(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 896 724**

(51) Int. CI.:

G06F 21/32 (2013.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **24.04.2020 E 20171282 (5)**

(97) Fecha y número de publicación de la concesión europea: **11.08.2021 EP 3731116**

(54) Título: **procedimiento de autenticación de un documento de identidad de un individuo y eventualmente de autenticación de dicho individuo**

(30) Prioridad:

25.04.2019 FR 1904406

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.02.2022

(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 de un documento de identidad de un individuo y eventualmente de autenticación de dicho individuo

Campo de la invención

La invención se refiere a procedimientos de autenticación de un documento de identidad de un individuo y de autenticación de este individuo.

Estado de la técnica

La posesión de un documento de identidad (tarjeta de identidad, pasaporte, permiso de conducir, tarjeta de seguridad social, etc.) válido justifica la identidad de un individuo.

Los documentos de identidad consisten en un soporte, generalmente, de papel o de plástico en el que están impresas una fotografía, así como información alfanumérica personal (apellido, nombre, fecha de nacimiento, etc.) de su poseedor. También se encuentra una banda denominada MRZ (“Machine-Readable Zone”, zona de lectura óptica), que contiene un código (generalmente, dos líneas de 36 caracteres) que resume la información alfanumérica del documento. Alternativamente a la MRZ, puede encontrarse un código de barras de tipo PDF-417 que contiene la misma información.

Generalmente, los documentos de identidad presentan un gran número de elementos de seguridad de alto nivel, tales como filigranas u hologramas, para prevenir la falsificación. La vida útil de un documento de este tipo es, generalmente, limitada (10 o 15 años), ya que el aspecto de su titular cambia progresivamente, y los elementos de seguridad evolucionan.

Durante un control de un individuo por una entidad, por ejemplo, a la entrada de un edificio, se le pide que presente su documento de identidad para la autenticación. Es deseable que este proceso sea lo más rápido posible, al tiempo que siga siendo lo más seguro posible. En efecto, el riesgo es, por ejemplo, que individuos buscados presenten un documento de identidad falsificado en el que se ha modificado información, por ejemplo, la fotografía.

Se conocen, a partir de las solicitudes FR3047688 y FR1759292, procedimientos de registro de datos destinados a usarse para controlar automáticamente la identidad de un individuo, y procedimientos asociados de control de identidad, basados en un mecanismo muy astuto de generación, a partir de un elemento visual de un documento de identidad (en particular, la foto), de un dato de seguridad denominado “Digital Photo Seal”. Este dato de seguridad constituye una especie de firma del elemento visual: imágenes adquiridas de un mismo elemento visual, independientemente de las condiciones de adquisición (es decir, incluyendo tras escaneo o fotocopia), conducen a la obtención de datos de seguridad sustancialmente idénticos. Por el contrario, la menor modificación del elemento visual conlleva una fuerte variación de este elemento de seguridad.

De este modo, basta con almacenar en una base de datos de un servidor el dato de seguridad de referencia “esperado” para un documento dado, y compararlo con el “candidato” generado a partir de una copia de este documento, para saber si el elemento visual de este documento está integrado o no.

En particular, para garantizar la seguridad del dato de referencia en el servidor, este se “enmascara” mediante aplicación de un proceso de codificación (normalmente, un proceso de boceto de tipo “secure sketch”) al dato de referencia y a un dato de aleatoriedad, y el dato de referencia enmascarado se almacena en la base de datos con una huella criptográfica, es decir, un resumen criptográfico, de una concatenación de la MRZ con dicho dato de aleatoriedad.

Entonces, puede autenticarse un documento de identidad presentado por un individuo basándose en su MRZ y en la fotografía: se obtiene un dato de seguridad candidato a partir de la fotografía del documento presentado y después es posible, mediante aplicación de un proceso de decodificación, recuperar el dato de aleatoriedad si la fotografía del documento presentado es idéntica a aquella en base a la cual se ha generado el dato de seguridad de referencia, y verificar que el resumen criptográfico de una concatenación de la MRZ, con dicho dato de aleatoriedad, corresponde al almacenado.

Esta solución aporta una total satisfacción. E incluso se ha propuesto recientemente, en la solicitud FR1904375, almacenar también en el servidor datos alfanuméricos, en particular, los datos denominados “visuales”, es decir, los datos impresos en el documento de identidad, tales como datos de estado civil (apellido, nombre, dirección, fecha de nacimiento, etc.) o datos técnicos, tales como la fecha de caducidad del documento de identidad, cifrados para garantizar la privacidad del individuo. Esto permite evitar volver a introducirlos manualmente si es necesario.

No obstante, se observa que, aunque los datos del individuo almacenados siguen estando cifrados y, por tanto, no son accesibles en sí mismos, sigue siendo necesario enviar una imagen del documento de identidad que comprende

de una determinada manera todos estos datos personales, mientras que el servicio sólo requiere, posiblemente, un subconjunto de los mismos. Además, un pirata podría intentar interceptar los datos que se le envían y acceder a la fotografía del individuo o a la información personal visible en la imagen del documento de identidad.

De este modo, sería deseable disponer de una solución sencilla, fiable, segura y totalmente respetuosa de la privacidad, de autenticación de un documento de identidad.

También sería deseable poder autenticar al individuo portador del documento de identidad.

Los documentos de la técnica anterior, WO2012156648-A1, EP3386143-A1 y XP19135848, divulgan procedimientos de registro de datos biométricos.

