

decodificado no es el valor correcto del primer dato aleatorio. Matemáticamente, el procedimiento de decodificación da, para un valor del primer dato codificado SSKD y para un valor de información candidata DpsCand, “el
5 valor $x = \text{dec}(\text{SSKD}, \text{DpsCand})$ de manera que exista un valor ε de norma inferior a un umbral dado que verifica $\text{SSKD} = \text{enc}(x, \text{DpsCand} + \varepsilon)$ ”, siendo x igual al valor del primer dato aleatorio RNGD si se tiene $\text{DpdCand} + \varepsilon = \text{DpsRef}$. Se recordará que tales procedimientos de codificación y decodificación
10 son conocidos por el experto en la técnica, y pueden ser objeto de numerosos modos de realización. También será posible aumentar la entropía de los datos codificados aplicando el procedimiento de codificación a más datos que solo la información representativa de la apariencia de
15 dicha fotografía y el primer dato aleatorio.

En una etapa (D) por último se almacenan en los medios de almacenamiento de datos 22 del servidor 2 y/o los medios de almacenamiento de datos 32 del equipo cliente 3 (llegado el caso, después de la transmisión):

- 20
 - dicho primer dato codificado SSKD;
 - la huella digital criptográfica de una primera concatenación del dato de lectura óptica del documento de identidad 1 y del primer dato aleatorio RNGD;
- 25
 - el eventual cifrado con la huella digital criptográfica de una segunda concatenación

del dato de lectura óptica del documento de
identidad 1 y del primer dato aleatorio RNGD,
diferente de la primera concatenación, de al
menos un dato biométrico de referencia de
5 dicho individuo.

Estos datos, en el caso en el que están almacenados
en el servidor 2, pueden indexarse en la memoria 22 con una
huella digital criptográfica de un identificador del
documento de identidad 1, generalmente obtenido de la MRZ.

10 Por huella digital criptográfica, o resumen
criptográfico (en inglés “hash”), se entiende el resultado de
una función hash criptográfica predeterminada.

Preferentemente, las concatenaciones primera y
segunda corresponden a concatenaciones en dos sentidos
15 diferentes, por ejemplo, MRZIRNGD para la primera
concatenación y RNGDIMRZ para la segunda concatenación, pero
se puede utilizar cualquier otra construcción como dos
concatenaciones en el mismo orden, pero incluyendo un
carácter predeterminado en el medio, por ejemplo, MRZI1IRNGD
20 y MRZI2IRNGD.

Se entiende que el dato de lectura óptica del
documento de identidad 1 y el primer dato aleatorio RNGD
pueden considerarse como secuencias de bits. El número de
bits de la concatenación es, por tanto, la suma de los números
25 de bits respectivos del dato de lectura óptica del documento
de identidad 1 y del primer dato aleatorio RNGD.

Por conveniencia, se denota primera huella digital a dicha huella digital criptográfica de la primera concatenación ($h(\text{MRZIRNGD})$ en particular), y segunda huella digital a la huella digital criptográfica de la segunda concatenación ($h(\text{RNGDIMRZ})$ en particular).

El truco de estas concatenaciones múltiples permite la formación de varias huellas digitales completamente independientes a partir de los mismos datos. De hecho, conociendo la primera huella digital (que se almacena en la memoria 22 y que, por lo tanto, podría ser obtenida por un hacker), no es posible obtener la segunda huella digital. Para obtener esta última, sigue siendo necesario conservar el valor del primer dato aleatorio RNGD, que solo se puede recuperar si se dispone de la información de referencia.

Por tanto, la huella digital biométrica de referencia cifrada con la segunda huella digital criptográfica (es decir, la segunda huella digital se utiliza como clave) solo permanece accesible para el titular del documento de identidad 1, de manera que el servidor 2 no puede manipular ni conocer los datos personales del usuario, que pueden almacenarse con total seguridad.

La primera huella digital puede asociarse en el servidor 2 con un descriptor del estado del documento de identidad 1, por ejemplo “OK”, “Caducado” o “KO”.

Se debe observar que el procedimiento de registro se puede repetir a intervalos regulares para verificar o actualizar los datos personales. Los datos recientes y fiables se pueden recuperar desde una entidad gubernamental.

5 Además, un documento de identidad 1 tiene una vida útil limitada y debe renovarse regularmente.

De acuerdo con un modo de realización preferido, el equipo cliente 3 o el servidor 2 dispone ventajosamente (en lugar del cifrado del dato biométrico de referencia) de un segundo dato codificado (denominado SSKT, de SSK-
10 TEMPLATE) obtenido mediante la aplicación de un procedimiento de codificación (típicamente el mismo procedimiento de codificación que para el primer dato codificado) al dato biométrico de referencia y a un segundo
15 dato aleatorio (denominado RNGT); y el servidor 2 dispone además de una huella digital criptográfica construida a partir del segundo dato aleatorio RNGT. Nuevamente, todos estos datos pueden almacenarse (al menos inicialmente) en los medios de almacenamiento de datos 22 del servidor 2 (y
20 asociarse con los otros datos)

Dicha huella digital criptográfica construida a partir del segundo dato aleatorio RNGT, denominada tercera huella digital criptográfica, puede ser una huella digital criptográfica directamente del segundo dato aleatorio RNGT,
25 o de cualquier función (por ejemplo, una concatenación) del segundo dato aleatorio RNGT y otro dato, ventajosamente de

la primera huella digital criptográfica (la huella digital criptográfica de una primera concatenación del dato de lectura óptica del documento de identidad 1 y del primer dato aleatorio RNGD).

