(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 597 808**

(21) Número de solicitud: 201531078

(51) Int. CI.:

G06Q 30/00 (2012.01)

(12) SOLICITUD DE PATENTE A1

(22) Fecha de presentación:

22.07.2015

(43) Fecha de publicación de la solicitud:

23.01.2017

(71) Solicitantes:

SANCHO PITARCH, José Carlos (100.0%)
Josep Anselm Clave, 7, piso 4º puerta 2ª
08950 Esplugues de Llobregat (Barcelona) ES

(72) Inventor/es:

SANCHO PITARCH, José Carlos

(74) Agente/Representante:

PONTI SALES, Adelaida

(54) Título: **MÉTODO Y SISTEMA DE AUTENTIFICACIÓN DE ELEMENTOS DE IDENTIFICACIÓN POR RADIOFRECUENCIA, Y PROGRAMA DE ORDENADOR**

(57) Resumen:

Método y sistema de autentificación de elementos de identificación por radiofrecuencia, y programa de ordenador.

El método comprende:

- aplicar una operación o un esquema matemático, por parte de un elemento de identificación por radiofrecuencia utilizando una clave privada de elemento (PriTAG), y enviar el resultado obtenido a un dispositivo lector (M); y
- verificar dicho resultado recibido, por parte del dispositivo lector (M), utilizando información de verificación asociada a dicha clave privada de elemento (PriTAG).

El método comprende obtener dicha información de verificación de un servidor de base de datos (DBT), y autentificar al servidor (DBT) y a una aplicación software (APP) del dispositivo lector (M) encargada de llevar a cabo la verificación del resultado recibido.

Un segundo y un tercer aspectos de la invención conciernen, respectivamente, a un sistema y a un programa de ordenador adaptados para implementar el método del primer aspecto.

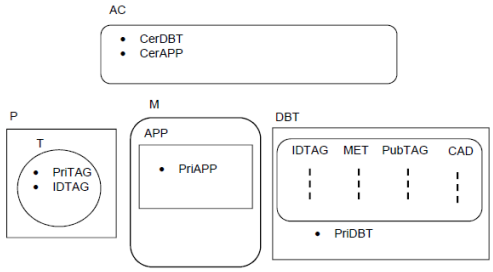

Fig. 1

ES 2 597 808 A1

DESCRIPCIÓN

MÉTODO Y SISTEMA DE AUTENTIFICACIÓN DE ELEMENTOS DE IDENTIFICACIÓN POR RADIOFRECUENCIA, Y PROGRAMA DE ORDENADOR

Sector de la técnica

La presente invención concierne, en un primer aspecto, a un método de autentificación de elementos de identificación por radiofrecuencia, basado en la verificación del resultado de la aplicación de una operación o un esquema matemático por parte del elemento a autentificar, y más particularmente a un método que comprende implicar en la autentificación del elemento de identificación por radiofrecuencia, y también autentificar, a unas entidades computacionales.

Un segundo aspecto de la invención concierne a un sistema adaptado para implementar el método del primer aspecto.

Un tercer aspecto de la invención concierne a un programa de ordenador adaptado para implementar el método del primer aspecto.

Estado de la técnica anterior

En el estado de la técnica son conocidas diferentes propuestas que describen métodos y sistemas de autentificación de elementos de identificación por radiofrecuencia, tal como etiquetas NFC (acrónimo de los términos en inglés “Near Field Communication”: Comunicación de campo cercano). A continuación se citan una serie de referencias representativas del estado de la técnica en cuanto a tales propuestas.

En primer lugar existen los denominados métodos físicos, basados por ejemplo en el uso de marcas invisibles al ojo humano, pero visibles por un aparato lector. En esta línea se encuentra la tecnología AuthentiGuard® que imprime con tinta unas marcas de varios de micrómetros (http://www.authentiguard.com/products.html#tab_authentiguard).

Otra tecnología en esta línea se encuentra el uso de tintas invisibles para el ojo humano, pero que se pueden ver fácilmente si una determinada luz se proyecta en ellas (http://www.wsj.com/video/smart-invisible-ink-could-foil-counterfeiters/EF371C30-02B6-4569-873A-6DA282A34284.html).

Los métodos físicos no son fáciles de utilizar ya que requieren de lectores o luces especiales. Esto limita el alcance de uso de estos sistemas, no es un sistema adecuado para la mayoría de las personas que no poseen estos dispositivos especiales. Además, estos métodos físicos podrían ser copiados y reproducidos con relativamente facilidad.

Por otra parte, existen los métodos basados en sistemas electrónicos, la mayoría de los cuales aportan una mayor facilidad al comprobar la autenticidad. Algunos de estos métodos se describen a continuación.

Uno de tales métodos basados en sistemas electrónicos se describe en la propuesta hecha en la Solicitud Internacional WO2013121356, que propone grabar un código en la etiqueta NFC, el cual se lee con una aplicación móvil para compararlo con un código que se guarda en una base de datos. Si los códigos coinciden entonces el producto asociado a la etiqueta NFC se considera auténtico.

La solicitud Internacional WO2014076720 describe un método y un sistema en donde se utiliza una etiqueta NFC, certificados digitales, criptografía asimétrica, y un lector de NFC. El método comprende grabar en la etiqueta la firma de la función hash del documento de autenticidad emitido por el centro de certificados digitales. Se comprueba la autenticidad comprobando que tiene un certificado valido usando las claves de criptografía asimétrica.

En la solicitud de patente CN103413155A se propone utilizar una etiqueta NFC con un área de memoria protegida por contraseña, criptografía y un dispositivo lector NFC. El método funciona escribiendo de forma cifrada la autenticidad de la etiqueta NFC en el área de memoria protegida por contraseña. El lector utiliza la contraseña para poder leer esa memoria protegida y descifra su contenido para corroborar su autenticidad.

Por otra parte, existe un método (descrito en https://blackseal.trustpoint.ca/features#how-it-works y propuesto por TrustPoint Innovation Ltd. ©) que utiliza criptografía, una etiqueta NFC y un lector NFC y que está basado en el último standard de la tecnología NFC que puede cifrar los mensajes NFC grabados en la etiqueta NFC. De esta manera se puede comprobar que la etiqueta es auténtica descifrando los mensajes grabados mediante un lector de NFC.

La solicitud de patente CN103745256A propone utilizar una etiqueta NFC, una imagen impresa en la etiqueta, un algoritmo de encriptado y un ordenador. La etiqueta NFC almacena un código encriptado obtenido a partir de la imagen impresa y de un código único de la etiqueta. Este código encriptado se almacena también en una base de datos. El ordenador lee el código encriptado de la etiqueta y lo envía al servidor de base de datos para comprobar si coinciden para determinar si el producto asociado a la etiqueta NFC es auténtico. Este método no aporta tanta facilidad al comprobar la autenticidad de la etiqueta NFC como los anteriores, ya que requiere de la toma de una imagen, por lo que es un procedimiento más laborioso.

La mayoría de estos métodos electrónicos siguen sin evitar el copiado de las etiquetas. Aunque se utilice criptografía para ver si realmente estos códigos grabados en la etiqueta han

sido escritos por una entidad autentificada, los mismos códigos se pueden leer y grabar fácilmente en otra etiqueta.

Solamente el método descrito en la solicitud de patente CN103413155A protege el copiado de la memoria de las etiquetas mediante el uso de una contraseña. Para poder leer de la etiqueta se necesita la contraseña que hay que enviar a la etiqueta. Este uso de contraseñas es un sistema débil de seguridad porque esta contraseña se transmite entre la aplicación del lector y la etiqueta NFC, por lo que un pirata informático podría fácilmente obtenerla.

Por otra parte existen documentos de patente que proponen verificar la autenticidad de la etiqueta NFC verificando la autenticidad de una firma digital generada por la misma. Tal es el caso de los documentos WO2014140807 y US8941469B1. En ambos casos existen problemas de vulnerabilidad en cuanto a la seguridad de las claves utilizadas para las firmas. Asimismo, en ambos casos la autentificación de las firmas no se lleva cabo por el lector NFC sino por parte de un servidor, con el consiguiente aumento de la carga de trabajo del mismo y de la existencia de mensajes intercambiados con el mismo a través de la red de comunicaciones (los cuales podrían ser interceptados)

No obstante, sí que existe una propuesta donde la autentificación de la firma digital generada por la etiqueta NFC sí que es verificada por el propio lector. Tal es el caso de la descrita en la solicitud Internacional WO2015001376, que propone un método que reúne las características del preámbulo de la reivindicación 1 de la presente invención.

Incluso en el método propuesto en WO2015001376 existen problemas de vulnerabilidad que no permiten garantizar que la verificación de la firma digital generada por la etiqueta NFC sea fiable, ya que los actores que intervienen en el proceso de verificación podrían haber sido suplantados o manipulados por un pirata informático.

Es, por lo tanto, necesario ofrecer una alternativa al estado de la técnica que cubra las lagunas halladas en el mismo, proporcionando un método y un sistema de autentificación de elementos de identificación por radiofrecuencia más robusto y sin los problemas de vulnerabilidad de los que adolecen los conocidos en el estado de la técnica.

Explicación de la invención

Con tal fin, la presente invención concierne, en un primer aspecto, a un método de autentificación de elementos de identificación por radiofrecuencia, que comprende, de manera en sí conocida:

- aplicar un método de protección matemático, que incluye una o varias operaciones matemáticas o un esquema matemático, por parte de un elemento de identificación por

radiofrecuencia con capacidad de procesamiento, sobre al menos un dato, utilizando al menos una clave privada de elemento almacenada en dicho elemento de identificación por radiofrecuencia, obteniendo un resultado de elemento;

- enviar dicho resultado de elemento, utilizando una tecnología de comunicación inalámbrica, por parte de dicho elemento de identificación por radiofrecuencia, a un dispositivo de computación lector (en general, también con capacidad para escribir) de elementos de identificación por radiofrecuencia; y

- verificar dicho resultado de elemento, por parte de dicho dispositivo de computación lector de elementos de identificación por radiofrecuencia, utilizando información de verificación asociada a dicha clave privada de elemento.

