

CASTELLANOS & Co.
Calle 84 A No. 7-09
Bogotá-Colombia

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
Rad: 06-121494-00002-0000
Fec: 2007-03-21 14:51:42 Dep. 2007-03-21 14:51:42
FOLIO 11 PATENTE
EVS: 3/0 FASE NACIONAL
ACT 444 RESPUESTA A EXAMEN DE FORMA

Señora

Jefe de la División de Nuevas Creaciones

Superintendencia de Industria y Comercio

Ministerio de Comercio, Desarrollo Industria y Turismo

E. S. D.

Ref.: Expediente No. 06.121.494

Solicitud de Patente PCT entrada Fase Nacional para:

**"PROCESO Y SISTEMA DE AUTENTIFICACIÓN DE PRODUCTOS
POR MEDIOS FUERA DE LINEA"**

Solicitante: ISAAC LEO BAIN

RESPUESTA A EXAMEN DE FORMA

MARGARITA CASTELLANOS ABONDANO, mayor de edad, identificada y domiciliada como aparece al pie de mi firma, en atención a su oficio No. 825 notificado el 26 de enero de 2007, atentamente me permito dar repuesta al mismo de la siguiente manera:

Establece el funcionario examinador lo siguiente:

- ***"El solicitante debe adjuntar la traducción de los anexos del reporte de examen preliminar internacional"***
- ***"la solicitud no contiene el poder debidamente otorgado, con el lleno de los requisitos exigidos por los artículos 63 y subsiguientes del Código de Procedimiento Civil. Adicionalmente, deberá presentar el documento que acredita la existencia y representación legal de la sociedad solicitante, cuando ésta fuere persona jurídica"***.

Con el objeto de atender a las anteriores observaciones, me permito presentar los siguientes documentos:

- Copia del Reporte de Examen Preliminar Internacional junto con los anexos.

- Nuevo texto en español el cual incluye las modificaciones contenidas en los anexos del IPRP (páginas 6, 8, 15, 28 a 31).
- Sustitución de poder a nombre de **MARGARITA CASTELLANOS**
- Copia auténtica del documento de poder otorgado por el solicitante debidamente notariado y legalizado por el cónsul de Colombia en Brasil.

Cumplido así con lo dispuesto, atentamente solicito a Ud. se continúe con el trámite correspondiente a esta solicitud de Patente de Invención.

De la Señora Jefe,


Margarita Castellanos Abondano

C.C. No. 39.779.654 de Usaquén

T.P.A. No. 70819 del C. Sup. de la Judicatura

Carrera 9 No. 93 - 09 - Santa Fe de Bogotá

Teléfonos: 610 74 80 y 610 74 60

Santa Fe de Bogotá, D.C., 21 MAR. 2007

Patentes/14/1422-FNPCT/MEMORIALES/MEMORIAL FORMA

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 1035-0002		FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/BR 2005/000025	International filing date (day/month/year) 1 March 2005 (01.03.2005)	Priority Date (day/month/year) 4 June 2004 (04.06.2004)	
International Patent Classification (IPC) or national classification and IPC IPC⁸: G06K 19/10 (2006.01); G06Q 30/00 (2006.01); G07G 1/00 (2006.01)			
Applicant BAIN ISAAC LEO			
1. This international preliminary examination report has been prepared by this International Preliminary Examination Authority and is transmitted to the applicant according to Article 36. 2. This REPORT consists of a total of <u>5</u> sheets, including this cover sheet. ☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT). These annexes consist of a total of <u>7</u> sheets. 3. This report contains indications relating to the following items: I. ☒ Basis of the opinion II. ☐ Priority III. ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability IV. ☐ Lack of unity of invention V. ☒ Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement VI. ☐ Certain documents cited VII. ☐ Certain defects in the international application VIII. ☐ Certain observations on the international application			
Date of submission of the demand 4 November 2005 (04.11.2005)		Date of completion of this report 29 August 2006 (29.08.2006)	
Name and mailing address of the IPEA/AT Austrian Patent Office Dresdner Straße 87 A-1200 Vienna Facsimile No. 1/53424/200		Authorized officer HARASEK S. Telephone No. 1/53424/574	

Form PCT/IPEA/409 (cover sheet) (July 1998)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/BR 2005/000025

I. Basis of the report

1. With regard to the elements of the international application:*

- ☐ the international application as originally filed
- ☒ the description:
pages 1-4, 6, 8-13, 15-26, as originally filed
pages 5, 7, 14, filed with the demand
pages _____, filed with the letter of _____
- ☒ the claims:
pages _____, as originally filed
pages _____, as amended (together with any statement) under Article 19
pages 1-4, filed with the demand
pages _____, filed with the letter of _____
- ☒ the drawings:
pages 1-5, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____
- ☐ the sequence listing part of the description:
pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

2. With regard to the language, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language _____ which is:

- ☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any nucleotide and/or amino acid sequence disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in printed form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

- ☐ the description, pages _____.
- ☐ the claims, Nos. _____.
- ☐ the drawings, sheets/fig. _____.

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(e)).**

* Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as „originally filed“ and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17).

** Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.

Form PCT/IBPA/409 (Box I) (July 1998)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/BR 2005/000025

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement Novelty (N)	Claims 1-32	YES
	Claims —	NO
Inventive step (IS)	Claims 2-10, 14, 17-19, 21, 26-30, 32	YES
	Claims 1, 11-13, 15, 16, 20, 22-25, 31	NO
Industrial applicability (IA)	Claims 1-32	YES
	Claims —	NO

Citations and explanations (Rule 70.7)

This report takes into consideration the submissions filed with the letter dated 28 June 2006.

The applicant submits that in the prior art cited in the international search report (D1: US20040034579A1; D2: US20030085797A1; D3: JP2003216710A; D4: JP2002183270A) product authentication is done on-line instead of off-line as claimed in the present application. It is further argued that off-line product authentication could not be considered obvious from the cited prior art.

All cited documents deal with methods or systems for authenticating products in connexion with a sales process. The use of a product code affixed to the product and its retrieval in the checking procedure is common to all disclosed embodiments. Furthermore, a message indicating the result of the checking procedure is also disclosed in the cited documents.

Therefore, documents D1-D4 clearly show features i) – v) of claim 1 of the application under consideration related to an authentication process. Feature vi), however, is explicitly mentioned only in D1 and D2, while especially in D4 updating of the data-storage is only implicitly disclosed as the database of D4 is described to also contain availability-data of products. Thus, the only difference between the embodiments disclosed in D1 and D2 and the subject-matter of claim 1 is that the system of claim 1 works off-line instead of on-line.

A possible way to realise an off-line system would for instance be to have the database stored on a local storage medium (instead of on a remote server) and perform updates from time to time by exchange of data carriers. With regard to security concerns – as also alluded to in the submissions filed – protection against unauthorised use and access must be accomplished in the case of on-line methods as well as for off-line methods.

This difference of the claimed subject matter from the state of the art can, thus, not be regarded as involving an inventive step, since it is more than obvious to anyone that the on-line system described in D1 or D2 can be substituted by an off-line system with periodical exchange of data to achieve a comparable functionality without the need for a permanent or instant data link to a remote database.

Supplemental Box

(To be used when the space in any of the preceding boxes is not sufficient)

Continuation of: Box V (page 1)

Further features of claims 11-13, 15, and 16, such as the code being realised as a bar code or being stored in an electronic chip and the code being inseparable from the product are again disclosed in D1-D4. The same applies to the features of claims 20, 22-25, and 31 relating to an authentication system.

The possible use of encrypted data is only outlined in D3 and D4, but is not described in detail like it is done in the application under consideration.

Summarising, only claims 2-10, 14, 17-19, 21, 26-30, and 32 can be considered involving an inventive step. Industrial applicability is given.

Additionally, it is pointed out that the subject matter protection is sought for is in part strongly related to methods of doing business which in several cases of regional or national patent regulations are excluded from patentability.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/BR 2005/000025

Supplemental Box
(To be used when the space in any of the preceding boxes is not sufficient)

Continuation of: Box I

In the demand for international preliminary examination the applicant indicates that the claims have been amended under Article 19 PCT. However, the International Preliminary Examining Authority (IPEA) was informed by the International Bureau that no amendments under Article 19 have been filed. This opinion is therefore based on the amendments filed before the IPEA with the demand.

vi. Updating the indication of the validity of said string of characters in a data-storage unit; and

vii. Periodically updating in said data-storage unit the validity indication of said string of characters and the validity indications of strings of characters that identify other products.

According to the process of the present invention, a string of characters is chosen in such manner as to exclusively identify a given product (i). Such a string of characters, as mentioned above, is defined as that product's identity (ID).

The ID can be, for instance, the product's serial number, thus preventing ambiguities with other products. However, any string of characters able to identify the product uniquely can be used as an ID in the process of the present invention. As soon as the product is put on the market, its ID becomes valid (authorized). This status can change later, as will be described.

The product's ID may contain information other than the minimum necessary to individualize the product. For instance, the ID may contain characters that help to check whether it is formally consistent, and/or characters used for delivering a message.

If an ID is not formally consistent, it is not considered valid. An example of characters that help to check if a product's ID is formally consistent is an identifier of the location where the product is supposed to be sold or distributed. An ID containing such an identifier will only be considered formally consistent if the verification of its consistency is done on the site the product had been destined to.

Another example is a string of characters which is a function of the contents of the ID, such as a digital signature or the input of a hash function. An example of a good hash function is a transformation that takes a string of characters (input) and, based on it, produces another string of characters (output) such that it is very difficult for those who do not know the algorithm that computes the function to produce a valid input-output pair not yet disclosed. An ID containing a digital signature or a hash input value will only be considered formally

checks whether the ID is valid or invalid, possibly by consulting the contents of a data-storage unit; and (v) delivers a message that depends on the validity of said ID. The message helps the person to decide if the product submitted to the process of the present invention is authentic or false.

5 The off-line checker may be, for instance, a personal computer equipped with a bar-code reader to retrieve and process the information in the ID represented by a bar code fixed on the product.

 The data-storage unit may be, for example, a database that contains a list of valid IDs or a list of invalid IDs in case hash-type redundancy is
10 used.

 If the ID contains characters to test formal consistency, the validity check (iv) of the retrieved ID includes testing its consistency. If the checker determines that the ID retrieved from the product is not formally consistent, it considers the ID invalid and, consequently, (v) displays a warning message or
15 an incomprehensible message.

 For example, if the ID contains an identifier of the site the product is intended for sale/distribution at, the checker verifies if the identifier does in fact correspond to the site where checking is taking place, in order to prevent shipments from being illegally diverted to other sites. In case such deviation is
20 detected, an alert or incomprehensible message is displayed.

 If the ID contains a digital signature, the checker tries to confirm that the signature is consistent with the rest of the data contained in the ID. If it is not, an alert or incomprehensible message is displayed.