5 Se entiende que ninguno de estos datos es nuevamente aprovechable en sí mismo porque:

- dicho segundo dato codificado SSKT por sí solo no permite recuperar ni el dato biométrico de referencia ni el segundo dato aleatorio RNGT;
- 10 • la huella digital criptográfica construida a partir del segundo dato aleatorio RNGT es una huella digital simple que no aporta ninguna información.

En tal modo realización, la etapa (a0) de registro
15 puede incluir, además:

- en la etapa (A) o en la etapa (B), la obtención de dicho dato biométrico de referencia (denominado TempRef de plantilla de referencia), por ejemplo, a partir de la
20 fotografía del documento de identidad 1;
- en la etapa (C), la generación del segundo dato aleatorio RNGT para calcular el segundo dato codificado SSKT mediante la aplicación de dicho procedimiento de codificación, es decir,
25 SSKT=enc(TempRef, RNGT);

- en la etapa (D), el almacenamiento en los medios de almacenamiento de datos 22 del servidor 2 y/o los medios de almacenamiento de datos 32 del equipo cliente 3 (llegado el caso, después de la transmisión) de dicho segundo dato codificado SSKT y de la huella digital criptográfica construida a partir del segundo dato aleatorio RNGT.

Debe observarse que estas acciones suplementarias relacionadas con el registro biométrico se pueden implementar en las nuevas etapas (A') a (D'), es decir, no necesariamente simultáneamente con las acciones relacionadas con el registro del documento de identidad 1.

Además, sigue siendo posible implementar un procedimiento de autenticación fuerte del individuo sin necesidad ni del cifrado del dato biométrico de referencia ni del segundo dato aleatorio RNGT y del segundo dato codificado SSKT, particularmente almacenándolos directamente en el equipo cliente 3 (sin cifrar), o incluso en un servidor dedicado a la biometría de tipo WebBIO, ver más adelante.

Autenticación

Ahora se supone que el registro se ha completado con éxito y que el documento de identidad ya es utilizable.

En un modo de realización preferido, el procedimiento de autenticación comienza con una etapa (a) de adquisición de una forma u otra (por ejemplo, a través de los medios de adquisición 30 del equipo cliente 3) de una imagen del documento de identidad 1, la imagen representa al menos la fotografía del individuo y el dato de lectura óptica del documento de identidad 1 (la MRZ) visibles en dicho documento de identidad 1. Preferentemente, dicha imagen representa todo el documento de identidad 1, al menos una cara completa. Como se ha explicado, puede ser necesario adquirir varias imágenes, por ejemplo, para ver todas las caras.

Típicamente, es el individuo el que toma una foto de su documento de identidad 1 con su terminal móvil, llegado el caso, a petición del servidor que desea una autenticación fuerte (por ejemplo, para el servicio para el que ha lanzado un procedimiento de recuperación, particularmente a través de una API dedicada).

Con respecto al dato biométrico candidato, “fresco”, este se puede obtener durante la etapa previa (a). Más precisamente, una vez que se ha adquirido la imagen del documento de identidad 1, el servidor 2 (o nuevamente el servidor de un tercero) puede solicitar entonces la adquisición del dato biométrico candidato.

Es importante entender que si la etapa de registro (a0) se puede implementar semanas antes de la implementación

de la autenticación, la etapa (a) se implementa en el peor de los casos unos minutos antes que el resto del procedimiento, para garantizar la “frescura” del dato biométrico candidato.

5 Por tanto, la etapa (a) comprende ventajosamente la generación del dato biométrico candidato a partir de un rasgo biométrico suministrado por los medios de adquisición biométrica del equipo cliente 3 (es decir, típicamente los medios de adquisición óptica 30). Esto
10 significa, por ejemplo, que el individuo primero toma una fotografía de su documento de identidad 1, y después una fotografía de su rostro.

 Para garantizar la frescura del dato candidato, la etapa (a) podrá comprender la marca de tiempo del dato
15 biométrico candidato por medio de un marcador de tiempo (denominado “timestamp” en inglés).

 El experto en la técnica sabrá cómo implementar tal marca de tiempo utilizando técnicas conocidas y, ventajosamente, se utiliza como marcador de tiempo un nonce
20 (es decir, un número arbitrario, es decir, un factor aleatorio de un solo uso, del inglés “number used once”).

 El objetivo del resto del procedimiento es verificar que la etapa (a) se haya desarrollado correctamente como se ha descrito anteriormente y que no estamos en
25 presencia de una falsificación (por ejemplo, una imagen que se hubiera modificado fraudulentamente) o de una usurpación

(un individuo que no es el portador del documento de identidad 1).