A diferencia de los métodos conocidos en el estado de la técnica, el propuesto por el primer aspecto de la presente invención comprende, de manera característica, obtener dicha información de verificación asociada a dicha clave privada de elemento de un servidor de base de datos, por parte del dispositivo de computación lector de elementos de identificación por radiofrecuencia, y autentificar también a dicho servidor de base de datos y a una aplicación software instalada en una memoria del dispositivo de computación lector de elementos de identificación por radiofrecuencia encargada de llevar a cabo dicha verificación del resultado de elemento.

Para un ejemplo de realización, dicha información de verificación incluye información identificativa sobre el método de protección matemático empleado para obtener dicho resultado de elemento.

De acuerdo con un ejemplo de realización, el método del primer aspecto de la invención comprende aplicar dicha o dichas operaciones matemáticas (suma, resta, multiplicación, división, etc.) por parte de dicho elemento de identificación por radiofrecuencia con capacidad de procesamiento, incluyendo dicha información de verificación el resultado de una función matemática aplicada sobre la clave privada de elemento, y realizando la aplicación software los siguientes pasos, de manera secuencial y sucesiva:

i) la aplicación de la operación u operaciones inversas a dicha o dichas operaciones matemáticas, sobre el resultado de elemento;

ii) la aplicación de dicha función matemática sobre el resultado obtenido en i); y

iii) la comparación del resultado obtenido en ii) con el resultado que constituye dicha información de verificación.

Para una variante de dicho ejemplo de realización, el método comprende, de manera previa a dicha etapa i) y con el fin de conocer qué operación u operaciones matemáticas ha aplicado el elemento de identificación por radiofrecuencia con capacidad de procesamiento, identificar, por parte de la aplicación software, el método de protección matemático aplicado a través de la citada información identificativa incluida en la información de verificación.

Para una variante preferida de dicho ejemplo de realización, dicha función matemática es una función Hash.

Para otro ejemplo de realización, el método del primer aspecto de la invención comprende aplicar, por parte de dicho elemento de identificación por radiofrecuencia con capacidad de procesamiento, dicho esquema matemático, el cual es una firma digital, siendo dicho resultado de elemento una firma digital de elemento e incluyendo dicha información de verificación una clave pública de elemento asociada a dicha clave privada de elemento. Para una variante de dicho ejemplo de realización, el método comprende, con el fin de conocer que el elemento de identificación por radiofrecuencia ha aplicado dicho esquema matemático, identificar, por parte de la aplicación software, el método de protección matemático aplicado a través de la citada información identificativa incluida en la información de verificación.

De acuerdo a un ejemplo de realización preferido, el método del primer aspecto de la invención permite determinar quée tipo de operaciones matemáticas son necesarias para verificar el resultado de elemento pudiendo ser el caso de que éstas cambien de un elemento a otro.

El método de protección matemático para cada elemento se determina en el servidor de base de datos y por lo tanto se desconoce a priori por el dispositivo de computación lector de elementos de identificación por radiofrecuencia.

La presente invención, a diferencia del estado de la técnica, permite emplear distintos métodos de protección matemáticos con diferente complejidad computacional asociada a la vez, siendo por lo tanto una técnica más flexible, y por lo tanto, permite adaptarse mejor a las necesidades de coste de los distintos productos a proteger.

Además, a diferencia de los métodos conocidos en el estado de la técnica, el método de protección matemático, descrito en cada una de las realizaciones anteriores, empleado para cada uno de los elementos de identificación por radiofrecuencia se determina a través de un servidor de base de datos, siendo posible que el dispositivo de computación lector de elementos de identificación por radiofrecuencia sea lo suficientemente versátil para ejecutar cualquiera de los métodos de protección matemáticos.

De acuerdo a un ejemplo de realización preferido, el método del primer aspecto de la invención comprende llevar a cabo la autentificación de dicho servidor de base de datos por parte de dicho dispositivo de computación lector de elementos de identificación por radiofrecuencia, utilizando dicha u otra aplicación software.

Preferentemente, el método del primer aspecto de la invención comprende llevar a cabo la autentificación de la aplicación software por parte de dicho servidor de base de datos.

Según un ejemplo de realización, el método del primer aspecto de la invención comprende llevar a cabo la autentificación del servidor de base de datos y la autentificación de la aplicación software, mediante la utilización de una clave asimétrica de base de datos que incluye una clave privada de base de datos y una clave pública de base de datos, y de una clave asimétrica de aplicación que incluye una clave privada de aplicación y una clave pública de aplicación, comprendiendo el método:

- firmar digitalmente, por parte de la aplicación software, la información que le transmite al servidor de base de datos utilizando la clave privada de aplicación y verificar, por parte del servidor de base de datos, la autenticidad de la firma digital recibida de la aplicación software utilizando la clave pública de aplicación, y

- firmar digitalmente, por parte del servidor de base de datos, la información que le transmite a la aplicación software utilizando la clave privada de base de datos y verificar, por parte de la aplicación software, la autenticidad de la firma digital recibida del servidor de base de datos utilizando la clave pública de base de datos.

Opcionalmente, el método del primer aspecto de la invención comprende además:

- encriptar, por parte de la aplicación software, la información que le transmite al servidor de base de datos, utilizando la clave pública de base de datos, y desencriptarla, por parte del servidor de base de datos, utilizando la clave privada de base de datos; y

- encriptar, por parte del servidor de base de datos, la información que le transmite a la aplicación software, utilizando la clave pública de aplicación, y desencriptarla, por parte de la aplicación software, utilizando la clave privada de aplicación.

En general, el método del primer aspecto de la invención comprende enviar junto con el resultado de elemento (firma digital o resultado de operación matemática), por parte del elemento de identificación por radiofrecuencia al dispositivo de computación lector de elementos de identificación por radiofrecuencia, un número identificativo único asociado al mismo.

Ventajosamente, el servidor de base de datos tiene almacenada información referente a una pluralidad de elementos de identificación por radiofrecuencia, o de productos asociados a los mismos, que incluye, para cada elemento, un número identificativo único, información de caducidad e información de verificación asociada a cada clave privada de elemento (clave pública de elemento o resultado de función matemática, p. ej. Hash, y, si es el caso, información del esquema matemático u operaciones matemáticas utilizadas), comprendiendo el método:

- solicitar, por parte de la aplicación software al servidor de base de datos, la información de verificación asociada a la clave privada de elemento y la información de caducidad asociada al número identificativo recibido junto con el resultado de elemento, mediante el envío de una solicitud que incluye o constituye dicha información al menos firmada digitalmente utilizando la clave privada de aplicación;

- verificar, por parte del servidor de base de datos, la autenticidad de la firma digital recibida de la aplicación software utilizando la clave pública de aplicación y en caso afirmativo enviar, por parte del servidor de base de datos a la aplicación software, la información de verificación asociada a la clave privada de elemento y la información de caducidad solicitadas, las cuales constituyen dicha información al menos firmada digitalmente utilizando la clave privada de base de datos; y

- verificar, por parte de la aplicación software la autenticidad de la firma digital recibida del servidor de base de datos utilizando la clave pública de base de datos y en caso afirmativo verificar la autenticidad del resultado de elemento y también la caducidad asociada a su número identificativo.

Por lo que se refiere al servidor de base de datos, éste puede implementar cualquier tipo de base de datos conocida, desde las más convencionales (que registran la información e tablas u otra forma de estructura de datos) a las de más reciente aparición conocidas como bases de datos de bloques de cadena, o “blockchain”, siendo esta última preferida al ser descentralizada y por tanto aportar una mayor seguridad y ser resistente a catástrofes. En cualquier caso, la invención no está limitada a ninguna clase de base de datos en concreto, ni a ningún tipo de servidor de base de datos particular.

Para un ejemplo de realización, el método del primer aspecto comprende realizar una autentificación adicional de la aplicación software por parte de una aplicación autentificadora de aplicaciones y una entidad computacional de base de datos de aplicaciones, en la cual la aplicación software ha sido previamente registrada, con el fin de notificar al usuario del dispositivo de computación lector de elementos de identificación por radiofrecuencia si la

aplicación software es auténtica y puede/debe utilizarla para leer/autentificar al elemento de identificación por radiofrecuencia, o incluso impedir el acceso de la aplicación software al servidor de base de datos.

Según una variante de dicho ejemplo de realización, el método comprende obtener la clave pública de base datos por parte de la aplicación software desde dicha entidad computacional de base de datos de aplicaciones a través de la aplicación autentificadora de aplicaciones, y condicionado a que el resultado de la autentificación adicional sea positivo. Esta variante es una manera de llevar a cabo el arriba mencionado impedimento del acceso de la aplicación software al servidor de base de datos.

La mencionada aplicación autentificadora de aplicaciones puede estar instalada en cualquier clase de dispositivo computacional capaz de comunicarse bidireccionalmente con la aplicación software y con la entidad computacional de base de datos de aplicaciones, o incluso puede estar instalada en la propia entidad computacional de base de datos de aplicaciones, en función del ejemplo de realización.

De acuerdo a un ejemplo de realización, el método del primer aspecto de la invención está aplicado a un escenario que incluye una pluralidad de servidores de bases de datos, al menos uno por fabricante, donde el citado número identificativo incluye información identificativa de fabricante, comprendiendo el método determinar, por parte de la aplicación software, cuál es el servidor de base de datos asociado al fabricante indicado por dicha información identificativa de fabricante a la que enviarle la citada solicitud y la obtención, por parte del servidor de base de datos, si no dispone del mismo, de un certificado digital de la aplicación software que incluye a la clave pública de aplicación.

Para otro ejemplo de realización, alternativo al descrito arriba para el que la clave pública de base datos se obtiene a través de la aplicación autentificadora de aplicaciones, el método del primer aspecto de la invención comprende la obtención, por parte de la aplicación software, si no dispone del mismo, de un certificado digital de base de datos que incluye a la clave pública de base de datos.