 If the ID contains redundancy characters such as a hash input
25 value, the checker applies the attendant hash algorithm to the data in the ID in order to determine consistency with the redundancy characters. If they are not consistent, an alert or incomprehensible message is displayed.

 In case the retrieved ID is not rejected in any of the formal consistency tests, the checker consults the data-storage unit to determine if
30 said ID is valid or invalid (iv).

 To make economic use of data storage capacity of said data-

04 NOVEMBER 2005

means, such as a printed bar code, or by any digital means, such as a magnetic strip or an electronic chip of the kind known as a Smart Tag, as long as the information contained in the ID can be retrieved. The means by which the ID is fixed to the product is not relevant for the scope of the present invention.

5 Fastening may also be done onto a product lot, or onto various products at the same time in the case of those sold in more than one unit per package.

The ID may contain identification of the intended site of sale or distribution (30). Inclusion of the site identification within the product ID permits verification of whether the product is effectively at the intended point of sale or
10 distribution.

The ID may also contain characters that are themselves a function of other characters in the ID, such as a digital signature or a hash input value. There are several methods to generate a secure digital signature, such as DSS, RSA and El Gamal, among others. There are also many secure hash functions,
15 such as MD-5 and SHS, among others.

Inclusion of a site identifier, or of a digital signature, or of a hash input value within the ID permits checking the formal consistency and integrity of the data.

The ID may contain a comprehensible message to be exhibited to
20 the consumer, or a code that serves as key or index for selecting in a data-storage unit (34) such a comprehensible message. If exhibited (105), said message will give the consumer information on the authenticity of the product. There is no restriction on the content of said comprehensible message, but preferably it should mention some of the relevant characteristics of the product.

25 The manufacturer (10) may optionally compress the selected ID (100) by means of some data-compression algorithm. Should that be the case, it is necessary to decompress the data when retrieving (103) the information contained in said ID.

30 At the sale or distribution site (30), or at any time deemed necessary, the information in the ID fixed on the product is retrieved (103) through an off-line checker (31), such as a personal computer equipped with the

CLAIMS

1. Off-line product authentication process comprising the steps
of:

i. Selecting for each product a string of characters to identify
it;

ii. Fixing said string of characters on the product;

iii. Retrieving said string of characters from the product at the
moment of checking product authenticity;

iv. Checking the validity of the string of characters retrieved;

v. Exhibiting a message dependent on the result of said
validity checking; and

vi. Updating in a data-storage unit the validity indication of said
string of characters.

2. The process of claim 1, characterized by additionally
comprising the step of periodically updating in said data-storage unit the validity
indications of said string of characters and of strings of characters that identify
other products.

3. The process of claim 1, characterized in that said string of
characters is the product's serial number.

4. The process of claim 1, characterized in that said string of
characters comprises characters to determine if said string of characters is
valid.

5. The process of claim 1, characterized in that said string of
characters comprises characters to determine the message to be exhibited.

6. The process of claim 4, characterized in that said string of
characters comprises an identifier of the intended site of sale or distribution of
the product.

7. The process of claim 4, characterized in that said string of
characters comprises a digital signature or the input of a hash function.

8. The process of claim 5, characterized in that said string of
characters contains a message comprehensible to humans.

9. The process of claim 5, characterized in that said string of characters contains an index or key to select a message stored in a data-storage unit.

10. The process of one of claims 1-9, characterized in that said string of characters is compressed.

11. The process of one of claims 1-9, characterized in that said string of characters is fixed on the product by physical means.

12. The process of claim 11, characterized in that said physical means is a printed bar code.

13. The process of claim 1, characterized in that said string of characters is fixed on the product by digital means.

14. The process of claim 13, characterized in that said digital means is a magnetic strip.

15. The process of claim 13, characterized in that said digital means is an electronic chip.

16. The process of one of claims 1-9, characterized in that said string of characters fixed on the product is inseparable from the product.

17. The process of one of claims 1-9, characterized by additionally comprising the steps of:

20 encrypting said string of characters with a private key of a public-key cryptography system before step (ii);

disclosing the public key corresponding to said private key before step (iii); and

decrypting said encrypted string of characters as part of step (iii).

25 18. The process of claim 17, characterized in that said encrypted string of characters is accompanied by the corresponding public key to promote its decryption.

19. The process of one of claims 1-9, characterized by additionally comprising the steps of:

30 encrypting said string of characters using a symmetric cryptography system before step (ii); and

04 NOVEMBER 2005

decrypting said string of characters as part of step (iii).

20. Off-line product authentication system comprising:

- a data-storage unit that can store at least one list of valid or invalid strings of characters;

5 - a checker that can verify in said data-storage unit the validity of said string of characters that identifies the product; and

- a message-delivery element to exhibit a message dependent on the result of the validity verification done by said checker.

10 21. The system of claim 20, characterized by additionally comprising a sales register able to record a commercial transaction involving said product and to indicate to the data-storage unit that the string of characters that identifies said product should no longer be considered valid.

15 22. The system according to claim 20 or 21, characterized by additionally comprising means to encrypt and/or decrypt a string of characters that identifies the product.

23. The system of claim 22, characterized in that said means is software.

24. The system of claim 20, characterized in that said data-storage unit is a database.

20 25. The system of claim 20, characterized in that said checker is a computer.

26. The system of claim 21, characterized in that said sales register is a computer.

25 27. The system of claim 21, characterized in that said sales register is a cash register at the point of sale or distribution.

28. The system of claim 20, characterized in that said checker and said sales register are combined in one single unit.

29. The system of claim 20, characterized in that said checker is portable.

30 30. The system of claim 21, 26 or 27, characterized in that said sales register is portable.

31. The system of claim 20, characterized in that said message-delivery element is a display or screen.

32. The system of claim 20, characterized in that said message-delivery element produces an audio signal or any form of
5 communication suitable for people who have difficulty reading.

Amended Sheet

MEMORIA DESCRIPTIVA

CAMPO DE LA INVENCION

La presente invención se refiere a un proceso y a un sistema de autenticación de productos.

Más específicamente, la presente invención se refiere a un proceso y a un sistema de autenticación de productos donde dichos productos están dotados de una información que puede ser recuperada en el punto de ventas y/o de distribución para autenticación por medios fuera de línea directamente por el consumidor y/o distribuidor.

FUNDAMENTOS DE LA INVENCION

Actualmente es notorio el problema de la piratería, robo, falsificación y contrabando de productos industrializados. Diariamente, se verifican muchos tipos de fraudes incluyendo productos tales como CDs de música, programas de computación, ropas y accesorios de marca, bebidas alcohólicas, remedios, cigarros, combustibles, entre otros.

A pesar de disponer de un tratamiento jurídico distinto, las diferentes formas de falsificación afectan tanto al fabricante de productos como al consumidor final. Ambos son perjudicados por las acciones ilícitas. Por un lado, el consumidor no tiene la certeza de estar adquiriendo un producto original, y cuando este producto está relacionado con la salud o la seguridad de los usuarios, como los medicamentos, equipos de seguridad para el trabajo, alimentos, productos del tabaco o equipos deportivos, por ejemplo, los daños causados por la falsificación pueden ser de gran impacto. Por otro lado el fabricante o representante del producto resulta perjudicado por las pérdidas económicas y de imagen de su marca.

Sin embargo, también es de interés del poder público la represión de estos actos, tanto para garantizar la seguridad y la salud de los ciudadanos, como para evitar la pérdida de ingreso por evasión de impuestos.

Por lo tanto, los fabricantes, los consumidores, y el poder público tienen gran interés en reprimir y evitar actos ilícitos que involucren productos industrializados.

En este contexto, hasta ahora se han adoptado algunas medidas preventivas a fin de evitar la falsificación de productos. Las acciones tomadas, generalmente tienen

como objetivo proveer un medio por el cual un consumidor fácilmente identifique o autentifique el producto adquirido.

Para la verificación de la autenticidad de productos existen medios físicos, tales como sellos holográficos, sellos inviolables u otros identificadores visuales. Todos estos medios son tanto más eficaces cuanto más difícil es su reproducción. También se verifica que los fabricantes de remedios utilizan un identificador visual en el embalaje del medicamento, que exhibe, por medio del raspado de una capa de tinta, el nombre del fabricante o del producto. Otros medios son lacres inviolables, frecuentemente utilizados en los embalajes de bebidas alcohólicas. En algunos casos específicos, como en el de los combustibles, se están utilizando reactivos químicos que, en contacto con el producto, dan un cierto patrón de coloración para la verificación de la autenticidad.

Sin embargo los medios físicos mencionados para la verificación de la autenticidad de un producto, a pesar de reprimir la falsificación, no son eficientes. Primeramente el consumidor no dispone de medios para identificar si el producto es realmente auténtico. A pesar de ser de difícil reproducción, nada impide a los falsificadores de reproducir, aun que con calidad inferior, los elementos distintivos del producto auténtico. Los consumidores, incluyendo a los más diligentes, generalmente no perciben las pequeñas diferencias que existen entre un sello, un lacre, o identificador visual original y el falsificado, y pueden adquirir el producto falso. Además los medios físicos no son eficientes en los casos en que un falsificador reutiliza una embalaje original después de desecharse y tampoco para desanimar la comercialización de productos originales robados o contrabandeados. El consumidor no percibe la diferencia.

También hay medios electrónicos para la verificación de la autenticidad del producto. Entre ellos están los sistemas en línea para la verificación en tiempo real. En estos casos, sin embargo, un consumidor puede verse obligado a esperar mucho tiempo para la autenticación, o ello se torna imposible debido a dificultades o imposibilidad de comunicación en el momento de la autenticación.

Máquinas verificadoras que se limitan a dar al consumidor apenas información del tipo "sí" o "no", esto es, "auténtico" o "falso" en relación al producto, también no garantizan completamente al consumidor respecto a la veracidad de la información

5 contenida, una vez que pueden ser alteradas para dar siempre resultados positivos. Lo mismo es cuando no son fraudulentas, tales máquinas no consiguen identificar si el producto es proveniente de robo, contrabando o reutilización de embalajes desechados, o sea son posibles de dar al usuario una impresión falsa de estar adquiriendo un producto que llega a sus manos por la cadena legítima de distribución. Un sistema que simplemente verifique el elemento visual grabado (como en el caso del uso de rayos ultravioleta) puede estar sujeto a los mismos problemas citados anteriormente.

10 Por lo tanto los medios existentes en el estado de la técnica para promover la verificación de la autenticidad de un producto no son eficientes y están sujetos a fallas. Existe la necesidad de un proceso de verificación de autenticidad de productos que resuelva los problemas citados más arriba.

De esta forma, un objetivo de la presente invención es proveer un proceso y un sistema de autenticación de productos donde la autenticidad del producto sea fácilmente reconocida por el consumidor.

15 Otro objetivo de la presente invención es proveer un proceso y un sistema de autenticación de productos en el cual sea imposible la reproducción del elemento de verificación.

