

Señor

**DIRECTOR DIVISIÓN DE NUEVAS CREACIONES
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

E. S. D.

REF: Expediente No. **NC2020/0005673**, solicitud de patente de invención a favor de **IDEMIA IDENTITY & SECURITY FRANCE**. Título: **MÉTODO PARA LA AUTENTICACIÓN FUERTE DE UN INDIVIDUO**

RESPUESTA A EXAMEN DE FONDO

JUAN PABLO CADENA SARMIENTO, portador de la tarjeta profesional No. 57.492 del C.S.J., obrando como apoderado de la sociedad solicitante me permito dar respuesta al Oficio No. 15807 relacionado con la patentabilidad de la presente invención y notificado el 28 de septiembre de 2023.

En respuesta a las observaciones realizadas como resultado del examen de fondo, es pertinente mencionar que las reivindicaciones cumplen a cabalidad con los requerimientos de patentabilidad establecidos en la Decisión 486 de 2000, razón por la que respetuosamente disiento de los comentarios del Examinador a este respecto. A continuación, sin embargo, se presentan argumentos y se mencionan las modificaciones realizadas para atender a cada uno de los requerimientos del Examinador:

1. Consideración inicial

Agradecemos a su despacho mejorar la redacción de los oficios técnicos. Vemos extractos del oficio que son complejos de entender y se debe hacer un trabajo investigativo adicional para tratar de entender lo que quiere transmitir su despacho.

2. Capítulo Reivindicatorio

Me permito dirigir la atención del Señor Examinador en el hecho que el Capítulo Reivindicatorio adjunto al presente memorial ha sido modificado de la siguiente manera:

- El capítulo reivindicatorio ha sido modificado para reemplazar la referencia a “*huella criptográfica*” por “*hash*”.
- La reivindicación 1 ha sido modificada para reemplazar “*una huella criptográfica*” por “*un primer hash*”. Adicionalmente las referencias a “*la denominada huella criptográfica*” y “*como se ilustra en la imagen captada*” han sido eliminadas.
- La reivindicación 5 ha sido modificada para eliminar la referencia al “*denominado tercera huella criptográfica*”.
- La reivindicación 15 ha sido modificada para eliminar la referencia a “*extraer, mediante análisis de una imagen captada del documento de identidad que representa al menos una fotografía de un individuo y un dato del lector óptico visible en dicho documento de identidad*” y demás materia relacionada a esto. Adicionalmente, ahora establece que el dispositivo cliente y/o el servidor comprenden medios de procesamiento de datos configurados para “implementar el método de acuerdo con una de las reivindicaciones 1-14”. Así mismo, hemos cambiado la traducción de la palabra en inglés “strong authentication assembly” por **conjunto** de autenticación fuerte en lugar de unidad de **unidad** de autenticación fuerte.
- La reivindicación 16 ha sido modificada para mencionar que el producto de programa informático es “*ejecutado por medios de procesamiento de datos (21, 31) de un servidor (2) y/o un dispositivo cliente (3) de un conjunto de autenticación fuerte, que 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 por los medios de procesamiento de datos*”. Adicionalmente, la referencia a “*en una computadora*” ha sido eliminada.

Así las cosas, es importante mencionar que las modificaciones realizadas a las reivindicaciones cumplen en su totalidad con los requisitos establecidos en el Artículo 34 de la Decisión 486, teniendo en cuenta que estas no involucran una ampliación a la protección correspondiente a la divulgación tal y como se presentó originalmente. Por el contrario, el Capítulo Reivindicatorio Modificado y adjunto al presente memorial cumple con los lineamientos establecidos por la Decisión Andina 486 y encuentra sustento a lo largo de la memoria descriptiva de la solicitud.