Presentación de la invención

Según un primer aspecto, la invención se refiere a un procedimiento de autenticación de un documento de identidad puesto en práctica por un servidor y un equipo cliente conectados;

disponiendo el equipo cliente de un primer dato codificado y de una imagen adquirida 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, 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, denominada primera huella criptográfica;

estando el procedimiento caracterizado porque comprende la puesta en práctica de etapas de;

(b) Extraer, por los medios de procesamiento de datos del equipo cliente, 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 por los medios de procesamiento de datos del equipo cliente:

- 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 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;

- una huella criptográfica de una primera concatenación del dato de lectura óptica extraído y del primer dato decodificado;

(d) generar, por los medios de procesamiento de datos del equipo cliente, 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;

(e) transmitir al servidor dicha prueba de divulgación nula de conocimiento y la huella criptográfica calculada;

(f) verificar por medios de procesamiento de datos del servidor que:

- la prueba de divulgación nula de conocimiento es válida, y

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

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 por medios de adquisición óptica del equipo cliente;

el equipo cliente no dispone inicialmente ni del primer dato codificado ni de la imagen adquirida de dicho documento de identidad, comprendiendo la etapa (b) la recepción por el equipo cliente del primer dato codificado desde el servidor;

dicha 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 una prueba de divulgación nula de conocimientos del hecho de que, dada una huella criptográfica, existe un dato de lectura óptica y un primer dato de aleatoriedad tales que su primera concatenación tiene como huella, dicha huella criptográfica dada;

el procedimiento 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;

la etapa (a0) comprende, además, una subetapa (D) de almacenar en medios de almacenamiento de datos del servidor, el primer dato codificado y la primera huella criptográfica;

el procedimiento es, además, un procedimiento de autenticación del individuo, en el que la etapa (d) comprende la generación por los medios de procesamiento de datos del equipo cliente, de una prueba de divulgación nula de conocimientos del hecho de que un dato biométrico de referencia y un dato biométrico candidato del individuo coinciden; la etapa (e) que comprende la transmisión al servidor, de dicha prueba de divulgación nula de conocimiento del hecho de que el dato biométrico de referencia y el dato biométrico candidato del individuo coinciden; y la etapa (f) que comprende la verificación por 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 equipo cliente dispone, además, de un segundo dato codificado y del dato biométrico candidato del individuo, y el servidor dispone de una huella criptográfica construida a partir de un segundo dato de aleatoriedad, denominada tercera huella criptográfica; la etapa (c) que comprende el cálculo por los medios de procesamiento de datos del equipo cliente de:

- un segundo dato decodificado mediante aplicación de un proceso de decodificación a dicho dato biométrico candidato y al primer dato codificado, tal que dicho segundo dato decodificado corresponde al segundo dato de aleatoriedad si dicho dato biométrico candidato coincide con el dato biométrico de referencia;

- una huella criptográfica construida a partir del segundo dato decodificado de la misma manera que se construye la tercera huella criptográfica a partir del segundo dato de aleatoriedad;

siendo dicha prueba de divulgación nula de conocimientos del hecho de que el dato biométrico de referencia y el dato biométrico candidato del individuo coinciden, 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; comprendiendo la etapa (e), además, la transmisión al servidor de la huella criptográfica calculada; y comprendiendo la etapa (f), además, la verificación mediante medios de procesamiento de datos del servidor, de que la huella criptográfica recibida coincide con dicha tercera huella criptográfica de la que dispone el servidor;

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;

la tercera huella criptográfica es la huella criptográfica de una concatenación del segundo dato de aleatoriedad y de la primera huella criptográfica;

la etapa (a) comprende, además, 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, siendo el equipo cliente un equipo electrónico personal de dicho individuo, en particular, de tipo terminal móvil o tarjeta inteligente;

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;

la etapa (f) también comprende la transmisión al servidor de un dato personal diana del individuo, la 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, también una prueba del hecho de que el al menos un dato personal diana que va a transmitirse, se selecciona de entre datos personales asociados al documento de identidad;

el equipo cliente dispone, además, de un cifrado con la 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, de al menos un dato personal de dicho individuo, denominada segunda concatenación; comprendiendo el procedimiento el descifrado del cifrado del al menos un dato personal de dicho individuo, por medio de la huella criptográfica de la segunda concatenación del dato de lectura óptica extraído y del dato decodificado;

dicho dato personal diana o bien se extrae del dato de lectura óptica o bien del al menos un dato personal cifrado;

dicho dato personal de dicho individuo es un dato alfanumérico asociado a dicho individuo, estando dicha fotografía del individuo, dicho dato de lectura óptica y dicho al menos un dato alfanumérico, impresos en el documento de identidad;

la información de referencia representativa de un aspecto esperado de dicha fotografía, es un dato de seguridad de tipo “Digital Photo Seal”;

la o las prueba(s) de divulgación nula de conocimientos es(son) un objeto criptográfico de tipo zkSNARK.

Según un segundo aspecto, la invención se refiere a un conjunto de autenticación que comprende un servidor y un equipo cliente conectados, caracterizado por que

- El equipo cliente comprende 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, denominada primera huella criptográfica;

○ una huella criptográfica de una primera concatenación del dato de lectura óptica extraído y del primer dato decodificado;

• generar 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;

• transmitir al servidor dicha prueba de divulgación nula de conocimiento y la huella criptográfica calculada;

- comprendiendo el servidor, medios de procesamiento de datos configurados para verificar que:

○ la prueba de divulgación nula de conocimiento es válida, y

○ la huella criptográfica recibida coincide con dicha primera huella criptográfica de la que dispone el servidor.

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 de un documento de identidad; y 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 de un documento de identidad.

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 puesta en práctica de los procedimientos según la invención.

Descripción detallada

Arquitectura

La presente invención se refiere a un procedimiento de autenticación de un documento 1 de identidad de un individuo, que consta posiblemente de un procedimiento de registro de información de este documento 1 de identidad. Según un modo de realización preferido, que se describirá a continuación, el presente procedimiento es, además, un procedimiento de autenticación de dicho individuo, es decir, permite verificar, si se ha autenticado de manera válida el documento 1 que, además, su portador es realmente el individuo cuya identidad se presenta por el documento 1. 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.

La autenticación del documento 1 permite detectar el primer nivel de fraude y la autenticación del individuo permite detectar el segundo nivel de fraude.

Haciendo referencia a la **Figura 1**, se ha representado, esquemáticamente, una arquitectura de sistema de autenticación para la puesta en práctica de los presentes procedimientos. 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 un título oficial, ventajosamente 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. 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, ventajosamente, interfaces de comunicaciones que les permiten dialogar en remoto. De manera 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).

