(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 910 352**

(51) Int. CI.:

H04L 29/06 (2006.01)
G06F 21/32 (2013.01)
G06F 21/36 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **19.05.2020 E 20175383 (7)**

(97) Fecha y número de publicación de la concesión europea: **09.03.2022 EP 3742699**

(54) Título: **Procedimiento de autenticación fuerte de un individuo**

(30) Prioridad:

24.05.2019 FR 1905521

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
12.05.2022

(73) Titular/es:

IDEMIA IDENTITY & SECURITY FRANCE (100.0%)
2 Place Samuel de Champlain
92400 Courbevoie, FR

(72) Inventor/es:

BAHLOUL, SÉBASTIEN

(74) Agente/Representante:

DEL VALLE VALIENTE, Sonia

DESCRIPCIÓN

Procedimiento de autenticación fuerte de un individuo

Campo de la invención

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

Estado de la técnica

En la actualidad se conocen procedimientos de autenticación fuerte (es decir, con varios factores de autenticación) muy robustos, concretamente tal como están definidos por las especificaciones de la alianza FIDO.

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

Estos procedimientos son completamente satisfactorios, pero presentan una debilidad con respecto a sus mecanismos de "recubrimiento" puestos en práctica en caso de olvido de código o de pérdida de su autenticador.

Más precisamente, o bien estos mecanismos de recubrimiento utilizan solo un único factor de autenticación (normalmente se envía un enlace a una dirección de correo electrónico de recuperación) y entonces se pierde todo el beneficio de la autenticación fuerte, o bien hace falta conservar información personal privada de tipo "respuesta a una pregunta secreta" o una foto de identidad.

Se observa, por una parte, que esta solución no es fiable (si la información solicitada es demasiado secreta, el usuario puede perderla/olvidarla, y si es demasiado común los piratas pueden conseguir recuperarla mediante ingeniería social) y, por otra parte, que la posesión de tal información plantea problemas en cuanto al respeto de la privacidad de los usuarios.

En la solicitud EP2656321 se ha propuesto utilizar como factor de autenticación una imagen de un objeto cualquiera elegido de forma secreta por el individuo, tal como una joya o un documento de identidad. Este método mejora la fiabilidad, pero sigue siendo problemático en lo referente a la gestión de la privacidad.

El documento WO 2018/233487 describe la autenticación fuerte de un individuo basándose en una fotografía presente en un documento de identidad, obtenidos los datos del documento de identidad y de un dato biométrico adquirido. Para aumentar la seguridad del procedimiento y tras la verificación del documento de identidad, se solicita al individuo que realice una secuencia de vídeo de algunos segundos durante la cual debe pronunciarse un código enviado por un servidor. El servidor verifica entonces que el código pronunciado por el individuo es correcto, así como que el individuo en la secuencia de vídeo es el asociado al documento de identidad

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

Presentación de la invención

Según un primer aspecto, la invención se refiere a un procedimiento de autenticación fuerte de un individuo llevado a cabo por un servidor y un equipo cliente conectados;

disponiendo el equipo cliente 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 disponiendo el servidor de una huella criptográfica de una primera concatenación de dicho dato de lectura óptica de dicho documento de identidad y de un primer dato de aleatoriedad, denominado primera huella criptográfica;

estando el procedimiento caracterizado por que comprende la ejecución, mediante medios de procesamiento de datos del servidor y/o del equipo cliente, de etapas de;

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

- una información candidata representativa del aspecto 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) Calcular un primer dato decodificado mediante aplicación de un proceso de decodificación a dicha información candidata representativa del aspecto de dicha fotografía y a un primer dato codificado, tal que dicho primer dato decodificado corresponde al primer dato de aleatoriedad si dicha información candidata representativa del

aspecto de dicha fotografía coincide con una información de referencia representativa del aspecto de dicha fotografía;

(d) Verificar que:

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

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

Según 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 mediante medios de adquisición biométrica;

Los medios de adquisición biométrica son los medios de adquisición óptica del equipo cliente, siendo el equipo cliente un equipo electrónico personal de 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 criptográfica de una segunda concatenación del dato de lectura óptica del documento de identidad y del primer dato de aleatoriedad, diferente de la primera concatenación; comprendiendo la etapa (c) el descifrado del al menos un dato biométrico de referencia de dicho individuo cifrado, por medio de la huella criptográfica de una segunda concatenación del dato de lectura óptica extraído y del primer dato decodificado;

El servidor dispone de una huella criptográfica construida a partir de un segundo dato de aleatoriedad, denominada tercera huella criptográfica; comprendiendo la etapa (c) el cálculo mediante los medios de procesamiento de datos del servidor o del equipo cliente de un segundo dato decodificado mediante la aplicación de un proceso de decodificación a dicho dato biométrico candidato y a un segundo dato codificado, de modo que dicho segundo dato decodificado corresponde al segundo dato de aleatoriedad 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 de que una huella criptográfica construida a partir del segundo dato decodificado de la misma forma en que se construye la tercera huella criptográfica a partir del segundo dato de aleatoriedad coincide con dicha tercera huella criptográfica de la que dispone el servidor;

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

El procedimiento comprende etapas (b) y (c) que se llevan a cabo mediante los medios de procesamiento de datos del equipo cliente, comprendiendo la etapa (c) el cálculo de la huella 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 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 criptográfica de una primera concatenación del dato de lectura óptica extraído y del dato decodificado coincide con la primera huella criptográfica, comprende la verificación de que:

- la prueba de divulgación nula de conocimiento del cálculo de dicha huella criptográfica a partir de la primera concatenación del dato de lectura óptica extraído y del primer dato decodificado es válida, y

- la huella criptográfica recibida coincide con dicha primera huella criptográfica de que dispone el servidor;

Las etapas (b) y (c) se llevan a cabo mediante los medios de procesamiento de datos del equipo cliente, comprendiendo la etapa (c) 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 biométrico candidato del individuo coinciden, comprende la verificación mediante los medios de procesamiento de datos del servidor de que la prueba de divulgación nula de conocimiento del 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 identidad que comprende unas subetapas de:

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

(B) Extraer, mediante análisis de dicha fotografía, información de referencia representativa del aspecto de dicha fotografía;

(C) Generar el primer dato de aleatoriedad; calcular el primer dato codificado, mediante aplicación de un proceso de codificación a dicha información de referencia representativa del aspecto de dicha fotografía y a dicho primer dato de aleatoriedad, y la primera huella criptográfica;

Durante la etapa (a0), la subetapa (A) o la subetapa (B) comprenden la obtención de dicho dato biométrico de referencia; y la subetapa (C) comprende, además, la generación del segundo dato de aleatoriedad y el cálculo del segundo dato codificado mediante aplicación de dicho proceso de codificación a dicho dato biométrico de referencia y a dicho segundo dato de aleatoriedad, y de la tercera huella criptográfica;

El proceso de decodificación es un proceso complementario de un proceso de boceto 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 un aspecto esperado de dicha fotografía es un dato de seguridad de tipo "Digital Photo Seal".

