

MÉTODO PARA LA AUTENTICACIÓN FUERTE DE UN INDIVIDUO

CAMPO TÉCNICO DE LA INVENCION

La invención se relaciona con un método para la autenticación fuerte de un individuo que porta un documento de identidad.

ESTADO DE LA TÉCNICA

Hoy en día, se conocen métodos de autenticación fuerte muy rigurosos (es decir, más factores de autenticación), específicamente definidos mediante las especificaciones de FIDO Alliance.

P. ej., un autenticador en posesión de un usuario (típicamente su dispositivo móvil, una tarjeta con chip, etc.) y cualquier cosa que el usuario “conozca” o “tenga” (un código, una característica biométrica, etc.).

Estos métodos son completamente satisfactorios, pero presentan un defecto en sus mecanismos de “recuperación” implementados en caso de olvidar el código o de perder el autenticador de uno.

Más específicamente, cualquiera de estos mecanismos de recuperación usa solo un único factor de autenticación (típicamente, se envía un enlace a una dirección de correo electrónico de recuperación) que

resulta en la pérdida de todos los beneficios de la autenticación fuerte, o es necesario guardar información personal confidencial como “respuesta a una pregunta secreta” o una fotografía de identificación.

En primer lugar, observamos que una parte de esta solución no es fiable (si la información solicitada es demasiado secreta, el usuario puede perderla/olvidarla, y si es demasiado común, determinados piratas informáticos pueden tener éxito en obtenerla mediante ingeniería social); y segundo, que mantener tal información plantea problemas en términos de respeto de la privacidad de los usuarios.

La solicitud núm. EP2656321 propone usar, como un factor de autenticación, una imagen de cualquier cosa elegida secretamente por el individuo, tal como un objeto o un documento de identidad. Este método mejora la fiabilidad, pero sigue siendo problemático en términos de protección de la privacidad.

Por lo tanto, sería deseable proporcionar una solución simple, confiable y segura que sea completamente respetuosa de la privacidad para la autenticación de un individuo, en particular para fines de recuperación.

BREVE DESCRIPCIÓN DE LA INVENCION

De acuerdo con un primer aspecto, la invención se relaciona con una autenticación fuerte de un individuo implementada por un servidor y un dispositivo cliente conectado;

el dispositivo cliente tiene un dato biométrico candidato del individuo y una imagen captada de un documento de identidad que representa al menos una fotografía de dicho individuo y un dato del lector óptico visible en dicho documento de identidad, y el servidor tiene una huella criptográfica de una primera concatenación de dicho dato del lector óptico de dicho documento de identidad y de un primer dato aleatorio, la denominada huella criptográfica; en donde el método se caracteriza porque comprende la implementación mediante el medio de procesamiento de datos del servidor y/o del dispositivo cliente de las etapas de;

(b) extraer, mediante el análisis de dicha imagen captada de dicho documento de identidad:

- una información candidata representativa de la apariencia de

- dicha fotografía como se ilustra en la imagen captada;
- dicho dato del lector óptico como se ilustra en la imagen captada;
- (c) calcular un primer dato decodificado mediante la aplicación de un proceso de decodificación a dicha información candidata representativa de la apariencia de dicha fotografía y a un primer dato codificado, de tal manera que el primer dato decodificado coincide con el primer dato aleatorio si dicha información candidata representativa de la apariencia de dicha fotografía coincide con una información de referencia representativa de la apariencia de dicha fotografía;
- (d) verificar que:
- una huella criptográfica de una primera concatenación del dato extraído del lector óptico y del dato codificado coincida con dicha primera huella criptográfica en el servidor; y
 - el dato biométrico de referencia y el dato biométrico candidato del individuo coincidan.

De acuerdo con otras características ventajosas y no limitantes:

el método comprende una etapa (a) de la captación previa de dicha imagen de dicho documento de identidad que representa al menos una fotografía de un individuo y un dato visible del lector de datos en dicho documento de identidad mediante el medio de captación óptico del dispositivo cliente, y la generación del dato biométrico candidato usando una característica biométrica proporcionada mediante los medios de captación biométrica; los medios de captación biométrica son los medios de captación óptica del dispositivo cliente, en donde el dispositivo cliente es un dispositivo electrónico personal de dicho individuo, en particular como un dispositivo móvil o una tarjeta con chip:

el servidor o dispositivo tiene un cifrado del dato biométrico de referencia de dicho individuo con una huella criptográfica de una segunda concatenación del dato del lector óptico del documento de identidad y del primer dato aleatorio, diferentes de la primera concatenación; en donde la etapa (c) comprende el descifrado de al menos un

dato biométrico de referencia cifrado de dicho individuo mediante la huella criptográfica de una segunda concatenación del dato extraído del lector óptico y del primer dato decodificado;

el servidor tiene una huella criptográfica construida usando un segundo dato aleatorio, denominado tercera huella criptográfica; la etapa (b) comprende el cálculo mediante el procesamiento de datos del servidor o del dispositivo cliente de un segundo dato decodificado mediante la aplicación de un proceso de decodificación a dicho dato biométrico candidato y a un segundo dato codificado, de tal manera que el segundo dato decodificado coincide con el segundo dato aleatorio si dicho dato biométrico candidato coincide con el dato biométrico de referencia; dicha verificación de la etapa (d) que el dato biométrico de referencia y el dato biométrico candidato del individuo que comprende la verificación que una huella criptográfica construida usando el segundo dato decodificado de la misma manera que la tercera huella criptográfica se construye

usando el segundo dato aleatorio que coincide con dicha tercera huella criptográfica del servidor.

La etapa (a) comprende la recepción mediante el servidor de la imagen captada de dicho documento de identidad y del dato biométrico candidato del dispositivo cliente, en donde las etapas (b) y (c) se implementan mediante el medio de procesamiento de datos del servidor;

el método comprende las etapas (b) y (c) que se implementan mediante el medio de procesamiento de datos del dispositivo cliente, la etapa (c) comprende el cálculo de la huella criptográfica desde una primera concatenación del dato extraído del lector óptico y desde el primer dato decodificado, y la generación de conocimiento cero prueba el cálculo de la huella criptográfica usando la primera concatenación del dato extraído del lector óptico y del primer dato decodificado; la verificación de la etapa (d) donde la huella criptográfica de una primera concatenación del dato extraído del lector óptico y del dato decodificado coincide con la primera huella criptográfica que comprende la verificación que:

- la prueba de la no divulgación del conocimiento del cálculo de dicha huella criptográfica usando la primera

concatenación del dato extraído del lector óptico y del primer dato decodificado es válida, y

- el primer dato criptográfico recibido coincide con la primera huella criptográfica en el servidor;

las etapas (b) y (c) se implementan mediante el medio de procesamiento del dato del dispositivo cliente, en donde la etapa (c) comprende la generación de conocimiento cero que prueba el hecho de que el dato biométrico de referencia y el dato biométrico candidato del individuo coinciden; dicha verificación de la etapa (d) donde el dato biométrico de referencia y el dato biométrico candidato del individuo coinciden, que comprende la verificación mediante el medio de procesamiento de datos del servidor de que el conocimiento cero prueba el hecho de que el dato biométrico de referencia y el dato biométrico candidato del individuo que coinciden son válidos.