20 Otro objetivo más de la presente invención es proveer un proceso y un sistema de autenticación de productos en el que sea posible detectar y desautorizar la reutilización ilegítima del elemento de verificación auténtico.

Otro objetivo más de la presente invención es proveer un proceso y un sistema de autenticación de productos en que sea posible la autenticación del producto por medios fuera de línea.

25 Otro objetivo más de la presente invención es proveer un proceso y un sistema de autenticación de productos en el que no sea posible alterar el medio de autenticación.

30 Otro objetivo más de la presente invención es proveer un proceso y un sistema de autenticación de productos que dé al fabricante y/o distribuidor medios para combatir el robo y el contrabando impidiendo la autenticación de productos auténticos provenientes de estos ilícitos.

Otro objetivo más de la presente invención es un sistema que promueva el proceso de la presente invención.

DESCRIPCIÓN RESUMIDA DE LA INVENCION

Para la presente memoria descriptiva, se utilizan las siguientes definiciones.

5 **Producto:** es una unidad de un producto cualquiera, o un lote de productos, o un embalaje de un producto cualquiera que puede contener una o más unidades de productos.

Identidad del producto: es una secuencia de caracteres que identifica un producto exclusivamente. Cada identidad corresponde a sólo un producto.

10 **"Fuera de línea":** se define que no existe comunicación o procesamiento de datos con un servidor remoto al momento de la verificación, sea por medio de una red o un canal dedicado de comunicación.

15 **Servidor remoto:** se define como un elemento capaz de procesar y enviar datos por medio de una red que no sea una red local (LAN) o por medio de un canal dedicado de comunicación con otro elemento significativamente distante del primero.

Fabricante: es el fabricante de un producto, o un beneficiador, distribuidor, representante o cualquier otro interesado en mantener la autenticidad del producto.

Consumidor: es cualquier persona interesada en verificar la autenticidad de un producto, sea esa persona comprador o no del producto.

20 **Verificador:** un dispositivo que ayuda al consumidor a verificar la autenticidad del producto.

Mensaje: un mensaje que contenga cualquier información comprensible a las personas, tal como una señal visual, una frase dentro de los patrones que forman la lengua, o una señal de audio.

25 **Venta:** se define como la ejecución de cualquier transacción comercial involucrando un producto, incluso cuando no hay un pago inmediato.

De acuerdo con una primera ejecución de la presente invención, el proceso de autenticación de productos comprende las etapas de:

- 30 i. seleccionar, para cada producto, una secuencia de caracteres que identifica el producto;
- ii. fijar dicha secuencia de caracteres al producto;

- iii. recuperar la información contenida en dicha secuencia de caracteres en el momento de la verificación de la autenticidad del producto;
- iv. verificar la validez de dicha secuencia de caracteres recuperada;
- v. enviar un mensaje dependiente del resultado de dicha verificación de validez;
- vi. actualizar la indicación de validez de dicha secuencia de caracteres en una base de datos; y
- vii. actualizar periódicamente en dicha base de datos las indicaciones de validez de dicha secuencia de caracteres y también de secuencias de caracteres que identifican otros productos.

De acuerdo con el proceso de la presente invención, se escoge una secuencia de caracteres que, de forma explícita o implícita, identifique un determinado producto exclusivamente (i). La secuencia caracteres, como se mencionó anteriormente, es definida como identidad.

La identidad puede ser, por ejemplo, un número de serie del producto, evitándose de ese modo ambigüedades con productos diferentes. Sin embargo, cualquier secuencia de caracteres capaz de identificar un producto de manera única puede ser utilizada como identidad en el proceso de la presente invención. Así cuando un producto es colocado el mercado, su identidad pasa a ser considerada válida (autorizada). Esta condición puede cambiar posteriormente.

La identidad del producto puede contener otras informaciones además del mínimo necesario para individualizar el producto. Por ejemplo, la identidad puede contener caracteres para determinar si ella es consistente en su forma y/o caracteres para enviar un mensaje.

Si una identidad no es consistente en su forma, ella no es considerada válida. Un ejemplo de caracteres que sirven para determinar si la identidad es consistente en su forma es un indicador del local a que se destina la venta o distribución del producto que está asociado a la identidad. Una identidad que contenga tal indicador solamente será considerada consistente si la verificación de su consistencia fue hecha en el local a que se destina el producto.

Otro ejemplo es una secuencia de caracteres que se extrae del contenido de la identidad, tal como una firma digital o la entrada de una función Hash. Una función Hash es una transformación que toma una secuencia de caracteres (entrada) y, a partir de ella, produce otra secuencia de caracteres (salida), de modo que, para quien no conoce el mecanismo de cálculo de la función, es muy difícil descubrir un par de entrada-salida válido que aún no ha sido divulgado.

La identidad también puede contener caracteres para enviar un mensaje. En ese caso, la identidad permite seleccionar un mensaje a ser enviado como consecuencia de validación de identidad. La identidad puede contener cualquier mensaje, como la descripción explícita de las principales características del producto o un código que permite implícitamente determinar un índice para seleccionar, en una tabla que contiene diversos mensajes, un mensaje que debe ser enviado.

La identidad puede también contener caracteres que sirven tanto para determinar su consistencia formal como para enviar un mensaje. Por ejemplo, los dígitos generados por una función Hash pueden ser usados como índices de la tabla de mensajes. En otro ejemplo, parte de la identidad puede ser usada para verificar la consistencia por comparación con una firma digital, mientras que otra parte es usada como índice de esa tabla. En otro ejemplo, la identidad puede ser el propio mensaje a ser enviado, o una parte de él.

Escogida la identidad asociada al producto, ella es entonces (ii) fijada al producto. La fijación puede ser efectuada tanto por medios físicos, tal como la impresión de una secuencia de caracteres o de un código de barras sobre el producto, como a través de la inserción de informaciones en un medio digital fijado al producto, tal como una banda magnética o un circuito microelectrónico del tipo conocido por la sigla RFID o Smart Tag, así como por cualquier otro medio apropiado. La elección del medio de fijación no es relevante para la finalidad de la presente invención. La fijación es, preferentemente, inseparable del producto, a fin de evitar que la identidad sea reutilizada en otros productos. Además, la identidad puede también ser puesta en otros lugares asociados al producto que lo acompañen y/o identifiquen. La identidad debe ser fijada de tal modo que la información contenida en ella pueda ser recuperada.

Luego, generalmente en el punto de venta o de distribución y en el momento de compra u obtención del producto, la persona interesada en verificar la autenticidad del producto lo somete a un dispositivo denominado aquí verificador fuera de línea, o simplemente verificador. El verificador, entonces, (iii) recupera la información contenida en la identidad fijada al producto, (iv) verifica, consultando el contenido de una base de datos, si dicha identidad es válida o no válida, y (v) envía un mensaje dependiente de la validez de dicha identidad. El mensaje enviado permite al comprador decidir si el producto sometido al proceso de la presente invención es auténtico o falso.

El verificador fuera de línea puede, por ejemplo, ser una microcomputadora dotada de un lector de código de barras para recuperar la información contenida en la identidad fijada al producto.

La base de datos puede, por ejemplo, ser una base de datos que contenga una relación de identidades válidas o una relación de identidades no válidas, en el caso en que se utilizan caracteres de redundancia de tipo Hash.

Si la identidad del producto contiene caracteres para determinar consistencia formal, la verificación de validez de identidad (iv) incluye el análisis de consistencia. Si el verificador determina que la identidad recuperada del producto no es formalmente consistente, la considera no válida y, consecuentemente, (v) envía un mensaje de alerta, o mensaje incomprensible.

Por ejemplo, en el caso de la identidad contener un identificador del local a que se destina la venta/distribución del producto, el verificador en el local de venta/distribución verifica si el identificador del local es el correcto, a fin de evitar que cargas sean ilegalmente desviadas a otros puntos de venta. En el caso en que el producto haya sido desviado, un mensaje de alerta o un mensaje incomprensible es enviado.

En el caso en que la identidad contenga una firma digital, el verificador intenta confirmar si la firma es consistente con las demás informaciones contenidas en la identidad. Si no lo es, un mensaje de alerta o incomprensible es enviado.

En el caso que la identidad contenga caracteres de redundancia tal como un valor de entrada Hash, el verificador aplica la función Hash correspondiente para confirmar si ellos son consistentes con las demás informaciones de la identidad. Si no lo fueren, un mensaje de alerta o no comprensible es enviado.

5 En el caso en que la identidad recuperada no sea rechazada por ninguna prueba de consistencia formal, el verificador consulta una tabla de identidades válidas, o de identidades inválidas, almacenada en la base de datos para determinar si dicha identidad consta ahí como válida o no válida (iv).

10 Para hacer uso económico de la capacidad de almacenamiento de datos en dicha base, la tabla de identidades válidas, o de identidades inválidas, no necesita almacenar el contenido completo de cada identidad, sino que solamente el mínimo necesario para individualizar sin ambigüedades la referencia a cada identidad.

15 Si la identidad fijada en el producto lo identifica de forma implícita, la tabla que es consultada para determinar la validez no necesita almacenar la identidad conforme está fijada en el producto, sino que solamente el resultado de una función o transformación de esa identidad, que produzca el mínimo necesario para individualizar sin ambigüedades la referencia a ella. Por ejemplo, la referencia a una identidad en la tabla de validez puede ser representada por el resultado de una función Hash o de una transformación criptográfica aplicada a la información fijada en el producto, o a parte de ella.

20 Si el verificador concluye que la identidad es válida, envía (v) un mensaje comprensible a los humanos en una pantalla o monitor de video y/o por medio de una señal de sonido y/o ambos simultáneamente. En el caso en que se haya concluido que la identidad no es válida, envía (v) un mensaje de alerta sobre la falsedad del producto o una información no comprensible a los humanos.

25 El mensaje enviado al consumidor, en el caso en que la identidad es válida, puede ser un mensaje estándar. De preferencia, sin embargo, dicho mensaje está relacionado con los caracteres de mensaje contenidos en la identidad. De mayor preferencia, dichos caracteres de mensaje están relacionados con las características del producto. En base al mensaje enviado, el consumidor decide si acepta que el producto es auténtico.

Si el consumidor decide adquirir el producto, la base de datos es actualizada (vi) después de haber sido registrada la venta, para que la identidad del producto vendido o entregado no sea considerada más como válida para futuras autenticaciones.

Alternativamente, el comprador o distribuidor del producto puede no adquirir el producto después de la autenticación a pesar de que dicho producto sea auténtico. En ese caso, la base de datos puede registrar el número de veces que el producto sea sometido a autenticación y, de acuerdo con las reglas definidas, invalidar una determinada identidad después de haber sido sometida a autenticación un número de veces mayor que un valor predeterminado.