Generalmente, los mencionados certificados digitales son obtenidos a través de una agencia de certificados digitales que los expide convenientemente.

En general, el elemento de identificación por radiofrecuencia está asociado, preferentemente fijado o integrado, a un producto cuya autenticidad se desea comprobar, implicando la verificación de la autenticidad del elemento de identificación por radiofrecuencia la autentificación del producto asociado al mismo, e implicando la verificación de la caducidad

asociada al número identificativo del elemento la verificación de la caducidad del producto, siendo el anteriormente mencionado fabricante el fabricante del producto.

De acuerdo con un ejemplo de realización, el elemento de identificación por radiofrecuencia es una etiqueta RFID, ventajosamente NFC, fijada al producto.

De acuerdo con un ejemplo de realización, el método propuesto por el primer aspecto de la invención está aplicado a un escenario que incluye una pluralidad de aplicaciones software aptas para llevar a cabo dicha verificación del resultado de elemento, instaladas en unas respectivas memorias de unos dispositivos de computación lectores de elementos de identificación por radiofrecuencia, teniendo asociado cada una de dichas aplicaciones software un correspondiente número de identificación, donde el método comprende incluir dicho número de identificación en la información enviada desde la aplicación software al servidor de base de datos, y realizar, por parte del servidor de base de datos, la identificación de la aplicación software por el número de identificación recibido.

Para una variante de dicho ejemplo de realización, cada una de dichas aplicaciones software tiene asociado un certificado digital único con sus respectivas claves privada y pública de aplicación y dicho correspondiente número de identificación, donde el método comprende realizar, por parte del servidor de base de datos, el acceso al certificado digital de la aplicación software identificada por su número de identificación para obtener la correspondiente clave pública de aplicación.

Para otra variante, parte o todas dichas aplicaciones software comparten un certificado digital común asociado a los números de identificación de dichas aplicaciones software que lo comparten, donde el método comprende realizar, por parte del servidor de base de datos, el acceso a dicho certificado digital común asociado a la aplicación software identificada por su número de identificación para obtener la correspondiente clave pública de aplicación.

Ventajosamente, el servidor de base de datos almacena dicho número de identificación para registrar qué aplicación está verificando cada elemento de identificación por radiofrecuencia, y por tanto cada producto, con el fin, por ejemplo, de proporcionar al fabricante información sobre qué cliente está usando cada producto.

En general, parte o todos los certificados digitales arriba mencionados tienen asociadas unas respectivas fechas de caducidad, por lo que cuando son utilizados para verificar la autenticidad de las firmas digitales generadas con las claves privadas de los mismos, tal verificación también incluye una comprobación de caducidad que concluye en la determinación de que la entidad que genera dicha firma digital (Aplicación software o servidor de base de datos) no es auténtica si su certificado digital ha caducado.

El fabricante del producto tiene tres mecanismos que funcionan en tiempo real para garantizar la seguridad del método de autentificación propuesto por la presente invención:

1- Cambiando la caducidad de las claves criptográficas del producto, si detectase que estas claves han sido comprometidas. El producto no sería válido en este caso.

2- Cambiando la caducidad del certificado digital de la aplicación software, si detectase que las claves de ésta han sido comprometidas. En este caso el cliente debería instalarse de nuevo la aplicación software, la cual contendría nuevas claves.

3- Cambiando la caducidad del certificado digital de base de datos, si detectase que sus claves han sido comprometidas.

De acuerdo a un ejemplo de realización, el método del primer aspecto de la invención comprende generar dicho dato, que es al menos uno, por parte del dispositivo de computación lector de elementos de identificación por radiofrecuencia, preferentemente de manera aleatoria, y enviarlo al elemento de identificación por radiofrecuencia utilizando dicha tecnología de comunicación inalámbrica.

Por lo que se refiere a la clave privada de elemento, de manera preferida ésta se encuentra contenida en código de programa no leíble desde el exterior que está grabado en el elemento de identificación por radiofrecuencia, siendo dicho código de programa el encargado de leer dicho dato, firmarlo digitalmente y enviárselo, junto con un número identificativo único, al dispositivo de computación lector de elementos de identificación por radiofrecuencia.

Aunque la invención no está limitada a una tecnología de comunicación inalámbrica particular, de manera muy preferida ésta es una tecnología de comunicación de campo cercano, es decir una tecnología NFC.

El elemento de identificación por radiofrecuencia en general es de tipo pasivo, es decir que se alimenta a partir de la energía contenida en la señal proporcionada por el dispositivo de computación lector de elementos de identificación por radiofrecuencia que incluye dicho dato (y/u otra información), aunque la presente invención también es aplicable a elementos de identificación por radiofrecuencia activos.

Un segundo aspecto de la invención concierne a un sistema de autentificación de elementos de identificación por radiofrecuencia, que comprende:

- un dispositivo de computación lector de elementos de identificación por radiofrecuencia, con capacidad de comunicación según una tecnología de comunicación inalámbrica; y

- al menos un elemento de identificación por radiofrecuencia que comprende unos medios de procesamiento, unos medios de almacenamiento y unos medios de comunicación que operan según una tecnología de comunicación inalámbrica, estando dicho elemento de identificación por radiofrecuencia configurado y adaptado para, mediante dichos medios de procesamiento, aplicar un método de protección matemático, que incluye una o varias operaciones o un esquema matemático, sobre al menos un dato, utilizando una clave privada de elemento almacenada en dichos medios de almacenamiento, obteniendo un resultado de elemento, y enviar, utilizando dichos medios de comunicación, dicho resultado de elemento a dicho dispositivo de computación lector de elementos de identificación por radiofrecuencia.

estando dicho dispositivo de computación lector de elementos de radiofrecuencia configurado y adaptado para verificar el resultado de elemento recibido utilizando información de verificación asociada a dicha clave privada de elemento.

A diferencia de los sistemas conocidos en el estado de la técnica, el propuesto por el segundo aspecto de la presente invención comprende, de manera característica:

- un servidor de base de datos que tiene registrada dicha información de verificación asociada a dicha clave privada de elemento y que es accesible, a través de una vía de comunicación, por parte del dispositivo de computación lector de elementos de identificación por radiofrecuencia, el cual está configurado y adaptado para obtener dicha información de verificación asociada a dicha clave privada de elemento accediendo a dicho servidor de base de datos;

- una aplicación software instalada en una memoria del dispositivo de computación lector de elementos de identificación por radiofrecuencia (M) y encargada de llevar a cabo dicha verificación del resultado de elemento;

- unos primeros medios de autentificación encargados de autentificar a dicho servidor de base de datos; y

- unos segundos medios de autentificación encargados de autentificar a dicha aplicación software.

De acuerdo con un ejemplo de realización preferido, los primeros medios de autentificación se encuentran implementados en el dispositivo de computación lector de elementos de identificación por radiofrecuencia, mediante la citada u otra aplicación software y/o los citados segundos medios de autentificación se encuentran implementados en como mínimo el mencionado servidor de base de datos.

De acuerdo con un ejemplo de realización, los segundos medios de autentificación se encuentran implementados también en una aplicación autentificadora de aplicaciones y una entidad computacional de base de datos de aplicaciones que operan según los correspondientes ejemplos de realización del método del primer aspecto de la invención descritos arriba.

En general, el dispositivo de computación lector de elementos de radiofrecuencia es portable, tal como un teléfono móvil inteligente (Smartphone) o una tableta digital (Tablet), aunque la invención no está limitada a ello, pudiendo utilizarse también dispositivos de computación no portables.

El sistema del segundo aspecto de la invención está adaptado para implementar el método del primer aspecto. Sirva, por tanto, la descripción anterior de las etapas del método del primer aspecto de la invención según diferentes ejemplos de realización válida para describir las funciones llevadas a cabo por los distintos actores del sistema del segundo aspecto de la invención para unos correspondientes y equivalentes ejemplos de realización.

De acuerdo a un ejemplo de realización del sistema del segundo aspecto de la invención para el cual éste está adaptado para implementar los ejemplos de realización del método del primer aspecto anteriormente descritos que implican la utilización de unos certificados digitales, del servidor de base de datos y de la(s) aplicación(es) software, el sistema comprende una agencia de certificación de certificados digitales encargada de expedir los anteriormente mencionados certificados digitales, siendo dicha agencia de certificación accesible tanto por lo(s) servidor(es) de bases de datos como por la(s) aplicación(es) software, a través de unas correspondientes vías de comunicación, para obtener dichos certificados digitales.

Un tercer aspecto de la invención concierne a un programa de ordenador que incluye instrucciones de código de programa que, cuando se ejecutan en unas entidades computacionales, específicamente parte en un elemento de identificación por radiofrecuencia con capacidad de procesamiento, parte en un dispositivo de computación lector de elementos de identificación por radiofrecuencia y parte en al menos un servidor de base de datos (y cuando es el caso también en una aplicación autentificadora de aplicaciones y una entidad computacional de base de datos de aplicaciones), implementan las etapas del método del primer aspecto de la invención.

Aunque la invención no está limitada a su aplicación a ningún producto en concreto, es de particular interés un caso práctico consistente en la autentificación de medicamentos en la industria farmacéutica. Existen muchos medicamentos que han sido falsificados y se venden por internet. Estos medicamentos falsos no poseen de los compuestos activos necesarios y

por lo tanto no producen ningún efecto al ser humano. Al no ser efectivos pueden producir complicaciones e incluso la muerte a los pacientes. Se estima que unas 70,000 personas mueren al año debido a la falsificación de medicamentos. Mediante la presente invención se puede verificar 100% si el medicamento es auténtico y además se comprueba la caducidad del mismo, siendo 100% seguro de tomar.