De manera preferida, en el caso de una autenticación del individuo, 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 manera particularmente 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 "selfie" (se indica que, alternativamente, pueden usarse medios de adquisición distintos, como un sensor de huella digital).

En cualquier caso, un dato biométrico de referencia usado para la eventual autenticación del individuo es, ventajosamente, 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 puesta en práctica de la invención, es suficiente con que el equipo cliente 3 pueda obtener una imagen adquirida del documento 1 de identidad de una manera u otra, incluyendo de manera 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 manera de obtener esta imagen y ninguna naturaleza en particular (la imagen adquirida puede estar en blanco y negro, deformada, etc.).

Como se verá, según un esquema conocido, pero poco habitual en la autenticación de documento de identidad, el equipo cliente 3 es una entidad, denominada de prueba, que pone en práctica la autenticación del documento 1 de identidad (incluso del individuo) y proporciona el resultado al servidor 2 que verifica este resultado, denominado entidad de verificación.

Se observa que es totalmente posible que otras entidades estén conectadas al servidor 2 y al equipo 3, en particular, servidores que ponen en práctica servicios que llevan a cabo las afirmaciones producidas por el equipo 3, es decir, de servicios que desean la autenticación del documento 1, por ejemplo, un servidor de un banco, de un hotel, etc.

Digital Photo Seal

De manera conocida, los presentes procedimientos usan una 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, tal 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 manera 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 sólo 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 manera fraudulenta. Esta verificación puede hacerse para cada uno de los otros elementos gráficos, tal como una firma.

Podrá usarse 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). Alternativamente, puede usarse 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

El presente procedimiento tiene como objetivo que el servidor 2 (la entidad de verificación) sólo tenga necesidad de que se le presente una prueba de la autenticación del documento 1 de identidad (y, eventualmente, una prueba de la autenticación del individuo), pero ningún dato explotable y, sobre todo, ningún dato personal.

De este modo, el predicado de base es que, al iniciarse el procedimiento, la entidad de prueba (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), sin que ninguno de estos datos deba transferirse al servidor 2.

El equipo cliente 3 tiene, además, necesidad de 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 se almacena, generalmente, por el servidor 2.

Por su parte, el servidor 2 sólo 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 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, de al menos un dato personal de dicho individuo (de nuevo, el cifrado se almacena a menudo por el servidor 2).

Se comprende que ninguno de estos datos es explotable 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 sólo 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 de los datos personales 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/el equipo cliente 3.

Esta etapa puede ponerse en práctica 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 es opcional). De este modo, puede considerarse que dichos datos mencionados anteriormente están predefinidos para la puesta en práctica 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, de al menos un dato personal de dicho individuo, en particular, un dato alfanumérico asociado a dicho individuo, aunque también sea posible tomar cualquier otro dato con respecto a la persona, tal como una plantilla biométrica o una prueba de identificación, véase más adelante. De manera preferida, dicho dato personal es un dato alfanumérico asociado más precisamente al documento 1 de identidad, en particular, un "dato visual" impreso en el documento 1, como se indicó anteriormente, pero se comprende que también puede tratarse de una dirección de correo electrónico, un identificador de acceso, etc., que no se imprimen, necesariamente, en el documento 1.

Esta etapa (A) puede, a su vez, ponerse en práctica por medio de una imagen del documento 1 de identidad (como se explicará para el procedimiento de autenticación), pero, de manera 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 personal) se manipulan directamente, en particular, si el registro se realiza 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 manera 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 manera 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 manera indirecta, es decir, a datos derivados de esta información de referencia para añadir entropía. Por ejemplo, puede usarse, 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 manera que puede volver a encontrarse por medio de un proceso de decodificación complementario del proceso de codificación.

Cuando el proceso de codificación usado 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 cual sucede normalmente si se extrae la información representativa de la misma fotografía que aquella a partir de la cual se ha generado la información de referencia, aunque se indique 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.

Finalmente, 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 personal 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 manera 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 usarse 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, el cual sólo puede encontrarse disponiendo de la información de referencia.

De este modo, el o los datos personales cifrados con la segunda huella criptográfica (es decir, se usa la segunda huella como clave) siguen siendo accesibles solo para el poseedor del documento 1 de identidad, 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 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 sólo tiene una vida útil limitada y debe renovarse regularmente.

Según el modo de realización preferido, que permite, además, la autenticación del individuo portador del documento 1 de identidad, el equipo cliente 3 también dispone, ventajosamente, de un segundo dato codificado (indicado SSKT, por SSK-TEMPLATE) obtenido mediante aplicación de un proceso de codificación (normalmente, el mismo proceso de codificación que para el primer dato codificado) a un 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 en los medios 22 de almacenamiento de datos del servidor 2 (y asociarse a los 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, ventajosamente, 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 sólo 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 manera 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 los medios 32 de almacenamiento de datos del equipo cliente 3 (dado el 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 ponerse en práctica en nuevas etapas (A') a (D'), es decir, no necesariamente de manera simultánea con las acciones asociadas al registro del documento 1 de identidad.

Por otro lado, sigue siendo posible poner en práctica un procedimiento de autenticación del individuo, sin necesitar un segundo dato de aleatoriedad RNGT y un segundo dato codificado SSKT, concretamente, usando el dato biométrico de referencia como dato personal, cifrado por medio de la segunda huella criptográfica.

Autenticación del documento de identidad

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

En un modo de realización preferido, el procedimiento de autenticación comienza por una etapa (a) de adquisición de una manera 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.

Normalmente, es el individuo el que toma una fotografía de su documento 1 de identidad con su terminal móvil.

Ahora va a describirse la parte principal del procedimiento de autenticación de un individuo que presenta un documento 1 de identidad como que es el suyo, y que proporciona para ello una imagen adquirida de ese documento 1 de identidad.

El objetivo es verificar que la etapa (a) se ha desarrollado realmente como se describió anteriormente y que no se está en presencia de una falsificación (por ejemplo, una imagen que se haya modificado de manera fraudulenta). El individuo, o cualquier otra entidad que desee la autenticación del documento 1, quiere demostrar esto al servidor 2.