En una etapa (b), los medios de procesamiento de datos 21, 31 del equipo cliente 3 o del servidor 2 analizan la imagen, para extraer:

- una información (DPS) candidata representativa de la apariencia de la fotografía tal como se representa en la imagen adquirida;
- el dato de lectura óptica del documento de identidad 1

La extracción de la información candidata comprende la identificación de la fotografía que aparece en la imagen y la obtención de la información candidata de la misma manera que se obtuvo información de referencia durante el registro. La identificación de la fotografía se puede hacer gracias a modelos y máscaras (en efecto, los documentos de identidad siempre tienen la misma organización) y, por tanto, el análisis de la imagen puede comprender el reconocimiento de un contorno del documento de identidad 1, el reencuadre de este contorno y la aplicación de las máscaras predeterminadas. Para esto, se pueden utilizar inteligentemente redes neuronales con convoluciones adecuadas. Similarmente, con respecto al dato de lectura óptica, existen algoritmos que permiten su extracción automática, especialmente dado que las zonas de

tipo MRZ están especialmente previstas para ser leídas fácilmente por una computadora.

Una vez que la fotografía ha sido “aislada” en la imagen, se aplican los mismos algoritmos que los aplicados a la fotografía original para obtener informaciones candidatas representativas de la apariencia de la fotografía tal como se representa.

Se entiende que las informaciones de referencia y candidata deberán obtenerse de manera idéntica para poder compararlas.

De acuerdo con un primer modo de realización, la etapa (b) es implementada por el servidor 2, de acuerdo con lo que se describe en la solicitud FR núm. 1904375. Se supone que este último almacena el primer dato codificado y, por eso mismo, la etapa (a) comprende la transmisión al servidor 2 de dicha imagen adquirida del documento de identidad 1. De acuerdo con un segundo modo de realización, la etapa (b) es implementada directamente por el equipo cliente 3 de acuerdo con lo descrito en la solicitud núm. FR1904406.

Preferentemente, en este segundo modo de realización, la etapa (b) comprende la interrogación del servidor 2 para recuperar al menos dicho primer dato codificado SSKD si está almacenado en este servidor 2, por ejemplo, proporcionándole la huella digital criptográfica del identificador del documento 1 (este identificador se puede

obtener de la MRZ, por ejemplo): el servidor 2 transmite el primer dato codificado asociado con la huella digital recibida. Se observa que, como alternativa, dicho primer dato codificado puede haberse proporcionado hace mucho tiempo y
5 almacenado desde entonces en los medios de almacenamiento de datos 32 del equipo cliente 3.

En cualquier caso, en una etapa (c), los medios de procesamiento de datos 21, 31 del servidor 2 o del equipo cliente 3 calculan un primer dato decodificado mediante la
10 aplicación de un procedimiento de decodificación a dicha información candidata (DPS) representativa de la apariencia de dicha fotografía y a dicho primer dato codificado.

Como se ha explicado, el procedimiento de decodificación (y el procedimiento de codificación) es tal
15 que dicho primer dato decodificado corresponde al primer dato aleatorio RNGD si dicha información candidata representativa de la apariencia de dicha fotografía coincide con la información de referencia representativa de la apariencia de dicha fotografía. En otras palabras,
20 si la información de referencia y la información candidata están lo suficientemente cerca, el valor decodificado corresponderá al valor aleatorio RNGD utilizado para obtener este primer dato codificado SSKD.

De manera general, el resultado de una comparación
25 de la información candidata y la información de referencia debe mostrar que son idénticas o al menos presentar una

distancia inferior a un umbral de error predeterminado. Por ejemplo, para los elementos gráficos de tipo fotografía, los datos de seguridad de tipo Digital Photo Seal coinciden si estos difieren en menos del 10 %.

5 Por tanto, se entiende que el valor del primer dato aleatorio “enmascarado” por el DPS se puede recuperar si el usuario dispone de una fotografía idéntica a la utilizada durante el registro, de la que se toma la información de referencia.

10 En una etapa (d), los medios de procesamiento de datos 21, 31 verifican que una huella digital criptográfica de una primera concatenación del dato de lectura óptica extraído y del dato decodificado coincida con la huella digital criptográfica de la primera concatenación del dato
15 de lectura óptica del documento de identidad 1 y del dato aleatorio almacenado en los medios de almacenamiento de datos 22 del servidor 2.

 En otras palabras, el servidor 2 o el equipo cliente 3 intenta reconstruir la primera huella digital
20 realizando la misma primera concatenación del dato de lectura óptica extraído y del primer dato decodificado.

Si:

- el dato de lectura óptica extraído coincide con el dato de lectura óptica utilizado durante
25 el registro; y

- el primer dato decodificado coincide con el primer dato aleatorio RNGD;

Entonces, la primera concatenación dará exactamente el mismo resultado y se llegará nuevamente a la primera huella digital.

En todos los demás casos, la entropía de las funciones hash criptográficas hace que se llegue a un resultado muy diferente. Si el documento 1 ha sido alterado (por ejemplo, reemplazando la fotografía), entonces las informaciones candidata y de referencia correspondientes no coincidirán, por lo tanto, se obtendrá un valor falso del factor aleatorio y, por lo tanto, de la primera huella digital, y la autenticación será rechazada.