El método también comprende una etapa previa (a0) a la inscripción de datos de dicho documento de identidad que comprende las subetapas de:

- (A) obtener la fotografía visible de dicho individuo en dicho documento de identidad y

de los datos del lector óptico del documento de identidad;

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

(C) generar el primer dato aleatorio codificado mediante la aplicación de un proceso de codificación a dicha información de referencia representativa de la apariencia de dicha fotografía y a dicho primer dato aleatorio, y de la primera huella criptográfica;

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

el proceso de decodificación es un proceso complementario a partir de un proceso de

bosquejo de un algoritmo tipo “bosquejo seguro”;

el dato del lector óptico del documento de identidad es un dato como MRZ, código QR o PDF417;

el método también comprende una etapa (e) de inscripción de un autenticador, en particular de Fast Identity Online, FIDO, alliance.

La información de referencia representativa de una apariencia esperada de dicha fotografía es un dato de seguridad del tipo sello de foto digital.

De acuerdo con un segundo aspecto, la invención se relaciona con una unidad de autenticación fuerte que comprende un dispositivo cliente y un servidor conectado, caracterizado porque el dispositivo cliente y/o el servidor comprenden medios de procesamiento de datos configurados para:

extraer, mediante análisis de una imagen captada de un documento de identidad que represente al menos una fotografía de un individuo y un dato del lector óptico visible en dicho documento de identidad:

- una información candidata representativa de la apariencia de dicha fotografía como se ilustra en la imagen captada;

- dicho dato del lector óptico como se ilustra en la imagen captada;

calcular un primer dato decodificado mediante la aplicación de un proceso de decodificación a dicha información candidata representativa de la apariencia de dicha fotografía y al primer dato codificado, de tal manera que dicho primer dato decodificado coincide con un primer dato aleatorio si dicha información candidata representativa de la apariencia de dicha fotografía coincide con una información de referencia representativa de la apariencia de dicha fotografía, en donde el servidor tiene una huella criptográfica de una primera concatenación de dicho dato del lector óptico de dicho documento de identidad y dicho primer dato aleatorio, denominados primera huella criptográfica;

que verifica que:

- una huella criptográfica de una primera concatenación del dato extraído del lector óptico y del dato codificado coincida con dicha primera huella criptográfica en el servidor; y

- el dato biométrico de referencia y el dato biométrico candidato del individuo coincidan.

De acuerdo con un tercer y un cuarto aspectos, la invención se relaciona con un producto de programa informático que comprende instrucciones de código para la ejecución de un método de acuerdo con el primer aspecto de autenticación fuerte de un individuo, tras lo cual el proceso se ejecuta en una computadora; y un medio de almacenamiento legible por un equipo informático, tras lo cual un producto de programa informático comprende instrucciones de código para ejecutar un método de acuerdo con el primer aspecto de autenticación fuerte de un individuo.

DESCRIPCIÓN DE LAS FIGURAS

Otras características, propósitos y beneficios de la presente invención resultarán evidentes al leer la descripción detallada a continuación, en relación con las figuras adjuntas, dadas como ejemplos no limitantes y tras las cuales:

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

DESCRIPCIÓN DETALLADA

Arquitectura

La presente invención se relaciona con un método para la autenticación fuerte de un individuo que porta un documento de identidad, es decir, permite verificar que esta persona tiene en efecto la identidad mostrada en el documento 1, que incluye posiblemente un método para inscribir información de este documento de identidad 1.

El presente método se llama autenticación fuerte porque combina “algo que el individuo posee”, es decir, su documento de identidad 1, y “algo que el individuo tiene/conoce”, en este caso, una característica biométrica. De hecho, existen dos posibles niveles de fraude:

- el primero es la falsificación del documento de identidad, por ejemplo, mediante el cambio de la fotografía,
- el segundo es el robo de identidad, por ejemplo, el uso de un documento de identidad 1 válido por un ladrón que lo usa como propio.

El presente método permite detectar los dos niveles de fraude debido a la fuerte naturaleza de la autenticación.

Ventajosamente, el presente método es un método de “inscripción de un factor de autenticación”, es decir,

de adición o modificación de un medio para la autoautenticación (que puede elegirse entre una contraseña, un dispositivo de autenticación física y, en particular, un “autenticador FIDO”, y una dirección de correo electrónico, etc.) que después se usará de manera recurrente para la autenticación diaria. Por lo tanto, el método anterior se implementa típicamente después del primer uso de dicho factor de autenticación, y específicamente en el caso de perder un factor de autenticación anterior (que se menciona como un proceso de recuperación: que es el caso en donde el usuario desea autenticarse nuevamente a pesar de esta pérdida).

Por autenticador FIDO se entiende un dispositivo de seguridad FIDO (identidad rápida en línea) que cumple específicamente con un estándar de autenticación tal como U2F (2.º factor universal), FIDO2, protocolo de cliente a autenticador (CTAP, por sus siglas en inglés), etc.; p. ej., un dispositivo móvil (tal como el dispositivo 3, ver más abajo), una memoria USB, una tarjeta con chip, cada uno almacena un secreto (una clave privada/un par de claves públicas). Por lo tanto, el presente método se usa típicamente en el caso de perder un autenticador FIDO, pero se entenderá que es completamente adecuado para cualquier tipo de factor de identificación, e incluso podría usarse en cada autenticación para acceder a un servicio para el que se requiere un nivel de seguridad

máximo (p. ej., para enviar una transferencia bancaria, comprar una propiedad, etc.)

De una manera particularmente preferida, dicho autenticador que se inscribirá es el dispositivo cliente 3, que permite un proceso de inscripción simple y transparente, en donde el dispositivo 3 proporciona en la migración todos los datos de identificación necesarios, tal como, p. ej., una dirección MAC, y es capaz de enviar, al final de este proceso, un secreto (por ejemplo, un par de claves) que les permita actuar después de eso como autenticador del individuo.

Con referencia a la **Figura 1**, una arquitectura del sistema de autenticación se representa en la presente descripción para la implementación del presente método. Este sistema comprende al menos un documento de identidad 1, un servidor 2 y un dispositivo cliente 3 conectado al servidor 2 mediante una red 20, tal como la internet.

El documento de identidad 1 es un objeto personal para una persona (muchos individuos pueden tener cada uno un documento de identidad) y preferentemente constituye un documento oficial, emitido ventajosamente por un organismo gubernamental. Este documento puede adoptar numerosas formas tales como una tarjeta de identidad o un pasaporte, y posiblemente puede ser electrónico. Alternativamente, este puede ser cualquier documento elegido por el individuo o por un proveedor de servicios con valor probatorio para

el autenticador, es decir, un documento representativo de la identidad del individuo, que podría ser, p. ej., un pase de viaje, una tarjeta profesional, una credencial de identificación corporativa, una licencia o incluso un documento personalizado hecho por un organismo de administración de autenticadores que sería necesario para inscribir un nuevo autenticador, por analogía, con documentos provistos de bloqueos de seguridad que se requieren para hacer un par de claves.