En una etapa (b), los medios 31 de procesamiento de datos del equipo cliente 3 analizan la imagen, de manera 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 manera 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 usarse, de manera astuta, redes neuronales de convoluciones adaptadas. De manera 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 manera idéntica de modo que puedan compararse.

De manera preferida, la etapa (b) comprende la interrogación del servidor 2, de manera que se recupera al menos dicho primer dato codificado SSKD si está almacenado en este servidor 2 (más adelante se verán los otros datos que pueden requerirse), 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, alternativamente, 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 una etapa (c), los medios 31 de procesamiento de datos 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 recibido desde el servidor 2.

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 usado para obtener este primer dato codificado SSKD.

De manera 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.

La etapa (c) comprende, además, el cálculo de la huella criptográfica de una primera concatenación del dato de lectura óptica extraído y del primer dato decodificado. Dicho de otro modo, el equipo cliente 3 intenta reconstituir la primera huella 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 usado 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.

En esta fase, el equipo cliente 3 podría enviar simplemente la primera huella calculada en la etapa (c) y dejar que los medios 21 de procesamiento de datos del servidor 2 verifiquen que coincide con aquella de la que dispone (es decir, verificar que una huella criptográfica de una primera concatenación del dato de lectura óptica extraído y del primer dato decodificado coincide con la huella criptográfica de la primera concatenación del dato de lectura óptica del documento 1 de identidad y del primer dato de aleatoriedad almacenado en los medios 22 de almacenamiento de datos del servidor 2).

No obstante, el valor correcto de la primera huella puede conocerse, aunque sólo sea de una autenticación anterior del documento 1. Por ello, el equipo cliente 3 va a demostrar que ha obtenido esta primera huella de manera correcta, es decir, a partir del documento 1 de identidad, y esto de manera 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, se usa un protocolo criptográfico que genera una "prueba" del cálculo de dicha huella criptográfica a partir de la primera concatenación del dato de lectura óptica extraído y del primer dato decodificado, no revelando esta prueba nada más que el hecho de que el productor de la prueba dispone realmente del dato de lectura óptica y del primer dato decodificado (es decir, el primer dato de aleatoriedad RNGD). Dicho de otro modo, el equipo 3 no dispone simplemente de la huella criptográfica, sino, además, del dato que se somete a resumen criptográfico en esta huella criptográfica.

El protocolo de Pinocchio presentado en la publicación "Bryan Parno, Craig Gentry, Jon Howell, and Mariana Raykova, Pinocchio: Nearly Practical Verifiable Computation, in Proceedings of the IEEE Symposium on Security and Privacy, IEEE, 21 de mayo de 2013" ha sido uno de los primeros protocolos de cálculo verificable que permiten a quien lo ejecuta, calcular de manera verificable la aplicación de cualquier función, y a quien da la orden, verificar la prueba asociada en un tiempo de cálculo inferior al necesario para realizar el cálculo por sí mismo.

En una etapa (d), los medios 31 de procesamiento de datos del equipo cliente 3 actúan como entidad de prueba que genera para ello 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 manera correcta.

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".

De este modo, puede asociarse la huella criptográfica proporcionada al dato de lectura óptica y a la información candidata representativa del aspecto de la fotografía, pero no puede obtenerse información sobre el contenido de estos datos. El protocolo criptográfico facilita una prueba rápida de verificar (menos de medio segundo) y que no puede falsificarse: es casi imposible (probabilidad inferior a $1/2^{80}$, incluso inferior a $1/2^{128}$ según los parámetros elegidos para realizar la prueba, siendo ésta entonces más lenta de realizar) hacer que se acepte una prueba de la afirmación anterior si el procedimiento no se desarrolla según lo que se ha especificado.

En la realización de la prueba, la entidad 3 de prueba usa la posibilidad de realizar pruebas de divulgación nula de conocimiento para ocultar los datos del documento 1 de identidad. De este modo, la prueba no da ninguna información sobre los propios datos. Más adelante se verá cómo puede generarse la prueba.

En una etapa (e), el equipo cliente 3 transmite al servidor 2 dicha prueba de divulgación nula de conocimiento generada en la etapa (d), y la huella criptográfica calculada en la etapa (c).

De este modo, en una etapa (f), los medios 21 de procesamiento de datos del servidor 2 verifican 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 manera 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.

Si se ha recuperado la primera huella y la prueba es válida, es que el documento 1 de identidad es válido, es decir, no está falsificado. Eventualmente, puede consultarse un descriptor asociado a la primera huella para obtener el estado del documento 1: "OK", "Caducado", "KO". Por ejemplo, este estado puede definir si el poseedor del documento 1 tiene derecho a penetrar en una zona a la entrada de la cual tiene lugar el control.

Si tiene el estado OK, puede entrar, y si tiene el estado Caducado es que normalmente tiene derecho a entrar, pero que hace falta que actualice su acceso. Si tiene el estado KO, esto significa que se le ha reconocido realmente, pero que no tiene el nivel de autorización suficiente.

Alternativamente, el servidor 2 puede transmitir, cuando el documento 1 se autentica satisfactoriamente, a la eventual entidad conectada ante la cual desea autenticarse el individuo (por ejemplo, un servidor que pone en práctica un servicio como se explica) una autorización, por ejemplo, cifrada con una clave pública de dicha entidad (la autenticación en sí misma es, normalmente, un testigo de un solo uso). Alternativamente, una autorización cifrada de este tipo puede transmitirse al equipo cliente 3, para retransmisión a la entidad conectada, y descifrado y verificación por esta última. Un modo de realización de este tipo es particularmente ventajoso, ya que permite una total confidencialidad: no solo el servidor 2 no tiene acceso a los datos personales del individuo, sino que además no tiene ningún contacto con la entidad conectada ante la cual el individuo desea la autenticación, de manera que ni siquiera tiene la posibilidad de saber por qué se requiere la autenticación.

Debe observarse que la consulta de un registro y/o la eventual emisión de una autorización de acceso, puede hacerse únicamente si se logra una autenticación del propio individuo, véase más adelante.

