

REIVINDICACIONES

1. Un método implementado por computadora para certificar un documento de seguridad (10), comprendiendo:

5 proporcionar un documento de seguridad (10) que tiene elementos seleccionados de: (a) elementos de seguridad de marcas de agua, hilos magnéticos, ventanas transparentes o relieves grabados, (b) imágenes por impresión en offset, (c) imágenes por impresión en intaglio, o (d) un número de serie de documento, teniendo tal documento de seguridad (10) características
10 únicas de registro de dichos elementos con respecto de otros documentos de seguridad también manufacturados con los mismos procesos;

seleccionar, vía procesadores, un área determinada del documento que tiene características únicas de registro de dichos elementos;

15 obtener una imagen digital de un documento de seguridad (10) que tiene características únicas de registro de dichos elementos;

obtener los datos (20) del conjunto de elementos del área determinada del documento que tiene características únicas de registro de dichos elementos;

obtener una medida del registro del conjunto de elementos del área determinada que tiene características únicas de registro de dichos elementos;

20 construir, a partir de la medida del registro del conjunto determinado de elementos del documento que tiene características únicas de registro de dichos elementos, un mensaje con una función de hash (40), en donde el mensaje de hash (50) es el mensaje obtenido después de ser codificado por medio de una función de hash (40) criptográfica unidireccional;

25 encriptar el mensaje de hash (50) construido a partir de la medida del registro del conjunto determinado de elementos del documento que tiene

características únicas de registro de dichos elementos utilizando una clave privada (70) en un sistema criptográfico de clave pública (60) para obtener un certificado digital (80); y

5 almacenar el certificado digital (80) obtenido y el número de serie del documento, a partir del mensaje hash encriptado, construido a partir de la medida del registro del conjunto determinado de elementos del documento que tiene características únicas de registro de dichos elementos, en una base de datos (90) externa.

10 2. El método para certificar un documento de seguridad (10) de conformidad con la reivindicación 1, en donde un número, código de barras o marca asociada al certificado digital (80) se marca o imprime (97) en el documento de seguridad (10).

15 3. El método para la certificación de acuerdo con la reivindicación 1, en donde la imagen digital es tomada con luz con una longitud de onda entre 200 y 1500 nanómetros.

20 4. El método para la certificación de acuerdo con la reivindicación 1, en donde la imagen digital es tomada con luz visible.

5. El método para la certificación de acuerdo con la reivindicación 1, en donde varias partes del mismo documento son certificadas independientemente.

6. El método para la certificación de acuerdo con la reivindicación 1, en donde el documento de seguridad (10) es un billete, un cheque, un pasaporte o un certificado de nacimiento.

5 7. El método para certificar un documento de seguridad (10) de acuerdo con la reivindicación 1, en donde los datos (20) se obtienen durante la línea de producción.

10 8. El método para certificar un documento de seguridad (10) de acuerdo con la reivindicación 1, en donde los datos (20) se obtienen durante la inspección de calidad.

9. Un método de autenticación de un documento de seguridad (10) comprendiendo los pasos de:

15 proporcionar un documento de seguridad (10) que tiene elementos seleccionados de: (a) elementos de seguridad de marcas de agua, hilos magnéticos, ventanas transparentes o relieves grabados, (b) imágenes por impresión en offset, (c) imágenes por impresión en intaglio, y (d) un número de serie de documento, teniendo tal documento de seguridad (10) características
20 únicas de registro de dichos elementos con respecto de otros documentos de seguridad también manufacturados con los mismos procesos;

verificar la autenticidad de los suministros y la existencia de los elementos de seguridad de marcas de agua, hilos magnéticos, ventanas transparentes o relieves grabados y descartar a los documentos que no los
25 incluyan;

recibir por parte de un usuario, una imagen digital de un documento de seguridad (10), presuntamente manufacturado por una pluralidad de diferentes procesos o etapas, que proporcionan al documento un número correspondiente de elementos, teniendo tal documento de seguridad (10) una variación en el registro o posición relativa de elementos única;

obtener datos (20) de un conjunto de elementos de un área determinada del documento,

obtener una medida del registro del conjunto determinado de elementos del documento y los datos (20) de la ID del documento,

aplicar una función de hash (40) para obtener un mensaje de hash (50) para la verificación,

obtener un certificado digital certificador, encriptado, asociado al documento (40) desde una base de datos (90) que se accesa ya sea por: (a) el número de serie del documento, ó (b) un código de barras, un código de barras bidimensional o una serie de caracteres marcados/impresos en el documento de seguridad (10);

desencriptar el certificado digital certificador con una clave pública, para obtener un mensaje de hash certificador; y

autenticar el documento comparando el mensaje con una función de hash (40) certificador y el mensaje con una función de hash (40) para la verificación, en donde si el mensaje certificador y el mensaje para la verificación coinciden, el documento se considera como genuino, si el mensaje certificador y el mensaje para la verificación no coinciden, el documento se considera como una falsificación.

10. El método para la autenticación de acuerdo con la reivindicación 9, en donde las materias primas son verificadas via análisis de imagen y métodos de patrón de reconocimiento.

5 11. El método para la autenticación de acuerdo con la reivindicación 9, en donde el documento de seguridad (10) es un billete.

12.- El método para la autenticación de un documento de seguridad (10) de acuerdo con la reivindicación 9, en donde la autenticación se realiza por
10 escáneres o cámaras digitales comercialmente disponibles conectados a computadoras.

13.- El método para la autenticación de un documento de seguridad (10) de acuerdo con la reivindicación 9, en donde la autenticación se realiza
15 mediante teléfonos inteligentes o tabletas.

14.- El método para la autenticación de un documento de seguridad (10) de acuerdo con la reivindicación 9, en donde la autenticación se realiza mediante equipo de procesamiento de billetes.