De acuerdo con una modalidad, toma la forma de una tarjeta con chip (como una “tarjeta inteligente”) de dimensiones estándar y generalmente de PVC o policarbonato.

En todos los casos, el documento de identidad 1 comprende una superficie dura tras la cual se imprime una cierta cantidad de información y, en particular:

- una fotografía del individuo que es el titular de la tarjeta (y posiblemente de otros datos de “gráfico”, tales como la firma del individuo);
- y el dato del lector óptico (es decir, legible automáticamente, destinado para computadoras), como MRZ, código QR o PDF417 (usaremos el ejemplo de MRZ en el resto del documento, pero se entiende que esto no se impone este tipo de datos de lector óptico como límite);

- diversos datos alfanuméricos, llamados “datos visuales”, elegidos específicamente de entre:
 - o número completo del documento de identidad 1;
 - o fecha de caducidad;
 - o fecha de emisión;
 - o apellidos;
 - o nombre(s) de pila;
 - o nacionalidad;
 - o fecha de nacimiento;
 - o lugar de nacimiento;
 - o género;
 - o altura;
 - o dirección;
 - o etc.

El servidor 2 es un dispositivo seguro, remoto, típicamente perteneciente a una autoridad o a un proveedor de soluciones de seguridad. Comprende el medio de procesamiento de datos 21 (como un procesador) y el medio de almacenamiento de datos 22 (una memoria, p. ej., o un disco duro).

El dispositivo cliente 3 es un dispositivo local que comprende o se conecta al medio de captación óptico 30 (típicamente un dispositivo de foto o escáner), y adecuado para captar una imagen (del documento 1, como veremos). Además, comprende el medio de procesamiento de datos 31 y

el medio de almacenamiento de datos 32. El dispositivo cliente 3 y el servidor 2 ventajosamente comprenden interfaces de comunicaciones haciendo posible el diálogo remoto. Preferentemente, el dispositivo cliente 3 es un dispositivo personal del documento de identidad 1 que porta el individuo, p. ej., un dispositivo móvil del individuo (específicamente, como un teléfono inteligente).

Preferentemente, el dispositivo cliente 3 es capaz de generar un dato biométrico usando una característica biométrica del individuo. La característica biométrica puede ser, p. ej., la forma de la cara, una huella dactilar, una impresión de palma, un iris del individuo, etc. La extracción del dato biométrico se implementa al procesar la imagen de la característica biométrica que es una función de la naturaleza de la característica biométrica. La persona experta conoce diversos medios de procesamiento de imágenes para extraer el dato biométrico. Como un ejemplo no limitante, la extracción del dato biométrico puede comprender una extracción de puntos específicos o de una forma de una cara, en el caso donde la imagen es una imagen de la cara del individuo.

El dispositivo cliente 3 comprende o se conecta, en este contexto, a medios de captación biométricos, típicamente un sensor de imagen y, en una manera particularmente preferencial, estos medios de captación

biométricos son los medios de captación ópticos 30, p. ej., un dispositivo fotográfico adecuado para captar una fotografía de la cara en modo “selfi” (observamos que, alternativamente, podrían usarse medios de captación diferentes, tal como un sensor de huella dactilar).

En todos los casos, un dato biométrico de referencia usado para la autenticación del individuo es ventajosamente un dato registrado previamente en presencia de una autoridad (ver más abajo), o un dato que se origina en el documento de identidad 1, tal como una fotografía.

Observamos que el dispositivo 3 puede tomar muchas formas de modalidad. Más específicamente, y como se verá, es suficiente para la modalidad de la invención que el dispositivo cliente 3 sea capaz de obtener una imagen captada del documento de identidad 1, de una manera u otra, incluso indirectamente, y procesar esta imagen.

En todos los casos, como se explicó, el dispositivo cliente 3 puede captar una imagen de una imagen del documento de identidad 1, es decir, fotografiar una fotocopia en lugar del documento 1 directamente, o fotocopiar una fotocopia, etc. Como se verá, será suficiente que la imagen captada represente al documento 1. Se entenderá que el método presente no se limita a ninguna forma de obtener esta imagen, ni a ninguna manera específica (la imagen captada puede ser en blanco y negro, estar distorsionada, etc.).

Observamos que es completamente posible que otras entidades se conecten al servidor 2 y al dispositivo 3, en particular, servidores que implementan servicios que reciben la información producida por el dispositivo 3, es decir, servicios que requieren la autenticación del individuo, p. ej., un servidor bancario, un servidor de hotel, etc. Específicamente, podemos imaginar que tal servidor tiene una solución de autenticación clásica (p. ej., con un autenticador FIDO), e iniciará el presente método (contactando con el dispositivo 3) tras lo cual el usuario desea inscribir un nuevo factor de autenticación. Este servidor de servicios puede, p. ej., implementar un API dedicado al interrogatorio del servidor 2 para la implementación del presente método.

Como veremos, el presente método hace posible que este servicio no almacene cualquier información personal del individuo.

Sello de foto digital

En la siguiente parte de la presente descripción, el experto puede referirse a las solicitudes núms. FR1904375 y FR1904406 que describen los mecanismos que pueden usarse independientemente o en combinación en el contexto de la invención.

De una manera conocida, el presente método usa información representativa de una apariencia de una

fotografía (u otro componente gráfico del documento 1), es decir, un dato descriptivo de al menos un fragmento de esta fotografía tal como aparece, es decir, una “firma”, que permitirá comparaciones.

Por información de “referencia” se entiende información representativa de la apariencia “teórica” de la fotografía, es decir, como se espera. En contraste, por información “candidata” se entiende la información representativa de la apariencia registrada de la fotografía, es decir, como se ilustra en una imagen captada del documento 1. Entendemos que esta apariencia registrada no es, generalmente, completamente idéntica a la apariencia esperada, debido al hecho de las condiciones defectuosas inherentes a la captación de una imagen, y a la variabilidad de condiciones de disparo (Iluminación, movimiento, distancia, etc.).

No obstante, dicha información representativa de la apariencia es elegida de tal manera que si ambas fotografías tienen una apariencia que coincide (es decir, es la misma fotografía incluso si las condiciones de toma no son idénticas), después su información representativa coincide también (es decir, muestra una diferencia de acuerdo con una métrica dada menor que un umbral).

Por lo tanto, la información de referencia y la información candidata coinciden si, y solo si, la apariencia registrada y la apariencia esperada de la

fotografía coinciden, es decir, que es, en efecto, la misma fotografía, en otras palabras, que la fotografía impresa en el documento de identidad 1 no se ha alterado fraudulentamente. Esta verificación puede realizarse para cada característica gráfica, tal como una firma.