Breve descripción de los dibujos

Las anteriores y otras ventajas y características se comprenderán más plenamente a partir de la siguiente descripción detallada de unos ejemplos de realización con referencia a los dibujos adjuntos, que deben tomarse a título ilustrativo y no limitativo, en los que:

La Figura 1 muestra un diagrama de bloques con los distintos componentes del sistema propuesto por el segundo aspecto de la invención, para un ejemplo de realización, utilizados para implementar el método del primer aspecto.

La Figura 2 muestra, de manera esquemática, el proceso de firma digital de elemento que forma parte del método propuesto por el primer aspecto de la invención, para un ejemplo de realización, llevado a cabo entre el elemento de identificación por radiofrecuencia, tal como una etiqueta NFC, y el dispositivo de computación lector de elementos de identificación por radiofrecuencia, tal como un lector NFC.

La Figura 3 ilustra, de manera esquemática, el proceso de verificación de la firma digital de elemento que forma parte del método propuesto por el primer aspecto de la invención, de acuerdo con un ejemplo de realización.

La Figura 4 ilustra, de manera esquemática, el proceso de autentificación adicional de la aplicación software que forma parte del método propuesto por el primer aspecto de la invención, para un ejemplo de realización.

Descripción detallada de unos ejemplos de realización

En el presente apartado se describen ejemplos de realización para los que el elemento de identificación por radiofrecuencia genera una firma digital que le envía al dispositivo de computación lector de elementos de identificación por radiofrecuencia, el cual determina el método de protección matemático (en este caso una firma digital) aplicado por el elemento a través de la información identificativa obtenida del servidor de base de datos y verifica la firma digital de elemento mediante una clave pública de elemento incluida también en la información de verificación obtenida del servidor de base de datos. Sirvan los ejemplos de realización aquí descritos también como válidos, ligeramente modificados, para el caso descrito en un apartado anterior para el que, en lugar de una firma digital, el elemento de identificación por

radiofrecuencia realiza una operación matemática más sencilla, y la información de verificación almacenada en el servidor de base de datos y obtenida y utilizada por parte del dispositivo de computación lector de elementos de identificación por radiofrecuencia no incluye una clave pública de elemento sino el resultado de la aplicación de una función matemática (p. ej. Hash) a la clave privada de elemento así como información identificativa sobre las operaciones matemáticas aplicadas por el elemento y por tanto necesarias para la verificación del resultado.

Para el ejemplo de realización de la Figura 1, el sistema propuesto por el segundo aspecto de la invención comprende los siguientes componentes, utilizados para implementar el método del primer aspecto de la invención:

1. Una etiqueta NFC, indicada con la referencia T, por cada producto. P

2. A cada producto P o etiqueta T se le asocia lo siguiente: una clave asimétrica única: clave privada PriTAG y su correspondiente clave pública; un número identificativo único (IDTAG); y una fecha de caducidad. El IDTAG contiene en los primeros dígitos el código del fabricante (F) y en el resto el número de serie del producto (P). Todos los productos tienen un número de serie único.

3. Un servidor de base de datos DBT accesible, por ejemplo por Internet. El servidor de base de datos DBT, en general pública, contiene cada uno de los números identificativos de los productos (IDTAG), información identificativa sobre sus correspondientes métodos de protección matemáticos (MET), sus correspondientes claves públicas (PubTAG) y la caducidad (CAD) de cada clave. Además, contiene la clave privada (PriDBT) del servidor de base de datos DBT.

4. Una agencia de certificación de certificados digitales AC. La empresa creadora del producto (fabricante) tendrá dos certificados únicos expedidos por esta agencia de certificados digitales AC. El primero, indicado como CerAPP, será para autentificar la aplicación APP que se ejecuta en el lector NFC, indicado como M, y el segundo, indicado como CerDBT, para autentificar el servidor de base de datos DBT. Estos certificados digitales contienen cada uno una de las dos claves públicas del fabricante.

5. La mencionada aplicación software A en el citado lector NFC M (portable o de otro tipo) que usará la persona que quiera autentificar el producto P. La aplicación software A contiene la clave privada de la aplicación PriAPP.

En cada etiqueta NFC T se graba de forma permanente el IDTAG y un programa. El contenido de la etiqueta NFC T es permanente, no puede ser regrabado o borrado. El programa que se

graba en la etiqueta NFC T contiene, entre otras cosas, de forma secreta, la clave privada PriTAG. El programa grabado es el que se ejecuta en la etiqueta NFC cuando un lector M se acerca lo suficiente a la misma. Este programa tiene la funcionalidad de leer del lector M un dato, firmarlo y devolver la firma y su IDTAG al lector. El programa en sí no se puede leer desde el lector M porque el mismo programa no implementa esta funcionalidad. De esta forma la clave privada PriTAG queda totalmente protegida. La etiqueta NFC firma el dato recibido del lector M mediante la clave privada PriTAG que se encuentra escondida en el programa.

Los siguientes cuatro procesos se llevan a cabo para autentificar la etiqueta T, y por tanto autentificar que el producto P es original del fabricante, según el método del primer aspecto de la invención:

A) Verificación de la autenticidad de la aplicación A.

B) Verificación de la autenticidad del servidor de base de datos DBT.

C) Obtención de la firma digital del producto P o etiqueta T.

D) Verificación de la firma digital de elemento.

Estos cuatro procesos son necesarios para garantizar la legitimidad de todos los componentes que se utilizan para autentificar una etiqueta NFC T, que son la aplicación APP y el servidor de base de datos DBT. La legitimidad de que provienen del fabricante garantiza que todo el proceso de autenticidad de la etiqueta NFC T es válido y no ha sido corrompido por hackers.

Para comprobar la autenticidad de la aplicación en el proceso A por parte del servidor de base de datos DBT se procede siguiendo los siguientes pasos:

A1) Toda información que transmite la aplicación APP se encripta usando la clave pública del servidor de base de datos DBT, que se encuentra en el certificado digital de base de datos CerDBT, generando así un mensaje encriptado de aplicación, el cual se firma digitalmente, por parte de la aplicación A, usando su propia clave privada PriAPP.

A2) El servidor de base de datos DBT comprueba la autenticidad de la aplicación APP comprobando que la firma digital que recibe de la aplicación APP es correcta usando la clave pública contenida en el certificado digital de la aplicación CerAPP.

Del mismo modo se procede a comprobar la autenticad del servidor de base de datos DBT en el paso B siguiendo los siguientes pasos:

B1) Toda información que transmite el servidor de base de datos DBT a la aplicación APP se encripta usando la clave pública de la aplicación, que se encuentra en el certificado

digital de la aplicación CerAPP, generando así un mensaje encriptado de base de datos, el cual es firmado digitalmente, por parte del servidor de base de datos DBT, usando su propia clave privada PriDBT.

B2) La aplicación APP comprueba la autenticidad del servidor de base de datos DBT comprobando que la firma digital que recibe del servidor de base de datos DBT es correcta usando la clave pública PubDBT, obtenida mediante el certificado digital de la base de datos CerDBT o, de manera alternativa, por otra vía, tal como la que se explicará más abajo en relación a la Figura 4.

Para la obtención de la firma digital de la etiqueta NFC T en el proceso C se realizan los siguientes cuatro pasos que se detallan a continuación en orden cronológico y se ilustran también en la Figura 2:

C1) El lector NFC M genera un dato aleatorio.

C2) El dato aleatorio se envía a la etiqueta NFC T.

C3) La etiqueta NFC T recibe el dato del lector NFC M y lo firma digitalmente usando su clave privada PriTAG, es decir genera la anteriormente denominada firma digital de elemento

C4) La firma digital de elemento y el IDTAG de la etiqueta T se envían a la aplicación APP del lector M.

En general, las etapas C1) y C2) se llevan a cabo por parte de la propia aplicación A, aunque, de manera alternativa y menos preferida, éstas se llevan a cabo por parte de otra aplicación o algoritmo.

Para la verificación de la firma digital de elemento, es decir la generada por la etiqueta NFC T, en el proceso D se realizan los siguientes cuatro pasos que se detallan a continuación en orden cronológico y que se ilustran también en la Figura 3:

D1) La aplicación APP determina el fabricante (F) viendo los primeros dígitos del IDTAG que recibe de la etiqueta NFC T.

D2) La aplicación APP obtiene el certificado digital de base de datos correspondiente a F, es decir CerDBT, de la agencia de certificados digitales AC, si aún no lo tiene.

D3) La aplicación APP pregunta al servidor de base de datos DBT por el método de protección matemático MET y por la clave pública PubTAG del producto P asociado a la etiqueta T y de la caducidad del producto CAD, según el paso A1) del proceso A) explicado

arriba, donde dicha pregunta, o solicitud, incluye o constituye la información que transmite la aplicación APP al servidor de base de datos DBT, encriptada y firmada.

D4) El servidor de base de datos DBT obtiene el certificado digital de la aplicación correspondiente a F, es decir CerAPP, de la agencia de certificados digitales AC, si aún no lo tiene

D5) El servidor de base de datos DBT verifica la autenticidad de la aplicación APP según el paso A2) del proceso A) explicado anteriormente.

D6) El servidor de base de datos DBT envía los datos pedidos usando el procedimiento descrito en el paso B1) del proceso B), donde dichos datos constituyen o incluyen la información que transmite el servidor de base de datos DBT a la aplicación A, encriptada y firmada.

D7) La aplicación APP verifica la autenticidad del servidor de base de datos DBT según el paso B2) del proceso B).

D8) Si la autenticidad del servidor de base de datos DBT ha sido verificada en D7), la aplicación APP verifica la autenticidad del producto y que éste no ha caducado (si el producto ha caducado la autenticidad podría no ser válida) mediante la verificación de la firma digital de elemento con la clave pública PubTAG recibida y de su caducidad comprobando la fecha indicada en CAD.

