



# Industria y Comercio

S U P E R I N T E N D E N C I A

Delegatura de propiedad Industrial

División de Nuevas Creaciones

PCT  
SOLICITUD

## PATENTE DE INVENCION

- PCT ENTRADA EN FASE NACIONAL -

06-121494

21. EXPEDIENTE No.

54. TÍTULO

PROCESO Y SISTEMA DE AUTENTIFICACION DE PRODUCTOS POR MEDIOS  
FUERA DE LINEA

51. CLASIFICACIÓN INTERNACIONAL

71. SOLICITANTE

ISAAC LEO BAIN

DOMICILIO

A1. Itu, 890 - Ap. 2, 01421-001 Sao Paulo - SP - BRASIL

74. APODERADO

DRA. MARGARITA CASTELLANOS ABONDANO

22. BOGOTÁ, D. C.,

1 DIC. 2006

F.N. 64-01-2007

P.J. 1, Anexos

(FORMA P-10)

**FORMULARIO UNICO DE SOLICITUD DE PATENTE  
PCT  
ENTRADA EN FASE NACIONAL**

## SOLICITUD DE:

①

☒ Patente de invención☐ Patente de Modelo de Utilidad☐ Capítulo I☒ Capítulo II

②

SOLICITANTE (71)

Nombre: ISAAC LEO BAIN

Dirección: Al. Itu, 890 - Ap. 2, 01421-001 Sao Paulo - SP - BRASIL

Nacionalidad o Domicilio: Sao Paulo - BRASIL

Lugar de Constitución: BRASIL

Teléfono: Fax

E-mail:

IDENTIFICACIÓN

C.C. ☐ NIT ☐C.E. ☐ Otro ☐

Cual

Número

③

REPRESENTANTE  
O APODERADO (74)

Nombre: MARGARITA CASTELLANOS A.

Dirección: CALLE 94A No. 7A-09

Teléfono: 610 7420 Fax: 610 0708

E-mail: [info@castellanosyco.com](mailto:info@castellanosyco.com)

IDENTIFICACIÓN

C.C. ☒ NIT ☐C.E. ☐ Otro ☐

Cual

Número 39779.554 TPA 70,819

④

INVENTOR (ES) (72)

Nombre: ISAAC LEO BAIN

Dirección: Al. Itu, 890 - Ap. 2, 01421-001 Sao Paulo - SP - BRASIL

Nacionalidad o Domicilio: BRASILEÑO

⑤

PCT (86)

Solicitud Internacional No. PCT/BR2006/000025

Fecha 01/03/2005

Publicación Internacional No. WO 2006/119635

Fecha 16/12/2006

⑥

Título (54)

PROCESO Y SISTEMA DE AUTENTIFICACION DE PRODUCTOS POR MEDIOS FUERA DE LINEA

⑦

Clasificación Internacional (51) G06F 17/60; G07G 1/00

⑧

Prioridad

(33) País de Origen

(32) Fecha

(31) Número de Solicitud

SI ☒ NO ☐

BR

04/08/2004

P10402291-2

⑨

Comprobante de pago No. 06-91260

Fecha Noviembre 28, 2006

Instrucciones para el diligenciamiento del presente formulario, ver reverso de esta página.