Como información representativa de la apariencia de la fotografía, podremos usar el “sello de foto digital” (DPS, por sus siglas en inglés) que usaremos como un ejemplo en la próxima sección de la presente solicitud, es decir, los datos de seguridad como se describe en las solicitudes citadas en la introducción, o más específicamente, la solicitud núm. EP3206192, con base en la posición de únicos puntos en la característica gráfica, o cualquier otra “firma” de un objeto gráfico tal como una fotografía.

El DPS de una fotografía es una característica de esa imagen que no es un modelo biométrico, y puede, p. ej., comprender un histograma de gradientes orientadas (de tal manera que hablamos de una característica de descriptor HOG). Alternativamente, puede usarse un algoritmo de clasificación del tipo que usa una red neuronal convolucional, también conocida mediante el acrónimo CNN, por sus siglas en inglés.

Inscripción

Al iniciar el método, suponemos que el dispositivo cliente 3 tiene al menos una imagen captada de dicho documento de identidad 1 que representa al menos una fotografía de un individuo y un dato del lector óptico visible en dicho documento de identidad 1 (en donde los datos personales individuales del individuo son legibles), y un dato biométrico candidato.

El dispositivo cliente 3 o el servidor 2 también necesitan tener un primer “dato codificado” (señalado como SSKD) obtenido mediante la aplicación de un proceso de codificación de la información DPS de la referencia representativa de la apariencia de la fotografía de dicho individuo visible en el dicho documento de identidad 1 y para un primer dato aleatorio (señalado como RNGD). En la práctica, el servidor 2 generalmente almacena este primer dato codificado (al menos inicialmente).

El servidor 2 solo necesita tener una huella criptográfica de una primera concatenación del dato del lector óptico del documento de identidad 1 y el primer dato RNGD aleatorio.

Posiblemente, el dispositivo cliente 3 o el servidor 2 pueden tener un cifrado con una huella criptográfica de una segunda concatenación del dato del lector óptico del documento de identidad 1 y del primer dato RNGD aleatorio, diferente de la primera

concatenación del dato biométrico de referencia de dicho individuo, y posiblemente otros datos personales (nuevamente, frecuentemente la encriptación se almacena en el servidor 2).

Entendemos que ninguno de estos datos puede usarse en sí (en particular, si todos están almacenados en el servidor 2) porque:

- dicho primer dato SSKD codificado no permitirá recuperar en sí la información DPS de referencia o el primer dato RNGD aleatorio;
- la huella criptográfica de una primera concatenación del dato del lector óptico del documento de identidad 1 y del primer dato RNGD aleatorio es una huella simple que no lleva información;
- el posible cifrado del dato biométrico no es legible para una persona sin la clave.

En una modalidad preferida, el método comprende una etapa previa (a0) “de inscripción” que permite integrar a una persona y su documento de identidad individual 1 y generar los datos que el servidor 2 y/o el dispositivo cliente 3 deben tener. En la presente descripción, es necesario hacer la distinción con la inscripción de un factor de autenticación que puede ser el resultado del presente método.

Esta etapa (a0) puede implementarse mucho tiempo antes de que el resto del método, y no tiene que repetirse en cada instancia del método (Hay que reseñar que podemos especificar repetirla de vez en cuando por motivos de seguridad o para actualizar la información personal, pero permanece opcional). Por lo tanto, podemos considerar que los datos de referencia anteriores son predefinidos para la implementación del método.

Este proceso de inscripción de los datos del documento de identidad 1 del individuo puede ejecutarse mediante el servidor 2 o mediante el servidor de una autoridad gubernamental, y después los datos obtenidos se transmiten al servidor 2 y/o al dispositivo cliente 3.

La inscripción comienza con una etapa (A) para obtener una fotografía visible de dicho individuo en el dicho documento de identidad 1 del dato del lector óptico del documento de identidad 1 y, si corresponde, del dato biométrico de referencia de dicho individuo.

Esta etapa (A) puede implementarse por sí misma mediante una imagen del dicho documento de identidad 1 (como se explicará para el proceso de autenticación), pero, de manera preferencial, para evitar los problemas de digitalización y pérdida de calidad, estos datos (es decir, la fotografía, el dato del lector óptico y/o el dato biométrico de referencia) se manejan directamente, en particular si la inscripción es realizada por una

autoridad gubernamental. Esto, además, hace que sea posible actualizar los datos. Ver más abajo.

En la etapa (B), como se explicó, la extracción mediante el análisis de la información de referencia (señalada como DPS por conveniencia, aunque como se explicó, el presente método no se limita al sello de foto digital) representativa de la apariencia de la fotografía, se ejecuta mediante un algoritmo conocido.

Después, en una etapa (C), se genera el primer dato RNGD aleatorio para calcular el primer dato codificado (señalados como SSKD para SSK-DATA por conveniencia, aunque, como se explicó, el presente método no se limita a un bosquejo seguro) mediante la aplicación de un proceso de codificación a dicha información DPS de referencia representativa de la apariencia de dicha fotografía y a dicho primer dato RNGD aleatorio, es decir, $SSKD = \text{enc}(DPS, \text{RNGD})$.

El primer dato RNGD aleatorio es, como su nombre lo indica, un dato de valor aleatorio que proporcionan aleatoriedad, que es importante porque su conocimiento permitirá probar que realmente se tiene el documento de identidad 1.

Preferentemente, el proceso de decodificación es un proceso de bosquejo de un algoritmo como “bosquejo seguro”. Este proceso de bosquejo es conocido por el experto. Fue descrito específicamente en el documento

“Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data”, por Dodis et al. (Ver la definición 3 dada en la página 11 de este documento).

Otros procesos de codificación pueden usarse, sin embargo, por la unidad de procesamiento 4 y en lugar de un proceso de bosquejo (p. ej., proceso de algoritmo como “extractor difuso” y, generalmente, lógica difusa.

Hay que reseñar que el proceso de codificación puede aplicarse directamente a dicha información representativa de referencia de la apariencia de la fotografía, pero también indirectamente, es decir, a los datos derivados de esta información de referencia para añadir entropía. Por ejemplo, como datos derivados podemos usar una combinación de información de referencia con el dato del lector óptico, específicamente un cierto número de primeros bits de su huella criptográfica (ver más abajo). Particularmente, esta combinación puede ser una “exclusiva o”, es decir, $XOR(DPS;HMRZ)$, en donde HMRZ son los n primeros bits de la huella criptográfica del dato del lector óptico (en el ejemplo donde se trata de MRZ) donde n es el número de bits de información de referencia (el mismo número de bits es necesario para el XOR).

En todos los casos, el proceso de codificación permite “enmascarar” el primer dato RNGD aleatorio por el resultado del procesamiento DPS de la fotografía, pero de

manera recuperable, mediante un proceso de decodificación complementario al proceso de codificación.

Cuando el proceso de codificación usado para la inscripción es un proceso de bosquejo de un algoritmo tipo “bosquejo seguro”, el proceso de decodificación es el proceso de recuperación en el mismo algoritmo como “bosquejo seguro”. Tal proceso de recuperación también es conocido por el experto (ver la definición 3 dada en la página 11 del documento “Fuzzy Extractors: How to Generate...” citado anteriormente).