3. No es una invención

i) El Examinador establece que la reivindicación 16 no se consideran como una invención, toda vez que, se refiere a un programa de ordenador.

ii) En respuesta a lo anterior, me permito señalar que la reivindicación 16 ha sido modificada para establecer que el producto de programa informático reclamado es ejecutado por medios de un procesamiento de datos (21, 31) de un servidor (2) y/o un dispositivo cliente (3) de un conjunto de autenticación fuerte, que 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 por los medios de procesamiento de datos.

Lo anterior, tiene pleno sustento en la memoria descriptiva de la solicitud y específicamente en la página 52 se establece que *“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 su 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)”*, por consiguiente es completamente evidente que la materia reclamada en el capítulo reivindicatorio si es una invención y cumple con los lineamientos del Artículo 15 de la Decisión 486 de 2000.

4. Claridad de las Reivindicaciones

i) El Examinador establece que las reivindicaciones independientes 1 y 15 hacen referencia a los dibujos, según la expresión *“como se ilustra en la imagen captada”*. Se sugiere eliminar la referencia al dibujo o imagen e indicar las características que se quieren reclamar de manera específica.

Esta es una lectura muy deficiente y simplista de su despacho. La característica objetada no es de ninguna manera una referencia a los dibujos. Por ejemplo, los siguientes párrafos de la descripción establecen claramente lo que se debe entender por la expresión *“como se ilustra en la imagen captada”*.

[0080] En todos los casos, como se explica, el dispositivo cliente 3 puede adquirir 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, bastará con que la imagen adquirida represente el documento 1. Se entenderá que el presente método no se limita a ninguna forma de obtener esta imagen, ni a ninguna manera específica (la imagen adquirida puede ser en blanco y negro, distorsionada, etc.)

*[0085] Por información de “referencia” se entiende la información representativa del modelo “teórico| apariencia de la fotografía, es decir, como se esperaba. Por el contrario, por información “candidata” se entiende la información representativa de la apariencia registrada de la fotografía, es decir, **tal como se representa en una imagen adquirida del documento 1** (negrilla fuera de texto)*

De los anteriores extractos, es claro que la expresión “*como se ilustra en la imagen captada*” es una característica esencial en el método reivindicado y simplemente se refiere a la imagen que ha sido captada del documento de identidad del cliente mediante una fotografía. Esto no es de ninguna manera una referencia a los dibujos como erróneamente interpreta su despacho. Para mayor claridad de su despacho, un ejemplo de referencia a los dibujos o a las tablas de la descripción sería como se evidencia a continuación:

- a. Un compuesto elegido de la tabla 1 de la descripción
- b. Un medio de sujeción tal como se observa en el dibujo 2 de la descripción.

No obstante las anteriores aclaraciones y considerando las excesivas restricciones de su despacho que no se observan en ninguna oficina de patentes a nivel mundial, me permito señalar que las reivindicaciones 1 y 15 han sido modificadas y la referencia a la expresión “*como se ilustra en la imagen captada*” ha sido eliminada. Por consiguiente, considero superadas las objeciones al respecto.

ii) El Examinador manifiesta que la reivindicación independiente 15 no es concisa porque repiten la materia reclamada en la reivindicación independiente 1 y solo se diferencian en el dispositivo, el cual está enfocado en cada uno de los productos que hacen parte de la invención en su conjunto. Se sugiere agrupar dichas alternativas teniendo en cuenta que exista una razonable generalización y que cada una de dichas alternativas tenga soporte en la descripción.

Con referencia a la anterior objeción no entendemos a qué se refiere su despacho cuando dice que “**solo se diferencian en el dispositivo, el cual está enfocado (...)**”. No comprendemos que tipo de objeción quiere transmitir su despacho con dicha objeción.

La reivindicación 1 claramente define un **método** con todas y cada una de sus etapas mientras que la reivindicación 15 reivindica un **conjunto** de autenticación fuerte que comprende (i) un servidor y (ii) un dispositivo de cliente que a su vez comprenden **medios de procesamiento de datos** que implementan o ejecutan el método de la reivindicación 1 y dependientes. Estas son claramente 2 categorías patentables muy diferentes, **método y producto** y son estrategias de protección ampliamente utilizadas y aceptadas en el lenguaje de patentes a nivel mundial. Agradecemos a su despacho hacer una lectura adecuada de las categorías patentables aceptadas por nuestra legislación de patentes.