Según 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 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 del aspecto 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 aplicación de un proceso de decodificación a dicha información candidata representativa del aspecto de dicha fotografía y al primer dato codificado, tal que dicho primer dato decodificado corresponde a un primer dato de aleatoriedad si dicha información candidata representativa del aspecto de dicha fotografía coincide con una información de referencia representativa del aspecto de dicha fotografía, disponiendo el servidor de una huella criptográfica de una primera concatenación de dicho dato de lectura óptica de dicho documento de identidad y dicho primer dato de aleatoriedad, denominado primera huella criptográfica;

verificar que:

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

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

Según un tercer y un cuarto aspecto, la invención se refiere a un producto de programa de ordenador 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 un ordenador; y a un medio de almacenamiento legible por un equipo informático en el que un producto de programa de ordenador comprende instrucciones de código para la ejecución de un procedimiento según el primer aspecto de autenticación fuerte de un individuo.

Descripción de las figuras

Otras características, objetivos y ventajas de la presente invención se desprenderán de la lectura de la siguiente descripción detallada, con referencia a las figuras adjuntas, facilitadas a modo de ejemplos no limitativos y en las que:

- La figura 1 representa esquemáticamente un sistema para la ejecuciónejecución de los procedimientos según la invención.

Descripción Detallada

Arquitectura

La presente invención se refiere a un 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 presenta el documento 1, incluyendo posiblemente un procedimiento de registro de información de este documento 1 de identidad.

El presente procedimiento se denomina de autenticación fuerte, ya que combina "algo que posee el individuo", es decir, su documento 1 de identidad, y "algo que es/sabe el individuo", en este caso un rasgo biométrico. En efecto, hay dos niveles de fraudes posibles:

- El primero, es la falsificación del documento de identidad, por ejemplo, el cambio de la fotografía,

- El segundo, es el robo de identidad, por ejemplo, el uso de un documento 1 de identidad 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 autenticación.

De forma ventajosa, el presente procedimiento es un procedimiento "de registro de un factor de autenticación", es decir, de adición o de modificación de un medio de autenticarse (que puede elegirse de entre una contraseña, un equipo físico de autenticación y, en particular, un "autenticador de FIDO", una dirección de correo electrónico, etc.) que podrá utilizarse a continuación de forma recurrente para la autenticación diaria. De este modo, el procedimiento anterior se ejecuta normalmente en el primer uso de dicho factor de autenticación y, concretamente, en caso de pérdida de un factor de autenticación anterior (se habla entonces de procedimiento de recubrimiento:el caso en el que el usuario desea autenticarse de nuevo a pesar de esta pérdida). Por autenticador de FIDO se entiende un equipo de seguridad de la alianza FIDO ("Fast IDentity Online"), concretamente según una norma de autenticación tal como U2F ("Universal 2nd Factor"), FIDO2, protocolo de cliente a autenticador (CTAP), etc.; por ejemplo, un terminal móvil (tal como el equipo 3, véase a continuación), una llave USB, una tarjeta inteligente, que almacenan cada uno un secreto (un par de clave privada/clave pública). De este modo, el presente procedimiento se inscribe normalmente en el caso de pérdida de un autenticador de FIDO, pero se comprenderá que está perfectamente adaptado para cualquier tipo de factor de identificación, y podría incluso llevarse a cabo en cada autenticación para el acceso a un servicio para el que se solicita un nivel de seguridad máximo (por ejemplo, para hacer una transferencia bancaria, una compra inmobiliaria, etc.)

De forma especialmente preferida, dicho autenticador que va a registrarse es el equipo cliente 3, lo cual permite un proceso de registro simple y transparente, proporcionando el equipo 3 de paso todos los datos de identificación necesarios como, por ejemplo, una dirección MAC, y pudiendo presentar al final de este proceso un secreto (por ejemplo, un par de claves) que le permiten actuar a continuación como autenticador del individuo.

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

El documento 1 de identidad es un objeto personal de un individuo (numerosos individuos pueden poseer, cada uno, un documento de identidad de este tipo), y constituye preferiblemente un título oficial, de forma ventajosa emitido por un organismo gubernamental. Este documento puede adoptar numerosas formas tal como una tarjeta de identidad o un pasaporte, y puede ser eventualmente electrónico. De forma alternativa, puede ser cualquier documento elegido por el individuo o por un proveedor de servicio que tenga un valor concluyente para su autenticación, es decir, un documento representativo de la identidad del individuo, podría ser, por ejemplo, una tarjeta de transporte, una tarjeta profesional, una credencial de empresa, una licencia o incluso un documento creado específicamente por un organismo de gestión de autenticadores que sería necesario para registrar un nuevo autenticador, por analogía con los documentos proporcionados con cerraduras de seguridad que son necesarias para hacer un duplicado de llaves.

Según un modo de realización, adopta la forma de una tarjeta inteligente (de tipo "smart card") de las dimensiones convencionales y generalmente de PVC o policarbonato.

En cualquier caso, el documento 1 de identidad incluye una superficie maciza sobre la cual está impresa una cierta cantidad de información, y en particular:

- Una fotografía del individuo poseedor de la tarjeta (y eventualmente otro dato "gráfico" tal como una firma del individuo);

- un dato de lectura óptica (es decir, legible automáticamente, destinado a ordenadores), de tipo MRZ, código QR o PDF417 (se adoptará el ejemplo de la MRZ a continuación del documento, pero se comprenderá que no se limita a este tipo de dato de lectura óptica);

- Diversos datos alfanuméricos, denominados "datos visuales", elegidos concretamente de entre:

- Número completo del documento 1 de identidad;
- Fecha de caducidad;
- Fecha de emisión;
- Apellido;
- Nombre(s);
- Nacionalidad;
- Fecha de Nacimiento;
- Lugar de Nacimiento;
- Sexo;
- Estatura;
- Dirección;
- etc.

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

El equipo cliente 3 es un terminal local que comprende o está conectado a medios 30 de adquisición óptica (normalmente, una cámara fotográfica o un escáner) y adaptado para adquirir una imagen (del documento 1 como se verá). Comprende, además, medios 31 de procesamiento de datos y medios 32 de almacenamiento de datos. El equipo cliente 3 y el servidor 2 comprenden de forma ventajosa interfaces de comunicaciones que les permiten dialogar en remoto. De forma preferida, el cliente 3 es un equipo personal del individuo portador del documento 1 de identidad, por ejemplo, un terminal móvil del individuo (en particular, de tipo teléfono inteligente).

Preferiblemente, el equipo cliente 3 puede generar un dato biométrico a partir de un rasgo biométrico del individuo. El rasgo biométrico puede ser, por ejemplo, la forma de la cara, una huella digital, una huella palmar, un iris del individuo, etc. La extracción del dato biométrico se pone en práctica mediante un procesamiento de la imagen del rasgo biométrico que depende de la naturaleza del rasgo biométrico. El experto en la técnica conoce diversos procesamientos de imágenes para extraer datos biométricos. A modo de ejemplo no limitativo, la extracción del dato biométrico puede comprender una extracción de puntos particulares o de una forma de la cara, en el caso en donde la imagen sea una imagen de la cara del individuo.