Más específicamente, si observamos como $DpsRef$ la información de referencia y como $DpsC$ una información candidata (con $SSKD = enc(RNGD, DpsRef)$), después los procesos de codificación y decodificación son de tal manera que si $DpsCand$ está lo suficientemente cerca de $DpsRef$ (es decir, diferente por menos de un umbral, que normalmente es el caso si extraemos la información representativa de la misma fotografía que se usó para generar la información de referencia, incluso si observamos que sigue siendo imposible que los dos valores coincidan, siempre tendremos $[DpsCand - DpsRef] > 0$), mientras que el primer dato decodificado es igual al primer dato RNGD aleatorio.

Si, por el contrario, $DpsCand$ no está lo suficientemente cerca de $DpsRef$, después el primer dato decodificado no tiene el valor correcto para el primer dato aleatorio.

Matemáticamente, el proceso de decodificación proporciona, para el primer dato SSKD codificado y para un valor de información candidato $DpsRef$, “el valor $x=dec(SSKD, DpeCand)$ de tal manera que exista un valor ε para el estándar menor que un umbral dado que verifica $SSKD=enc(x, DpsCand+\varepsilon)$ ”, en donde x es igual al valor del primer valor RNGD aleatorio, si en efecto tenemos $DpdCand+\varepsilon=DpsRef$.

Se recordará que tales procesos de codificación y decodificación son conocidos por el experto, y pueden realizarse de numerosas maneras. Además, también será posible incrementar la entropía del dato codificado mediante la aplicación del proceso de codificación a más datos además de la información representativa de la apariencia de dicha fotografía y dicho primer dato aleatorio.

Por último, en una etapa (D), lo siguiente se almacena en el medio de almacenamiento de datos 22 del servidor 2 y/o el medio de almacenamiento de datos 32 del dispositivo cliente 3 (si corresponde después de la transmisión):

- dicho primer dato SSKD codificado;
- la huella criptográfica de una primera concatenación del dato del lector óptico del documento de identidad 1 y del primer dato RNGD aleatorio;

- el cifrado potencial con la huella criptográfica de una segunda concatenación del dato del lector óptico del documento de identidad 1 y del primer dato RNGD aleatorio, diferentes de la primera concatenación, al menos en el dato biométrico de referencia de dicho individuo.

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

Por huella criptográfica, o hash, entendemos el resultado de una función hash encriptada predeterminada.

Preferentemente, la primera y segunda concatenaciones coinciden con concatenaciones en dos direcciones diferentes, por ejemplo, MRZ|RNGD para la primera concatenación y RNGD|MRZ para la segunda concatenación, pero podemos usar cualquier otra construcción, tal como dos concatenaciones en el mismo orden, pero que incluyen un carácter predeterminado en el medio, p. ej., MRZ|1|RNGD y MRZ|2|RNGD.

Se entiende que el dato del lector óptico del documento de identidad 1 y el primer dato RNGD aleatorio pueden considerarse como patrones de bits. El número de bits en la concatenación es, por lo tanto, la suma de los

respectivos números de bits del dato del lector óptico del documento de identidad 1 y del primer dato RNGD aleatorio.

Por conveniencia, observamos como la primera huella criptográfica dicha huella criptográfica de la primera concatenación ($h(\text{MRZ}|\text{RNGD})$ en particular), y como la segunda huella, la huella criptográfica de la segunda concatenación ($h(\text{RNGD}|\text{MRZ})$ en particular).

El ingenio de estas concatenaciones múltiples hace posible la formación de huellas más completamente independientes usando los mismos datos. De hecho, conociendo la primera huella (que se almacena en la memoria 22, y que, por lo tanto, un pirata informático podría obtenerla), no es posible obtener la segunda huella. Sigue siendo necesario, para obtenerla, tener el valor del primer dato RNGD aleatorio, que solo puede recuperarse al tener la información de referencia.

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

La primera huella puede asociarse en el servidor 2 con un descriptor del estado del documento de identidad 1, p. ej., “verdadero”, “vencido” o “falso”.

Hay que reseñar que el proceso de inscripción puede repetirse en intervalos regulares para actualizar los datos personales. Una entidad gubernamental será capaz de recuperar datos recientes y fiables. Además, un documento de identidad 1 solo tiene una vida útil limitada, y debe renovarse periódicamente.

De acuerdo con una modalidad preferida, el dispositivo cliente 3 o el servidor 2 tiene ventajosamente (en el lugar del cifrado del dato biométrico de referencia) un segundo dato codificado (señalado como SSKT para SSK-TEMPLATE) obtenido mediante la aplicación de un proceso de codificación (típicamente, el mismo proceso de codificación que el de un primer dato codificado) al dato biométrico de referencia y al segundo dato RNGD aleatorio (señalado como RNGT). y el servidor 2 también tiene un segundo dato criptográfico construido usando el segundo dato RNGDT aleatorio. Nuevamente, todos estos datos pueden almacenarse (al menos, inicialmente) en el medio de almacenamiento de datos 22 del servidor 2 (y asociarse con otros datos).

Dicha huella criptográfica construida usando el segundo dato RNGT aleatorio, denominada tercera huella criptográfica, puede ser una huella criptográfica directamente del segundo dato RNGT aleatorio, o de cualquier función (p. ej., una concatenación) del segundo dato RNGT aleatorio y de otros datos, ventajosamente de la primera huella criptográfica (la huella criptográfica de

una primera concatenación del dato del lector óptico del documento de identidad 1 y del primer dato RNGD aleatorio).

Entendemos que ninguno de estos datos puede usarse, nuevamente, en sí, porque:

- dicho primer dato SSKD codificado no permitirá recuperar, por sí solo, el dato biométrico de referencia o el primer dato RNGT aleatorio;
- la huella criptográfica construida que usa el segundo dato aleatorio es una huella simple y no aporta ninguna información.

En tal modalidad, la etapa de inscripción (a0) puede comprender, además:

- en la etapa (A) o en la etapa (B), la obtención de dicho dato biométrico de referencia (señalado como TempRef para la plantilla de referencia), por ejemplo, a partir de una fotografía del documento de identidad 1;
- en la etapa (C), la generación del segundo dato RNGT aleatorio para calcular el segundo dato SSKT codificado mediante la aplicación de dicho proceso de codificación, es decir, $SSKT = \text{enc}(\text{TempRef}, \text{RNGT})$;
- en la etapa (D), el almacenamiento en el medio de almacenamiento de datos 22 del

servidor 2 y/o el medio de almacenamiento de datos 32 del dispositivo cliente 3 (si corresponde, después de la transmisión) de dicho segundo dato SSKT codificado y de la huella criptográfica construida usando el segundo dato RNGT aleatorio.

Hay que reseñar que estas acciones complementarias vinculadas con la inscripción biométrica pueden implementarse nuevamente en las etapas (A') a (D'), es decir, no necesariamente de manera simultánea con las acciones vinculadas a la inscripción del documento de identidad 1.