La base de datos pasa por actualizaciones periódicas (vii) para recibir nuevas relaciones de identidades válidas o inválidas. Esas actualizaciones traen informaciones sobre identidades que dejaran de ser válidas desde la última actualización y sobre identidades que pasaran a ser válidas por corresponder, por ejemplo, a nuevos productos colocados en el mercado; y recolectan informaciones similares para que puedan ser enviadas a otras bases de datos. Opcionalmente, esas actualizaciones modifican otras informaciones contenidas en la base de datos como, por ejemplo, el contenido de una tabla de mensajes. Opcionalmente aunque, las informaciones sobre identidades que dejaran de ser válidas también pueden ser enviadas al fabricante del producto o a terceros. La periodicidad de actualización puede ser de acuerdo con lo estipulado por el fabricante, o conforme un nuevo lote de productos llega al punto de venta o de distribución. El medio por el cual la actualización es efectuada es indiferente. Tanto por medios en línea, sea Internet, intranet, o red privada, como por medios fuera de línea, como, por ejemplo, un CD-ROM grabado. Tanto la periodicidad como el medio por el que se efectúa la actualización de la base de datos no son relevantes para la finalidad de la presente invención.

En una segunda ejecución de la presente invención, la identidad del producto es encriptada. De acuerdo con esta segunda ejecución, se utiliza un sistema de criptografía asimétrica, también conocido como sistema de criptografía de clave pública.

En la criptografía de clave pública, se utilizan dos claves relacionadas entre sí, una clave pública y una clave privada. La clave pública, como lo indica su propia

denominación, está disponible al público, es de conocimiento de todos. La clave privada, a su vez, es mantenida en secreto por el portador y no debe ser divulgada.

En la forma de empleo conocida como firma criptográfica, la clave privada es utilizada para encriptar los datos. Solamente el portador de la clave privada es el que consigue transformar los datos comprensibles en datos completamente incomprensibles que podrán recuperarse por medio del uso de la correspondiente clave pública. La clave pública es utilizada para desencriptar los datos, o sea, cualquier persona que posea la clave pública puede desencriptar los datos para recuperar el contenido original previamente encriptado.

Existen diversos sistemas de criptografía de clave pública reconocidamente seguros. Un ejemplo es aquel conocido por la sigla RSA, disponible de la empresa RSA Security, Bedford Massachusetts, USA. Otros ejemplos incluyen a McEliece y a El Gamal. La elección del sistema de criptografía de clave pública no es relevante para los fines de la presente invención.

El proceso de autenticación de productos, de acuerdo con la segunda ejecución de la presente invención, comprende adicionalmente la etapa de encriptar dicha secuencia de caracteres que identifica el producto utilizándose la clave privada de un sistema de criptografía de clave pública antes de la etapa (ii) y después de la etapa (i). La segunda ejecución del proceso de la presente invención incluye adicionalmente la etapa de divulgar, en cualquier momento antes de la etapa (iii), la clave pública correspondiente a la clave privada utilizada para encriptar la identidad. La segunda ejecución del proceso de la presente invención incluye, también, la etapa de desencriptar los datos encriptados y fijados al producto utilizándose la clave pública correspondiente a la clave privada de un sistema de criptografía de clave pública como parte del paso (iii) de recuperar la información contenida en dicha secuencia de caracteres.

Por lo tanto, de acuerdo con una segunda ejecución de la presente invención, la identidad del producto es encriptada como una clave privada antes de (ii) proceder a la fijación de la identidad al producto. La clave pública correspondiente a la clave privada utilizada debe ser divulgada a fin de permitir la desencriptación en el momento de la recuperación de la información contenida en la identidad. La divulgación de la clave

pública puede ocurrir en cualquier momento, siempre que ocurra antes de (iii) la recuperación de información contenida en la identidad encriptada, para permitir su descriptación.

En el empleo de la segunda ejecución de la invención, una manera de divulgar la clave pública es grabarla en una base de datos a que el verificador tenga acceso. Si hubiera más de una clave pública guardada en la base de datos, debe ir fijada al producto, de forma no encriptada, algún identificador que permita seleccionar la clave pública adecuada. Otra manera de divulgar la clave pública es grabarla explícitamente en el propio producto, de modo que no sea necesario utilizar otros medios para su divulgación. Sin embargo, el medio de divulgación de la clave pública no es relevante para la finalidad de la presente invención.

Después de descriptada, la información contenida en la identidad (iii) puede ser recuperada, y el proceso de la presente invención sigue las etapas subsiguientes, tal como se describió más arriba.

De acuerdo con una tercera ejecución de la presente invención, la identidad del producto es encriptada utilizándose un sistema de criptografía simétrica, también conocido como criptografía de clave privada. En este tipo de criptografía, la misma clave es utilizada para encriptar y descriptar los datos, por eso la clave debe ser secreta. Un ejemplo de sistema de criptografía simétrica es aquel conocido por la sigla DES, aunque hay varios otros. La elección del sistema de criptografía simétrica no es relevante para la finalidad de la presente invención.

De acuerdo con la tercera ejecución de la presente invención, el proceso de autenticación de productos comprende adicionalmente la etapa de encriptar dicha secuencia de caracteres que identifica el producto utilizándose un sistema de criptografía de clave privada antes de la etapa (ii) y después de la etapa (i). La tercera ejecución del proceso de la presente invención incluye, también, la etapa de descriptar la secuencia de caracteres que identifica el producto con la misma clave utilizada para su encriptación, para recuperar (iii) la información ahí contenida.

Por lo tanto, de acuerdo con la tercera ejecución de la presente invención, también debe procederse a la encriptación de la identidad antes fijarla en el producto. Sin embargo, de acuerdo con esta tercera ejecución no existe la etapa de divulgación

de la clave utilizada para la descriptación de la información contenida en la identidad. Ella debe quedar guardada en la base de datos de forma secreta.

En cualquiera de las ejecuciones de la presente invención, las informaciones contenidas en la identidad pueden ser protegidas por capas adicionales de encriptación. Por ejemplo, después de la etapa (i) y antes de la etapa (ii) se realiza una encriptación más, con una clave correspondiente al punto de venta/distribución. La elección de tal clave, que depende del destino del producto, puede ser hecha por el propio fabricante u, opcionalmente, comunicada al fabricante por el responsable del punto de venta/distribución.

En cualquiera de las ejecuciones de la presente invención, la identidad puede ser comprimida antes de la etapa (ii) de fijarse al producto. En ese caso, basta que la identidad sea descomprimida durante la etapa (iii) de recuperación de la información contenida en la identidad.

La presente invención también se refiere a un sistema de autenticación de productos que comprende:

- una base de datos para almacenar por lo menos una relación de secuencias de caracteres válidas o no válidas;
- un verificador para verificar la validez de dicha secuencia de caracteres que identifica el producto; y
- un elemento de emisión de un mensaje;

El sistema de la presente invención puede adicionalmente comprender:

- un registrador de ventas capaz de registrar una transacción comercial que involucra dicho producto, e indicar a la base de datos que la secuencia de caracteres que identifica aquel producto no debe ser más considerada como válida;

Cuando se emplea la segunda o tercera ejecución del proceso de la presente invención, el sistema debe comprender también un medio para encriptar y descriptar una secuencia de caracteres que identifica el producto.

El dicho medio para encriptar y descriptar la identidad es, de preferencia, un software, tal como el software RSA mencionado más arriba. Medios manuales también

pueden ser empleados. No obstante, son de menor preferencia por ser mucho más laboriosos y costosos.

La base de datos debe, preferentemente, ser una base de datos cualquiera capaz de almacenar una relación de identidades. No hay limitaciones sobre el tipo de base de datos empleada. Planillas en formato físico también pueden ser empleadas, pero son de menor preferencia.

El elemento verificador, de acuerdo con el sistema de la presente invención, preferentemente debe ser una computadora capaz de realizar el proceso de recuperación de informaciones contenidas en la identidad, y de verificar la validez de la identidad en dicha base de datos. Una computadora personal provista de un dispositivo adecuado de entrada de datos es plenamente capaz de realizar las etapas del proceso de la presente invención.

El elemento de emisión del mensaje puede ser tanto una pantalla o el monitor de video del elemento verificador, cuando es empleada una computadora personal, como un monitor o video empleado específicamente para emitir un mensaje. El elemento de emisión del mensaje puede ser, también, un parlante que trasmite una señal de audio. El elemento de emisión puede también conjugar tanto el monitor o video con un parlante para enviar la señal de audio. Cualquier elemento capaz de transmitir un mensaje a una persona puede ser utilizado en el proceso de la presente invención.

El registrador de ventas, aquí denominado simplemente registrador, puede ser una computadora o una caja del punto de ventas, siempre que se le agreguen las funciones de registrar la venta del producto y también la de actualizar la base de datos.

En una otra ejecución del sistema de la presente invención, el verificador está integrado con el registrador para, en un dispositivo único, verificar la autenticidad del producto, registrar la venta del producto y actualizar la base de datos, o, en el caso de que el producto sea considerado falso, bloquear la transacción.

En aún otra ejecución del sistema de la presente invención, el verificador es portátil, de modo de permitir la autenticación del producto en un local remoto.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Los anteriores y otros objetivos, perfeccionamientos y efectos del proceso y del sistema de la presente invención se toman aparentes a las personas experimentadas

en las materias a partir de la descripción detallada presentada a continuación, haciéndose referencia a las figuras adjuntas, dadas sólo a título ilustrativo de ejecuciones particulares de la invención. Tales figuras son esquemáticas, cuyas dimensiones o proporciones pueden no corresponder a la realidad, toda vez que pretenden sólo ilustrar la invención de forma didáctica, sin imponer ninguna limitación sino sólo aquellas de las reivindicaciones dadas más adelante.

- La figura 1 es un diagrama de bloques que representa esquemáticamente la primera ejecución del proceso de la presente invención;
- La figura 2 es un diagrama de bloques que representa esquemáticamente la segunda ejecución del proceso de la presente invención.
- La figura 3 es un diagrama de bloques que representa esquemáticamente la tercera ejecución del proceso de la presente invención;
- La figura 4 es un diagrama esquemático que representa el sistema de acuerdo con el proceso de la presente invención; y
- La figura 5 es una imagen ampliada del código de barras creado por la simbología PDF-417 de acuerdo con el ejemplo ilustrativo de la presente invención.

DESCRIPCIÓN DETALLADA DE LA INVENCION

Con referencia primeramente a las figuras 1 y 4, se ilustra el proceso y el sistema de acuerdo con una ejecución de la presente invención. Un fabricante (10) inicialmente selecciona (100) una secuencia de caracteres que identifican un producto (20). Como se mencionó más arriba, la secuencia de caracteres que identifican al producto es definida como identidad.