En la Figura 4 se ilustra el anteriormente descrito proceso de autentificación adicional de la aplicación software (proceso E)) a través del cual la aplicación software APP obtiene la clave pública PubDBT de manera alternativa a la descrita en B2), es decir sin la utilización de un certificado digital. En este proceso la clave pública PubDBT es obtenida por la APP de la entidad computacional de base de datos de aplicaciones DBA (que en este caso es de tipo “blockchain” pero podría ser de cualquier otro tipo) a través de la aplicación autentificadora de aplicaciones, según los pasos que se explicarán a continuación, asumiendo que la APP ha sido previamente registrada en la DBA por parte de AAA:

E1) La AAA puede iniciar la autentificación de la APP o la misma APP la puede iniciar también. Caso de iniciar la AAA, ésta pregunta por el identificador de aplicación IDAPP a APP sin encriptar el mensaje. En el caso en que la APP la inicia, se continúa con el paso E2).

E2) APP pide el certificado digital de AAA, es decir CerAAA, a la agencia de certificación ACD.

E3) ACD envía CerAAA a APP, de manera que ésta obtiene la clave pública de AAA, es decir PubAAA.

E4) APP envía IDAPP a AAA con una comunicación segura, es decir encriptando con la PubAAA y firmando digitalmente con su clave privada PriAPP.

E5) AAA una vez recibido el APPID, lo envía a la DBA mediante una comunicación segura, es decir encriptando con la PubDBA y firmando digitalmente con su clave privada PriAAA.

E6) DBA responde a AAA con la PubAPP mediante una comunicación segura, es decir encriptando con la PubAAA y firmando digitalmente con su clave privada PriDBA.

E7) AAA asocia con IDAPP la correspondiente PubAPP recibida.

E8) AAA envía un dato aleatorio (RND) a APP mediante una comunicación segura, es decir encriptando con la PubAPP y firmando digitalmente con su clave privada PriAAA.

E9) APP confirma que AAA es auténtica (comprobando la firma digital recibida de ésta) y devuelve el RND a AAA mediante una comunicación segura, es decir encriptando con la PubAAA y firmando digitalmente con su clave privada PriAPP.

E10) AAA confirma la autenticidad de APP mediante la comprobación de que el RND recibido coincide con el previamente enviado y comprobando su firma.

E11) AAA envía la PubDBT a APP.

La presente invención aporta numerosas ventajas técnicas con respecto a los métodos/sistemas del estado de la técnica, incluyendo las siguientes:

- Mayor seguridad

  La presente invención proporciona una mayor seguridad que los métodos conocidos, evitando así el copiado o “hackeo” de las etiquetas NFC ya producidas. Esto se consigue mediante los mecanismos descritos anteriormente:

  - El copiado está protegido mediante la protección de una clave privada secreta de criptografía la cual esta algorítmicamente protegida de cualquier lectura externa a la etiqueta.
  - Además, se evita el copiado del resultado utilizado en el procedimiento de autentificación ya que el cómputo del resultado se realiza sobre un dato que se desconoce a priori y por lo tanto no puede ser predecible.

- Se garantiza que todos los componentes de comprobación de la autenticidad (aplicación y base de datos) también son auténticos reduciendo notablemente el posible ataque de hackers por suplantación de la identidad de los componentes.
- Las claves generadas por cada producto son temporales y pueden ser revocadas en cualquier momento con lo que aumenta aún más el nivel de seguridad del mecanismo propuesto, ya que, por ejemplo, evita que las claves se reutilicen una vez desechados los productos.
- Ninguna clave privada se transmite entre los distintos componentes por lo que quedan secretas a cualquier hacker.
- Se utilizan claves independientes por cada elemento a autentificar.
- Las comunicaciones entre los distintos componentes se encriptan para garantizar que solamente el receptor de los mensajes pueda leer su contenido y su vez se firman para determinar el emisor de los mensajes y comprobar que su contenido no ha sido modificado.
- El método de protección matemático empleado en cada elemento no está divulgado públicamente, quedando por el contrario protegido en la base de datos. Para conocerlo se requiere previa autentificación en el servidor de la base de datos para obtener la información de verificación del elemento.

- Mayor control
  - Los productos pueden ser fácilmente quitados del consumo, solamente cambiando la fecha de caducidad de las claves asociadas en el servidor de base de datos. Los otros métodos necesitan tener físicamente el producto para destruir su mecanismo de autenticidad o reprogramar de nuevo la etiqueta NFC.
  - Las aplicaciones de autentificación pueden registrar datos de consumo de los usuarios.
  - La complejidad computacional del método de autentificación puede ser controlada independientemente por cada elemento. La complejidad puede ser mayor usando firmas digitales o menor usando operaciones matemáticas.

- Mayor fiabilidad

  La fiabilidad del mecanismo está respaldada por la agencia de certificados digitales en donde previamente ha tenido que autentificar legalmente los distintos certificados digitales usados en la presente invención. Además, permite reducir al mínimo el número de certificados digitales requeridos, pudiendo ser necesario solo un certificado.

- Menor costo de los elementos

  El costo de los elementos está directamente relacionado con la complejidad computacional requerida del método de autentificación. Con la presente invención se puede emplear una complejidad mínima y por lo tanto minimizar así el costo de los elementos para productos que son más sensibles al precio.

Un experto en la materia podría introducir cambios y modificaciones en los ejemplos de realización descritos sin salirse del alcance de la invención según está definido en las reivindicaciones adjuntas.

REIVINDICACIONES

1.- Método de autentificación de elementos de identificación por radiofrecuencia, que comprende:

- aplicar una o varias operaciones aritméticas o una firma digital, por parte de un elemento de identificación por radiofrecuencia (T) con capacidad de procesamiento, sobre al menos un dato, utilizando al menos una clave privada de elemento (PriTAG) almacenada en dicho elemento de identificación por radiofrecuencia (T), obteniendo un resultado de elemento;

- enviar dicho resultado de elemento, utilizando una tecnología de comunicación inalámbrica, por parte de dicho elemento de identificación por radiofrecuencia, a un dispositivo de computación lector de elementos de identificación por radiofrecuencia (M); y

- verificar dicho resultado de elemento, por parte de dicho dispositivo de computación lector de elementos de identificación por radiofrecuencia (M), utilizando información de verificación asociada a dicha clave privada de elemento (PriTAG);

estando el método **caracterizado** porque comprende obtener dicha información de verificación asociada a dicha clave privada de elemento (PriTAG) de un servidor de base de datos (DBT), por parte de dicho dispositivo de computación lector de elementos de identificación por radiofrecuencia (M), y porque el método comprende autentificar también a dicho servidor de base de datos (DBT) y a una aplicación software (APP) instalada en una memoria del dispositivo de computación lector de elementos de identificación por radiofrecuencia (M) encargada de llevar a cabo dicha verificación del resultado de elemento.

2.- Método según la reivindicación 1, caracterizado porque dicha información de verificación incluye información identificativa sobre la operación u operaciones aritméticas empleadas o sobre la firma digital empleada para obtener dicho resultado de elemento.

3.- Método según la reivindicación 1 ó 2, caracterizado porque comprende aplicar dicha o dichas operaciones aritméticas por parte de dicho elemento de identificación por radiofrecuencia (T) con capacidad de procesamiento, incluyendo dicha información de verificación el resultado de una función Hash aplicada sobre la clave privada de elemento (PriTAG), y realizando la aplicación software (APP) los siguientes pasos, de manera secuencial y sucesiva:

i) la aplicación de la operación u operaciones inversas a dicha o dichas operaciones aritméticas, sobre el resultado de elemento;

ii) la aplicación de dicha función Hash sobre el resultado obtenido en i); y

iii) la comparación del resultado obtenido en ii) con el resultado que constituye dicha información de verificación.

4.- Método según la reivindicación 3 cuando depende de la 2, caracterizado porque comprende, de manera previa a dicha etapa i) y con el fin de conocer qué operación u operaciones aritméticas ha aplicado el elemento de identificación por radiofrecuencia (T) con capacidad de procesamiento, identificar, por parte de la aplicación software (APP), la operación u operaciones aritméticas aplicadas, a través de dicha información identificativa incluida en la información de verificación.

5.- Método según la reivindicación 1 ó 2, caracterizado porque comprende, por parte de dicho elemento de identificación por radiofrecuencia (T) con capacidad de procesamiento, aplicar dicha firma digital, siendo dicho resultado de elemento una firma digital de elemento e incluyendo dicha información de verificación una clave pública de elemento (PubTAG) asociada a dicha clave privada de elemento (PriTAG).

6.- Método según una cualquiera de las reivindicaciones, caracterizado porque comprende llevar a cabo dicha autentificación de dicho servidor de base de datos (DBT) por parte de dicho dispositivo de computación lector de elementos de identificación por radiofrecuencia (M), utilizando dicha (APP) u otra aplicación software.

7.- Método según una cualquiera de las reivindicaciones, caracterizado porque comprende llevar a cabo dicha autentificación de dicha aplicación software (APP) por parte de dicho servidor de base de datos (DBT).

8.- Método según la reivindicación 7 cuando depende de la 6, caracterizado porque comprende llevar a cabo dicha autentificación del servidor de base de datos (DBT) y dicha autentificación de la aplicación software (APP), mediante la utilización de una clave asimétrica de servidor de base de datos que incluye una clave privada de servidor de base de datos (PriDBT) y una clave pública de servidor de base de datos (PubDBT), y de una clave asimétrica de aplicación que incluye una clave privada de aplicación (PriAPP) y una clave pública de aplicación (PubAPP), comprendiendo el método:

- firmar digitalmente, por parte de la aplicación software (APP), la información que le transmite al servidor de base de datos (DBT) utilizando la clave privada de aplicación (PriAPP) y verificar, por parte del servidor de base de datos (DBT), la

autenticidad de la firma digital recibida de la aplicación software (APP) utilizando la clave pública de aplicación (PubAPP), y

- firmar digitalmente, por parte del servidor de base de datos (DBT), la información que le transmite a la aplicación software (APP) utilizando la clave privada de DBT (PriDBT) y verificar, por parte de la aplicación software (APP), la autenticidad de la firma digital recibida del servidor de base de datos (DBT) utilizando la clave pública de base de datos (PubDBT).