Además, sigue siendo posible implementar un proceso de autenticación fuerte del individuo sin necesidad de encriptar el dato biométrico de referencia o el segundo dato RNGT aleatorio y el segundo dato SSKT codificado, específicamente almacenándolos directamente en el dispositivo cliente 3 (texto sin formato), concretamente en un servidor dedicado a la biometría como WebBIO, ver más abajo.

Autenticación

En la actualidad, suponemos que la inscripción se ejecutó con éxito y que el documento de identidad puede usarse actualmente.

En una modalidad preferida, el proceso de autenticación comienza con una etapa (a) de captación, de una manera u otra (p. ej., mediante el medio de captación 30 del dispositivo cliente 3) de una imagen del documento de identidad 1, la imagen que representa al menos la fotografía del individuo y del dato del lector óptico del documento de identidad 1 (el MRZ) visible en dicho documento de identidad 1. Preferentemente, dicha imagen representa a todo el documento de identidad 1, al menos todo un lado. Como se explicó, puede ser necesario captar más imágenes, p. ej., para ver todos los lados.

Típicamente, es el individuo que toma una foto de su documento de identidad 1 con su dispositivo móvil, si es necesario, previa solicitud emitida por el servidor que desea una autenticación fuerte (p. ej., para el servicio desde el cual inició un proceso de recuperación, específicamente a través de un dispositivo API dedicado).

Con referencia al “nuevo” dato biométrico candidato, este puede obtenerse durante la etapa anterior (A). Más específicamente, una vez que se capta la imagen del documento de identidad 1, el servidor 2 (o, nuevamente, el servidor de terceros) después puede reclamar la captación de dato biométrico candidato.

Es importante entender que si la etapa de inscripción (a0) puede implementarse semanas antes de la autenticación, la etapa (a), en el peor de los casos, se

implementa varios minutos antes del reinicio del proceso, para garantizar la “frescura” del dato biométrico candidato.

Por lo tanto, la etapa (A) ventajosamente comprende la generación del dato biométrico candidato usando una característica biométrica proporcionada por el medio de captación biométrico del dispositivo cliente 3 (es decir, típicamente el medio de captación óptico 30). Esto significa, por ejemplo, que el individuo primero toma una fotografía de su documento de identidad 1, después una imagen de su cara.

Para garantizar la frescura del dato candidato, la etapa (a) puede comprender el marcar la hora de registro del dato biométrico candidato mediante una marca de hora de registro.

El experto conocerá cómo implementar tal marca de hora registro usando técnicas conocidas, y ventajosamente, usamos como un marcador de tiempo un número usado una vez (es decir, un número arbitrario, es decir, aleatorio, usado una sola vez).

El propósito del resto del proceso es verificar que la etapa (a) se haya ejecutado correctamente como se describió anteriormente, y que no tenemos una falsificación (p. ej., una imagen modificada fraudulentamente) o un robo de identidad (una persona que no es el portador del documento de identidad 1).

En una etapa (a), el medio de procesamiento de datos 21, 31 del dispositivo cliente 3 o del servidor 2, analiza la imagen a extraerse:

- una información candidata representativa (DPS) de la apariencia de la fotografía como se ilustra en la imagen captada;
- los datos del lector óptico del documento de identidad 1.

La extracción de la información candidata comprende la identificación de la fotografía que aparece en la imagen y la obtención de la información candidata de la misma manera que se obtuvo la información de referencia durante la inscripción. La identificación de la fotografía puede hacerse usando modelos y máscaras (de hecho, los documentos de identidad siempre tienen la misma organización) y, por lo tanto, el análisis de la imagen puede comprender el reconocimiento de un contorno del documento de identidad 1, la reformulación de este contorno y la aplicación de máscaras predeterminadas. Para hacer esto, las redes neuronales convolucionales adaptadas podrán inteligentemente. Similarmente, con respecto al dato del lector óptico, existen algoritmos que hacen posible su extracción automática, especialmente porque las zonas como MRZ están especialmente especificadas para que una computadora pueda leerlas fácilmente.

Una vez que la fotografía ha sido “aislada” en la imagen, aplicamos los mismos algoritmos que los que se aplicaron a la fotografía original para obtener información candidata representativa de la apariencia de la fotografía como se representa.

Se entiende que la información de referencia y la información candidata debe obtenerse de manera idéntica para que puedan compararse.

De acuerdo con una primera modalidad, la etapa (a) se implementa mediante el servidor 2, de acuerdo con la descripción en la solicitud núm. FR1904375. Se supone que este último almacena el primer dato codificado, y la etapa (a) comprende, en este contexto, la transmisión al servidor 2 de dicha imagen captada del documento de identidad 1. De acuerdo con una segunda modalidad, la etapa (a) se implementa directamente mediante el dispositivo cliente 3, de acuerdo con la descripción en la solicitud núm. FR1904406.

Preferentemente, en esta segunda modalidad, la etapa (b) comprende la interrogación del servidor 2 para recuperar al menos dicho primer dato SSKD codificado si se almacenan en este servidor 2, por ejemplo, proporcionándole la huella criptográfica del documento 1 (en donde este identificador se obtiene del MRZ, p. ej.): el servidor 2 transmite el primer dato codificado asociado con la huella recibida. Señalamos que, alternativamente,

dicho primer dato codificado puede haberse proporcionado mucho antes y almacenarse desde ese momento en el medio de almacenamiento de datos 32 del dispositivo cliente 3.

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

Como se explicó, el proceso de decodificación (y el proceso de codificación) es de tal manera que dicho primer dato decodificado corresponde al primer dato RNGD aleatorio si dicha información candidata representativa de la apariencia de dicha fotografía coincide con la información de referencia representativa de la apariencia de dicha fotografía. En otras palabras, si la información de referencia y la información candidata están lo suficientemente cerca, el valor decodificado coincidirá con el valor RNGD aleatorio usado para obtener este primer valor SSKD codificado.

En general, el resultado de una comparación de la información candidata y de la información de referencia debe mostrar que son idénticas o, al menos, tienen una diferencia que es menor que un umbral predeterminado. Por ejemplo, para características gráficas como fotografías,

los datos de seguridad como el sello de foto digital coinciden si difieren en menos del 10 %.

Por lo tanto, se entiende que el valor del primer dato aleatorio “enmascarado” por el DPS puede recuperarse si el usuario tiene una fotografía idéntica a la usada en el momento de la inscripción de la que se toma la información de referencia.

En una etapa (d), los medios de procesamiento de datos 21, 31 verifican que una huella criptográfica de una primera concatenación del dato extraído del lector óptico y del dato decodificado coinciden con la huella criptográfica de la primera concatenación del dato del lector óptico del documento de identidad 1 y del dato aleatorio almacenado en el medio de almacenamiento de datos 22 del servidor 2.

En otras palabras, el servidor 2 o el dispositivo cliente 3 intentan reconstituir la primera huella ejecutando la misma concatenación del dato extraído del lector óptico y del primer dato decodificado.