Debe observarse que, si es el equipo cliente 3 el que ha implementado hasta ahora las etapas descritas, es necesario informar al servidor 2 del resultado de la verificación. Sin embargo, se puede conocer el valor correcto de la primera huella digital, aunque fuera una autenticación anterior del individuo. Esta es la razón por la cual el equipo cliente 3 demostrará ventajosamente que ha obtenido esta primera huella digital de manera correcta, es decir, a partir del documento de identidad 1, y esto de manera no interactiva, es decir con solo una “ida” de información desde el equipo cliente 3 al servidor 2, y no hay “vuelta”. Y, sobre todo, como se ha explicado, el servidor 2 no recibirá ni el primer dato aleatorio RNGD, ni la información candidata

representativa de la apariencia de dicha fotografía, ni el dato de lectura óptica (ni ningún dato que permita volver a esto últimos), aunque es posible que el servidor 2 sepa con certeza que la primera huella digital se ha calculado correctamente. Además, todos los datos transmitidos no son sensibles y podrían ser interceptados sin que esto suponga un problema.

Para esto, en la etapa (d), los medios de procesamiento de datos 31 del equipo cliente 3 que actúan como una entidad de prueba generan ventajosamente una prueba de divulgación nula de conocimientos del cálculo de dicha huella digital criptográfica a partir de la primera concatenación del dato de lectura óptica extraído y del primer dato decodificado, es decir, que la primera huella digital criptográfica realmente se ha calculado, y de manera correcta, dicha prueba es transmitida por el equipo cliente 3 al servidor 2, dicha prueba de divulgación nula de conocimiento con la huella digital criptográfica calculada.

Más precisamente, dicha prueba de divulgación nula de conocimientos garantiza la siguiente afirmación: “dada una huella digital criptográfica H , existe un dato de lectura óptica y un primer dato aleatorio RNGD (el dato decodificado) tales que su primera concatenación tiene como huella digital esta huella digital criptográfica H dada”. El

experto en la técnica podrá consultar el documento núm. FR1904406 para más información.

Por tanto, los medios de procesamiento de datos 21 del servidor 2 solo tienen que verificar que la prueba
5 de divulgación nula de conocimiento es válida y que la huella digital criptográfica recibida coincide con la de la primera concatenación de un dato de lectura óptica de dicho documento de identidad 1 y de un primer dato aleatorio del que dispone el servidor 2.

10 Si la prueba no es válida, esto significa que la primera huella digital criptográfica no se obtuvo válidamente y, por lo tanto, potencialmente el individuo no dispone del documento de identidad y está tratando de usurpar una identidad. Si la prueba es válida pero la huella digital
15 criptográfica recibida no corresponde a aquella de la que dispone la entidad de verificación 2, esto significa que el primer dato decodificado no corresponde al primer factor aleatorio o que el dato de lectura extraído no es el original, es decir, que el documento de identidad 1 ha sido falsificado
20 (a nivel de la fotografía o del dato de lectura óptica). Se puede emitir una alerta por utilización fraudulenta. En la etapa (d), los medios de procesamiento de datos 21, 31 verifican, además, que el dato biométrico de referencia y el dato biométrico candidato del individuo coinciden, el
25 procedimiento implica, por lo tanto, una comparación entre el dato biométrico candidato y el dato biométrico de

referencia. Debe observarse que puede estar implicado un control en vivo, para verificar, por ejemplo, que el dato biométrico de referencia no proviene de una falsificación (por ejemplo, una máscara facial o un dedo de resina).

5 Esta etapa se puede implementar de muchas maneras conocidas, utilizando el equipo cliente 3, el servidor 2 o incluso un servidor de biometría dedicado.

 Debe observarse que todas las combinaciones son posibles: cada uno del equipo cliente 3 y del servidor 2
10 pueden implementar 0, 1 o 2 de las verificaciones de la etapa (d).

 Por ejemplo, es completamente posible que el servidor 2 reciba en la etapa (a) tanto la imagen adquirida del documento de identidad 1 como el dato biométrico
15 candidato.

 De manera particularmente preferida, incluso se puede imaginar que durante la etapa (a), el servidor 2 recibe primero la imagen adquirida del documento de identidad 1, y a continuación solicita al equipo 1 el dato
20 biométrico candidato que le es transmitido entonces en un segundo momento.

 Alternativamente o, además, el servidor 2 o el equipo 3 puede transmitir (llegado el caso, retransmitir) el dato biométrico candidato a un servidor de confianza dedicado
25 a la biometría, que almacena el dato biométrico de

referencia, que implementa la comparación y envía el resultado al servidor.

En cualquier caso, la implementación de la comparación comprende típicamente el cálculo de una distancia
5 entre los datos, cuya definición varía en función de la naturaleza de los datos biométricos considerados. El cálculo de la distancia comprende el cálculo de un polinomio entre los componentes de los datos biométricos y, ventajosamente, el cálculo de un producto escalar.

10 Por ejemplo, en el caso en que los datos biométricos se obtuvieron a partir de imágenes del iris, una distancia utilizada convencionalmente para comparar dos datos es la distancia de Hamming. En el caso en que los datos biométricos se hayan obtenido a partir de imágenes
15 del rostro de un individuo, es habitual utilizar la distancia euclidiana. Este tipo de cálculo de distancia es conocido por el experto en la técnica y no se describirá con más detalle.

En el caso en el que el servidor 2 o el equipo
20 cliente 3 almacena un cifrado del dato biométrico de referencia de dicho individuo con una huella digital criptográfica de una segunda concatenación del dato de lectura óptica del documento de identidad 1 y del dato aleatorio (la segunda huella digital criptográfica), la etapa
25 (d) comprende el desciframiento de este dato biométrico de referencia, por medio de la huella digital criptográfica de

una segunda concatenación del dato de lectura óptica extraído y del dato decodificado (cada uno obtenido en la etapa (c)), para poder realizar la comparación. Nuevamente, el experto en la técnica podrá consultar la solicitud núm. FR1904375.