El equipo cliente 3 comprende, o está conectado para ello a medios de adquisición biométrica, normalmente, un sensor de imagen y, de forma especialmente preferida, estos medios de adquisición biométrica son los medios 30 de adquisición óptica, por ejemplo, una cámara fotográfica adaptada para adquirir una fotografía de la cara en modo “selfi” (se indica que, de forma alternativa, pueden utilizarse medios de adquisición distintos, como un sensor de huella digital).

En cualquier caso, un dato biométrico de referencia utilizado para la autenticación del individuo es, de forma ventajosa, un dato previamente grabado en presencia de una autoridad (véase más adelante) o un dato procedente del documento 1 de identidad, tal como la fotografía.

Se observa que el equipo 3 puede adoptar numerosos modos de realización. Más precisamente, y como se verá, para la ejecución de la invención, es suficiente con que el equipo cliente 3 pueda obtener una imagen adquirida del documento 1 de identidad de una forma u otra, incluyendo de forma indirecta, y procesar esta imagen.

En cualquier caso, como se explica, el equipo cliente 3 puede adquirir una imagen de una imagen del documento 1 de identidad, es decir, fotografiar una fotocopia en vez del documento 1 directamente, incluso de una fotocopia de una fotocopia, etc. Como se verá, será suficiente con que la imagen adquirida represente el documento 1. Se comprenderá que el presente procedimiento no se limita a ninguna forma de obtener esta imagen y ninguna naturaleza en particular (la imagen adquirida puede estar en blanco y negro, deformada, etc.).

Se observa que es perfectamente posible que otras entidades estén conectadas al servidor 2 y al equipo 3, en particular servidores que llevan a cabo 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. Concretamente, puede imaginarse que un servidor de este tipo dispone de una solución de autenticación clásica (por ejemplo, con un autenticador de FIDO), y va a iniciar el presente procedimiento (poniéndose en contacto con el equipo 3) cuando el usuario desea registrar un nuevo factor de autenticación. Este servidor de servicio puede ejecutar, por ejemplo, una API dedicada a la interrogación del servidor 2 para la ejecución 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

A continuación, en la presente descripción, el experto en la técnica podrá hacer referencia a las solicitudes FR1904375 y FR1904406 que describen mecanismos que pueden utilizarse de forma independiente o en combinación en el ámbito de la invención.

De forma conocida, el presente procedimiento utiliza información representativa de un aspecto 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 va a permitir comparaciones.

Se designa como información "de referencia" la información representativa del aspecto "teórico" de la fotografía, es decir, tal como se espera. En cambio, se designa como información "candidata" la información representativa del aspecto constatado de la fotografía, es decir, como se representa en una imagen adquirida del documento 1. Se comprende que generalmente este aspecto constatado no es perfectamente idéntico al aspecto esperado, debido a condiciones de defectos inherentes a la adquisición de una imagen, y a la variabilidad de las condiciones de captura (iluminación, movimiento, distancia, etc.).

No obstante, dicha información representativa del aspecto se elige de tal forma que, si dos fotografías tienen aspectos que coinciden (es decir, se trata de la misma fotografía, aunque las condiciones de captura no sean idénticas), entonces su información representativa también coincide (es decir, presenta una distancia según una métrica dada inferior a un umbral).

De este modo, la información de referencia y la información candidata coinciden si y solo si el aspecto constatado y el aspecto esperado de la fotografía coinciden, es decir, que se trata realmente de la misma fotografía, dicho de otro modo, que la fotografía impresa en el documento 1 de identidad no se ha alterado de forma fraudulenta. Esta verificación puede hacerse para cada uno de los otros elementos gráficos, tal como una firma. Podrá utilizarse como información representativa del aspecto de la fotografía el "Digital Photo Seal" (DPS) que se tomará como ejemplo a continuación de la presente solicitud, es decir, el dato de seguridad tal como se describe en las solicitudes mencionadas en la introducción o, más precisamente, la solicitud 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 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). De forma alternativa, puede utilizarse un algoritmo de clasificación del tipo que emplea una red de neuronas convolucional, también conocida con el acrónimo CNN (por el inglés "Convolutional Neural Network").

Registro

Al iniciarse el procedimiento, se supone que el equipo cliente 3 dispone al menos de una imagen adquirida de dicho documento 1 de identidad, que representa al menos una fotografía de un individuo y un dato de lectura óptica visibles en dicho documento 1 de identidad (en el que pueden leerse los datos personales del individuo) y de un dato biométrico candidato.

El equipo cliente 3 o el servidor 2 requiere además disponer de un primer "dato codificado" (designado SSKD) obtenido mediante aplicación de un proceso de codificación a la información DPS de referencia representativa del aspecto de la fotografía de dicho individuo visible en dicho documento 1 de identidad y a un primer dato de aleatoriedad (designado RNGD). En la práctica, este primer dato codificado es almacenado de forma general (al menos inicialmente) por el servidor 2.

Por su parte, el servidor 2 solo tiene necesidad de disponer de una huella criptográfica de una primera concatenación del dato de lectura óptica del documento 1 de identidad y el primer dato de aleatoriedad RNGD.

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

Se comprende que ninguno de estos datos puede explotarse en sí mismo (en particular, si todos ellos se almacenan en el servidor 2), ya que:

- Dicho primer dato codificado SSKD no permite por sí solo ni recuperar la información DPS de referencia ni el primer dato de aleatoriedad RNGD;

- La huella criptográfica de una primera concatenación del dato de lectura óptica del documento 1 de identidad y del primer dato de aleatoriedad RNGD es una simple huella que no aporta ninguna información;

- El cifrado eventual del dato biométrico no puede leerlo nadie sin la clave.

En un modo de realización preferido, el procedimiento comprende una etapa previa (a0) "de registro" que permite integrar un individuo y su documento 1 de identidad, y generar los datos de los que debe disponer el servidor 2 y/o el equipo cliente 3. En este caso, hace falta distinguirlo de un registro de un factor de autenticación que puede ser el resultado del presente procedimiento.

Esta etapa (a0) puede llevarse a cabo mucho tiempo antes que el resto del procedimiento, y no necesita reiterarse en cada ocasión del procedimiento (debe observarse que puede preverse repetirla de vez en cuando por seguridad y para actualizar los datos personales, pero esto sigue siendo opcional). De este modo, puede considerarse que dichos datos mencionados anteriormente están predefinidos para la ejecución del procedimiento.

Este procedimiento de registro de datos del documento 1 de identidad del individuo puede realizarse 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 por una etapa (A) de obtención de una fotografía de dicho individuo visible en dicho documento 1 de identidad, de un dato de lectura óptica del documento 1 de identidad y, dado el caso, del dato biométrico de referencia de dicho individuo.

Esta etapa (A) puede, a su vez, llevarse a cabo por medio de una imagen del documento 1 de identidad (como se explicará para el procedimiento de autenticación), pero, de forma preferida, para evitar los problemas de digitalización y de pérdida de calidad, estos datos (es decir, la fotografía, el dato de lectura óptica y/o el dato biométrico de referencia) se manipulan directamente, en particular, si el registro es llevado a cabo por una autoridad gubernamental. Esto permite por otro lado una eventual actualización de los datos, véase más adelante.