9.- Método según la reivindicación 8, caracterizado porque comprende además:

- encriptar, por parte de la aplicación software (APP), la información que le transmite al servidor de base de datos (DBT), utilizando la clave pública de base de datos (PubDBT), y desencriptarla, por parte del servidor de base de datos (DBT), utilizando la clave privada de del servidor de base de datos (PriDBT); y

- encriptar, por parte del servidor de base de datos (DBT), la información que le transmite a la aplicación software (APP), utilizando la clave pública de aplicación (PubAPP), y desencriptarla, por parte de la aplicación software (APP), utilizando la clave privada de aplicación (PriAPP).

10.- Método según una cualquiera de las reivindicaciones, caracterizado porque comprende enviar junto con dicho resultado de elemento, por parte del elemento de identificación por radiofrecuencia (T) al dispositivo de computación lector de elementos de identificación por radiofrecuencia (M), un número identificativo único (IDTAG) asociado al mismo.

11.- Método según la reivindicación 10, caracterizado porque dicho servidor de base de datos (DBT) tiene almacenada información referente a una pluralidad de elementos de identificación por radiofrecuencia (T), o de productos (P) asociados a los mismos, que incluye, para cada elemento, un número identificativo único (IDTAG), información de caducidad (CAD), e información de verificación asociada a cada clave privada de elemento (PriTAG), comprendiendo el método:

- solicitar, por parte de la aplicación software (APP) al servidor de base de datos, la información de verificación asociada a la clave privada de elemento (PriTAG) y la información de caducidad (CAD) asociada al número identificativo (IDTAG) recibido junto con el resultado de elemento, mediante el envío de una solicitud que incluye o constituye dicha información al menos firmada digitalmente utilizando la clave privada de aplicación (PriAPP);

- verificar, por parte del servidor de base de datos (DBT), la autenticidad de la firma digital recibida de la aplicación software (APP) utilizando la clave pública de aplicación y en caso afirmativo enviar, por parte del servidor de base de datos (DBT) a la aplicación software (APP), la información de verificación asociada a la clave privada de elemento (PriTAG) y la información de caducidad (CAD) solicitadas, las cuales constituyen dicha información al menos firmada digitalmente utilizando la clave privada de base de datos (PriDBT); y

- verificar, por parte de la aplicación software (APP) la autenticidad de la firma digital recibida del servidor de base de datos (DBT) utilizando la clave pública de base de datos (PubDBT) y en caso afirmativo verificar la autenticidad del resultado de elemento y también la caducidad (CAD) asociada a su número identificativo (IDTAG).

12.- Método según una cualquiera de las reivindicaciones, caracterizado porque comprende realizar una autentificación adicional de la aplicación software (APP) por parte de una aplicación autentificadora de aplicaciones (AAA) y una entidad computacional de base de datos de aplicaciones (DBA).

13.- Método según la reivindicación 12 cuando depende de la 11, caracterizado porque comprende obtener dicha clave pública de base datos (PubDBT) por parte de la aplicación software (APP) desde dicha entidad computacional de base de datos de aplicaciones (DBA) a través de dicha aplicación autentificadora de aplicaciones (AAA), y condicionado a que el resultado de dicha autentificación adicional sea positivo.

14.- Método según la reivindicación 11 cuando depende de la 8 o la 9, caracterizado porque está aplicado a un escenario que incluye una pluralidad de servidores de bases de datos, al menos uno por fabricante, donde dicho número identificativo (IDTAG) incluye información identificativa de fabricante, comprendiendo el método determinar, por parte de la aplicación software (APP), cuál es el servidor de base de datos (DBT) asociado al fabricante indicado por dicha información identificativa de fabricante a la que enviarle dicha solicitud y la obtención, por parte del servidor de base de datos (DBT), si no dispone del mismo, de un certificado digital de la aplicación software (CerAPP) que incluye la clave pública de aplicación (PubAPP).

15.- Método según la reivindicación 14, caracterizado porque comprende la obtención, por parte de la aplicación software (APP), si no dispone del mismo, de un certificado digital de base de datos (CerDBT) que incluye a la clave pública de base de datos (PubDBT).

16.- Método según la reivindicación 14 ó 15, caracterizado porque está aplicado a un escenario que incluye una pluralidad de aplicaciones software aptas para llevar a cabo dicha verificación del resultado de elemento, instaladas en unas respectivas memorias de unos dispositivos de computación lectores de elementos de identificación por radiofrecuencia (M), teniendo asociado cada una de dichas aplicaciones software un correspondiente número de identificación (IDAPP), donde el método comprende incluir dicho número de identificación en la información enviada desde la aplicación software (APP) al servidor de base de datos (DBT), y realizar, por parte del servidor de base de datos (DBT), la identificación de la aplicación software (APP) por el número de identificación (IDAPP) recibido.

17.- Método según la reivindicación 16, caracterizado porque cada una de dichas aplicaciones software tiene asociado un certificado digital único con sus respectivas claves privada y pública de aplicación y dicho correspondiente número de identificación (IDAPP), donde el método comprende realizar, por parte del servidor de base de datos (DBT), el acceso al certificado digital de la aplicación software (APP) identificada por su número de identificación (IDAPP) para obtener la correspondiente clave pública de aplicación (PubAPP).

18.- Método según la reivindicación 16, caracterizado porque varias o todas dichas aplicaciones software comparten un certificado digital común asociado a todos los números de identificación de las aplicaciones software que lo comparten, donde el método comprende realizar, por parte del servidor de base de datos, (DBT) el acceso a dicho certificado digital común asociado a la aplicación software (APP) identificada por su número de identificación (IDAPP) para obtener la correspondiente clave pública de aplicación (PubAPP).

19.- Método según una cualquiera de las reivindicaciones, caracterizado porque comprende generar dicho dato, que es al menos uno, de manera aleatoria por parte de dicho dispositivo de computación lector de elementos de identificación por radiofrecuencia (M) y enviarlo a dicho elemento de identificación por radiofrecuencia (T) utilizando dicha tecnología de comunicación inalámbrica.

20.- Método según la reivindicación 19, caracterizado porque dicha clave privada de elemento (PriTAG) se encuentra contenida en código de programa no leíble desde el exterior que está grabado en el elemento de identificación por radiofrecuencia (T), siendo dicho código de programa encargado de leer dicho dato, firmarlo digitalmente y

enviárselo, junto con un número identificativo único (IDTAG), al dispositivo de computación lector de elementos de identificación por radiofrecuencia (M).

21.- Método según una cualquiera de las reivindicaciones anteriores, caracterizado porque dicha tecnología de comunicación inalámbrica es una tecnología de comunicación de campo cercano.

22.- Sistema de autentificación de elementos de identificación por radiofrecuencia, caracterizado porque está adaptado para implementar el método según una cualquiera de las reivindicaciones 1 a 21, y comprende:

- un dispositivo de computación lector de elementos de identificación por radiofrecuencia (M), con capacidad de comunicación según una tecnología de comunicación inalámbrica; y

- al menos un elemento de identificación por radiofrecuencia (T) que comprende unos medios de procesamiento, unos medios de almacenamiento y unos medios de comunicación que operan según una tecnología de comunicación inalámbrica, estando dicho elemento de identificación por radiofrecuencia (T) configurado y adaptado para, mediante dichos medios de procesamiento, aplicar una o varias operaciones aritméticas o una firma digital, sobre al menos un dato, utilizando una clave privada de elemento (PriTAG) almacenada en dichos medios de almacenamiento, obteniendo un resultado de elemento, y enviar, utilizando dichos medios de comunicación, dicho resultado de elemento a dicho dispositivo de computación lector de elementos de identificación por radiofrecuencia (M);

estando dicho dispositivo de computación lector de elementos de radiofrecuencia (M) configurado y adaptado para verificar el resultado de elemento recibido utilizando información de verificación asociada a dicha clave privada de elemento (PriTAG);

estando el sistema **caracterizado** porque comprende:

- un servidor de base de datos (DBT) que tiene registrada dicha información de verificación asociada a dicha clave privada de elemento (PriTAG) y que es accesible, a través de una vía de comunicación, por parte del dispositivo de computación lector de elementos de identificación por radiofrecuencia (M), el cual está configurado y adaptado para obtener dicha información de verificación asociada a dicha clave privada de elemento (PriTAG) accediendo a dicho servidor de base de datos (DBT);

- una aplicación software (APP) instalada en una memoria del dispositivo de computación lector de elementos de identificación por radiofrecuencia (M) y encargada de llevar a cabo dicha verificación del resultado de elemento;

- unos primeros medios de autentificación encargados de autentificar a dicho servidor de base de datos (DBT); y

- unos segundos medios de autentificación encargados de autentificar a dicha aplicación software (APP).

23.- Sistema según la reivindicación 22, caracterizado porque dichos primeros medios de autentificación se encuentran implementados en el dispositivo de computación lector de elementos de identificación por radiofrecuencia (M), mediante dicha (APP) u otra aplicación software y/o dichos segundos medios de autentificación se encuentran implementados en al menos dicho servidor de base de datos (DBT).

24.- Sistema según la reivindicación 23, caracterizado porque los segundos medios de autentificación se encuentran implementados también en una aplicación autentificadora de aplicaciones (AAA) y una entidad computacional de base de datos de aplicaciones (DBA) que operan según el método de la reivindicación 12 ó 13.

25.- Sistema según la reivindicación 24, caracterizado porque comprende una agencia de certificación (AC) de certificados digitales encargada de expedir dichos certificados digitales, siendo dicha agencia de certificación (AC) accesible tanto por lo(s) servidor(es) de bases de datos (DBT) como por la(s) aplicación(es) software (APP), a través de unas correspondientes vías de comunicación, para obtener dichos certificados digitales con el fin de implementar el método según la reivindicación 14, 15, 16 ó 17.