5 En el caso en que se tiene un segundo dato codificado SSKT obtenido mediante la aplicación de un procedimiento de codificación a un dato biométrico de referencia y a un segundo dato aleatorio RNGT, y una huella digital criptográfica construida a partir del segundo dato
10 aleatorio RNGT, se puede utilizar un procedimiento de decodificación para verificar si el dato biométrico candidato y el dato biométrico de referencia coinciden, de la misma manera que lo que se hizo para la información de tipo DPS en la fotografía.

15 Nuevamente, cuando el procedimiento de codificación utilizado para el registro es un procedimiento de bosquejo de un algoritmo de tipo “secure sketch”, el procedimiento de decodificación es el procedimiento de recuperación (“recovery” en inglés) del mismo algoritmo de
20 tipo “secure sketch”, y el experto en la técnica podrá utilizar otros procedimientos.

 Matemáticamente, el procedimiento de decodificación da, para un valor del segundo dato codificado SSKT y para un dato biométrico candidato TempCand, “el valor
25 $x = \text{dec}(\text{SSKT}, \text{TempCand})$ de manera que haya un valor ε por norma inferior a un umbral dado que verifica $\text{SSKT} = \text{enc}(x,$

TempCand+ ε)”, siendo x igual al valor del primer dato aleatorio RNGT si tenemos TempCand+ ε =TempRef.

Por tanto, la etapa (c) comprende, además, ventajosamente el cálculo por los medios de procesamiento de
5 datos 21, 31 del servidor 2 o del equipo cliente 3 de

- un segundo dato decodificado mediante la aplicación de un procedimiento de decodificación a dicho dato biométrico candidato y al segundo dato codificado (de
10 nuevo, el dato codificado es tal que dicho segundo dato decodificado corresponde al segundo dato aleatorio RNGT si dicho dato biométrico candidato coincide con el dato biométrico de referencia);
- una huella digital criptográfica construida a partir del segundo dato decodificado (se
15 entenderá que esta huella digital criptográfica debe construirse de la misma manera que la tercera huella digital criptográfica a partir del segundo dato
20 aleatorio RNGT, particularmente la huella digital criptográfica de una concatenación del segundo dato aleatorio RNGT y de la primera huella digital criptográfica).

25 En cualquier caso, la comparación de los datos biométricos puede ser realizada por los medios de

procesamiento de datos 21 del servidor 2, pero es preferible que se realice en el equipo cliente 3 para garantizar totalmente la privacidad del individuo. Para esto, se puede utilizar nuevamente un protocolo
5 criptográfico que genera una “prueba” de que el dato biométrico candidato y el dato biométrico de referencia coinciden, esta prueba no revela nada más que el hecho de que estos datos biométricos están efectivamente en posesión del productor de la prueba.

10 En otras palabras, se pueden utilizar hasta dos pruebas de divulgación nula de conocimiento:

- la primera prueba es la prueba del cálculo de dicha huella digital criptográfica a partir de la primera concatenación del dato de
15 lectura óptica extraído y del primer dato decodificado;
- la segunda prueba es la prueba del hecho de que el dato biométrico candidato y el dato biométrico de referencia coinciden.

20 En este caso, la etapa (d) comprende ventajosamente la generación por los medios de procesamiento de datos 31 del equipo cliente 3 de la prueba de divulgación nula de conocimientos del hecho de que el dato biométrico candidato y el dato biométrico de
25 referencia coinciden, lo que es, en particular, una prueba del cálculo de dicha huella digital criptográfica a partir

del segundo dato decodificado, esta prueba no revela nada más que el hecho de que el segundo dato decodificado (es decir, el segundo dato aleatorio RNGT) están correctamente en posesión del productor de la prueba. Nuevamente, la
5 prueba pretende garantizar que la tercera huella digital criptográfica se ha calculado efectivamente y de manera correcta.

Más precisamente, dicha prueba de divulgación nula de conocimientos garantiza la siguiente afirmación:
10 “dada una huella digital criptográfica T, existe un segundo dato aleatorio RNGT (y, llegado el caso, un dato de lectura óptica) tal que una función dada de este segundo dato aleatorio RNGT tiene como huella digital esta huella digital criptográfica T dada”. En el caso específico en el
15 que la tercera huella digital es la huella digital criptográfica de una concatenación del segundo dato aleatorio RNGT y de la primera huella digital criptográfica, la afirmación garantizada es la siguiente:
“dada una huella digital criptográfica T, existe un segundo
20 dato aleatorio RNGT y otra huella digital criptográfica H tal que una concatenación de este segundo dato aleatorio RNGT y de esta otra huella digital criptográfica H tiene como huella digital dicha huella digital criptográfica T dada”.

25 La segunda prueba de divulgación nula de conocimiento puede generarse de la misma manera que la

primera prueba de divulgación nula de conocimiento, y transmitirse al servidor 2 con la nueva huella digital criptográfica calculada (la tercera huella digital), ver también el documento núm. FR1904406.