En una etapa (B), como se explica, se pone en práctica la extracción mediante análisis de dicha fotografía de la información (designada DPS por comodidad, aunque, como se explica, el presente procedimiento no se limita al Digital Photo Seal) de referencia representativa del aspecto de dicha fotografía, por medio de un algoritmo conocido.

A continuación, en una etapa (C) se genera el primer dato de aleatoriedad RNGD, de forma que se calcula el primer dato codificado (designado SSKD por SSK-DATA por comodidad, aunque, como se explica, el presente documento no se limita al "secure sketch") mediante aplicación de un proceso de codificación a dicha información DPS de referencia representativa del aspecto de dicha fotografía y a dicho primer dato de aleatoriedad RNGD, es decir, SSKD = enc (DPS, RNGD).

El primer dato de aleatoriedad RNGD es, como su nombre indica, un dato de valor aleatorio que aporta aleatoriedad, que tiene importancia, ya que su conocimiento va a permitir demostrar que se dispone realmente del documento 1 de identidad.

Preferiblemente, el proceso de codificación es un proceso de boceto de un algoritmo de tipo "secure sketch". El experto en la técnica conoce este proceso de boceto. Se describe concretamente en el documento "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data", de Dodis *et al.* (véase la definición 3 facilitada en la página 11 de ese documento).

No obstante, la unidad 4 de procesamiento puede usar otros procesos de codificación en lugar de un proceso de boceto (por ejemplo, procesos de algoritmos de tipo "fuzzy extractor" y, de forma general, la lógica difusa).

Debe observarse que el proceso de codificación puede aplicarse directamente a dicha información de referencia representativa del aspecto de dicha fotografía, pero también de forma indirecta, es decir, a datos derivados de esta información de referencia para añadir entropía. Por ejemplo, puede utilizarse como dato derivado una combinación de la información de referencia con el dato de lectura óptica, concretamente un determinado número de los primeros bits de su huella criptográfica (véase más adelante). En particular, esta combinación puede ser un "o exclusivo", es decir, XOR(DPS;HMRZ), siendo HMRZ los n primeros bits de la huella criptográfica del dato de lectura óptica (en el ejemplo en donde es la MRZ) en donde n es el número de bits de la información de referencia (se necesita el mismo número de bits para XOR).

En cualquier caso, el proceso de codificación permite "enmascarar" el primer dato de aleatoriedad RNGD mediante el resultado del procesamiento DPS de la fotografía, pero de forma que puede volver a encontrarse por medio de un proceso de decodificación complementario del proceso de codificación.

Cuando el proceso de codificación utilizado para el registro es un proceso de boceto de un algoritmo de tipo "secure sketch", el proceso de decodificación es el proceso de recuperación ("recovery" en inglés) del mismo algoritmo de tipo "secure sketch". El experto en la técnica también conoce un proceso de recuperación de este tipo (véase la definición 3 facilitada en la página 11 del documento "Fuzzy Extractors: How to Generate..." anteriormente mencionado).

Más precisamente, si se indica DpsRef la información de referencia y DpsCand una información candidata [con SSKD = enc(RNGD, DpsRef)], entonces los procesos de codificación y de decodificación son tales que si DpsCand es lo suficientemente próxima a DpsRef (es decir, diferente en menos que un umbral, lo que normalmente es el caso si se extrae la información representativa de la misma fotografía que aquella a partir de la cual se ha generado la información de referencia, aun cuando se observe que sigue siendo imposible que los dos valores coincidan, siempre se tendrá |DpsCand - DpsRef| > 0), entonces el primer dato decodificado es igual al primer dato de aleatoriedad RNGD.

Por el contrario, si DpsCand no es lo suficientemente próxima a DpsRef, entonces el primer dato decodificado no es el valor correcto del primer dato de aleatoriedad.

Matemáticamente, el proceso de decodificación da, para un valor del primer dato codificado SSKD y para un valor de información candidata DpsCand, "el valor x = dec(SSKD, DpsCand) tal que existe un valor ε de norma inferior a un umbral dado que verifica SSKD = enc(x, DpsCand + ε)", siendo x igual al valor del primer dato de aleatoriedad RNGD si se tiene realmente DpdCand + ε = DpsRef.

Se recuerda que tales procesos de codificación y de decodificación los conoce el experto en la técnica y pueden ser objeto de numerosos modos de realización. Por otro lado, será posible aumentar la entropía del dato codificado, aplicando el proceso de codificación a más datos que solo la información representativa del aspecto de dicha fotografía y el primer dato de aleatoriedad.

Por último, en una etapa (D) se almacenan en los medios 22 de almacenamiento de datos del servidor 2 y/o los medios 32 de almacenamiento de datos del equipo cliente 3 (dado el caso tras transmisión):

- Dicho primer dato codificado SSKD;

- La huella criptográfica de una primera concatenación del dato de lectura óptica del documento 1 de identidad y del primer dato de aleatoriedad RNGD;

- El cifrado eventual con la huella criptográfica de una segunda concatenación del dato de lectura óptica del documento 1 de identidad y del primer dato de aleatoriedad RNGD, diferente de la primera concatenación, del al menos un dato biométrico de referencia de dicho individuo.

Estos datos, en el caso en donde se almacenan en el servidor 2, pueden indexarse en la memoria 22 con una huella criptográfica de un identificador del documento 1 de identidad, generalmente, obtenido a partir de la MRZ.

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

De forma preferida, las concatenaciones primera y segunda corresponden a concatenaciones en dos sentidos diferentes, por ejemplo, MRZ|RNGD para la primera concatenación y RNGD|MRZ para la segunda concatenación, pero podrá utilizarse cualquier otra construcción tal que dos concatenaciones en el mismo orden, pero que constan de un carácter predeterminado entre medias, por ejemplo, MRZ|1|RNGD y MRZ|2|RNGD.

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

Por comodidad, se denomina primera huella dicha huella criptográfica de la primera concatenación (h(MRZ|RNGD) en particular), y segunda huella la huella criptográfica de la segunda concatenación (h(RNGD|MRZ) en particular).

La astucia de estas múltiples concatenaciones permite la formación de varias huellas completamente independientes a partir de los mismos datos. En efecto, conociendo la primera huella (que está almacenada en la memoria 22, y que, por tanto, podría obtenerla un pirata), no es posible obtener la segunda huella. Para obtenerla sigue siendo necesario poseer

el valor del primer dato de aleatoriedad RNGD, que solo puede encontrarse disponiendo de la información de referencia. Por lo tanto, la huella biométrica de referencia cifrada con la segunda huella criptográfica (es decir, se utiliza la segunda huella como clave) sigue siendo accesible solo para el poseedor del documento 1 de identidad, de forma que el servidor 2 no puede manipular ni conocer los datos personales del usuario, que pueden almacenarse con total seguridad.

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

Debe observarse que el procedimiento de registro puede repetirse a intervalos regulares para verificar o actualizar los datos personales. Los datos recientes y fiables podrán recuperarse desde una entidad gubernamental. Por lo demás, un documento 1 de identidad tiene una vida útil limitada y debe renovarse regularmente.