Luego, la identidad es fijada (102) al producto (20). Preferentemente, la fijación de la identidad es inseparable del producto. La fijación puede ser efectuada tanto por medios físicos, tal como un código de barras impreso, como por medios digitales, tal como una banda magnética o un circuito electrónico del tipo RFID, desde que las informaciones contenidas en la identidad puedan ser recuperadas. El medio por el cual

la identidad es fijada al producto no es relevante para la finalidad de la presente invención. La fijación puede ocurrir también en un lote de productos o en varios productos simultáneamente, en el caso de productos vendidos en más de una unidad en el mismo embalaje.

5 La identidad puede contener un identificador del local (30) al que se destina la venta o distribución del producto. La inclusión de tal identificador junto a la identidad permite verificar si el producto efectivamente se encuentra en el local de venta o distribución destinado.

10 La identidad puede contener aún una secuencia de caracteres cuyo contenido es el resultado de otros caracteres contenidos en la identidad, tal como una firma digital o el valor de entrada de una función "Hash". Existen diversos métodos de generar una firma digital segura, tales como el método DSS, o el RSA y El Gamal, entre otros. También existen innumerables funciones Hash seguras, tales como la función conocida por MD-5 y la conocida por SHA, entre otras.

15 La inclusión de un identificador local, o de una firma digital, o de un valor de entrada Hash en la identidad, permite confirmar la consistencia formal e integridad de los datos.

20 La identidad puede contener un mensaje comprensible a ser enviado, o un identificador que sirve de índice para seleccionar en la base de datos (34) un mensaje comprensible a ser enviado asociado a la identidad de aquel producto. Al emitirse (105), dicho mensaje dará al interesado información sobre la autenticidad del producto. No hay restricción en cuanto al contenido de dicho mensaje comprensible, pero de preferencia él menciona alguna de las características relevantes del producto.

25 La secuencia de caracteres fijada en el producto puede identificarlo de forma implícita, o sea, referencias a ese producto en la base de datos (34) pueden ser hechas por el resultado de una función o transformación aplicada a la información fijada en el producto, tal como, por ejemplo, una función Hash o una transformación criptográfica.

30 El fabricante (10) puede, opcionalmente, comprimir la identidad seleccionada (100), por medio de algún algoritmo de compresión de datos. Sin embargo, es necesario descomprimir la identidad comprimida para recuperar (103) la información contenida en dicha identidad.

En el local de venta o de distribución del producto (30), en cualquier momento que se juzgue necesario se recupera (103) la información contenida en la identidad fijada en el producto por medio de un verificador fuera de línea (31), tal como una computadora capaz de verificar la autenticidad del producto. La recuperación de la información contenida en la identidad puede ser hecha por medio de digitación de los caracteres que la componen, por medio de lectura de un código de barras o de una banda magnética, por medio de recepción de señales de radiofrecuencia, o por cualquier otro medio adecuado. Habiendo recuperado (103) la información contenida en la identidad fijada al producto, el verificador fuera de línea (31) la procesa de modo que verifica si dicha identidad es válida (104).

Si el verificador detecta alguna inconsistencia formal en la identidad recuperada, ella es considerada no válida. En el caso que eso no ocurra, la identidad sólo es considerada válida si en la base de datos dicha identidad consta como válida. Siendo así, la verificación de la validez de la identidad (104) puede darse por dos criterios.

Primero, si la identidad contiene caracteres que permiten la verificación de su consistencia e integridad, el verificador hace los cálculos apropiados para hacer esa verificación. No habiendo reprobado el criterio de consistencia e integridad, el verificador confiere la validez de la identidad del producto por medio de consulta (C) a una tabla de identidades válidas o no válidas almacenada en una base de datos (34).

En este caso, la respuesta (D) a esa consulta va a determinar la validez de la identidad.

La base de datos (34) es, por ejemplo, una base de datos que corre en la dicha computadora personal, o a la cual la computadora tiene acceso local o fuera de línea.

Un mensaje dependiente de la validez de la identidad del producto es emitido (105) en una pantalla (33). La pantalla (33) puede ser por ejemplo una pantalla o un monitor de video. Opcionalmente, la pantalla (33) emite una señal de audio o de otra naturaleza, especialmente útil para personas con dificultades de lectura.

El mensaje enviado da la base para que la persona interesada en la autenticación del producto decida si él es auténtico o no. En el caso que el verificador (31) haya considerado (104) la identidad inválida, es emitido (105) un mensaje de alerta o alternativamente, un mensaje incomprensible. Si, por el contrario, el verificador (31) considera (104) la identidad válida, se envía un mensaje comprensible. No hay

restricción en cuanto al contenido del mensaje comprensible, aunque de preferencia él está relacionado con el contenido de la identidad recuperada.

Después de emitido el mensaje (105), se actualiza (106) en la base de datos (34) las informaciones relativas específicamente a dicha identidad. Esa actualización (106) registra que aquella identidad acaba de ser sometida a una verificación de validez, pudiendo incluso ser registrada la fecha y hora en que eso ocurrió. En caso que la identidad haya sido considerada (104) válida, la actualización de la identidad (106) también actúa en el sentido de hacer que dicha identidad pierda su condición de validez. Esta pérdida de validez puede ser inmediata o, alternativamente, mediada por algunas condicionantes, por ejemplo, haciendo que la identidad sea no válida solamente después de ocurrido cierto tiempo desde la verificación de validez o, en otro ejemplo, contando cuántas veces dicha identidad fue sometida a verificación de validez y tomándola no válida solamente cuando se ha superado un determinado número de veces. Por otro lado, en caso de que dicha identidad haya sido considerada (104) no válida, la actualización (106) puede registrar que un producto falso con esa identidad fue sometido a verificación de autenticidad.

El registro de una venta del producto (20) también hace una actualización (106) de la base de datos (34). El dispositivo (35) que registra la venta es capaz de recuperar (103) la información contenida en la identidad del producto y verificar (104) su validez de manera análoga a la del verificador (31). En caso de que dicha identidad sea (H) no válida, el dispositivo registrador (35) bloquea la consumación de la venta. En el caso que dicha identidad sea (H) válida y la venta sea registrada, el registrador (35) actualiza (G) la base de datos (34) de modo que la identidad correspondiente a aquel producto pase (106) a constar como no válida.

El verificador (31) y el registrador de ventas (35) pueden estar disociados, siendo dispositivos separados. En esta implementación, por ejemplo, el comprador del producto puede verificar la autenticidad del producto en el mostrador de la tienda, y el registrador (35) estar en la caja de la tienda y actualizar (G) la base de datos (34) solamente después de concluida la venta. En una otra implementación, el verificador (31) y el registrador (35) de ventas están asociados, y son parte de un mismo dispositivo. En esta forma, por ejemplo, el comprador del producto puede verificar la

autenticidad del producto y realizar la compra directamente, al mismo tiempo, en la caja de la tienda.

El verificador y la base de datos pueden también ser portátiles (40). De esta forma, dicho verificador puede ser transportado al local de consumo o de distribución, al lugar del consumidor o el distribuidor transportarse al punto de ventas. Esa implementación es especialmente útil cuando hay un envío de un producto o de un lote de productos. El producto o lote de productos enviado al consumidor o distribuidor es sometido a la autenticación en el lugar de destino. Estando la base de datos en el mismo local, la verificación fuera de línea se hace de manera completamente análoga a la descrita anteriormente. El verificador portátil puede ser, por ejemplo, una computadora portátil, del tipo conocido como "Lap Top ", dotada de un lector de datos, siendo su disco magnético usado como base de datos. Por las mismas razones, el registrador también puede ser portátil, de modo que se pueda registrar una venta en el local de destino del producto.

Las personas experimentadas en la materia entenderán que los mismos resultados pueden ser obtenidos haciéndose la actualización de la identidad (106) en la base de datos antes del envío del mensaje (105), o al mismo tiempo que ésta. La orden temporal exacta de esas dos etapas no es relevante para la finalidad de la presente invención.

La base de datos (34) es actualizada (107) periódicamente con informaciones originadas en sitios remotos, informaciones esas que validan determinadas identidades, por ejemplo a medida que nuevos productos son producidos y colocados en el mercado, y/o que invalidan otras identidades, por ejemplo a medida que productos son sometidos a autenticación y vendidos en otros locales, o en caso que algún otro evento como un robo o un "recall" justifique la cancelación de la validez de determinadas identidades. Esas actualizaciones (107) también pueden incluir el envío de informaciones contenidas en la base de datos (34) para sitios remotos. Opcionalmente, esas actualizaciones también cambian otras informaciones en la base de datos, por ejemplo el contenido de una tabla de mensajes. La exacta periodicidad con la cual se efectúa la actualización (107) de la base de datos no es relevante para el objetivo de la presente invención.

La figura 4 ilustra los cambios de informaciones con un administrador central (50). El fabricante del producto envía (A) al administrador central una relación de las identidades auténticas de productos (20). Durante uno de los trueques de información (107) entre el administrador central y la base de datos, la dicha relación es, a su vez, actualizada (B) en la base de datos (34) para los nuevos productos colocados en el mercado. La base de datos (34) envía (E) al administrador del sistema (50) una relación de identidades que no son más válidas, o que fueron sometidas a autenticación un número mayor de veces a lo estipulado, o una relación de identidades de productos falsos sometidos a autenticación. Esa relación enviada (E) al administrador del sistema puede, opcionalmente, ser enviada (F) al fabricante (10) para control estadístico o cualquier otro fin.

La administración del sistema de la presente invención puede ser realizada por medio de un administrador central (50), tal como es mostrado en la figura 4, como por el propio fabricante (10) del producto (20). Las personas experimentadas en la materia entenderán que la administración también puede ser hecha de forma distribuida, por diversos procesadores de datos. En este caso, el administrador puede ser entendido como siendo los softwares que, en conjunto, pero de forma distribuida, implementan las etapas descritas anteriormente. El medio por el cual la administración se realiza no es relevante para la finalidad de la presente invención.

La actualización de la base de datos (107) puede ser realizada tanto por medio de un canal dedicado de comunicación, como por una red privada en conexión con el administrador, como por la Internet, o, cuando no hay acceso por algún medio de telecomunicación, por medio de un dispositivo portátil de almacenamiento de informaciones tal como un disquete o un CD distribuido en los puntos de ventas/distribución. Tanto el medio por el cual se efectúa la actualización de la base de datos, como la periodicidad en la que dicha actualización es efectuada no son relevantes para la finalidad de la presente invención.

La figura 2 ilustra la segunda ejecución del proceso de acuerdo con la presente invención, en donde la identidad es encriptada utilizándose un sistema de criptografía de clave pública. De acuerdo con esta ejecución, después de seleccionada la identidad (100) se procede a la encriptación (101) por un sistema de criptografía de clave pública.

Opcionalmente, los fabricantes pueden comprimir las informaciones de identidad fijadas al producto. Por lo tanto, en ese caso, las informaciones de la identidad son descomprimidas al ser sometidas a la etapa de recuperación (103).