Ahora bien, no obstante la anterior aclaración, me permito señalar que la reivindicación 15 ha sido modificada para referirse a “*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 implementar el método de acuerdo con una de las reivindicaciones 1-14*”.

Precisamente, por lo anterior, la reivindicación 15 ahora presenta dependencia de la reivindicación 1 (**conocido como falsa dependencia en el instructivo de patentabilidad**). Adicionalmente, esta modificación encuentra sustento en la descripción de la presente solicitud y por ejemplo, en la página 50 se menciona que “*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*”. En este sentido, respetuosamente solicito a ese Despacho retirar las objeciones al respecto, ya que el capítulo reivindicatorio modificado y aquí adjunto cumple con los lineamientos dispuestos en el Artículo 30 de la Decisión 486.

Por otra parte, en cuanto a la objeción según la cual “*Se sugiere agrupar dichas alternativas teniendo en cuenta que exista una razonable generalización y que cada una de dichas alternativas tenga soporte en la descripción*”, tampoco entendemos a qué se refiere su despacho o qué tipo de objeción quiere transmitir. No nos queda claro cuál es la relación entre la supuesta falta de concisión entre la reivindicación de método (1) y producto (15) con reivindicar una generalización razonable de la invención.

5. Nivel Inventivo

i) El Examinador asegura que la reivindicación 1 carece de nivel inventivo debido a las enseñanzas de D1 y D2. Identifica por diferencia el hecho que esta solicitud incluye una huella criptográfica de una primera concatenación y verificar que dicha huella criptográfica coincida con la huella criptográfica almacenada en el servidor e identifica que el efecto que se logra con esto es calcular una diferencia de acuerdo con que una métrica dada sea menor que un umbral para determinar la veracidad de la información.

No obstante, el Examinador menciona que D2 ya divulgaba las características de la presente invención y en consecuencia, la persona normalmente versada en la materia al verse enfrentada al problema técnico objetivo de calcular una diferencia de acuerdo con que una métrica dada sea menor que un umbral para determinar la veracidad de la información estaría motivada a incluir una huella criptográfica de una primera concatenación y verificar que dicha huella criptográfica coincida con la huella criptográfica almacenada en el servidor del D2 en el método de D1, para así llegar al objeto de la reivindicación 1. Por lo cual se considera obvia.

De igual forma, el Examinador menciona que las reivindicaciones dependientes 2, 3, 6, 8, 12 y 17 tampoco cumplen con el requisito de nivel inventivo.

ii) En respuesta a lo anterior, me permito señalar que difiero de los señalamientos emitidos por el Examinador ya que el método de la reivindicación 1 modificada difiere de D1 porque incluye la implementación por parte de los medios de procesamiento de datos del servidor, identificado como el sistema de identidad digital 1 en D1, y/o del dispositivo cliente, identificado como el portador o el validador en D1, de los pasos de:

➤ (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;*



De hecho, D1 revela como máximo que la solicitud cifrada $Sk(Req)$ recibida previamente por el portador se descifra utilizando la clave compartida Sk ;

➤ (d) *Verificar que un hash de una primera concatenación del dato extraído del lector óptico y de los datos decodificados coincide con dicho primer hash en posesión del servidor.*

tal como acertadamente afirmó el Examinador al establecer que *“La diferencia entre la invención definida entre la reivindicación 1 y el método divulgado en D1, consiste en que la solicitud en estudio incluye una huella criptográfica de una primera concatenación y verificar que dicha huella criptográfica coincida con la huella criptográfica almacenada en el servidor.”*

Por lo tanto, en comparación con el análisis expuesto por el Examinador, el método de la reivindicación 1 modificada difiere aún más del D1 ya que incluye el paso c) anteriormente mencionado. De hecho, los pasos c) y d) del método para autenticación fuerte de un individuo implementada mediante un servidor y un dispositivo cliente conectado de la presente solicitud funcionan en sinergia para lograr el efecto de proporcionar un mecanismo de recuperación para permitir al usuario autenticarse nuevamente después de perder su autenticador (ver, por ejemplo, las páginas 1 y 5 de la memoria descriptiva de la presente solicitud).