5 Si todas las verificaciones se han efectuado con éxito, el servidor 2 acepta la autenticación del individuo y transmite típicamente un “token” al servidor que ha solicitado la autenticación/recuperación del individuo. Más precisamente, si el procedimiento es un procedimiento de
10 registro de un autenticador en particular FIDO, este registro se lleva entonces a cabo. En otras palabras, el procedimiento comprende ventajosamente una etapa de registro de un autenticador. Si este autenticador que se va a registrar es directamente el equipo 3, puede enviar un
15 secreto o bien enviar la clave pública correspondiente a un par de claves de las cuales tiene la clave privada, lo que le permite ser utilizado como autenticador del individuo. Alternativamente, podría recibir tal secreto.

Se observará que en lugar de implementar
20 simultáneamente la verificación del documento 1 y la verificación biométrica (es decir, utilizar las mismas etapas (a) a (d)), es completamente posible implementar los procedimientos uno detrás de otro, es decir, tendremos las etapas (a') a (d') para el procedimiento implementado en
25 segundo lugar (en particular la verificación biométrica, incluso si es posible el orden inverso).

Se entiende que el presente procedimiento limita al máximo la necesidad de información personal y las posibles fugas asociadas, al tiempo que garantiza un nivel máximo de seguridad.

5

Servidor

De acuerdo con un segundo aspecto, se propone el conjunto de servidor 2 y equipo cliente 3 conectados, para la implementación del procedimiento de acuerdo con el primer aspecto, es decir, la autenticación de un individuo portador de un documento de identidad.

Como se ha explicado, el equipo cliente 3 y/o el servidor 2 comprenden unos medios de procesamiento de datos 21, 31 (según el caso, donde hay un procesamiento de datos directamente por el servidor 2, o si es el equipo 3 el que realiza este procesamiento y transmite al servidor 2 una prueba de divulgación nula de conocimiento de su correcta ejecución), configurados para:

- extraer, mediante análisis de una imagen adquirida de un documento de identidad 1 que representa al menos una fotografía de un individuo y un dato de lectura óptica visibles en dicho documento de identidad 1:
 - o una información candidata representativa de la apariencia de dicha fotografía tal

como se representa en la imagen
adquirida;

o dicho dato de lectura óptica tal como se
representa en la imagen adquirida;

5 • calcular un primer dato decodificado
mediante la aplicación de un procedimiento
de decodificación a dicha información
candidata representativa de la apariencia de
dicha fotografía y al primer dato
10 codificado, de manera que dicho primer dato
decodificado corresponda a un primer dato
aleatorio si dicha información candidata
representativa de la apariencia de dicha
fotografía coincide con una información de
15 referencia representativa de la apariencia
de dicha fotografía, el servidor 2 dispone
de una huella digital criptográfica de una
primera concatenación de dicho dato de
lectura óptica de dicho documento identidad
20 1 y dicho primer dato aleatorio, denominada
primera huella digital criptográfica;

 • verificar que:

 - una huella digital criptográfica de una
primera concatenación del dato de
25 lectura óptica extraído y del dato
decodificado coincide con dicha primera

huella digital criptográfica de la que
dispone el servidor 2; y

- un dato biométrico de referencia y el dato biométrico candidato del individuo coinciden.

5

El equipo cliente 3 puede comprender, además, (o estar conectado a) medios de adquisición óptica 30 y/o medios de adquisición biométrica, en particular los medios de adquisición óptica 30, para la adquisición del dato biométrico candidato.

10

Producto de programa informático

De acuerdo con un tercer y un cuarto aspectos, la invención se refiere a un producto de programa informático que comprende instrucciones de código para la ejecución (en particular en los medios de procesamiento de datos 21 del servidor 2 y los medios de procesamiento de datos 31 de equipo cliente 3) de un procedimiento de acuerdo con el primer aspecto de la invención, así como medios de almacenamiento legibles por un equipo informático (una memoria 22 del servidor 2 y una memoria 32 del equipo cliente 3) en el que se encuentra este producto de programa informático.

15

20

REIVINDICACIONES

1. Procedimiento de autenticación fuerte de un individuo implementado por un servidor (2) y un equipo
5 cliente (3) conectados;

el equipo cliente (3) dispone de un dato biométrico candidato del individuo y de una imagen adquirida de un documento de identidad (1) que representa al menos una fotografía de
10 dicho individuo y un dato de lectura óptica visibles en dicho documento de identidad (1), y el servidor (2) dispone de una huella digital criptográfica de una primera concatenación de dicho dato de lectura óptica de dicho documento
15 de identidad (1) y de un primer dato aleatorio, denominada primera huella digital criptográfica;

el procedimiento está caracterizado por que comprende la implementación mediante medios de
20 procesamiento de datos (21, 31) del servidor (2) y/o del equipo cliente (3), de las etapas de;

(b) extracción, mediante análisis de dicha imagen adquirida de dicho documento de
25 identidad (1), de:

- o una información candidata representativa de la apariencia de dicha fotografía tal como se representa en la imagen adquirida;
 - 5 o dicho dato de lectura óptica tal como se representa en la imagen adquirida;
- (c) cálculo de un primer dato decodificado mediante la aplicación de un procedimiento de decodificación a dicha información
- 10 candidata representativa de la apariencia de dicha fotografía y a un primer dato codificado, de manera que dicho primer dato decodificado corresponda al primer dato aleatorio si dicha información
- 15 candidata representativa de la apariencia de dicha fotografía coincide con una información de referencia representativa de la apariencia de dicha fotografía;
- (d) verificación de que:
 - 20 - una huella digital criptográfica de una primera concatenación del dato de lectura óptica extraído y del dato decodificado coincide con dicha primera huella digital criptográfica
 - 25 de la que dispone el servidor (2); y

- un dato biométrico de referencia y el dato biométrico candidato del individuo coinciden.