La identidad es sometida a encriptación (101). El resultado de la encriptación se trata de una secuencia de caracteres no comprensible para los humanos. La encriptación es realizada utilizándose la clave privada de un sistema de criptografía de clave pública escogido y, por lo tanto, dicha clave privada no debe ser divulgada, siendo de propiedad única y exclusiva del fabricante (10) o del administrador (50).

Luego, el resultado de la encriptación es fijado (102) al producto (20). La fijación de la identidad encriptada es preferentemente inseparable del producto. De mayor preferencia, la fijación debe ser realizada en el propio producto. La fijación puede ser realizada tanto por medios físicos, tal como un código de barras impreso, como digital, tal como una banda magnética o un circuito electrónico del tipo RFID, siempre que las informaciones contenidas en la identidad encriptada puedan ser recuperadas. El medio por el cual la identidad encriptada es fijada al producto no es relevante para la finalidad de la presente invención. La fijación puede ocurrir también en un lote de productos o en varios productos simultáneamente, en el caso de productos vendidos en más de una unidad en el mismo embalaje.

La clave pública correspondiente a la clave privada se divulga (108) para posibilitar la desencriptación de la información contenida en la identidad. La divulgación de la clave pública puede ocurrir en cualquier momento, tanto antes de seleccionar la identidad (100), como después de seleccionarla y antes de encriptarla (101), como después de la encriptación y antes de la fijación de la identidad encriptada en el producto (102), o aún después de la fijación de la identidad encriptada en el producto (102), siempre que ocurra antes de la recuperación de la información contenida en la identidad encriptada (103), porque solamente al poseer la clave pública es posible la realización de la etapa de verificación (104). El medio por el cual la clave pública es divulgada no es relevante para la finalidad de la presente invención. Enseguida, el proceso se desarrolla en forma análoga al proceso de la primera ejecución de la invención siendo que en el paso (iii) es necesario desencriptar la identidad para recuperar las informaciones ahí contenidas.

De acuerdo con esta segunda implementación, la base de datos (34), opcionalmente, es capaz de almacenar la(s) clave(s) pública(s) divulgada(s) por el(los) fabricante(s). De preferencia, el verificador (31) tiene la capacidad de reconocer la identidad del fabricante y seleccionar la clave pública adecuada.

5 Opcionalmente, la clave pública correspondiente a la clave privada con la cual los datos fueron encriptados está fijada al producto. En este caso, no es necesario el almacenamiento de las claves públicas en la base de datos, ni tampoco la divulgación de la clave pública por otros medios.

10 La figura 3 ilustra una tercera ejecución del proceso de la presente invención, donde en lugar de utilizarse un sistema de criptografía de clave pública se utiliza un sistema de criptografía de clave privada. El proceso se desarrolla en forma análoga al proceso descrito en la segunda ejecución de la presente invención, diferenciándose sin embargo porque no incluye la etapa de divulgación de la clave pública, una vez que la clave utilizada en la encriptación de la identidad es la misma utilizada en la
15 desencriptación, debiendo, por eso, ser mantenida en secreto por el portador.

La presente invención también se refiere a un sistema de autenticación de productos, tal como es ilustrado en la figura 4, que comprende:

- un medio para fijar una secuencia de caracteres que identifica el producto en el producto (20), de modo que la secuencia de caracteres pueda ser recuperada;
- una base de datos (34) para almacenar por lo menos una relación de secuencias de caracteres válidas o no válidas;
- un verificador (31) para verificar la validez de dicha secuencia de caracteres que identifica el producto; y
- 25 - un elemento de emisión de un mensaje (33).

30 El sistema de la presente invención puede adicionalmente comprender un elemento registrador de ventas (35), para registrar una transacción comercial involucrando a dicho producto y, a continuación, actualizar la base de datos para que la secuencia de caracteres que identifica a dicho producto no sea más considerada como válida.

El medio utilizado para la fijación de la secuencia de caracteres que identifica el producto es preferentemente un medio físico, tal como una impresión o un código de barras. También se pueden emplear medios electrónicos, tal como microcircuitos electrónicos del tipo comúnmente denominado RFID, banda magnética, o cualquier otro medio apropiado.

Cuando se emplea la segunda o la tercera ejecución del proceso de la presente invención, el sistema debe comprender también un medio para encriptar y desencriptar una secuencia de caracteres que identifica el producto. Dicho medio para encriptar la identidad es, de preferencia, un software, tal como el software RSA mencionado más arriba. También pueden ser empleados medios manuales. Sin embargo, por ser mucho más laboriosos y costosos, son de menor preferencia.

La base de datos (34) debe, preferentemente, ser una base de datos cualquiera capaz de almacenar identidades. No hay limitaciones en el tipo de base de datos empleada. También pueden ser empleadas planillas en formato físico, aunque de menor preferencia.

El verificador (31) de acuerdo con el sistema de la presente invención, preferentemente debe ser una computadora capaz de realizar el proceso de recuperación de la información contenida en la identidad y verificar la validez de la misma en dicha base de datos. Una computadora personal dotada de dispositivos periféricos adecuados es plenamente capaz de efectuar las etapas del proceso de la presente invención.

El registrador de ventas (35) puede ser una computadora o una caja en el punto de ventas, siempre que agregue las funciones de registrar la venta del producto y también la de actualizar la base de datos.

En otra ejecución del sistema de la presente invención, el verificador (31) forma un conjunto con el registrador (35) de modo que en un único dispositivo se verifique la autenticidad del producto, se registre la venta del producto y se actualice la base de datos (34).

En aún otra ejecución de la presente invención, el verificador es portátil (40), de modo que se pueda obtener la autenticación del producto en un local que no sea el punto de ventas.

En aún otra ejecución de la presente invención, el registrador de ventas es portátil, de modo que se pueda conseguir el registro de venta del producto en un local que no sea un punto de ventas.

De acuerdo con lo anteriormente descrito, será evidente para las personas experimentadas en la materia que la presente invención resuelve los problemas del estado de la técnica al proporcionar un proceso y un sistema de autenticación de productos en el que la autenticidad del producto es fácilmente reconocida por el consumidor por medio de la interpretación de un mensaje, tanto visual como auditivo. Además, la presente invención evita que el elemento de autenticación del producto sea reproducido, así como también imposibilita la reutilización de la identidad del producto. No solamente, la autenticación del producto es implementada por medios fuera de línea, evitando que sea necesaria una conexión en línea con un servidor remoto en el momento de la autenticación, sino que también inhibe acciones ilícitas tales como el contrabando, el robo de cargas y la piratería.

EJEMPLO

La presente invención se describe ahora con un ejemplo práctico de la aplicación de una de las ejecuciones descritas anteriormente, dado sólo a título ilustrativo, sin implicar ningún carácter limitativo afuera aquel contenido en las reivindicaciones anexas.

En el presente ejemplo, un fabricante de medicamentos graba el embalaje de uno de sus productos con un código que le va a permitir al consumidor verificar que el producto es auténtico. Esa verificación de autenticidad es realizada en la farmacia, en un modo fuera de línea, antes de la compra del producto. El fabricante es catalogado como número 01 en un listado de fabricantes. Este fabricante, en algún momento, selecciona un par de claves del sistema de criptografía RSA, siendo una la clave pública y la otra la correspondiente clave privada.

Para generar el par de claves a ser utilizadas, el fabricante se vale de un software que funciona en una computadora convencional. Cuatro números aleatorios, denominados A1, A2, A3, y A4, son elegidos por el fabricante:

- A1 = 123456789
- A2 = 235619181

- $A3 = 126171819$

- $A4 = 121256171$

El software produce, a partir de los números de entrada A1 al A4, una salida con dos números primos largos P y Q, que en notación decimal son:

5 $P = 77300639724168335413320743479725556994840079969368275051368928$
 424940196293451

$Q = 90026005122192115427466058169524256985400621971043875415635710$
 094429895131083

Ese mismo software calcula el producto de P y Q, denominado N, o sea $N = P \times Q$, cuyo valor en notación decimal es:

10 $N = 6959067787756705876553835596165330393095183089839319075724666$
 $3757348016863545591338532426783559571765453427537120582295229$
 $823306581086097206402868379437433$

15 La clave pública del fabricante consiste de dos números: uno de ellos es el número N de arriba y el otro es el número 3, que sirve de exponente en el proceso de decodificación.

Los números que constituyen la clave pública son almacenados en la base de datos a la cual el verificador fuera de línea tiene acceso, tal como el disco rígido de una computadora personal en el punto de venta.

20 La clave privada consiste del par de números P y Q. La clave privada está disponible para un software generador, que corre en el computador del fabricante, y sirve para generar el código a ser grabado en el producto. La clave privada no es divulgada por el fabricante.

25 A partir de P y Q, el software generador genera otros dos valores: uno llamado "Fi", que es el valor del producto $(P - 1) \times (Q - 1)$; y otro llamado D, que es el inverso multiplicativo de 3, módulo Fi. Solamente el fabricante conoce los valores de Fi y de D.

El software generador también recibe como entrada el número que identifica al fabricante, en este caso, el número 01, el número de serie del producto en cuestión y un texto cualquiera, escogido por el fabricante.

30 En este ejemplo, el fabricante produce una caja del antibiótico amoxicilina oral, caja ésta que tiene el número de serie 1234567890. El software generador agrega la

representación binaria del número 01, como si fuera prefijo, en la representación binaria de ese número de serie. El resultado es entonces agregado, también como prefijo, en la representación binaria en código ASCII del texto "AMOXICILINA 750 MG. CONSUMIR HASTA EL 03 MAYO 2009". La secuencia de bits resultante es la identidad, y es considerada por el software como un valor numérico M.

A continuación, el software hace el cálculo matemático: M elevado a la potencia D, módulo N. El resultado X, que es la identidad encriptada, está abajo transcrito en notación hexadecimal:

X=50 47 2B 89 8C 35 12 41 37 3B 58 09 19 A1 9A 34 D7 2F C3 8C 86 99 DA 14
AB F9 11 2F E5 F5 81 E7 76 3B BB F5 E1 72 EA 7C 40 04 46 70 4D E8 67 79 8A 15 81
54 17 8C 5F B0 AA 6C 2C 3D D1 1C D5 5D

La representación binaria del número 01, que identifica al fabricante, es agregada, como prefijo, a la representación binaria del valor de X. La secuencia de bits resultante es la siguiente, en notación hexadecimal:

01 50 47 2B 89 8C 35 12 41 37 3B 58 09 19 A1 9A 34 D7 2F C3 8C 86 99 DA 14
AB F9 11 2F E5 F5 81 E7 76 3B BB F5 E1 72 EA 7C 40 04 46 70 4D E8 67 79 8A 15 81
54 17 8C 5F B0 AA 6C 2C 3D D1 1C D5 5D

Esta secuencia de bits es luego convertida a un tipo de representación que permita recuperarla electrónicamente. En este ejemplo, fue escogido el código de barras y, de entre las varias simbologías de código de barras existentes, fue escogida la simbología bidimensional PDF-417. El resultado del código de barras generado es representado en la figura 5, en escala ampliada para facilitar su visualización. El fabricante fija en el embalaje del remedio ese código de barras.