Por lo tanto, un problema que el método de la reivindicación 1 modificada pretende resolver es el de **no** calcular una diferencia según si una métrica dada es menor que un umbral para determinar la veracidad de la información, ya que un problema que el método de la reivindicación 1 modificada **si pretende resolver** es proporcionar un mecanismo de recuperación que permita al usuario autenticarse nuevamente después de perder su autenticador. Por consiguiente, me permito exponer la siguiente pregunta *¿El experto en la materia, partiendo de D1 y enfrentado a este problema, se habría visto impulsado por D2 a modificar el proceso descrito en D1 para llegar a la invención?*, cuya respuesta es negativa ya que D2 **no propone ninguna solución para solucionar este problema**. De hecho, D2 solo revela un método para verificar una clave secreta más rápidamente (página 9, líneas 3 a 9: *“lo que reduce significativamente el tiempo de búsqueda para verificar el resto de la clave”*). Es más, D2 divulga como máximo un único método de autenticación y en efecto, el método descrito en D2 propone verificar claramente dos partes de la clave. Por lo tanto, cada parte de la clave se verifica únicamente mediante una simple autenticación.

Así las cosas, D2 no habría incitado al experto en la técnica a modificar el proceso descrito en D1. Incluso si ese fuera el caso, D2 no describe la etapa c) del método de esta solicitud porque no describe un proceso de decodificación.

Por otro lado, D2 **no divulga** una verificación de que un hash de una primera concatenación de los datos extraídos del lector óptico y de los datos decodificados coincida con dicho primer hash en posesión del servidor. En efecto, D2 **no divulga** el primer hash de una concatenación de datos de un lector óptico de un documento de identidad y de un primer dato aleatorio porque, en D2, **los caracteres aleatorios no son codificados mediante una función hash criptográfica sino insertados en el hash (reivindicación 1)**. Además, D2 no divulga un hash de una primera concatenación de los datos del lector óptico extraídos y de los datos decodificados porque, el identificador o código del proyecto de dicho documento no es un dato del lector óptico, como por ejemplo un código QR, ni datos decodificados que revelen el paso c) del método de esta solicitud. Por lo tanto, el método de la reivindicación 1 no es obvio frente a las enseñanzas de este documento.

Ahora bien, con referencia a las reivindicaciones dependientes también objetadas, me permito señalar que las mismas dependen de la reivindicación 1 independiente por lo tanto adquieren las características allí mencionadas que también las hacen inventivas frente a las enseñanzas de D1 y D2.

iii) Así las cosas, un experto en la materia no habría encontrado la solución al problema técnico planteado por esta invención en estos documentos citados y en este sentido, las reivindicaciones aquí adjuntas no son obvias respecto a las enseñanzas de D1 en combinación con D2.

Así las cosas, en este punto me permito resaltar la Guía de la SIC establece que en la etapa de evaluar si la invención reivindicada, partiendo del estado de la técnica cercano y del problema técnico objetivo, habría sido obvia para la persona medianamente versada en la materia “***consiste en responder a la pregunta de si en el estado de la técnica en su conjunto hay un segundo documento que contiene una enseñanza que indicaría (no sólo que podría indicar, sino que indicaría) a la persona medianamente versada en la materia, enfrentada al problema técnico, cómo modificar o adaptar el estado de la técnica más cercano para resolver el problema, de la forma reivindicada***”. Por lo tanto, el análisis de nivel inventivo de solicitudes de patente, no se trata de encontrar en el arte previo una simple invitación a experimentar con uno o más cambios aleatorios, sino de identificar en los documentos citados

una enseñanza y guía específica para hacer las modificaciones necesarias y no otras que lo lleven con certeza a la materia reclamada, que tal y como se encuentra definida en el Capítulo Reivindicatorio Modificado y adjunto al presente memorial de respuesta, difiere de gran forma de las enseñanzas del arte anterior citado.