Si:

- el dato extraído del lector óptico coincide con el dato del lector óptico usado durante la inscripción; y
- el primer dato decodificado coincide con el primer dato RNGD aleatorio;

Después, la primera concatenación dará exactamente el mismo resultado y volveremos a tener nuevamente la primera huella.

En todos los demás casos, la entropía de las funciones hash criptográficas lleva a un resultado muy diferente. Si el documento 1 se ha alterado (por ejemplo, sustituyendo la fotografía), después la información candidata que coincide y la información de referencia no coincidirán; por lo tanto, se obtiene un valor falso para el aleatorio uno y, por lo tanto, para la primera huella, y la autenticación será rechazada.

Hay que reseñar que, si es el dispositivo cliente 3 que ha implementado hasta ese momento las etapas descritas, sería necesario informar al servidor 2 del resultado de la verificación.

Sin embargo, puede conocerse el valor correcto de la primera huella, este no sería de una autenticación anterior del individuo. Esta es la razón por la que el dispositivo cliente 3 demostrará ventajosamente que obtuvo esta primera huella correctamente, es decir, no interactivamente, es decir, con solo una “marcha” de la información del dispositivo cliente 3 al servidor 2, y sin un “retorno”. Y, especialmente como se explicó, el servidor 2 no recibirá el primer dato RNGD aleatorio o la información candidata representativa de la apariencia de dicha fotografía, ni el dato del lector óptico (ni ningún

dato que haga posible retornar a este último), incluso puede ser posible para que el servidor 2 conozca con certeza que la primera huella se calculó correctamente. Además, todos los datos transmitidos no son confidenciales, y podrían interceptarse sin que esto suponga un problema.

Para hacer esto, en la etapa (d), el medio de procesamiento de datos 31 del dispositivo cliente 3 que actúa como una entidad de prueba genera ventajosamente una prueba de conocimiento cero del cálculo de dicha huella criptográfica que usa la primera concatenación del dato extraído del lector óptico y el primer dato decodificado, es decir, que la primera huella criptográfica se calculó efectivamente, y correctamente, en donde dicha prueba se transmite mediante el dispositivo cliente 3 al servidor 2, dicha prueba de conocimiento cero con la huella criptográfica calculada.

Más específicamente, dicha prueba de conocimiento cero garantiza la siguiente información: “dada una huella criptográfica H , existe un dato del lector óptico y un primer dato RNGD aleatorio (el dato decodificado) de tal manera que su primera concatenación tiene para la huella esta huella criptográfica H dada”. El experto puede consultar el documento núm. FR1904406 para obtener más información.

Por lo tanto, el medio de procesamiento de datos 21 del servidor 2 solo debe verificar que la prueba de

conocimiento cero es válida y que la huella criptográfica recibida coincide con la de la primera concatenación de un dato del lector óptico de dicho documento de identidad 1 y desde un primer dato aleatorio que tiene el servidor 2.

Si la prueba no es válida, después la primera huella criptográfica no se obtuvo válidamente y, por lo tanto, potencialmente, el individuo no tiene el documento de identidad y está intentando robar la identidad. Si la prueba es válida, pero la huella criptográfica recibida no coincide con la que posee la entidad de verificación 2, después el primer dato decodificado no coincide con el primer aleatorio, o el dato extraído del lector no es el original, es decir, el documento de identidad 1 se falsificó (a nivel de la fotografía o del dato del lector óptico). Puede emitirse una precaución por fraude.

En la etapa (d), los medios de procesamiento de datos 21, 31 también verifican que el dato biométrico de referencia y el dato biométrico candidato del individuo coincidan; por lo tanto, el proceso implica una comparación entre el dato biométrico candidato y el dato biométrico de referencia. Hay que reseñar que puede involucrarse un control del proceso biométrico para verificar, p. ej., que el dato biométrico de referencia no es el resultado de una amenaza (p. ej., una máscara facial o un dedo de resina).

Esta etapa puede implementarse de numerosas maneras conocidas usando el dispositivo cliente 3, el servidor 2, o un servidor biométrico dedicado.

Notamos de que todas las combinaciones son posibles: cada uno del dispositivo cliente 3 y del servidor 2 puede implementar las verificaciones 0, 1 o 2 de la etapa (d).

Es, por ejemplo, completamente posible que el servidor 2 reciba en la etapa (a), tanto la imagen captada del documento de identidad 1 como el dato biométrico candidato. De una manera especialmente preferida, incluso podemos imaginar que durante la etapa (a), el servidor 2 recibe primero la imagen captada del documento de identidad 1, después solicita al dispositivo 1 el dato biométrico candidato que después se le transmiten por segunda vez.

Alternativamente, o, además, el servidor 2 o el dispositivo 3 pueden transmitir (si corresponde, retransmitir) el dato biométrico candidato a un servidor confiable dedicado a la biometría, almacenando el dato biométrico de referencia, que implementan la comparación y envían el resultado al servidor.

En todos los casos, la implementación de la comparación típicamente comprende el cálculo de cualquier distancia entre los datos, cuya definición varía en base al dato biométrico en cuestión. El cálculo de la distancia comprende el cálculo de un polinomio entre los

componentes del dato biométrico y, ventajosamente, el cálculo de un producto escalar.

Por ejemplo, en caso de que el dato biométrico se obtenga usando imágenes del iris, una distancia usada clásicamente para comparar dos datos es la distancia de Hamming. En el caso donde los datos biométricos se obtengan usando imágenes de la cara del individuo, es común usar la distancia euclidiana. Este tipo de cálculo de distancias es conocido por el experto y no se describirá con más detalle.

En caso de que el servidor 2 o el dispositivo cliente 3 almacenen un cifrado del dato biométrico de referencia de dicho individuo con una huella criptográfica de una segunda concatenación del dato del lector óptico del documento de identidad 1 y del dato aleatorio (la segunda huella criptográfica), la etapa (d) comprende el descifrado de este dato biométrico de referencia, mediante la huella criptográfica de una segunda concatenación del dato extraído del lector óptico y del dato decodificado (cada uno obtenido en la etapa (d)) para poder hacer la comparación. Nuevamente, el experto puede referirse a la solicitud núm. FR1904375.

En caso de que un segundo dato SSKT codificado obtenido mediante la aplicación de un proceso de codificación a un dato biométrico de referencia y a un segundo dato RNGT aleatorio y una huella criptográfica construida usando el segundo dato RNGT aleatorio, 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 se hizo para la información como DPS en la fotografía.

Nuevamente, debido a que el proceso de codificación usado para la inscripción es un proceso de bosquejo de un algoritmo tipo “bosquejo seguro”, el proceso de decodificación es el proceso de recuperación en el mismo algoritmo tipo “bosquejo seguro”, y el experto puede usar otros procesos.

Matemáticamente, el proceso de decodificación proporciona, para el segundo dato SSKD codificado y para un candidato TempCand, “el valor $x = \text{dec}(\text{SSKT}, \text{TempCand})$ de tal manera que existe un valor ε para el estándar menor que un umbral dado que verifica $\text{SSKD} = \text{enc}(x, \text{TempCand} + \varepsilon)$, en donde x es igual al valor del primer valor RNGT aleatorio, si en efecto tenemos $\text{TempCand} + \varepsilon = \text{TempRef}$ ”.