2. Procedimiento de acuerdo con la reivindicación

5 1, que comprende una etapa (a) de adquisición previa de dicha imagen de dicho documento de identidad (1) que representa al menos una fotografía de un individuo y un dato de lectura óptica visibles en dicho documento de identidad (1) mediante unos medios de adquisición óptica (30) del equipo cliente
10 (3), y la generación del dato biométrico candidato a partir de un rasgo biométrico proporcionado por medios de adquisición biométrica.

3. Procedimiento de acuerdo con la

reivindicación 2, en el que los medios de adquisición
15 biométrica son los medios de adquisición óptica (30) del equipo cliente (3), el equipo cliente (3) es un equipo electrónico personal para dicho individuo, en particular de tipo terminal móvil o tarjeta inteligente.

4. Procedimiento de acuerdo con una de las

20 reivindicación 1 a 3, en el que el servidor (2) o el equipo (3) dispone de un cifrado del dato de referencia biométrico de dicho individuo con una huella digital criptográfica de una segunda concatenación del dato de lectura óptica del documento de identidad (1) y del primer dato aleatorio,
25 diferente de la primera concatenación; la etapa (c) comprende el desciframiento de al menos un dato biométrico

de referencia de dicho individuo cifrado, mediante la huella digital criptográfica de una segunda concatenación del dato de lectura óptica extraído y del primer dato decodificado.

5 5. Procedimiento de acuerdo con una de las reivindicación 1 a 3, en el que el servidor (2) dispone de una huella digital criptográfica construida a partir de un segundo dato aleatorio, denominada tercera huella digital criptográfica; la etapa (c) comprende el cálculo por los
10 medios de procesamiento de datos (21, 31) del servidor (2) o del equipo cliente (3) de un segundo dato decodificado mediante la aplicación de un procedimiento de decodificación a dicho dato biométrico candidato y a un segundo dato codificado, de manera que dicho segundo dato
15 decodificado corresponda al segundo dato aleatorio si dicho dato biométrico candidato coincide con el dato biométrico de referencia; dicha verificación de la etapa (d) de que el dato biométrico de referencia y el dato biométrico candidato del individuo coinciden comprende la verificación
20 de que una huella digital criptográfica, construida a partir del segundo dato decodificado de la misma manera que se construye la tercera huella digital criptográfica a partir del segundo dato aleatorio, coincide con dicha tercera huella digital criptográfica de la que dispone el
25 servidor (2).

6. Procedimiento de acuerdo con una de las reivindicaciones 1 a 5, en el que la etapa (a) comprende la recepción por parte del servidor (2) de la imagen adquirida de dicho documento de identidad (1) y del dato biométrico candidato desde el equipo cliente (3), las etapas (b) a (d) son implementadas por los medios de procesamiento de datos (21) del servidor (2).

7. Procedimiento de acuerdo con una de las reivindicaciones 1 a 5, en el que las etapas (b) y (c) son implementadas por los medios de procesamiento de datos (31) del equipo cliente (3), la etapa (c) comprende el cálculo de la huella digital criptográfica de una primera concatenación del dato de lectura óptica extraído y del primer dato decodificado, y la generación de una prueba de divulgación nula de conocimientos del cálculo de dicha huella digital criptográfica a partir de la primera concatenación del dato de lectura óptica extraído y del primer dato decodificado; la verificación de la etapa (d) de que la huella digital criptográfica de una primera concatenación del dato de lectura óptica extraído y del dato decodificado coincide con la primera huella digital criptográfica comprende la verificación de que:

- la prueba de divulgación nula de conocimiento del cálculo de dicha huella digital criptográfica a partir de la primera concatenación del dato de

lectura óptica extraído y del primer dato decodificado es válida, y

- la huella digital criptográfica recibida coincide con dicha primera huella digital criptográfica de la que dispone el servidor (2).

5

8. Procedimiento de acuerdo con una de las reivindicaciones 1 a 7, en el que las etapas (b) y (c) son implementadas por los medios de procesamiento de datos (31)

10 del equipo cliente (3), la etapa (c) comprende la generación de una prueba de divulgación nula de conocimientos del hecho de que el dato biométrico de referencia y el dato biométrico candidato del individuo coinciden; dicha verificación de la etapa (d) de que el dato biométrico de referencia y el dato

15 biométrico candidato del individuo coinciden comprende la verificación por los medios de procesamiento de datos (21) del servidor (2) de que la prueba de divulgación nula del conocimiento del hecho de que el dato biométrico de referencia y el dato biométrico candidato del individuo

20 coinciden es válida.

9. Procedimiento de acuerdo con una de las reivindicación 1 a 8, que comprende una etapa anterior (a0) de registro de datos de dicho documento de identidad (1) que comprende las subetapas de:

25 (A) obtención de la fotografía de dicho individuo visible en dicho documento de

identidad (1) y del dato de lectura óptica del documento de identidad (1);

5 (B) extracción, mediante análisis de dicha fotografía de la información de referencia representativa de la apariencia de dicha fotografía;

(C) generación del primer dato aleatorio; cálculo del primer dato codificado mediante la aplicación de un procedimiento de codificación a dicha información de referencia representativa de la apariencia de dicha fotografía y a dicho primer dato aleatorio, y de la primera huella digital criptográfica.