Teniendo en cuenta lo anterior, no es posible prever la misma composición y/o proceso de esta solicitud con sus características, a partir de la lectura del arte anterior citado, ya que **las invenciones de patente tienen nivel inventivo cuando el producto o procedimiento no es fácilmente derivable por la persona medianamente versada en la materia o cuando presentan un efecto inesperado o mejorado impredecible de los documentos citados, como en la presente invención.** Por lo anterior, nada en el arte previo sugiere ni enseña la materia de la presente solicitud.

Así las cosas, y en vista de lo anteriormente expuesto, respetuosamente solicito el retiro de las objeciones de la presente solicitud y la concesión del privilegio solicitado, ya que en opinión del solicitante cumple con todos los requisitos establecidos en la Decisión 486.

Anexos

- Capítulo Reivindicatorio Modificado
- Tasa Oficial

JUAN PABLO CADENA SARMIENTO

T.P. No. 57.492 del C.S.J.
C.C. 80.410.337 de Usaquén
Calle 70 A No. 4 – 41



REIVINDICACIONES

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

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

en donde el método se caracteriza porque comprende la implementación mediante los 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 documento de identidad (1) de:
 - una información candidata representativa de la apariencia de dicha fotografía;
 - dicho dato de lector óptico;
- (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:
 - un hash de una primera concatenación del dato extraído del lector óptico y del dato decodificado coincida con dicho primer hash en posesión del servidor (2); y
 - el dato biométrico de referencia y el dato biométrico candidato del individuo coincidan.

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 medios de captación óptico (30) del dispositivo cliente (3), y la generación del dato biométrico candidato usando una característica biométrica proporcionada mediante los medios de captación biométrica.

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.

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 un hash de una segunda concatenación del dato del lector óptico del documento de identidad (1) y del primer dato aleatorio, diferente de la primera concatenación; en donde la etapa (c) comprende el descifrado de al menos un dato biométrico de referencia de dicho individuo cifrado mediante el hash de una segunda concatenación del dato 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 un tercer hash construido usando un segundo dato aleatorio; la etapa (c) que 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 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 biométrico candidato del individuo coinciden, comprende la verificación de que un hash construido usando el segundo dato decodificado de la misma manera que el tercer hash se construye usando el segundo dato aleatorio que coincide con dicho tercer hash 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 los medios 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 medios de procesamiento de datos (31) del dispositivo cliente (3), la etapa (c) comprende el cálculo del hash 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 dicho hash usando la primera concatenación del dato extraído del lector óptico y del primer dato decodificado; la verificación de la etapa (d) donde el hash de una primera concatenación del dato extraído del lector óptico y del dato decodificado coincide con el primer hash que comprende la verificación de que:

- la prueba de no divulgación del conocimiento del cálculo de dicho hash usando la primera concatenación del dato extraído del lector óptico y del primer dato decodificado es válida, y
- el dato criptográfico recibido coincide con dicho primer hash 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 medios de procesamiento de datos (31) 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 medios 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;
- (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 fotografía y a dicho primer dato aleatorio, y del primer hash.

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 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 aleatorio, y del tercer hash.

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”.

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 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. Un conjunto 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 implementar el método de acuerdo con una de las reivindicaciones 1-14.

16. Un producto de programa informático, ejecutado por medios de procesamiento de datos (21, 31) de un servidor (2) y/o un dispositivo cliente (3) de un conjunto de autenticación fuerte, que 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 por los medios de procesamiento de datos.

17. 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 una de las reivindicaciones 1 a 14 para la autenticación fuerte de un individuo.