26.- Programa de ordenador, que incluye instrucciones de código de programa que, cuando se ejecutan en unas entidades computacionales, específicamente parte en un elemento de identificación por radiofrecuencia con capacidad de procesamiento, parte en un dispositivo de computación lector de elementos de identificación por radiofrecuencia y parte en al menos un servidor de base de datos, implementan las etapas del método según una cualquiera de las reivindicaciones 1 a 21.

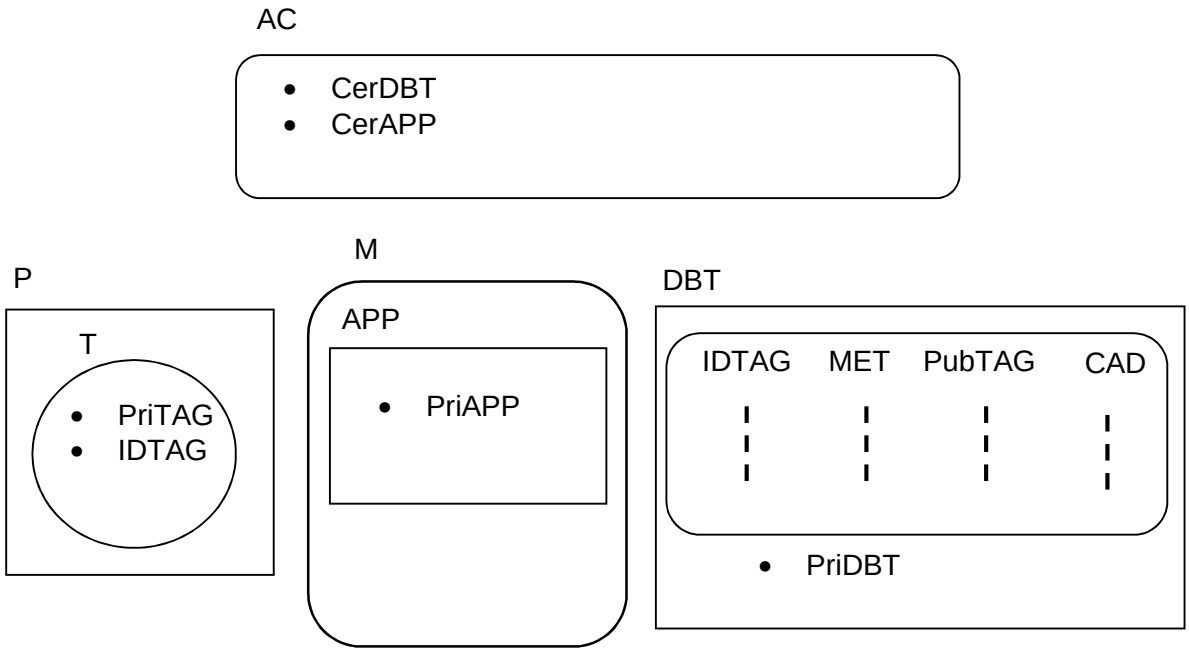
AC
CerDBT
CerAPP
P
T
PriTAG
IDTAG
M
APP
PriAPP
DBT
IDTAG
MET
PubTAG
CAD
PriDBT

Fig. 1

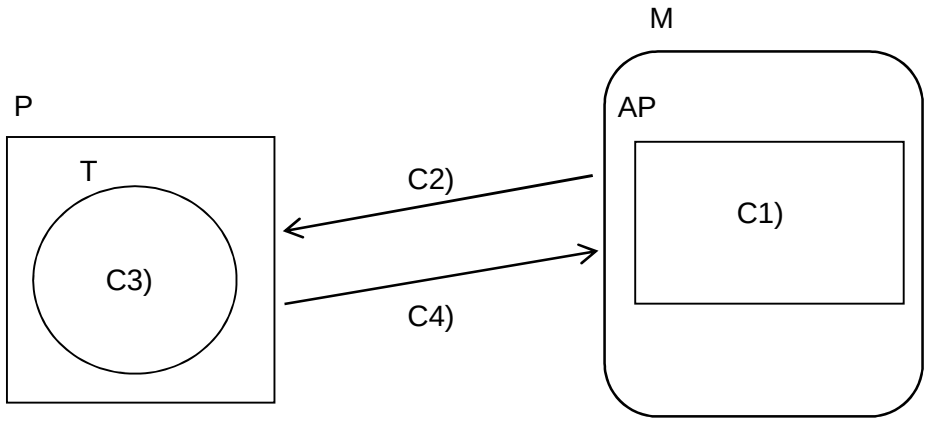
M
P
AP
T
C2)
C1)
C3)
C4)

Fig. 2

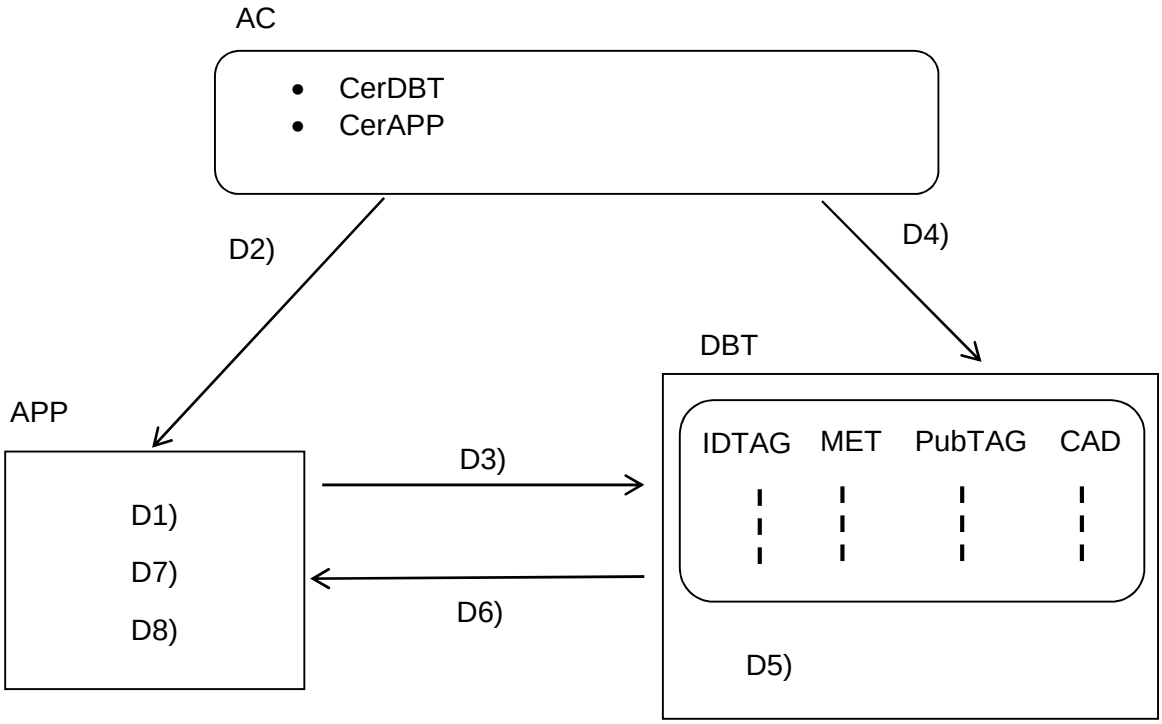
AC
CerDBT
CerAPP
D2)
D4)
DBT
APP
IDTAG
MET
PubTAG
CAD
D3)
D1)
D7)
D8)
D6)
D5)

Fig. 3

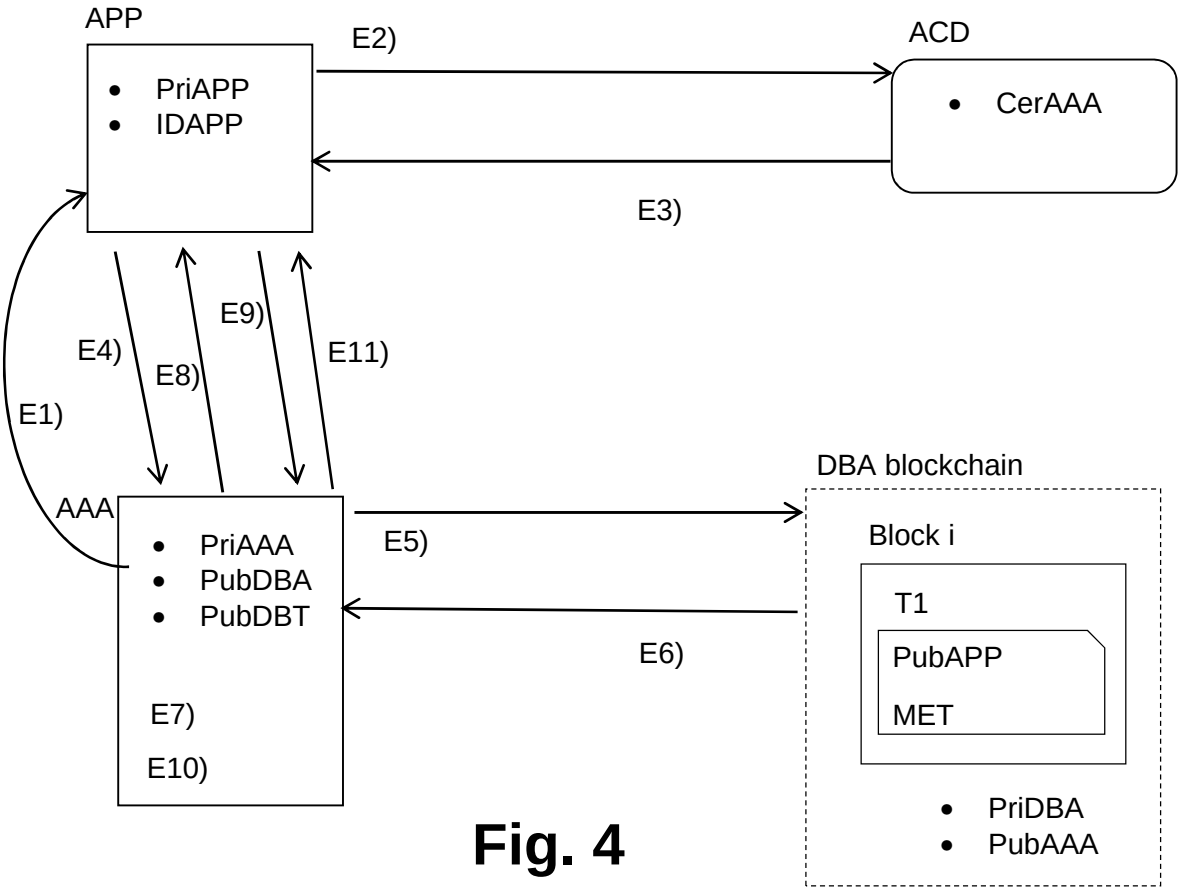
APP
PriAPP
IDAPP
E2)
ACD
CerAAA
E3)
E4)
E8)
E9)
E11)
E1)
AAA
PriAAA
PubDBA
PubDBT
E7)
E10)
E5)
E6)
DBA blockchain
Block i
T1
PubAPP
MET
PriDBA
PubAAA