En esta fase, se le puede pedir al individuo que proporcione al menos un dato personal (denominado dato personal diana a continuación de la presente descripción), por ejemplo, datos alfanuméricos para rellenar un registro si se le ha autorizado el acceso, o para rellenar un formulario solicitado por el servicio puesto en práctica por la entidad conectada. Ahora, va a poder usar de manera astuta la segunda concatenación para obtener automáticamente estos datos.

Para ello, en una eventual etapa complementaria (g) (que puede estar eventualmente condicionada a un estado particular, por ejemplo, únicamente si el individuo tiene derecho a ir más lejos y/o al autenticarse al individuo), entonces los medios 21 de procesamiento de datos transmiten al equipo cliente 3 (si no dispone todavía de ello) para descifrado el al menos un dato personal de dicho individuo cifrado almacenado en los medios 22 de almacenamiento de datos del servidor 2. Como se explica, este descifrado puede hacerse por medio de la huella criptográfica de una segunda concatenación del dato de lectura óptica extraído y del dato decodificado.

En efecto, en esta fase se sabe que el dato decodificado corresponde al dato de aleatoriedad y que el individuo ha podido reconstituir satisfactoriamente la primera huella en el equipo cliente 3. Cambiando solo la concatenación (en particular, invirtiendo la MRZ y la aleatorización) y aplicando de nuevo la función de resumen criptográfico, puede reconstituir la segunda huella, que constituye la clave privada de los datos personales.

La totalidad o parte de los mismos, a petición suya, pueden volver a transferirse entonces al servidor 2.

Debe observarse que podría preverse que el usuario esté autorizado a aprovechar para actualizar estos datos personales: si, por ejemplo, ha cambiado su dirección, modifica los datos antes de volver a cifrarlos y volver a transmitir el conjunto al servidor 2 para almacenamiento.

Se observa realmente que, con una solución de este tipo, no se almacena ningún dato sensible en el lado del servidor 2 ni se transmite desde el equipo cliente 3 (solamente una huella criptográfica no explotable) y, por tanto, que un ataque no pondrá en peligro ni la seguridad de la solución ni los datos personales de los usuarios.

Alternativas

En vez de proporcionar un dato personal diana requerido en una etapa (g) que necesita una interacción complementaria, puede simplificarse el procedimiento proporcionando este dato al mismo tiempo que la prueba en la etapa (e). Para ello, basta con adaptar la prueba de divulgación nula de conocimiento, de manera que también sea una prueba del hecho de que el al menos un dato personal diana que va a transmitirse se selecciona realmente de entre los datos personales asociados al documento 1 de identidad.

En efecto, la prueba puede implicar parámetros públicos complementarios tales como este dato personal diana.

Según un primer modo de realización, dicho dato personal diana es un fragmento del dato de lectura óptica, por ejemplo, el nombre simple del individuo, es decir, se extrae del dato de lectura óptica y la prueba es, de este modo, una prueba de esta extracción. Más precisamente, la prueba de divulgación nula de conocimiento puede

ser una prueba de la siguiente afirmación: “dada una huella criptográfica y un dato personal diana, existe un dato de lectura óptica y un primer dato de aleatoriedad RNGD (el primer dato decodificado) tales que:

- su primera concatenación tiene como huella esta huella criptográfica dada, y

- el dato personal diana se extrae del dato de lectura óptica”.

Según un segundo modo, el eventual 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, de al menos un dato personal de dicho individuo, está disponible desde el origen en el equipo cliente 3, o bien se proporciona directamente por el servidor 2 (por ejemplo, en la etapa (b), al mismo tiempo que el primer dato codificado). En efecto, un suministro de este tipo no resulta problemático debido al cifrado.

Entonces, como se explica, si el individuo puede reconstituir satisfactoriamente la primera huella en el equipo cliente 3, puede reconstituir la segunda huella, que constituye la clave privada de los datos personales, cambiando solo de concatenación (en particular, invirtiendo la MRZ y el primer dato de aleatoriedad) y aplicando de nuevo la función de resumen criptográfico.

La prueba de divulgación nula de conocimiento es entonces una prueba del hecho de que el dato personal diana procede de los datos personales cifrados, es decir, garantiza la siguiente afirmación “dada una huella criptográfica y un dato personal diana, existe un dato de lectura óptica, un primer dato de aleatoriedad RNGD (el primer dato decodificado) y un dato personal cifrado tales que:

- la primera concatenación del dato de lectura óptica y del primer dato de aleatoriedad RNGD tiene como huella esta huella criptográfica dada, y

- dicho dato personal cifrado se descifra para dar dicho dato personal diana”.

Se observa que son posibles otras alternativas, por ejemplo, si el dato personal que va a transmitirse es la fotografía del individuo, y el experto en la técnica sabrá adaptar la prueba para cada caso.

Generación de prueba

De manera preferida, dicha prueba de divulgación nula de conocimientos es un objeto criptográfico de tipo zkSNARK.

zkSNARK significa “zero-knowledge Succinct Non Interactive ARgument of Knowledge”, es decir, Argumento de conocimiento no interactivo de divulgación nula de conocimientos. Se trata de una criptografía primitiva construida en torno a la noción de prueba. Los investigadores de informática teórica y de criptografía están interesados desde hace mucho tiempo en la noción de prueba. Existen resultados teóricos que permiten producir una prueba muy corta y segura de un algoritmo, pero el tiempo para realizar esta prueba está fuera del alcance y seguirá siendo así a pesar del aumento de la potencia de cálculo de los ordenadores. Uno de los motivos se debe al poder que se asigna a la entidad que realiza la prueba, el equipo cliente 3 (también denominado el probador). En los resultados teóricos con las pruebas, el probador tiene una potencia de cálculo infinita y las pruebas siguen siendo seguras a pesar de ello.

A continuación, se ha relajado la noción de prueba, buscando el protocolo protegerse únicamente de un probador que tenga una potencia de cálculo importante pero limitada. El resultado del protocolo ya no es una prueba sino un argumento. Es a partir de esta noción de argumento, que se construyen los sistemas prácticos de cálculo verificables. Una exigencia complementaria en un sistema que produce un argumento, es que este argumento no sea interactivo: el verificador y el probador no tiene necesidad de interaccionar para producir el argumento.