Por lo tanto, la etapa (c) también comprende ventajosamente el cálculo mediante los medios de procesamiento de datos 21, 31 del servidor 2 o del dispositivo cliente 3.

- un segundo dato decodificado mediante la aplicación de un proceso de descodificación a dicho dato biométrico candidato y al segundo dato codificado (nuevamente, el dato codificado es de tal manera que el

segundo dato decodificado coincide con el segundo dato RNGT aleatorio si dicho dato biométrico candidato coincide con el dato biométrico de referencia);

- una huella criptográfica construida usando el segundo dato decodificado (se entiende que esta huella criptográfica debe construirse de la misma manera que la tercera huella criptográfica usando el segundo dato RNGT aleatorio, específicamente la huella criptográfica de una concatenación del segundo dato RNGT aleatorio y de la primera huella criptográfica).

En todos los casos, la comparación del dato biométrico puede hacerse mediante el medio de procesamiento de datos 21 del servidor 2, pero es preferible que se haga en el dispositivo cliente 3 para garantizar completamente la privacidad del individuo.

Para hacer esto, puede usarse un nuevo protocolo criptográfico en donde se genera una “prueba” de que el dato biométrico candidato y el dato biométrico de referencia coinciden, en donde esta prueba no revela nada más que el hecho de que el productor de la prueba tiene, en efecto, estos datos biométricos.

En otras palabras, podemos usar hasta dos pruebas de no divulgación de conocimiento:

- la primera prueba es la prueba válida del cálculo de dicha huella criptográfica usando la primera concatenación del dato extraído del lector óptico y del primer dato decodificado;
- la segunda prueba es una prueba del hecho de que el dato biométrico candidato y el dato biométrico de referencia coinciden.

En este caso, la etapa (d) comprende ventajosamente la generación mediante el medio de procesamiento de datos 31 del dispositivo cliente 3 de la prueba de conocimiento cero del 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 usando el segundo dato decodificado (es decir, el segundo dato RNGT aleatorio) están en efecto en posesión del productor de la prueba. Una vez más, la prueba pretende garantizar que la tercera huella criptográfica fue eficaz y correctamente calculada.

Más específicamente, dicha prueba de conocimiento cero garantiza la siguiente información: “dada una huella criptográfica T , existe un segundo dato RNGT aleatorio (y, si corresponde, un dato del lector óptico) de tal manera que una función dada de este segundo dato RNGT aleatorio tenga como huella esta huella criptográfica dada”. En el caso específico donde la

tercera huella es la huella criptográfica de una concatenación del segundo dato RNGT aleatorio y de la primera huella criptográfica, la afirmación de garantía es la siguiente: “dada una huella criptográfica T, existe un segundo dato RNGT aleatorio y otro dato criptográfico H de tal manera que una concatenación de este segundo dato RNGT aleatorio y de esta otra huella criptográfica H tiene para la huella dicha huella criptográfica T dada”.

La segunda prueba de conocimiento cero puede generarse de la misma manera que la primera prueba de no divulgación de conocimiento, y transmitirse al servidor 2 con la nueva huella criptográfica calculada (la tercera huella), ver nuevamente el documento núm. FR 1904406.

Si todas las verificaciones se realizan con éxito, el servidor 2 aprueba la autenticación del individuo y típicamente transmite un “token” al servidor que solicitó la autenticación/recuperación del individuo. Más específicamente, si el proceso es un proceso de inscripción para un autenticador, en particular FIDO, después se ejecuta esta inscripción. En otras palabras, el método comprende ventajosamente una etapa para inscribir un autenticador. Si este autenticador que se va a inscribir va directamente al dispositivo 3, puede presentar un secreto o incluso presentar la clave pública que coincide con una de un par de claves para las cuales posee la clave privada, lo

que hace posible su uso como un autenticador del individuo. Como alternativa, podría recibir tal secreto.

Se señalará que en lugar de implementar simultáneamente la verificación del documento 1 y la verificación biométrica (es decir, usando las mismas etapas (a) a (d)), es completamente posible implementar los métodos uno tras otro, es decir, que habrá etapas (a') a (d') para el proceso implementado en segundo lugar (en particular, la verificación biométrica, incluso si es posible el orden inverso).

Se entiende que este proceso limita, en la mayor medida posible, la necesidad de información personal y las posibles pérdidas asociadas, al tiempo que garantiza el máximo nivel de seguridad.

Servidor

De acuerdo con un segundo aspecto, se propone la unidad del servidor conectado 2 y del dispositivo cliente 3 para la implementación del proceso de acuerdo con el primer aspecto, es decir, la autenticación del individuo que porta un documento de identidad.

Como se explicó, el dispositivo cliente 3 y/o el servidor 2 que comprenden el medio de procesamiento de datos 21, 31 (de acuerdo con el caso donde el servidor 2 procesa directamente los datos, o si es el dispositivo 3 el que realiza este procesamiento y transmite al servidor

2 una prueba de conocimiento cero de su ejecución correcta), configurado para:

- extraer, mediante análisis de una imagen captada del documento de identidad 1 que representa al menos una fotografía de un individuo y un dato del lector óptico visible en dicho documento de identidad 1:
 - o una información candidata representativa de la apariencia de dicha fotografía como se ilustra en la imagen captada;
 - o dicho dato del lector óptico como se ilustra en la imagen captada;
- calcular un primer dato decodificado mediante la aplicación de un proceso de decodificación a dicha información candidata representativa de la apariencia de dicha fotografía y al primer dato codificado, de tal manera que dicho primer dato decodificado coincide con un primer dato aleatorio si dicha información candidata representativa de la apariencia de dicha fotografía coincide con una información de referencia representativa de la apariencia de dicha fotografía, en donde el servidor tiene una huella criptográfica de una primera concatenación de dicho dato

del lector óptico de dicho documento de identidad 1 y dicho primer dato aleatorio, denominados primera huella criptográfica;

- verificar que:
 - una huella criptográfica de una primera concatenación del dato extraído del lector óptico y del dato decodificado coincide con dicha primera huella criptográfica en el servidor 2; y
 - el dato biométrico de referencia y el dato biométrico candidato del individuo coinciden.

El dispositivo cliente 3 también puede comprender (o estar conectado a) un medio de captación óptico 30 y/o un medio de captación biométrico, en particular un medio de captación óptico 30, para la captación del dato biométrico candidato.

Producto de programa informático

De acuerdo con un tercer y un cuarto aspectos, la invención se relaciona con un producto de programa informático que comprende instrucciones de código para la ejecución (en particular en el medio de procesamiento de datos 21 del servidor 2 y el medio de procesamiento de datos 31 del dispositivo cliente 3) de un método de acuerdo con el primer aspecto de la invención (una

memoria 22 del servidor 2 y una memoria 32 del dispositivo cliente 3) en el cual se encuentra dicho producto de programa informático.