

REIVINDICACIONES

1. Método para autenticación fuerte de un individuo implementada mediante un servidor (2) y un
5 dispositivo cliente conectado (3);

el dispositivo cliente (3) que tiene un dato biométrico candidato del individuo y una imagen captada de un documento de identidad (1) que representa al menos una
10 fotografía de dicho individuo y un dato del lector óptico visible en dicho documento de identidad (1), y el servidor (2) tiene una huella criptográfica de una primera concatenación de dicho dato del lector
15 óptico de dicho documento de identidad (1) y de un primer dato aleatorio, la denominada huella criptográfica;

en donde el método se caracteriza porque comprende la implementación mediante los
20 medios de procesamiento de datos (21, 31) del servidor (2) y/o del dispositivo cliente (3) de las etapas de;

(b) extraer, mediante el análisis de dicha imagen captada de dicho
25 documento de identidad (1):

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

5 o 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

10 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

15 si dicha información candidata representativa de la apariencia de dicha fotografía coincide con una información de referencia representativa de la apariencia de

20 dicha fotografía;

(d) verificar que:

- una huella criptográfica de una primera concatenación del dato extraído del lector óptico y del

25 dato decodificado coincida con

dicha primera huella criptográfica
en posesión del servidor (2); y

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

5

2. Un método de acuerdo con la reivindicación
1, que comprende una etapa (a) de captación previa de
dicha imagen 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) mediante el medio de captación óptico (30)
del dispositivo cliente (3), y la generación del dato
biométrico candidato usando una característica biométrica
proporcionada mediante el medio de captación biométrico.

10

15

3. Un método de acuerdo con la reivindicación
2, en donde los medios de captación biométrica son el
medio de captación óptico (30) del dispositivo cliente
(3), en donde el dispositivo cliente (3) es un
dispositivo electrónico personal de dicho individuo, en
particular del tipo dispositivo móvil o tarjeta con chip.

20

4. Un método de acuerdo con cualquiera de las
reivindicaciones 1 a 3, en donde el servidor (2) o el
dispositivo (3) 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 (1) y del primer dato aleatorio,

25

diferente 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
5 extraído del lector óptico y del primer dato decodificado.

5. Un método de acuerdo con cualquiera de las reivindicaciones 1 a 3, en donde el servidor (2) tiene una huella criptográfica construida usando un segundo dato aleatorio, denominado tercera huella criptográfica;
10 la etapa (c) comprende el cálculo mediante los medios de procesamiento de datos (21, 31) del servidor (2) o del dispositivo cliente (3) de un segundo dato decodificado mediante la aplicación de un proceso de decodificación a dicho dato biométrico candidato y a un segundo dato
15 codificado, de tal manera que dicho 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) donde el dato biométrico de referencia y el dato
20 biométrico candidato del individuo coinciden comprende la verificación de 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 coincide con dicha tercera
25 huella criptográfica en posesión del servidor (2).

6. Un método de acuerdo con cualquiera de las reivindicaciones 1 a 5, en donde la etapa (a) comprende la recepción mediante el servidor (2) de la imagen captada de dicho documento de identidad (1) y del dato biométrico candidato del dispositivo cliente (3), en donde las etapas (b) a (d) se implementan mediante el medio de procesamiento de datos (21) del servidor (2).

7. Un método de acuerdo con una de las reivindicaciones 1 a 5, en donde las etapas (b) y (c) se implementan mediante el medio de procesamiento de datos (31) del dispositivo cliente (3), la etapa (c) comprende el cálculo de la huella criptográfica desde una primera concatenación del dato extraído del lector óptico y del primer dato decodificado, y la generación de una prueba de conocimiento cero del cálculo de dicha 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 de que:

- la prueba de 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 dato criptográfico recibido coincide con dicha primera huella criptográfica en posesión del servidor (2).

8. Un método de acuerdo con una de las reivindicaciones 1 a 7 en donde las etapas (b) y (c) se implementan mediante el medio de procesamiento de datos (31) del dispositivo del dispositivo cliente (3), en donde la etapa (c) comprende la generación de una prueba de conocimiento cero del 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 comprende la verificación mediante el medio de procesamiento de datos (21) del servidor (2) de que el conocimiento cero prueba del hecho de que el dato biométrico de referencia y el dato biométrico candidato del individuo que coinciden es válido.

9. Un método de acuerdo con una de las reivindicaciones 1 a 8 que comprende una etapa previa (a0) de inscripción de datos de dicho documento de identidad (1) que comprende las subetapas de:

(A) obtener la fotografía de dicho individuo visible en dicho documento de identidad (1) y del dato del lector óptico del documento de identidad (1);

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

5 (C) generar el primer dato aleatorio; calculando el primer dato codificado mediante la aplicación de un proceso de codificación a dicha información de referencia representativa de la apariencia de dicha

10 fotografía y a dicho primer dato aleatorio, y de la primera huella criptográfica.

10. Un método de acuerdo con las reivindicaciones 5 y 9 en combinación, en donde durante la etapa (a0), la subetapa (A) o la subetapa (B) comprende la

15 obtención de dicho dato biométrico de referencia; y la subetapa (C) comprende, además, la generación del segundo dato aleatorio y el cálculo del segundo dato codificado mediante la aplicación de dicho proceso de codificación a dicho dato biométrico de referencia y a dicho segundo dato

20 aleatorio, y de la tercera huella criptográfica.

11. Un método de acuerdo con una de las reivindicaciones 1 a 10 en donde el proceso de decodificación es un proceso complementario de un proceso de bosquejo de un algoritmo de tipo “bosquejo seguro”.

25 12. Un método de acuerdo con una de las reivindicaciones 1 a 11 en donde el dato del lector

óptico del documento de identidad (1) es un MRZ, código QR o dato del PDF417.

13. Un método de acuerdo con una de las reivindicaciones 1 a 12, que comprende una etapa (e) de inscripción de un autenticador, en particular de la Fast Identity Online, FIDO, alliance.

14. Un método de acuerdo con una de las reivindicaciones 1 a 13 en donde la información de referencia representativa de una apariencia esperada de dicha fotografía es un dato de seguridad de tipo sello de foto digital.

15. Una unidad de autenticación fuerte que comprende un servidor conectado (2) y un dispositivo cliente (3), caracterizado porque el dispositivo cliente (3) y/o el servidor (2) comprenden medios de procesamiento de datos (21, 31) configurados 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 coincida 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 (2) 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, denominada primera huella criptográfica;
- verificar que:
 - una huella criptográfica de una primera concatenación del dato extraído del lector óptico y del dato decodificado coincida con dicha primera huella criptográfica en posesión del servidor (2); y

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

16. Un producto de programa informático que
5 comprende instrucciones de código para la ejecución de un método de acuerdo con una de las reivindicaciones 1 a 14 para la autenticación fuerte de un individuo tras lo cual dicho programa se ejecuta en una computadora.

17. Un medio de almacenamiento legible por un
10 equipo informático tras lo cual un producto de programa informático comprende instrucciones de código para ejecutar un método de acuerdo con una de las reivindicaciones 1 a 14 para autenticación fuerte de un individuo.