Desde 2010, se han presentado realizaciones de zkSNARK: se trata de argumentos cuyo tamaño es corto (algunos elementos de una curva elíptica), que no necesitan interactividad y que, además, permiten al probador realizar una prueba de divulgación nula de conocimiento, es decir, la prueba no contiene ninguna información no trivial sobre las entradas proporcionadas por el probador.

Existen varios protocolos que realizan concretamente zkSNARK y el experto en la técnica podrá usarlos indistintamente en el presente procedimiento:

- El protocolo de Pinocchio ya mencionado;

- El protocolo de Gepetto, presentado en la publicación “Craig Costello, Cedric Fournet, Jon Howell, Markulf Kohlweiss, Benjamin Kreuter, Michael Naehrig, Bryan Parno, and Samee Zahur, Geppetto: Versatile Verifiable Computation, in Proceedings of the IEEE Symposium on Security and Privacy, IEEE, 18 de mayo de 2015”, que es una mejora del de Pinocchio

- El protocolo presentado en la publicación y siguientes “Eli Ben-Sasson, Alessandro Chiesa, Daniel Genkin, Eran Tromer, Madars Virza. SNARKs for C: Verifying Program Executions Succinctly and in Zero Knowledge. En Proceedings of the 33rd Annual International Cryptology Conference, CRYPTO '13, páginas 90-108, 2013”, implementado a modo de código abierto, en forma de una biblioteca denominada libsnark, optimizando el protocolo que produce un zkSNARK en Pinocchio, mejorando la capacidad de expresión, es decir, el tipo de programas o de algoritmo que es posible verificar.

Para tomar como ejemplo el protocolo de Pinocchio, este protocolo incluye varias partes:

1. Se traduce un programa clásico en forma de un circuito aritmético, es decir, un conjunto de relaciones entre las entradas y las salidas del programa, traducidas únicamente con la ayuda de adiciones y multiplicaciones de elementos de un cuerpo finito. Hace falta indicar que, en teoría, todos los programas pueden traducirse en esta forma, pero que sólo una parte de estos programas admiten una traducción eficaz en forma de circuito.

2. El circuito aritmético obtenido se representa eficazmente con la ayuda de tres familias de polinomios, a las cuales se les añade un polinomio complementario, denominado polinomio diana. Estas familias de polinomios forman “Quadratic Arithmetic Programs” (QAP, programas aritméticos cuadráticos). Codifican las relaciones entre las entradas y las salidas de cada puerta multiplicativa del circuito, integrándose las relaciones de las puertas aditivas en la primera puerta multiplicativa que sigue en el cálculo.

Estos QAP están relacionados con el cálculo verificable mediante el siguiente punto: un cálculo y = C(x) es correcto para una entrada x si y sólo si todas las relaciones que describen el circuito aritmético correspondiente se satisfacen fijando como valor de entrada x, y como valor de salida y.

Los QAP permiten, de alguna manera, comprimir todas las restricciones que van a verificarse en una única relación que va a verificarse: un polinomio construido a partir del valor x, y de las tres familias del QAP debe dividir el polinomio diana.

3. Un protocolo criptográfico toma entonces en la entrada un QAP asociado a un programa, genera claves de evaluación y de verificación que usan curvas elípticas para ocultar las relaciones polinomiales. El polinomio que prueba que el cálculo se ha realizado correctamente, se calcula entonces directamente con la ayuda de las relaciones ocultadas en la curva elíptica. La relación de divisibilidad se traduce, únicamente, con la ayuda de un número constante de elementos de la curva elíptica, es decir, que la prueba es de tamaño constante. La verificación de esta prueba es extremadamente rápida.

El protocolo permite, además, obtener que entradas del cálculo proporcionadas por el probador sean privadas: permite ocultar los valores del probador en la realización de la prueba, multiplicándolos por un múltiplo del polinomio diana, lo cual no modifica el hecho de que el polinomio “prueba” sea divisible entre el polinomio diana.

Este polinomio “prueba”, cuando se oculta en una curva elíptica, constituye un zkSNARK.

El protocolo de Pinocchio permite a quien realiza la prueba, ocultar determinadas entradas del cálculo en el que realiza la prueba. En el presente caso, se trata de realizar el siguiente cálculo:

Entrada: la huella criptográfica de la primera concatenación del dato de lectura óptica extraído y del primer dato decodificado, dado el caso un dato personal que va a transmitirse y un vector de inicialización IV (y otros datos públicos si es necesario).

Entrada privada: el dato de lectura óptica extraído y el primer dato decodificado. Salida: la prueba π de que el probador conoce realmente el dato de lectura óptica extraído y el primer dato decodificado cuya concatenación se somete a resumen criptográfico en la huella criptográfica dada y, dado el caso, a partir de los cuales puede recuperarse el dato personal que va a transmitirse.

Debe observarse que se conocen protocolos previstos para la generación de una prueba de buen desarrollo de una función de resumen criptográfico, que el experto en la técnica podrá usar directamente, aunque no sean óptimos. La dificultad es obtener un tiempo de cálculo razonable para realizar la prueba y tamaños de claves de evaluación y de verificación que no sean demasiado significativos.

- el protocolo de Zerocash (IEEE Security & Privacy 2014) de Ben-Sasson *et al.*, propone la definición de un circuito aritmético para verificar la función de compresión de SHA-256, que incluye aproximadamente 30.000 puertas multiplicativas. Esto da un tiempo de realización de prueba de aproximadamente 5 segundos (por cada nivel de compresión, verificar la función de resumen criptográfico completa que comprende numerosas iteraciones de la función de compresión, será netamente más prolongado), lo cual sigue siendo elevado y ampliamente mejorable;

- el protocolo de ZKBoo, presentado en la publicación "ZKBoo: faster zero-knowledge for boolean circuits" de Giacomelli, Madsen y Orlandi (Usenix Security, 2016) permite rendimientos mejores (prueba en 50 ms, verificación en 70 ms) mediante iteración de la función de compresión, pero el tamaño de la prueba es significativo (800 Ko) tanto más en cuanto que parece haberse medido únicamente en una aplicación de la función de compresión.