Como mencionado anteriormente, el fabricante divulga la clave pública del sistema de criptografía utilizado, es decir, se divulga en algún momento antes de la descriptación y recuperación de los datos, los números N y 3.

Después que esa caja de antibiótico llega al punto de venta, el consumidor, que está en la farmacia y desea verificar la autenticidad de ese producto antes de comprarlo, lo somete a la lectora de código de barras que forma parte del verificador, que puede ser una computadora. El verificador recupera la información contenida en el

código de barras y lo ingresa como entrada a un software que funciona en la CPU en el punto de ventas.

El software encuentra inicialmente el identificador del fabricante, leyendo el primer byte del código, en este caso el número 01, para escoger, en una tabla de claves públicas, la clave pública adecuada para desencriptar la identidad encriptada, una vez que otros fabricantes pueden emplear otras claves. Luego, descartando el primer byte, todo lo restante es el valor X. De acuerdo con el sistema de criptografía utilizado, se recupera la información M contenida en X, efectuando el cálculo matemático $M = X^3 \text{ módulo } N$.

Habiendo obtenido M, la identidad del producto, el software separa el mensaje del número de serie. En el caso que el número de serie contenido en la identidad no conste de una relación de números de serie válidos para el fabricante 01, relación que está almacenada en la base de datos del punto de ventas, la identidad es considerada no válida y, consecuentemente, el equipo alerta al consumidor de que el producto es falsificado, exhibiendo en su pantalla la palabra "FALSO", que simultáneamente es pronunciada por su sintetizador de voz. Lo mismo se da en el caso de que ese número de serie, aún cuando conste en la relación de válidos, termine por ser sometido a verificación de autenticidad por la décima vez, por ejemplo. En el presente ejemplo, diez veces es el límite escogido por ese fabricante para servir de alerta de que hay algo extraño que está sucediendo, que merece ser investigado, y entremedias invalidar ese número de serie.

En el caso que el número de serie sea considerado válido, el texto "AMOXICILINA 750 MG. CONSUMIR HASTA EL 03 MAYO 2009" que está contenido en M, es enviado a la pantalla del computador y, simultáneamente, el sintetizador de voz lo pronuncia.

Al leer y/o escuchar claramente el nombre del remedio que está comprando y las demás informaciones comprensibles contenidas en aquel texto, el consumidor tiene la certeza de que el producto es auténtico.

Una vez convencido de que el medicamento es auténtico, el consumidor pasa con él por la caja, efectuando el pago y recibiendo la boleta fiscal. El equipo registrador de ventas, o sea, el terminal de la caja, al registrar la venta de ese producto, entonces,

actualiza la relación de números de series válidos en la base de datos, invalidando ese número de serie para que otro producto con el mismo número de serie no pueda ser considerado auténtico.

5 En la próxima actualización en línea de la base de datos, que en el presente ejemplo es realizada dos días después, la información de que ese número de serie fue invalidado es enviada al administrador, que la comunica a todas las demás bases de datos. Durante la misma actualización en línea, la base de datos recibe informaciones sobre los números de serie que deben pasar a ser considerados no válidos y, eventualmente, sobre otros que deben pasar a ser considerados válidos.

10 Debe ser reconocido que, a pesar de que la presente invención ha sido descrita con relación a sus ejecuciones preferidas, las personas técnicas experimentadas en la materia pueden desarrollar una amplia variedad de detalles y expandir los procesos y el sistema antes expuesto para otros tipos de aplicaciones particulares, sin apartarse de los principios de la invención. Por ejemplo, los varios elementos mostrados en las
15 implementaciones diferentes pueden ser combinados de una manera no ilustrada anteriormente. Por lo tanto, las reivindicaciones anexas deben ser interpretadas como cubriendo todos los equivalentes que se encuadran dentro del ámbito y carácter de la invención.

REIVINDICACIONES

1. Un proceso de autenticación de productos por medios fuera de línea, **CARACTERIZADO** porque comprende las etapas de:

- 5 i. Seleccionar, para cada producto, una secuencia de caracteres que identifica el producto;
- ii. Fijar dicha secuencia de caracteres al producto;
- iii. Recuperar la información contenida en dicha secuencia de caracteres en el momento de la verificación de la autenticidad del producto;
- 10 iv. Verificar la validez de dicha secuencia de caracteres recuperada;
- v. Enviar un mensaje dependiente del resultado de dicha verificación de validez de dicha secuencia de caracteres;
- vi. Actualizar la indicación de validez de dicha secuencia de caracteres en una base de datos.

15 2. Un proceso, de acuerdo con la reivindicación 1, **CARACTERIZADO** porque comprende adicionalmente la etapa de actualizar periódicamente en dicha base de datos las indicaciones de validez de dicha secuencia de caracteres y también de secuencias de caracteres que identifican otros productos.

20 3. Un proceso, de acuerdo con la reivindicación 1, **CARACTERIZADO** por el hecho de que dicha secuencia de caracteres es un número de serie del producto.

 4. Un proceso, de acuerdo con la reivindicación 1, **CARACTERIZADO** por el hecho de que dicha secuencia de caracteres comprende caracteres para determinar si dicha secuencia de caracteres es válida.

25 5. Un proceso, de acuerdo con la reivindicación 1, **CARACTERIZADO** por el hecho de que dicha secuencia de caracteres comprende caracteres para elegir un mensaje a ser emitido.

 6. Un proceso, de acuerdo con la reivindicación 4, **CARACTERIZADO** por el hecho de que dicha secuencia de caracteres comprende un identificador del local a que se destina la venta o la distribución del producto.

7. Un proceso, de acuerdo con la reivindicación 4, CARACTERIZADO por el hecho de que dicha secuencia de caracteres comprende una secuencia de caracteres resultante de la aplicación de una firma digital o de una función Hash.

8. Un proceso de acuerdo con la reivindicación 5, CARACTERIZADO por el hecho de que dichos caracteres son un mensaje comprensible para los humanos.

9. Un proceso, de acuerdo con la reivindicación 5, CARACTERIZADO por el hecho de que dichos caracteres son un índice para seleccionar un mensaje almacenado en una base de datos.

10. Un proceso de acuerdo con una de las reivindicaciones 1 a 9, CARACTERIZADO porque dicha secuencia de caracteres es comprimida.

11. Un proceso, de acuerdo con una de las reivindicaciones 1 a 9, CARACTERIZADO porque dicha secuencia de caracteres es fijada al producto por medios físicos.

12. Un proceso, de acuerdo con la reivindicación 11, CARACTERIZADO por el hecho de que dicho medio físico es un código de barras impreso.

13. Un proceso, de acuerdo con la reivindicación 1, CARACTERIZADO por el hecho de que dicha secuencia de caracteres está contenida en un medio digital.

14. Un proceso, de acuerdo con la reivindicación 13, CARACTERIZADO por el hecho de que dicho medio digital es una banda magnética.

15. Un proceso, de acuerdo con la reivindicación 13, CARACTERIZADO por el hecho de que dicho medio digital es un micro circuito electrónico.

16. Un proceso, de acuerdo con una de las reivindicaciones 1 a 9, CARACTERIZADO porque dicha fijación es inseparable del producto.

17. Un proceso, de acuerdo con una de las reivindicaciones 1 a 9, CARACTERIZADO porque comprende adicionalmente las etapas de:

- encriptar dicha secuencia de caracteres utilizándose un sistema de criptografía asimétrica antes de la etapa (ii);
- divulgar la clave pública de dicho sistema de criptografía asimétrica antes de la etapa (iii); y
- desencriptar dicha secuencia de caracteres en la etapa (iii).

18. Un proceso, de acuerdo con la reivindicación 17, CARACTERIZADO por el hecho de que dicha secuencia de caracteres encriptada es acompañada por la clave pública adecuada para realizar su descriptación.

19. Un proceso, de acuerdo con una de las reivindicaciones 1 a 9, CARACTERIZADO porque comprende adicionalmente las etapas de:

- encriptar dicha secuencia de caracteres utilizándose un sistema de criptografía simétrica antes de la etapa (ii); y
- descriptar dicha secuencia de caracteres en la etapa (iii).

20. Un sistema de autenticación de productos por medios fuera de línea, CARACTERIZADO porque comprende:

- una base de datos para almacenar por lo menos una relación de secuencias de caracteres válidas o no válidas para productos que serán sometidos a autenticación;
- un verificador que accesa dicha base de datos para verificar la validez de dicha secuencia de caracteres que identifica el producto; y
- un elemento de emisión de mensajes que envía un mensaje a partir del resultado de la verificación de validez hecha por dicho verificador

21. Un sistema, de acuerdo con la reivindicación 20, CARACTERIZADO porque comprende adicionalmente un registrador de ventas capaz de registrar una transacción comercial involucrando dicho producto, e indicar a la base de datos que la secuencia de caracteres que identifica aquel producto no debe más ser considerada válida.

22. Un sistema, de acuerdo con la reivindicación 20 o 21, CARACTERIZADO porque comprende adicionalmente un medio para encriptar y/o descriptar una secuencia de caracteres que identifica el producto.

23. Un sistema, de acuerdo con la reivindicación 22, CARACTERIZADO por el hecho de que dicho medio es un software.

24. Un sistema, de acuerdo con la reivindicación 20, CARACTERIZADO por el hecho de que dicha base de datos opera en un dispositivo de almacenamiento de datos de una computadora.

25. Un sistema, de acuerdo con la reivindicación 20, CARACTERIZADO por el hecho de que dicho verificador es una computadora.

26. Un sistema, de acuerdo con la reivindicación 21, CARACTERIZADO por el hecho de que dicho registrador de ventas es una computadora.

5 27. Un sistema, de acuerdo con la reivindicación 21, CARACTERIZADO por el hecho de que dicho registrador de ventas es un terminal/caja registradora en el punto de ventas y/o distribución.

10 28. Un sistema, de acuerdo con la reivindicación 20, CARACTERIZADO por el hecho de que dicho verificador y dicho registrador de ventas están conformados en un dispositivo único.

29. Un sistema, de acuerdo con la reivindicación 20, CARACTERIZADO por el hecho de que dicho verificador es portátil.

30. Un sistema, de acuerdo con la reivindicación 21, 26 o 27, CARACTERIZADO por el hecho de que dicho registrador de ventas es portátil.

15 31. Un sistema, de acuerdo con la reivindicación 20, CARACTERIZADO por el hecho de que dicho elemento de emisión de mensajes es una pantalla de monitor o un video.

20 32. Un sistema, de acuerdo con la reivindicación 20, CARACTERIZADO por el hecho de que dicho elemento de emisión de mensajes produce señales de audio o cualquier otra forma de comunicación adecuada para personas con dificultad de lectura.