Según un modo de realización preferido, el equipo cliente 3 o el servidor 2 dispone de forma ventajosa (en vez del cifrado del dato biométrico de referencia) de un segundo dato codificado (indicado SSKT, por SSK-TEMPLATE) obtenido mediante aplicación de un proceso de codificación (de forma típica, el mismo proceso de codificación que para el primer dato codificado) al dato biométrico de referencia y a un segundo dato de aleatoriedad (indicado RNGT); y el servidor 2 dispone, además, de una huella criptográfica construida a partir del segundo dato de aleatoriedad RNGT. De nuevo, todos estos datos pueden almacenarse (al menos inicialmente) en los medios 22 de almacenamiento de datos del servidor 2 (y asociarse a otros datos)

Dicha huella criptográfica construida a partir del segundo dato de aleatoriedad RNGT, denominada tercera huella criptográfica, puede ser una huella criptográfica directamente del segundo dato de aleatoriedad RNGT, o de cualquier función (por ejemplo, una concatenación) del segundo dato de aleatoriedad RNGT y de otro dato, de forma ventajosa, de la primera huella criptográfica (la huella criptográfica de una primera concatenación del dato de lectura óptica del documento 1 de identidad y del primer dato de aleatoriedad RNGD).

Se comprende que ninguno de estos datos puede explotarse de nuevo en sí mismo, ya que:

- Dicho segundo dato codificado SSKT no permite por sí solo ni recuperar el dato biométrico de referencia ni el segundo dato de aleatoriedad RNGT;

- La huella criptográfica construida a partir del segundo dato de aleatoriedad RNGT es una simple huella que no aporta ninguna información.

En un modo de realización de este tipo, la etapa (a0) de registro puede comprender, además:

- En la etapa (A) o en la etapa (B), obtener dicho dato biométrico de referencia (indicado TempRef por plantilla de referencia), por ejemplo, desde la fotografía del documento 1 de identidad;

- En la etapa (C), generar el segundo dato de aleatoriedad RNGT, de forma que se calcula el segundo dato codificado SSKT mediante aplicación de dicho proceso de codificación, es decir, SSKT = enc (TempRef, RNGT);

- En la etapa (D), almacenar en los medios 22 de almacenamiento de datos del servidor 2 y/o en los medios 32 de almacenamiento de datos del equipo cliente 3 (en su caso tras transmisión), dicho segundo dato codificado SSKT y la huella criptográfica construida a partir del segundo dato de aleatoriedad RNGT.

Debe observarse que estas acciones complementarias asociadas al registro biométrico, pueden llevarse a cabo en nuevas etapas (A') a (D'), es decir, no necesariamente de forma simultánea con las acciones asociadas al registro del documento 1 de identidad.

Por otro lado, sigue siendo posible llevar a cabo un procedimiento de autenticación fuerte del individuo sin necesitar ni cifrado del dato biométrico de referencia ni segundo dato de aleatoriedad RNGT y segundo dato codificado SSKT, concretamente almacenándolo directamente en el equipo cliente 3 (en claro), incluso en un servidor dedicado a la biometría de tipo WebBIO, véase más adelante.

Autenticación

Ahora se supone que se ha realizado satisfactoriamente el registro y que ahora puede utilizarse el documento de identidad.

En un modo de realización preferido, el procedimiento de autenticación comienza por una etapa (a) de adquisición de una forma u otra (por ejemplo, mediante los medios 30 de adquisición del equipo cliente 3) de una imagen del documento 1 de identidad, representando la imagen al menos la fotografía del individuo y el dato de lectura óptica del documento 1 de identidad (la MRZ) visibles en dicho documento 1 de identidad. Preferiblemente, dicha

imagen representa todo el documento 1 de identidad, al menos la totalidad de una cara. Como se explica, puede ser necesario adquirir varias imágenes, por ejemplo, para ver todas las caras.

De forma típica, es el individuo el que hace una foto de su documento 1 de identidad con su terminal móvil, dado el caso a petición emitida por el servidor que desea la autenticación fuerte (por ejemplo, para el servicio del que ha lanzado un proceso de recubrimiento, concretamente mediante una API dedicada).

En lo que se refiere al dato biométrico candidato, "reciente", este puede obtenerse durante la etapa previa (a). Más precisamente, una vez adquirida la imagen del documento 1 de identidad, el servidor 2 (o de nuevo el servidor de terceros) puede reclamar entonces la adquisición del dato biométrico candidato.

Es importante comprender que, si bien la etapa de registro (a0) puede llevarse a cabo semanas antes de la ejecución de la autenticación, la etapa (a) se pone en práctica, como mucho, unos minutos antes que el resto del procedimiento, para garantizar que el dato biométrico candidato es "reciente".

De este modo, la etapa (a) comprende, de forma ventajosa, la generación del dato biométrico candidato a partir de un rasgo biométrico proporcionado por los medios de adquisición biométrica del equipo cliente 3 (es decir, normalmente, los medios 30 de adquisición óptica). Esto significa, por ejemplo, que el individuo toma en primer lugar una fotografía de su documento 1 de identidad y después una fotografía de su cara.

Para garantizar que el dato candidato es reciente, la etapa (a) puede comprender el fechado del dato biométrico candidato por medio de un marcador temporal (denominado "timestamp" en inglés).

El experto en la técnica sabrá poner en práctica un fechado de este tipo usando técnicas conocidas y, de forma ventajosa, se usa como marcador temporal un nonce (es decir, un número arbitrario, es decir, una aleatoriedad, de uso único, del inglés "number used once").

El objetivo de la siguiente parte del procedimiento es verificar que la etapa (a) se ha desarrollado como se ha descrito anteriormente y que no se está en presencia de una falsificación (por ejemplo, una imagen que se haya modificado de forma fraudulenta) o de una usurpación (un individuo que no es el portador del documento 1 de identidad).

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

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

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 forma que se ha obtenido la información de referencia durante el registro. La identificación de la fotografía puede hacerse gracias a modelos y máscaras (en efecto, los documentos de identidad siempre tienen la misma organización) y, de este modo, el análisis de la imagen puede comprender el reconocimiento de un contorno del documento 1 de identidad, el reencuadre de ese contorno y la aplicación de las máscaras predeterminadas. Para ello, podrán utilizarse de forma astuta redes neuronales de convoluciones adaptadas. De forma similar, en lo que se refiere al dato de lectura óptica, existen algoritmos que permiten su extracción automática, tanto más en cuanto que las zonas de tipo MRZ están previstas muy especialmente para leerse fácilmente mediante un ordenador.

Una vez "aislada" la fotografía en la imagen, se aplican los mismos algoritmos que los que se han aplicado en la fotografía original para obtener la información candidata representativa del aspecto de la fotografía tal como se representa.

Se comprende que las informaciones de referencia y candidata deberán obtenerse de forma idéntica de modo que puedan compararse.

Según un primer modo de realización, la etapa (b) se pone en práctica por el servidor 2, según lo que se describe en la solicitud FR1904375. Se supone que este último almacena el primer dato codificado y la etapa (a) comprende para ello la transmisión al servidor 2 de dicha imagen adquirida del documento 1 de identidad. Según un segundo modo de realización, la etapa (b) es llevada a cabo directamente por el equipo cliente 3 según lo que se describe en la solicitud FR1904406. Preferiblemente, en este segundo modo de realización, la etapa (b) comprende la interrogación del servidor 2, de forma que se recupera al menos dicho primer dato codificado SSKD si está almacenado en este servidor 2, por ejemplo, proporcionándole la huella criptográfica del identificador del documento 1 (pudiendo obtenerse este identificador de la MRZ, por ejemplo): el servidor 2 transmite el primer dato codificado asociado a la huella recibida. Se observa que, de forma alternativa, dicho primer dato codificado puede haberse proporcionado hace mucho tiempo y almacenado desde entonces en los medios 32 de almacenamiento de datos del equipo cliente 3.