Fig. 4

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 201531078

(22) Fecha de presentación de la solicitud: 22.07.2015

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl. :** ***G06Q30/00*** (2012.01)

DOCUMENTOS RELEVANTES

Categoría	(56) **Documentos citados**	**Reivindicaciones afectadas**
Y	US 2005033689 A1 (BONALLE DAVID S et al.) 10/02/2005, Descripción; páginas. 71-75. Figura 4.	1-26
Y	KR 20120010604 A (IAC IN NAT UNIV CHUNGNAM) 06/02/2012, Resumen Epodoc, resumen WPI	1-26
A	CN 101662366 A (CHINA INSTANT WIRELESS NETWORK) 03/03/2010, Resumen Epodoc, resumen WPI	3
A	EP 1209576 A1 (SONY CORP) 29/05/2002, Descripción; páginas. 87-207	5
A	US 2010001840 A1 (KANG YOU SUNG et al.) 07/01/2010, Todo el documento.	1
A	US 2007052525 A1 (QUAN CHENGHAO et al.) 08/03/2007, Todo el documento.	1
A	CN 102737260 A (SHENZHEN ZHIYUAN BEIJING TECHNOLOGY CO LTD) 17/10/2012, Todo el documento.	1

Categoría de los documentos citados
X: de particular relevancia
Y: de particular relevancia combinado con otro/s de la misma categoría
A: refleja el estado de la técnica
O: referido a divulgación no escrita
P: publicado entre la fecha de prioridad y la de presentación de la solicitud
E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado

☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	**Examinador**	**Página**
09.12.2016	M. Muñoz Sanchez	1/5

Documentación mínima buscada (sistema de clasificación seguido de los símbolos de clasificación)

H04L, G06Q

Bases de datos electrónicas consultadas durante la búsqueda (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)

INVENES, EPODOC, WPI

Fecha de Realización de la Opinión Escrita: 09.12.2016

Declaración

Novedad (Art. 6.1 LP 11/1986)	Reivindicaciones	1-26	**SI**
	Reivindicaciones		**NO**
Actividad inventiva (Art. 8.1 LP11/1986)	Reivindicaciones		**SI**
	Reivindicaciones	1-26	**NO**

Se considera que la solicitud cumple con el requisito de aplicación industrial. Este requisito fue evaluado durante la fase de examen formal y técnico de la solicitud (Artículo 31.2 Ley 11/1986).

Base de la Opinión.-

La presente opinión se ha realizado sobre la base de la solicitud de patente tal y como se publica.

1. Documentos considerados.-

A continuación se relacionan los documentos pertenecientes al estado de la técnica tomados en consideración para la realización de esta opinión.

Documento	Número Publicación o Identificación	Fecha Publicación
D01	US 2005033689 A1 (BONALLE DAVID S et al.)	10.02.2005
D02	KR 20120010604 A (IAC IN NAT UNIV CHUNGNAM)	06.02.2012
D03	CN 101662366 A (CHINA INSTANT WIRELESS NETWORK)	03.03.2010
D04	EP 1209576 A1 (SONY CORP)	29.05.2002
D05	US 2010001840 A1 (KANG YOU SUNG et al.)	07.01.2010
D06	US 2007052525 A1 (QUAN CHENGHAO et al.)	08.03.2007
D07	CN 102737260 A (SHENZHEN ZHIYUAN BEIJING TECHNOLOGY CO LTD)	17.10.2012

2. Declaración motivada según los artículos 29.6 y 29.7 del Reglamento de ejecución de la Ley 11/1986, de 20 de marzo, de Patentes sobre la novedad y la actividad inventiva; citas y explicaciones en apoyo de esta declaración

Se considera D01 el documento más próximo del estado de la técnica al objeto de la solicitud.

Reivindicaciones independientes

Reivindicación 1: El documento D01 divulga en un modo de realización particular un sistema de gestión y control de etiquetas RFID que comprende un servidor de base de datos con información de identificación y verificación asociadas a las etiquetas RFID (identificador y clave de cifrado) y un lector de etiquetas RFID. En la autenticación mutua entre el lector y la etiqueta, un dato (código de autenticación, aleatorio) se firma (cifra), con la clave de la etiqueta y se le transmite dicho dato al lector de tarjetas RFID. Dicho lector solicita a la base de datos la clave de descifrado correspondiente al identificador de la etiqueta (obtenido previamente de la etiqueta). El lector descifra el dato comprobando entonces si coincide con el generado previamente por él y en dicho caso confirmando la identidad de la etiqueta y continuando el procesamiento (figura 4, páginas. 71-75).
La diferencia entre el documento D01 y la reivindicación 1 es que no se realiza una autenticación del servidor y del lector, lo que aumenta la seguridad del procedimiento evitando que sea ejecutado por dispositivos fraudulentos. Por tanto, el problema técnico objetivo sería cómo añadir esta seguridad adicional.
En el documento D02, por su parte identifica este problema técnico, concretamente la suplantación de identidad del servidor y el lector (resumen Epodoc, resumen WPI). Por tanto, la combinación de los documentos D01 y D02 afecta a la actividad inventiva de la reivindicación 1 según el art. 8.1 de la Ley de Patentes.

Reivindicación 22: el sistema reivindicado se corresponde directamente con las funcionalidades y operaciones del procedimiento reivindicado. Por tanto, la combinación de los documentos D01 y D02 afecta a la actividad inventiva de la reivindicación 22 según el art. 8.1 de la Ley de Patentes.

Reivindicación 26: el programa de ordenador reivindicado se corresponde directamente con las operaciones del procedimiento reivindicado. Por tanto, la combinación de los documentos D01 y D02 afecta a la actividad inventiva de la reivindicación 26 según el art. 8.1 de la Ley de Patentes.

Reivindicaciones dependientes

Reivindicación 2: el contenido de esta reivindicación está incluido en el documento D01.

Reivindicación 3: el uso de operaciones aritméticas sin más es una alternativa a la firma que no tiene efecto técnico definido (adicional al de la firma) y, por tanto, resulta evidente para el experto en la materia. Por otra parte, el uso de funciones hash en procedimientos de autenticación es comúnmente conocida. Ilustrativamente, se cita el documento D03 que da muestra de este hecho (resumen Epodoc, resumen WPI).

Reivindicación 4: el contenido de esta reivindicación está incluido en el documento D01.

Reivindicaciones 5-9: el contenido de estas reivindicaciones especifica la autenticación mutua entre dos dispositivos comúnmente conocida en el campo técnico de la solicitud. Ilustrativamente se cita el documento D04 (por ejemplo, páginas. 87-207) que da muestra de este hecho.

Reivindicación 10: el contenido de esta reivindicación está incluido en el documento D01.

Reivindicación 11: la información adicional relativa a la caducidad no supone la alteración de la esencia del procedimiento ni un efecto técnico adicional al margen del mismo. Por tanto, a la hora de evaluar la actividad inventiva de esta reivindicación, se considera que dicha información no contribuye a la misma.

Reivindicaciones 12-13: la autenticación adicional de la aplicación del lector y la obtención indirecta del certificado/ clave pública de la base de datos a través de una aplicación autenticadora de aplicaciones se considera un complemento no necesario y que no altera el procedimiento de reivindicado. Por tanto, como alternativa accesoria se considera evidente para el experto en la materia.

Reivindicaciones 14-18: los escenarios planteados con los identificadores particulares para cada fabricante y las posibles estrategias de asignación de certificados común o individualmente para las aplicaciones resultan alternativas igualmente posibles, opcionales o complementarias que suponen una mera extensión de la esencia del procedimiento a la existencia de una pluralidad de entidades de cada tipo en lugar de una única aplicación y un único fabricante. En consecuencia, el contenido de estas reivindicaciones se considera evidente para el experto en la materia.

Reivindicación 19: la aleatoriedad del dato se menciona en el documento D01.

Reivindicación 20: el almacenamiento de la clave privada en una zona de seguridad, o elemento seguro, es comúnmente conocida y, por tanto, considerada evidente para el experto en la materia.

Reivindicación 21: las tecnologías NFC aplicadas al intercambio de información entre dispositivos es comúnmente conocida y, por tanto, considerada evidente para el experto en la materia.

Reivindicaciones 23-25: la ubicación de medios autenticadores es la correspondiente a la indicada en el procedimiento reivindicado. La existencia de una autoridad de certificación es una alternativa comúnmente conocida en la validación/ emisión de certificados digitales y, por tanto considerada evidente para el experto en la materia.
Por tanto, la combinación de los documentos D01 y D02 afecta a la actividad inventiva de las reivindicaciones 2-21, 23-25 según el art. 8.1 de la Ley de Patentes.