130

CASTELLANOS & CO LTDA
ABOGADOS
Calle 94 A No. 7 A-09
Bogotá, D.C. – COLOMBIA

Señor

Jefe de la División de Nuevas Creaciones

Superintendencia de Industria y Comercio

Ministerio de Comercio, Desarrollo, Industria y Turismo

E. S. D.

Ref.: **PODER** conferido por **ISAAC LEO BAIN**

Yo, **XIMENA CASTELLANOS ABONDANO**, mayor de edad, identificada y domiciliada como aparece al pie de mi firma, atentamente manifiesto a Uds. que sustituyo en la Dra. **MARGARITA CASTELLANOS ABONDANO**, el poder que me confirió **ISAAC LEO BAIN**, con domicilio en Al. Itu, 890 – Ap. 2 – 01421-001 – Sao Paulo – SP - BRASIL, debidamente legalizado por el Ministerio de Relaciones Exteriores bajo el No. 577608, el día 9 de Marzo de 2007, con las mismas facultades que me fueron conferidas, para tramitar la solicitud de Patente PCT Entrada en Fase Nacional, para: "PROCESO Y SISTEMA DE AUTENTIFICACION DE PRODUCTOS POR MEDIOS FUERA DE LINEA" (Expediente No. 06.121.494).-

Del Señor Jefe,

Acepto


Ximena Castellanos Abondano
C.C. No. 39.773.330 de Usaquén
T.P.A. No. 58.236 del C.S.J.
Calle 94 A No. 7 A-09 – Bogotá
PBX: 610 74 20


Margarita Castellanos Abondano
C.C. No. 39.779.654 de Usaquén
T.P.A. No. 70.819 del C.S.J.
Calle 94 A No. 7 A-09 – Bogotá
PBX: 610 74 20

Bogotá, D.C.
XCA/MCA/gcb/P1422

**AUTENTICACION DE FIRMA
MEDIANTE COMPARECENCIA PERSONAL**
(Art. 84 C.R.C. mod. Decr. 2282 de 1989, art. 1 mod. 38)

Ante mí Notario Cuarenta y Uno (41) del círculo de esta ciudad compareció personalmente: [Firma]
identificado con C.C. [Firma]
expedida en: [Firma] y tarjeta profesional de abogado(a) No. [Firma] del Consejo Superior de la Judicatura, con documento dirigido a [Firma]
y declaró que la firma puesta en este escrito es suya.

[Firma]
Firma del declarante

En Bogotá D.C. a 16 MAR 2007
AUTORIZO ESTA DILIGENCIA EL SUSCRITO



**AUTENTICACION DE FIRMA
MEDIANTE COMPARECENCIA PERSONAL**
(Art. 84 C.R.C. mod. Decr. 2282 de 1989, art. 1 mod. 38)

Ante mí Notario Cuarenta y Uno (41) del círculo de esta ciudad compareció personalmente: [Firma]
identificado con C.C. [Firma]
expedida en: [Firma] y tarjeta profesional de abogado(a) No. [Firma] del Consejo Superior de la Judicatura, con documento dirigido a [Firma]
y declaró que la firma puesta en este escrito es suya.

[Firma]
Firma del declarante

En Bogotá D.C. a 16 MAR 2007
AUTORIZO ESTA DILIGENCIA EL SUSCRITO NOTARIO



COLOMBIA

PODER

El

Isaac Léo Bain

Domiciliado en Al. Itu, 890 - Ap. 2 - 01421-001 - Sao Paulo - SP - Brazil

Nombran por el presente a XIMENA CASTELLANOS A. y/o MARGARITA CASTELLANOS A. abogadas con oficinas en la Calle 94 A No. 7 A-09, Bogotá-Colombia para obtener la protección de mi (nuestra) propiedad industrial y con este fin autorizamos a dichos apoderados para que nos representen ante cualesquiera autoridades o personas de los órdenes administrativo, contencioso - administrativo y judicial en todo lo relacionado con los siguientes actos y gestiones:

- Obtención de patentes de invención, modelos y dibujos industriales; registro de marcas de fabrica, de servicio, colectivas o defensivas y de denominaciones de origen, depósito de nombres y enseñas comerciales; su renovación, prórroga, inscripción de traspaso y cambio de nombre o domicilio, cancelación voluntaria y el registro de licencias de uso de esos derechos;
- Para la obtención de registros sanitarios;
- Acciones de oposición, observación, cancelación, nulidad, medidas cautelares y en general los juicios civiles, penales, administrativos o contencioso - administrativos que promovamos o se nos promuevan.

Pudiendo en todos los actos y gestiones arriba mencionados sustituir éste mandato, transgír, desistír, recibir, cancelar, renunciar, aceptar notificaciones y nombrar apoderados judiciales y extrajudiciales.

Finalmente, este poder ratifica la validez de todos los actos y solicitudes que, a nombre de la poderdante hubieren realizado los apoderados en relación con las facultades anteriormente enumeradas, antes de la suscripción del presente poder

Dado y firmado hoy

en Sao Paulo, 04 de diciembre de 2006

18
PIRANGA
por 

(Se requiere legalización consular o mediante apostilla)

POWER OF ATTORNEY

I the undersigned

Isaac Léo Bain

Of Al. Itu, 890 - Ap. 2 - 01421-001 - Sao Paulo -SP - Brazil

hereby grant(s) Power of Attorney to XIMENA CASTELLANOS A. and for MARGARITA CASTELLANOS A. attorneys residing at Calle 94 A No. 7 A-09, Bogotá-Colombia, to obtain the protection of my (our) Industrial Property, for which purpose we authorize the said attorneys to represent us before any authorities, or persons, specially those, administrative, contentious and judicial, in all matters concerning the following:

- Obtainment of patents, models and designs, registration of trademarks, service, collective and defensive marks, and of designations of origin; the deposit of trade names and ensigns; its renewal, extension, recordal of assignments, change of name or domicile, voluntary cancellation, and the registration of licenses of use of the above rights;
- For the obtainment of Sanitary registrations;
- Actions of opposition, cancellation, nullity, infringement, granting of licenses; and in general the civil, criminal and administrative suits related to those rights; actions and suits instituted by us or against us;

In all the above matters they may substitute this power of attorney, compromise, deal, cancel, receive, renounce, accept notifications and appoint attorneys in fact, in or out of court.

Finally, this power of attorney ratifies the validity of all acts and applications made by the representatives in the name of the signatory of this power of attorney, with regard to the faculties above given, before the execution of the present power of attorney.

Given and signed

at Sao Paulo, December 04, 2006

by

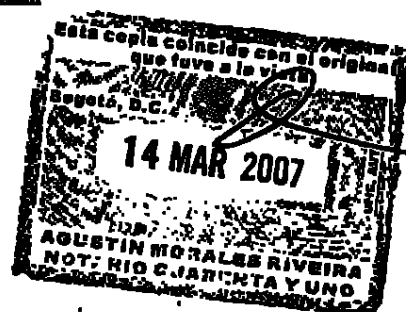
(Consular legalization or apostille is required)

CASTELLANOS & CO

ABOGADOS COLOMBIA

Calle 94A No. 7A-09 - P.O. Box 6349 - Bogotá, Colombia

Tel.: (571) 610 74 20 / - Fax: (571) 610 07 04 - e-mail: info@castellanosyca.com



47

4707

CONSULADO GENERAL DE COLOMBIA EN SÃO PAULO

Nº 789

El suscrito Cónsul General de Colombia CERTIFICA: que el señor MARCELO JOSE SILVA DOS SANTOS que autoriza el presente documento ejerció legalmente, en la fecha allí expresada las funciones de ESCRIBIENTE y que la firma y sello que en el documento aparecen como suyos, son los que usa y acostumbra en sus actos oficiales. El Cónsul no asume responsabilidad alguna por el contenido del documento.

23 02 2007

São Paulo, 24 DE FEBRERO DE 2007



CARLOS RODRIGUEZ AGUIRRE MONTEJO
CONSUL GENERAL

"Si está conforme con el servicio prestado, diríjase al Área de Quejas y Reclamos del Ministerio de Relaciones Exteriores, Carrera 8 Nº 9-46, Bogotá, D.C., Colombia; email: cdejas@minreter.gov.co"

PAGADO IMPUESTO DE TIMBRE

MINISTERIO DE
RELACIONES EXTERIORES

571608
COPIA AFILIADA EN LA
DOCUMENTACIÓN DE SERVICIO
LAS FUNCIONES INDICADAS

NO SE ASUME
RESPONSABILIDAD DEL TEXTO

2007 MAR - 9 A 9 59

Jefe de LEGALIZACIONES
BOGOTÁ D.C.

CONSULADO
DE COLOMBIA

1821
Paseo, por semejanza, a firma del ISAC LEO BAI, en documento sin valor
económico, del fº.
São Paulo, 16 de febrero de 2007.
En Teste
REL. MARCELO JOSE SILVA DOS SANTOS - ESCRIBIENTE (Nº 1821 de 2007)
RUA BOB PASTOR, 100 - CEP 04209-000 - IRAPURANGA - SÃO PAULO/SP - FONE/FAX: (11) 5103-4651 - 0215-0000



1 MAR 2007
ABUSTIN MOTAE RIVERA
NOTA: 1 GUARDA LA Y UNO
Esta copia colacionada con el original
que lleva a la vista.

132

TRADUCCIÓN OFICIAL NO. 4707 DE LOS SELLOS DE UN DOCUMENTO
ESCRITOS EN PORTUGUÉS, REALIZADA EL 12 DE MARZO, 2007 POR
LETICIA SALAMANCA ALVES, C.C. 41.322.380 DE BOGOTÁ, TRADUCTORA
E INTÉRPRETE JURAMENTADA SEGÚN RESOLUCIÓN NO. 289 DEL
MINISTERIO DE JUSTICIA, BOGOTÁ, COLOMBIA. _____

PODER DE CASTELLANOS & CO - Abogados - Colombia, firmado
Paulo el 4 de Diciembre, 2006 y firmado.

Por el reverso del documento aparece un sello de la Notaría 18 de Registro
Civil de las Personas Naturales, reconociendo la firma de este documento.
Dado en São Paulo, 16 de febrero, 2007 con la firma del Escribiente Autorizado
y una estampilla de certificación.

Un sello del Consulado General de Colombia en São Paulo, No. 789
certificando la firma del Escribiente Autorizado. Dado en São Paulo, el
23.01.2007 con la firma de Carlos Mauricio Acero Montejo, Cónsul General.

Otro sello del Ministerio de Relaciones Exteriores No. 577808 legalizando la
firma del Cónsul en São Paulo. Dado en Bogotá, D.C. el 9 de Marzo, 2007 con
la firma del Jefe de Legalizaciones. _____

TRADUCCIÓN FIEL Y COMPLETA DE SU ORIGINA, COPIA DE LA CUAL
QUEDA EN EL ARCHIVO DE LETICIA SALAMANCA ALVES PARA SU
CONFRONTACION,