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

Como se explica, el proceso de decodificación (y el proceso de codificación) es tal que dicho primer dato decodificado corresponde al primer dato de aleatoriedad RNGD si dicha información candidata representativa del aspecto de dicha fotografía coincide con la información de referencia representativa del aspecto de dicha fotografía. Dicho de otro modo, si la información de referencia y la información candidata son suficientemente próximas, el valor decodificado corresponderá al valor de aleatoriedad RNGD utilizado para obtener este primer dato codificado SSKD.

De forma general, el resultado de una comparación de la información candidata y de 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, datos de seguridad de tipo Digital Photo Seal coinciden si difieren en menos del 10 %.

De este modo, se comprende que el valor del primer dato de aleatoriedad "enmascarado" mediante el DPS puede recuperarse si el usuario dispone de una fotografía idéntica a la usada durante el registro de la que se obtiene la información de referencia.

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

Dicho de otro modo, el servidor 2 o el equipo cliente 3 intenta reconstituir la primera huella efectuando 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 el registro; y
- el primer dato decodificado coincide con el primer dato de aleatoriedad RNGD;

Entonces la primera concatenación dará exactamente el mismo resultado y se obtendrá de nuevo la primera huella.

En todos los demás casos, la entropía de las funciones de resumen criptográfico hace que se obtenga un resultado muy diferente. Si el documento 1 se ha alterado (por ejemplo, sustituyendo la fotografía), entonces las informaciones candidata y de referencia correspondientes no coincidirán, por tanto, se obtendrá un valor falso de la aleatoriedad y, por tanto, de la primera huella, y se rechazará la autenticación.

Debe observarse que, si es el equipo cliente 3 el que ha llevado a cabo hasta ahora las etapas descritas, es necesario informar al servidor 2 del resultado de la verificación.

No obstante, el valor correcto de la primera huella puede conocerse, aunque solo sea de una autenticación anterior del individuo. Por ello, el equipo cliente 3 va a demostrar de forma ventajosa que ha obtenido esta primera huella de forma correcta, es decir, a partir del documento 1 de identidad, y esto de forma no interactiva, es decir solo con una "ida" de información del equipo cliente 3 hacia el servidor 2, y sin "retorno". Y, sobre todo, como se explica, el servidor 2 no va a recibir ni el primer dato de aleatoriedad RNGD, ni la información candidata representativa del aspecto de dicha fotografía, ni el dato de lectura óptica (ni ningún dato que permita llegar hasta estos últimos), aunque sea, no obstante, posible para el servidor 2 saber con certeza que la primera huella se ha calculado correctamente. Por lo demás, ninguno de los datos transmitidos es sensible y podrían interceptarse sin que eso suponga ningún problema.

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

Más precisamente, dicha prueba de divulgación nula de conocimientos garantiza la siguiente afirmación: "dada una huella criptográfica H, existe un dato de lectura óptica y un primer dato de aleatoriedad RNGD (el dato decodificado) tales que su primera concatenación tiene como huella esta huella criptográfica H dada". El experto en la técnica podrá consultar el documento FR1904406 para obtener más información.

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

Si la prueba no es válida, es que la primera huella criptográfica no se ha obtenido de forma válida y, por tanto, que posiblemente el individuo no dispone del documento de identidad e intenta usurpar una identidad. Si la prueba es válida, pero la huella criptográfica recibida no corresponde a aquella de la que dispone la entidad 2 de verificación, es que el primer dato decodificado no corresponde a la primera aleatoriedad o que el dato de lectura extraído no es el original, es decir, que se ha falsificado el documento 1 de identidad (a nivel de la fotografía o del dato de lectura óptica). Puede emitirse una alerta por uso fraudulento.

En la etapa (d) los medios 21, 31 de procesamiento de datos verifican además que el dato biométrico de referencia y el dato biométrico candidato del individuo coinciden, implicando por tanto el procedimiento una comparación entre el dato biométrico candidato y el dato biométrico de referencia. Debe observarse que puede estar implicado un control en vivo, de forma que se verifica, por ejemplo, que el dato biométrico de referencia no procede de una falsificación (por ejemplo, una máscara de la cara o un dedo en resina).

Esta etapa puede llevarse a cabo de numerosas formas conocidas, usando el equipo cliente 3, el servidor 2 incluso un servidor de biometría dedicado.

Se observa que todas las combinaciones son posibles: cada uno del equipo cliente 3 y del servidor 2 puede poner en práctica 0, 1 o 2 de las verificaciones de la etapa (d).

Por ejemplo, es perfectamente posible que el servidor 2 reciba en la etapa (a) a la vez la imagen adquirida del documento 1 de identidad y el dato biométrico candidato. De forma especialmente preferida, puede incluso imaginarse que durante la etapa (a), el servidor 2 reciba en primer lugar la imagen adquirida del documento 1 de identidad, después requiere del equipo 1 el dato biométrico candidato que entonces se le transmite en un segundo momento.

De forma alternativa o complementaria, el servidor 2 o el equipo 3 puede transmitir (dado el caso, volver a transmitir) el dato biométrico candidato a un servidor de confianza dedicado a la biometría, que almacena el dato biométrico de referencia, que realiza la comparación y envía el resultado al servidor.

En todos los casos, la ejecución de la comparación comprende normalmente el cálculo de una distancia 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, de forma ventajosa, el cálculo de un producto escalar.

Por ejemplo, en caso de que los datos biométricos se han obtenido a partir de imágenes de iris, una distancia habitualmente usada para comparar dos datos es la distancia de Hamming. En el caso en donde los datos biométricos se hayan obtenido a partir de imágenes de la cara del individuo, resulta habitual usar la distancia euclidiana. Este tipo de cálculo de distancia lo conoce el experto en la técnica y no se describirá más en detalle.

En caso de que el servidor 2 o el equipo cliente 3 almacena un cifrado del dato biométrico de referencia de dicho individuo con una huella criptográfica de una segunda concatenación del dato de lectura óptica del documento 1 de identidad y del dato de aleatoriedad (la segunda huella criptográfica), la etapa (d) comprende el descifrado de este dato biométrico de referencia, por medio de la huella criptográfica de una segunda concatenación del dato de lectura óptica extraído y del dato decodificado (cada uno obtenido en la etapa (c)), con vistas a poder realizar la comparación. De nuevo, el experto en la técnica podrá consultar la solicitud FR1904375.

En el caso de que se tenga un segundo dato codificado SSKT obtenido mediante aplicación de un proceso de codificación a un dato biométrico de referencia y a un segundo dato de aleatoriedad RNGT, y una huella criptográfica construida a partir del segundo dato de aleatoriedad RNGT, puede utilizarse un proceso de decodificación para verificar si el dato biométrico candidato y el dato biométrico de referencia coinciden, de la misma forma en que se ha hecho para la información de tipo DPS en la fotografía.