En la actualidad, se prefiere un sistema de prueba ligero, pero cuya generación tarde algunos segundos, de manera que se permite una autenticación rápida.

Segunda prueba de divulgación nula de conocimientos

Según un modo particularmente preferido, el presente procedimiento también es un procedimiento de autenticación del individuo, que implica una comparación entre un dato biométrico candidato y un dato biométrico de referencia.

Se supone que el equipo cliente 3 dispone de dicho dato biométrico candidato y de dicho segundo dato codificado SSKT, o al menos del dato biométrico de referencia.

En lo que se refiere al dato biométrico candidato, "reciente", éste puede obtenerse durante la etapa previa (a). Dicho de otro modo, el equipo cliente 1 puede no disponer inicialmente (es decir, tras la etapa de registro (a0)) absolutamente de ningún dato.

Es importante comprender que, si bien la etapa de registro (a0) puede ponerse en práctica semanas antes de la puesta en práctica 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, ventajosamente, 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, ventajosamente, se usa como marcador temporal un nonce (es decir, un número arbitrario, es decir, una aleatoriedad, de uso único, del inglés "number used once").

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 usarse 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, se usan 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.

Podrán usarse numerosas pruebas de divulgación nula de conocimiento y, concretamente, las propuestas en la solicitud FR17599292.

De manera particularmente preferida, en el modo de realización en el que se dispone de 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 usarse un proceso de decodificación para verificar si el dato biométrico candidato y el dato biométrico de referencia coinciden, de la misma manera que lo que se ha hecho para la información de tipo DPS en la fotografía.

De nuevo, cuando el proceso de codificación usado 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.

De este modo, la puesta en práctica de la comparación comprende 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, ventajosamente, el cálculo de un producto escalar.

Por ejemplo, en el caso en donde 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.

De este modo, la etapa (c) comprende, además, ventajosamente, el cálculo por los medios 31 de procesamiento de datos 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 manera que se construye 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).

A continuación, la etapa (d) comprende 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, a parte del hecho de que el productor de la prueba dispone realmente del segundo dato decodificado (es decir, el segundo dato de aleatoriedad RNGT). De nuevo, la prueba tiene como objetivo garantizar que la tercera huella criptográfica se ha calculado efectivamente y de manera 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 donde 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 manera que la primera prueba de divulgación nula de conocimiento, véase anteriormente.

Entonces, en la etapa (e), el equipo cliente 3 transmite además al servidor 2 dicha segunda prueba de divulgación nula de conocimiento y la nueva huella criptográfica calculada (la tercera huella).

De este modo, en la etapa (f), los medios 21 de procesamiento de datos del servidor 2 verifican que la segunda prueba de divulgación nula de conocimiento es válida y que la huella criptográfica recibida coincide con la construida a partir del segundo dato de aleatoriedad RNGT del que dispone el servidor 2.

Si la prueba no es válida, es que la tercera huella criptográfica no se ha obtenido de manera válida y, por tanto, que no ha habido ninguna comparación entre los datos biométricos candidato y de referencia y que se trata posiblemente de una usurpación de identidad. Si la prueba es válida, pero la huella criptográfica recibida no coincide con aquella de la que dispone la entidad 2 de verificación, es que el dato biométrico candidato no coincide con el dato biométrico de referencia y, por tanto, que el individuo no es el esperado, es decir, fracasa la autenticación del individuo.

Si se ha recuperado la tercera huella y la prueba es válida, es que se confirma la identidad del individuo y pueden producirse otras acciones (la consulta de un descriptor, la emisión de autorización hacia el equipo 3 o una entidad conectada, el suministro de datos de la etapa (f), etc.).

Se observará que, en lugar de poner simultáneamente en práctica la autenticación del documento 1 y la autenticación del individuo (es decir, usar las mismas etapas (a) a (f)), es totalmente posible poner en práctica los procedimientos uno después de otro, es decir, que habrá etapas (a') a (f') para el procedimiento puesto en práctica en segundo lugar (en particular, el procedimiento de autenticación del individuo, aunque el orden inverso es posible).

Servidor

Según un segundo aspecto, se propone el conjunto del servidor 2 y del equipo cliente 3 conectados, para la puesta en práctica del procedimiento según el primer aspecto, es decir, de autenticación de un documento 1 de identidad de un individuo y, eventualmente, de autenticación de dicho individuo.

El equipo cliente 3 comprende medios 31 de procesamiento de datos configurados para:

- Extraer, mediante análisis de una imagen adquirida (en particular, por medios 30 de adquisición óptica del equipo cliente 3) del 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, denominada primera huella criptográfica;

  - una huella criptográfica de una primera concatenación del dato de lectura óptica extraído y del primer dato decodificado;

  - eventualmente, un segundo dato decodificado mediante aplicación del proceso de decodificación a un dato biométrico candidato y a un segundo dato codificado, tal que dicho segundo dato decodificado corresponde a un segundo dato de aleatoriedad, si dicho dato biométrico candidato coincide con un dato biométrico de referencia;

  - y, eventualmente, otra huella criptográfica construida a partir del segundo dato decodificado, de la misma manera que se construye una tercera huella criptográfica de la que dispone el servidor 2 a partir del segundo dato de aleatoriedad;

- generar 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, así como, eventualmente, una prueba de divulgación nula de conocimientos del cálculo de dicha otra huella criptográfica a partir del segundo dato decodificado;

- transmitir al servidor 2 dicha o dichas prueba(s) de divulgación nula de conocimiento y dicha o dichas huella(s) criptográfica(s) asociada(s) calculada(s); el servidor 2 comprende, por su parte, medios 22 de procesamiento de datos configurados para verificar que:

  - la o las prueba(s) de divulgación nula de conocimiento es(son) válida(s), y

  - la o las huella(s) criptográfica(s) recibida(s) coincide(n) (respectivamente) con dicha o dichas huella(s) criptográfica(s) primera/tercera de las que dispone el servidor 2.