10

15 10. Procedimiento de acuerdo con las reivindicaciones 5 y 9 combinadas, en el que durante la etapa (a0), la subetapa (A) o la subetapa (B) comprende la obtención de dicho dato biométrico de referencia; y la subetapa (C) comprende, además, la generación del segundo dato aleatorio y el cálculo del segundo dato codificado mediante la aplicación de dicho procedimiento de codificación a dicho dato biométrico de referencia y a dicho segundo dato aleatorio, y de la tercera huella digital criptográfica.

20

11. Procedimiento de acuerdo con una de las reivindicaciones 1 a 10, en el que el procedimiento de decodificación es un procedimiento complementario de un

25

procedimiento de bosquejo de un algoritmo de tipo “secure sketch”.

12. Procedimiento de acuerdo con una de las reivindicaciones 1 a 11, en el que el dato de lectura óptica del documento de identidad (1) es un dato de tipo MRZ, código QR o PDF417.

13. Procedimiento de acuerdo con una de las reivindicaciones 1 a 12, que comprende una etapa (e) de registro de un autenticador, en particular de la alianza Fast IDentity Online, FIDO.

14. Procedimiento de acuerdo con una de las reivindicaciones 1 a 13, en el que la información de referencia representativa de una apariencia esperada de dicha fotografía es un dato de seguridad de tipo Digital Photo Seal.

15. Conjunto de autenticación fuerte que comprende un servidor (2) y un equipo cliente (3) conectados, caracterizado por que el equipo cliente (3) y/o el servidor (2) comprenden medios de procesamiento de datos (21, 31) configurados para:

- extraer, mediante análisis de una imagen adquirida de un documento de identidad (1) que representa al menos una fotografía de un individuo y un dato de lectura óptica visibles en dicho documento de identidad (1):

- o una información candidata representativa de la apariencia de dicha fotografía tal como se representa en la imagen adquirida;
 - 5 o dicho dato de lectura óptica tal como se representa en la imagen adquirida;
- calcular un primer dato decodificado mediante la aplicación de un procedimiento de decodificación a dicha información
- 10 candidata representativa de la apariencia de dicha fotografía y al primer dato codificado, de manera que dicho primer dato decodificado corresponda a un primer dato aleatorio si dicha información
- 15 candidata representativa de la apariencia de dicha fotografía coincide con una información de referencia representativa de la apariencia de dicha fotografía, el servidor (2) dispone de una huella digital
- 20 criptográfica de una primera concatenación de dicho dato de lectura óptica de dicho documento identidad (1) y dicho primer dato aleatorio, denominada primera huella digital criptográfica;
- 25 • verificar que:

- una huella digital criptográfica de una primera concatenación del dato de lectura óptica extraído y del dato decodificado coincide con dicha primera huella digital criptográfica de la que dispone el servidor (2); y
- un dato biométrico de referencia y el dato biométrico candidato del individuo coinciden.

10 16. Producto de programa informático que comprende instrucciones de código para la ejecución de un procedimiento de acuerdo con una de las reivindicaciones 1 a 14 de autenticación fuerte de un individuo, cuando dicho procedimiento se ejecuta en una computadora.

15 17. Medio de almacenamiento legible por un equipo informático en el que un producto de programa informático comprende instrucciones de código para la ejecución de un procedimiento de acuerdo con una de las reivindicaciones 1 a 14 de autenticación fuerte de un individuo.

RESUMEN

La invención propone un procedimiento de autenticación fuerte de un individuo implementado por un
5 servidor (2) y un equipo cliente (3) conectados;

el equipo cliente (3) dispone de un dato biométrico candidato del individuo y de una imagen adquirida de un documento de identidad (1) que representa al menos una fotografía de dicho
10 individuo y un dato de lectura óptica visibles en dicho documento de identidad (1), y el servidor (2) dispone de una huella digital criptográfica de una primera concatenación de dicho dato de lectura óptica de dicho documento de identidad
15 (1) y de un primer dato aleatorio, denominada primera huella digital criptográfica;

que comprende la implementación de etapas de;
(b) extracción, mediante un análisis de dicha imagen adquirida de dicho documento de
20 identidad (1), de una información candidata representativa de la apariencia de dicha fotografía tal como se representa en la imagen adquirida; y de dicho dato de lectura óptica tal como se representa en la imagen
25 adquirida;

- (c) cálculo de un primer dato decodificado mediante la aplicación de un procedimiento de decodificación a dicha información candidata representativa de la apariencia de dicha fotografía y a un primer dato codificado, de manera que dicho primer dato decodificado corresponda al primer dato aleatorio si dicha información candidata representativa de la apariencia de dicha fotografía coincide con una información de referencia representativa de la apariencia de dicha fotografía;
- (d) verificación de que:
- una huella digital criptográfica de una primera concatenación del dato de lectura óptica extraído y del dato decodificado coincide con dicha primera huella digital criptográfica de la que dispone el servidor (2); y
 - un dato biométrico de referencia y el dato biométrico candidato del individuo coinciden.

Figura para el resumen: Fig. 1

[Fig. 1]