De nuevo, cuando el proceso de codificación utilizado para el registro es un proceso de boceto de un algoritmo de tipo “secure sketch”, el proceso de decodificación es el proceso de recuperación (“recovery” en inglés) del mismo algoritmo de tipo “secure sketch” y el experto en la técnica podrá usar otros procesos.

Matemáticamente, el proceso de decodificación da, para un valor del segundo dato codificado SSKT y para un dato biométrico candidato TempCand, “el valor x = dec (SSKT, TempCand) tal que existe un valor ε de norma inferior a un umbral dado que verifica SSKT = enc (x, TempCand + ε)”, siendo x igual al valor del primer dato de aleatoriedad RNGT si se tiene realmente TempCand + ε = TempRef. Por lo tanto, la etapa (c) comprende, además, de forma ventajosa, el cálculo mediante los medios 21, 31 de procesamiento de datos del servidor 2 o del equipo cliente 3 de

• un segundo dato decodificado mediante aplicación de un proceso de decodificación a dicho dato biométrico candidato y al segundo dato codificado (de nuevo, el dato codificado es tal que dicho segundo dato decodificado corresponde al segundo dato de aleatoriedad RNGT, si dicho dato biométrico candidato coincide con el dato biométrico de referencia);

• una huella criptográfica construida a partir del segundo dato decodificado (se comprenderá que esta huella criptográfica debe construirse de la misma forma que la tercera huella criptográfica a partir del segundo dato de aleatoriedad RNGT, concretamente, la huella criptográfica de una concatenación del segundo dato de aleatoriedad RNGT y de la primera huella criptográfica).

En todos los casos, la comparación de los datos biométricos puede hacerse mediante los medios 21 de procesamiento de datos del servidor 2, pero es preferible que se haga en el equipo cliente 3 para garantizar totalmente la privacidad del individuo.

Para ello, puede utilizarse de nuevo un protocolo criptográfico que genera una "prueba" de que el dato biométrico candidato y el dato biométrico de referencia coinciden, no revelando esta prueba nada más, aparte del hecho de que estos datos biométricos pertenecen realmente al productor de la prueba.

Dicho de otro modo, pueden utilizarse hasta dos pruebas de divulgación nula de conocimiento:

- la primera prueba es la prueba del cálculo de dicha huella criptográfica a partir de la primera concatenación del dato de lectura óptica extraído y del primer dato decodificado;

- la segunda prueba es una prueba del hecho de que el dato biométrico candidato y el dato biométrico de referencia coinciden.

En este caso, la etapa (d) comprende de forma ventajosa la generación mediante los medios 31 de procesamiento de datos del equipo cliente 3 de la prueba de divulgación nula de conocimientos, por el hecho de que el dato biométrico candidato y el dato biométrico de referencia coinciden, que es, en particular, una prueba del cálculo de dicha huella criptográfica a partir del segundo dato decodificado, no revelando esta prueba nada más, a parte del hecho de que el segundo dato decodificado (es decir, el segundo dato de aleatoriedad RNGT) pertenece realmente al productor de la prueba. De nuevo, la prueba tiene como objetivo garantizar que la tercera huella criptográfica se ha calculado efectivamente y de forma correcta.

Más precisamente, dicha prueba de divulgación nula de conocimientos garantiza la siguiente afirmación: "dada una huella criptográfica T, existe un segundo dato de aleatoriedad RNGT (y, dado el caso, un dato de lectura óptica) tal que una función dada de este segundo dato de aleatoriedad RNGT tiene como huella esta huella criptográfica T dada". En el caso preciso en el que la tercera huella es la huella criptográfica de una concatenación del segundo dato de aleatoriedad RNGT y de la primera huella criptográfica, la afirmación garantizada es la siguiente: "dada una huella criptográfica T, existe un segundo dato de aleatoriedad RNGT y otra huella criptográfica H tal que una concatenación de este segundo dato de aleatoriedad RNGT y de esta otra huella criptográfica H tiene como huella dicha huella criptográfica T dada".

La segunda prueba de divulgación nula de conocimiento puede generarse de la misma forma que la primera prueba de divulgación nula de conocimiento, y transmitirse al servidor 2 con la nueva huella criptográfica calculada (la tercera huella), véase una vez más el documento FR1904406.

Si todas las verificaciones se han efectuado de forma satisfactoria, el servidor 2 acepta la autenticación del individuo y transmite normalmente un "testigo" al servidor que ha requerido la autenticación/el recubrimiento del individuo. Más precisamente, si el procedimiento es un procedimiento de registro de un autenticador, en particular de FIDO, entonces se realiza este registro. Dicho de otro modo, el procedimiento comprende de forma ventajosa una etapa de registro de un autenticador. Si este autenticador que va a registrarse es directamente el equipo 3, puede presentar un secreto o bien presentar la clave pública correspondiente a un par de clave del que dispone de la clave privada que le permite usarla como autenticador del individuo. De forma alternativa, podría recibir un secreto de este tipo.

Se observará que, en vez de ejecutar simultáneamente la verificación del documento 1 y la verificación biométrica [es decir, utilizar las mismas etapas (a) a (d)], es perfectamente posible llevar a cabo los procedimientos uno tras otro, es decir, que habrá etapas (a') a (d') para el procedimiento llevado a cabo en segundo lugar (en particular, la verificación biométrica, aun cuando se posible un orden inverso).

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

Servidor

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

Como se ha explicado, el equipo cliente 3 y/o el servidor 2 comprenden medios 21, 31 de procesamiento de datos (según el caso en el que hay directamente procesamiento de los datos por el servidor 2, o si es el equipo 3 el que hace 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 1 de identidad que representa al menos una fotografía de un individuo y un dato de lectura óptica visibles en dicho documento 1 de identidad:
  - una información candidata representativa del aspecto 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 aplicación de un proceso de decodificación a dicha información candidata representativa del aspecto de dicha fotografía y al primer dato codificado, tal que dicho primer dato decodificado corresponde a un primer dato de aleatoriedad si dicha información candidata representativa del aspecto de dicha fotografía coincide con una información de referencia representativa del aspecto de dicha fotografía, disponiendo el servidor 2 de una huella criptográfica de una primera concatenación de dicho dato de lectura óptica de dicho documento 1 de identidad y dicho primer dato de aleatoriedad, denominado primera huella criptográfica;
- verificar que:

- una huella criptográfica de una primera concatenación del dato de lectura óptica extraído y del dato decodificado coincide con dicha primera huella criptográfica de que dispone el servidor 2; y

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

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

Producto de programa de ordenador

Según un tercer y cuarto aspectos, la invención se refiere a un producto de programa de ordenador que comprende instrucciones de código para la ejecución (en particular, en los medios 21 de procesamiento de datos del servidor 2 y los medios 31 de procesamiento de datos del equipo cliente 3) de un procedimiento según 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 de ordenador.