El equipo cliente 3 puede comprender, además, 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 de un documento (1) de identidad puesto en práctica por un servidor (2) y un equipo cliente (3) conectados;
disponiendo el equipo cliente (3) de un primer dato codificado y 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, 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, denominada primera huella criptográfica;
comprendiendo el procedimiento la puesta en práctica de las etapas de;

(b)Extraer, por los medios (31) de procesamiento de datos del equipo cliente (3), 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 por los medios (31) de procesamiento de datos del equipo cliente (3):

- 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 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;
- una huella criptográfica de una primera concatenación del dato de lectura óptica extraído y del primer dato decodificado;

(d)generar por los medios (31) de procesamiento de datos del equipo cliente (3) 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;
(e)transmitir al servidor (2) dicha prueba de divulgación nula de conocimiento y la huella criptográfica calculada;
(f)verificar por medios (21) de procesamiento de datos del servidor (2) que:

- la prueba de divulgación nula de conocimiento es válida, y
- la huella criptográfica recibida coincide con dicha primera huella criptográfica de la que dispone el servidor (2).

2. Procedimiento según la reivindicación 1, que comprende una etapa (a) de adquisición 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 por medios (30) de adquisición óptica del equipo cliente (3).

3. Procedimiento según la reivindicación 2, en el que el equipo cliente (3) no dispone inicialmente ni del primer dato codificado ni de la imagen adquirida de dicho documento (1) de identidad, comprendiendo la etapa (b) la recepción por el equipo cliente (3) del primer dato codificado desde el servidor (2).

4. Procedimiento según una de las reivindicaciones 1 a 3, en el que dicha 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 una prueba de divulgación nula de conocimientos del hecho de que, dada una huella criptográfica, existe un dato de lectura óptica y un primer dato de aleatoriedad tales que su primera concatenación tiene como huella dicha huella criptográfica dada.

5. Procedimiento según una de las reivindicaciones 1 a 4, que comprende una etapa anterior (a0) de registro de datos de dicho documento (1) de identidad que comprende las 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;

y, opcionalmente, (D) almacenar en medios (22) de almacenamiento de datos del servidor (2) el primer dato codificado y la primera huella criptográfica.

6. Procedimiento según una de las reivindicaciones 1 a 5, que es, además, un procedimiento de autenticación del individuo, en el que la etapa (d) comprende la generación por los medios (31) de procesamiento de datos del equipo cliente (3) de una prueba de divulgación nula de conocimientos del hecho de que un dato biométrico de referencia y un dato biométrico candidato del individuo coinciden; la etapa (e) que comprende la transmisión al servidor (2) de dicha prueba de divulgación nula de conocimiento del hecho de que el dato biométrico de referencia y el dato biométrico candidato del individuo coinciden; y la etapa (f) que comprende la verificación por 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.

7. Procedimiento según la reivindicación 6, en el que el equipo cliente (3) dispone, además, de un segundo dato codificado y del dato biométrico candidato del individuo, y el servidor (2) dispone de una huella criptográfica construida a partir de un segundo dato de aleatoriedad, denominada tercera huella criptográfica; la etapa (c) que comprende el cálculo por los medios (31) de procesamiento de datos del equipo cliente (3) de:

- ○un segundo dato decodificado mediante aplicación de un proceso de decodificación a dicho dato biométrico candidato y al primer dato codificado, tal que dicho segundo dato decodificado corresponde al segundo dato de aleatoriedad, si dicho dato biométrico candidato coincide con el dato biométrico de referencia;
- ○una huella criptográfica construida a partir del segundo dato decodificado de la misma manera que se construye la tercera huella criptográfica a partir del segundo dato de aleatoriedad;

siendo dicha prueba de divulgación nula de conocimientos del hecho de que el dato biométrico de referencia y el dato biométrico candidato del individuo coinciden 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; comprendiendo la etapa (e), además, la transmisión al servidor (2) de la huella criptográfica calculada; y comprendiendo la etapa (f), además, la verificación mediante medios (21) de procesamiento de datos del servidor (2) de que la huella criptográfica recibida coincide con dicha tercera huella criptográfica de la que dispone el servidor (2).

8. Procedimiento según las reivindicaciones 5 y 7 en combinación, en el que, 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.

9. Procedimiento según una de las reivindicaciones 6 a 7, en el que la tercera huella criptográfica es la huella criptográfica de una concatenación del segundo dato de aleatoriedad y de la primera huella criptográfica.

10. Procedimiento según una de las reivindicaciones 6 a 9 en combinación con la reivindicación 2, en el que la etapa (a) comprende, además, la generación del dato biométrico candidato a partir de un rasgo biométrico proporcionado por medios de adquisición biométrica, preferiblemente los medios (30) de adquisición óptica del equipo cliente (3), siendo el equipo cliente (3), en particular, un equipo electrónico personal de dicho individuo.

11. Procedimiento según una de las reivindicaciones 1 a 10, en el que la etapa (f) también comprende la transmisión al servidor (2) de un dato personal diana del individuo, la 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, también una prueba del hecho de que el al menos un dato personal diana que va a transmitirse se selecciona de entre datos personales asociados al documento (1) de identidad; siendo dicho dato personal de dicho individuo, en particular, un dato alfanumérico asociado a dicho individuo.

12. Procedimiento según una de las reivindicaciones 1 a 11, en el que el equipo cliente (3) dispone, además, de un cifrado con la 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, de al menos un dato personal de dicho individuo, denominada segunda concatenación; comprendiendo el procedimiento el descifrado del cifrado del al menos un dato personal de dicho individuo, por medio de la huella criptográfica de la segunda concatenación del dato de lectura óptica extraído y del dato decodificado.

13. Procedimiento según la reivindicación 11 y 12 en combinación, en el que dicho dato personal diana o bien se extrae del dato de lectura óptica o bien del al menos un dato personal cifrado.

14. Producto de programa de ordenador, que comprende instrucciones de código para la ejecución de un procedimiento según una de las reivindicaciones 1 a 13, de autenticación de un documento (1) de identidad, 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 13 de autenticación, de un documento (1) de identidad.

Fig. 1