REIVINDICACIONES

1. Procedimiento de autenticación fuerte de un individuo llevado a cabo por un servidor (2) y un equipo cliente (3) conectados;

disponiendo el equipo cliente (3) de un dato biométrico candidato del individuo y de una imagen adquirida de un documento (1) de identidad que representa al menos una fotografía de dicho individuo y un dato de lectura óptica visibles en dicho documento (1) de identidad, y disponiendo el servidor (2) de una huella criptográfica de una primera concatenación de dicho dato de lectura óptica de dicho documento (1) de identidad y de un primer dato de aleatoriedad, denominado primera huella criptográfica;
estando el procedimiento **caracterizado por que** comprende la ejecución, mediante medios (21, 31) de procesamiento de datos del servidor (2) y/o del equipo cliente (3), de etapas de;
(b) Extraer, mediante análisis de dicha imagen adquirida de dicho documento (1) de identidad:

- una información candidata representativa del aspecto 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) Calcular un primer dato decodificado mediante aplicación de un proceso de decodificación a dicha información candidata representativa del aspecto de dicha fotografía y a un primer dato codificado, de modo que dicho primer dato decodificado corresponde al primer dato de aleatoriedad si dicha información candidata representativa del aspecto de dicha fotografía coincide con una información de referencia representativa del aspecto de dicha fotografía;
(d) Verificar que:

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

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

3. Procedimiento según la reivindicación 2, en donde los medios de adquisición biométrica son los medios (30) de adquisición óptica del equipo cliente (3), siendo el equipo cliente (3) un equipo electrónico personal de dicho individuo, en particular, de tipo terminal móvil o tarjeta inteligente

4. Procedimiento según una de las reivindicaciones 1 a 3, en donde el servidor (2) o el equipo (3) dispone de un cifrado del dato de referencia biométrico de dicho individuo con una huella criptográfica de una segunda concatenación del dato de lectura óptica del documento (1) de identidad y del primer dato de aleatoriedad, diferente de la primera concatenación; comprendiendo la etapa (c) el descifrado del al menos un dato biométrico de referencia de dicho individuo cifrado, por medio de la huella criptográfica de una segunda concatenación del dato de lectura óptica extraído y del primer dato decodificado.

5. Procedimiento según una de las reivindicaciones 1 a 3, en donde el servidor (2) dispone de una huella criptográfica construida a partir de un segundo dato de aleatoriedad, denominada tercera huella criptográfica; comprendiendo la etapa (c) el cálculo mediante los medios (21, 31) de procesamiento de datos del servidor (2) o del equipo cliente (3) de un segundo dato decodificado mediante aplicación de un proceso de decodificación a dicho dato biométrico candidato y a un segundo dato codificado, de modo que dicho segundo dato decodificado corresponde al segundo dato de aleatoriedad si dicho dato biométrico candidato coincide con el dato biométrico de referencia; comprendiendo dicha verificación de la etapa (d) de que el dato biométrico de referencia y el dato biométrico candidato del individuo coinciden, comprendiendo la verificación de que una huella criptográfica construida a partir del segundo dato decodificado de la misma forma que se construye la tercera huella criptográfica a partir del segundo dato de aleatoriedad coincide con dicha tercera huella criptográfica de la que dispone el servidor (2).

6. Procedimiento según una de las reivindicaciones 1 a 5, en donde la etapa (a) comprende la recepción por el servidor (2) de la imagen obtenida de dicho documento (1) de identidad y del dato biométrico candidato desde el equipo cliente (3), ejecutándose las etapas (b) a (d) mediante los medios (21) de procesamiento de datos del servidor (2).

7. Procedimiento según una de las reivindicaciones 1 a 5, en donde las etapas (b) y (c) se llevan a cabo mediante los medios (31) de procesamiento de datos del equipo cliente (3), comprendiendo la etapa (c) el cálculo de la huella 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 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 criptográfica de una primera concatenación del dato de lectura óptica extraído y del dato decodificado coincide con la primera huella criptográfica, comprende la verificación de que:

- la prueba de divulgación nula de conocimiento del cálculo de dicha huella criptográfica a partir de la primera concatenación del dato de lectura óptica extraído y del primer dato decodificado es válida, y
- la huella criptográfica recibida coincide con dicha primera huella criptográfica de la que dispone el servidor (2).

8. Procedimiento según una de las reivindicaciones 1 a 7, en donde las etapas (b) y (c) se llevan a cabo mediante los medios (31) de procesamiento de datos del equipo cliente (3), comprendiendo la etapa (c) 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 biométrico candidato del individuo coinciden comprende la verificación mediante los medios (21) de procesamiento de datos del servidor (2) de que la prueba de divulgación nula de conocimiento del hecho de que el dato biométrico de referencia y el dato biométrico candidato del individuo coinciden, es válida.

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

(A) Obtener la fotografía de dicho individuo visible en dicho documento (1) de identidad y el dato de lectura óptica del documento (1) de identidad;
(B) Extraer, mediante análisis de dicha fotografía, información de referencia representativa del aspecto de dicha fotografía;
(C) Generar el primer dato de aleatoriedad; calcular el primer dato codificado, mediante aplicación de un proceso de codificación a dicha información de referencia representativa del aspecto de dicha fotografía y a dicho primer dato de aleatoriedad, y la primera huella criptográfica.

10. Procedimiento según las reivindicaciones 5 y 9 en combinación, en donde, durante la etapa (a0), la subetapa (A) o la subetapa (B) comprenden la obtención de dicho dato biométrico de referencia; y la subetapa (C) comprende, además, la generación del segundo dato de aleatoriedad y el cálculo del segundo dato codificado mediante aplicación de dicho proceso de codificación a dicho dato biométrico de referencia y a dicho segundo dato de aleatoriedad, y de la tercera huella criptográfica.

11. Procedimiento según una de las reivindicaciones 1 a 10, que comprende una etapa (e) de registro de un autenticador, en particular de la alianza "Fast IDentity Online", FIDO

12. Procedimiento según una de las reivindicaciones 1 a 11, en donde la información de referencia representativa de un aspecto esperado de dicha fotografía es un dato de seguridad de tipo "Digital Photo Seal".

13. 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 (21, 31) de procesamiento de datos configurados para:

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

  ○ una información candidata representativa del aspecto 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 aplicación de un proceso de decodificación a dicha información candidata representativa del aspecto de dicha fotografía y al primer dato codificado, tal que dicho primer dato decodificado corresponde a un primer dato de aleatoriedad si dicha información candidata representativa del aspecto de dicha fotografía coincide con una información de referencia representativa del aspecto de dicha fotografía, disponiendo el servidor (2) de una huella criptográfica de una primera concatenación de dicho dato de lectura óptica de

dicho documento (1) de identidad y dicho primer dato de aleatoriedad, denominado primera huella criptográfica;
• verificar que:

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

14. Producto de programa de ordenador, que comprende instrucciones de código para la ejecución de un procedimiento según una de las reivindicaciones 1 a 12, de autenticación fuerte de un individuo, cuando se ejecuta dicho procedimiento en un ordenador.

15. Medio de almacenamiento legible por un equipo informático, en el que un producto de programa de ordenador comprende instrucciones de código para la ejecución de un procedimiento según una de las reivindicaciones 1 a 12, de autenticación fuerte de un individuo.

Fig. 1