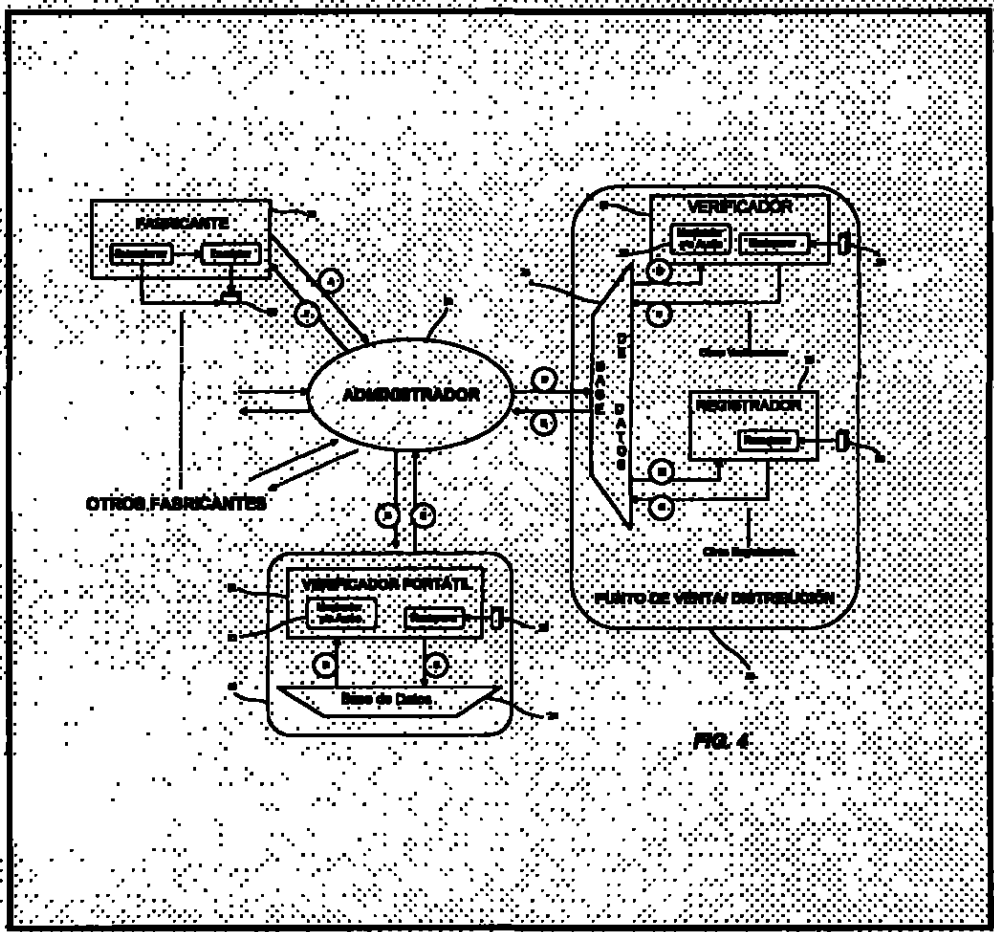
10

Anexos

- ☒ Comprobante de pago de la tasa de presentación de la solicitud.
- ☐ Documento que acredite la existencia y representación legal cuando el solicitante sea persona jurídica.
- ☐ Poderes, si fuere el caso, junto con la sustitución del mismo a mi favor
- ☐ Documento de cesión del inventor al solicitante o a su causante. - NO APLICABLE
- ☐ Declaraciones.
- ☒ Copia de la solicitud internacional (Resumen, descripción, reivindicaciones, dibujos).
- ☒ Traducción de la solicitud internacional al castellano (Resumen, descripción, reivindicaciones, dibujos).
- ☐ Copia del examen preliminar internacional efectuado por la Autoridad Internacional de Examen Preliminar (IPEA).
- ☐ Traducción del examen preliminar internacional efectuado por la IPEA.
- ☐ De ser el caso, copia del contrato de acceso.
- ☐ De ser el caso, documento que acredite la licencia o autorización de uso de conocimientos tradicionales de las comunidades indígenas.
- ☐ De ser el caso, certificado de depósito del material biológico.
- ☐ Arte final 12x12
- ☐ De ser el caso, Información sobre otras solicitudes de patente o títulos obtenidos en el extranjero por el mismo titular o su causante, relacionadas parcial o totalmente con la invención de esta solicitud.
- ☐ De ser el caso, modificaciones efectuadas a la solicitud internacional.
- ☒ Otros Tarjeta Propietario, Tarjeta Temática y Extracto para la Publicación

11

FIGURA CARACTERÍSTICA:



12

Solicito la concesión de la patente,

NOMBRE: MARGARITA CASTELLANOS ABONDANO

FIRMA: Margarita Castellanos

C.C. No. 38.775.654 Usaquén - TPA 70.819 C.S.J.

- 1 DIC. 2006

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

NIT : 800176089-2

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO  
Rad: 08-121494-00000-0000  
Fec: 2006-12-01 14:36:19 Dep. 2020 NUECREACIONE  
Tib. 11 PATENTERII  
X8: 579 FASENACIONALI  
487411 PRESENTACION  
Folios: 24

RECIBO OFICIAL DE CAJA : 06 - 91,260  
FECHA : NOVIEMBRE 28 DE 2006

\*\*\*\*\* CONSIGNACION \*\*\*\*\*

| DEPOSITANTE        | TIPO PAGO    | BANCO         | CUENTA      | No. PAGO | FECHA PAGO | Vr. PAGO     |
|--------------------|--------------|---------------|-------------|----------|------------|--------------|
| ALVARO CASTELLANOS | CONSIGNACION | BANCO POPULAR | 050-00110-6 | 50962580 | 28/11/2006 | 2,136,000.00 |

\*\*\*\*\* CONCEPTO \*\*\*\*\*

| CANT. | DETALLE                 | CONCEPTO                            | TOTAL CONCEPTO |
|-------|-------------------------|-------------------------------------|----------------|
| 1     | 50003-01-01 SOLICITUDES | 1 TRAMITES DE SOL. DE PATENTE DE IN | 463,000.00     |
|       |                         | TOTAL :                             | \$ 463,000.00  |

SON: CUATROCIENTOS SESENTA Y TRES MIL PESOS

RESPONSABLE : \_\_\_\_\_

RECIBO DE CAJA APLICADO AL EXPEDIENTE No. \_\_\_\_\_

(19) World Intellectual Property  
Organization  
International Bureau



(43) International Publication Date  
15 December 2005 (15.12.2005)

PCT

(10) International Publication Number  
WO 2005/119535 A1

- (51) International Patent Classification<sup>7</sup>: G06F 17/60, G07G 1/00
- (21) International Application Number: PCT/BR2005/000025
- (22) International Filing Date: 1 March 2005 (01.03.2005)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data: PID402291-2 4 June 2004 (04.06.2004) BR

AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

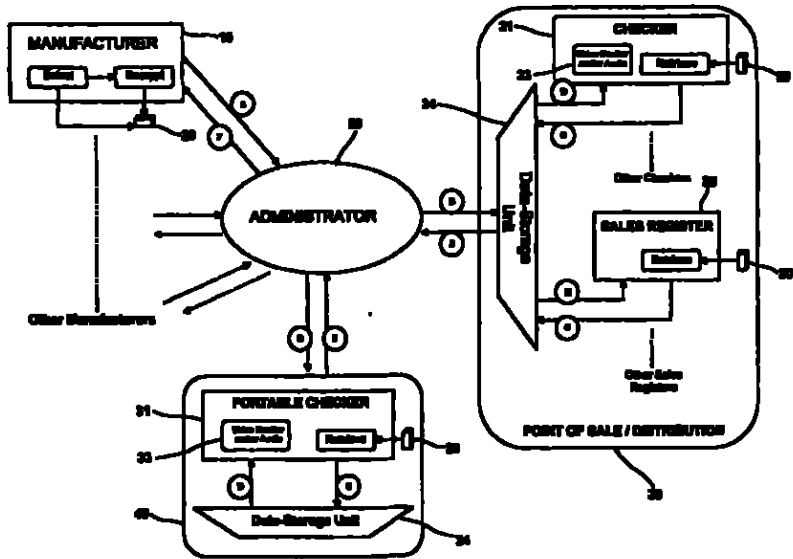
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

- (71) Applicant and  
(72) Inventor: BAIN, Isaac Léo [BR/BR]; AL Itu, 890 - Ap. 2, 01421-001 São Paulo - SP (BR).
- (74) Agents: GALARSA, Lucas M. et al.; Av. Brig. Faria Lima, 1485 - 11º andar, 01451-904 São Paulo - SP (BR).
- (81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM,

Published:  
— with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: OFF-LINE PRODUCT AUTHENTICATION PROCESS AND SYSTEM



(57) Abstract: The present invention refers to a process and system for product authentication by off-line means. According to one embodiment of the present invention, the authentication process comprises the steps of: (i) selection for each product a string of characters (20) to identify it; (ii) fixing said string of characters to the product; (iii) using a checker (31) to retrieve information from said string of characters at the moment of checking the product's authenticity and to check the validity of said string of characters retrieved; (iv) displaying a message dependent on the result of said validity check; (v) updating the indication of the validity of said string of characters in a data-storage unit (34); and (vi) periodically updating in said data-storage unit the indications of validity of said string of characters and of strings of characters that identify other products.

WO 2005/119535 A1

5

## **"OFF-LINE PRODUCT AUTHENTICATION PROCESS AND SYSTEM"**

### **FIELD OF INVENTION**

The present invention refers to a process and system for off-line product authentication.

5           More specifically, the present invention refers to a product authentication process and system wherein said products carry information that can be retrieved at the point of sale and/or distribution, for authentication by off-line means directly before the consumer and/or distributor.

### **BACKGROUND OF INVENTION**

10           Currently, piracy, theft, counterfeiting and contraband of industrialized goods are notorious problems. Daily, the media reports on fraud involving products such as CDs, software, brand-name clothes and accessories, liquors, pharmaceutical products, tobacco items, batteries and fuel, among others.

15           Despite their different juridical treatment, the different forms of falsification affect the manufacturer as well as the end consumer. Both are harmed by the illegal actions. On one side, the consumer is not sure if the product being purchased is original, and when such product is related to the safety or health of its user, as is the case of pharmaceutical products, safety  
20           equipments, food, tobacco or sports equipments, for instance, the damages caused by counterfeits can be enormous. On the other hand, the manufacturer, representative or distributor of the product suffers economic losses and damage to the reputation of its brand.

              Nonetheless, it is also of the public authorities' interest to suppress  
25           these acts, to ensure the safety and health of its citizens as well as to prevent tax revenue losses.

              Therefore, manufacturers, consumers and public authorities have great interest in repressing and preventing illegal acts involving industrialized goods.

30           For this purpose, some preventive measures have so far been adopted to prevent counterfeiting. These actions generally aim at providing

some means by which the consumer can easily identify the authenticity of the product.

There exist physical means for confirming the authenticity of products, such as holographic seals, scratch-and-see logotypes, tamper-evident seals or other visual identifiers. All of these are the more effective the more difficult their reproduction. In some specific cases, such as that of fuels, chemical reagents are available which, when put in contact with the product, produce special color patterns that indicate the product is authentic.

However, the aforementioned physical means of authenticity verification, despite inhibiting counterfeiting, are less efficient than would be desirable. Difficult to reproduce as the original visual identifier may be, nothing prevents falsifiers from copying it, even if with inferior quality. Consumers, even the most attentive, generally do not notice the small differences that exist between an original seal or identifier and a fake one, and may purchase the counterfeit product. Besides, if a visual means of authentication is not tamper-evident as well, it will have no efficacy should the counterfeiter re-use discarded original packaging. Finally, such visual means of authentication do not help to prevent the sale of stolen original goods, contraband or products that were tampered with to show a false expiration date, concentration or similarly important characteristic. The consumer cannot tell the difference.

There also exist electronic means of authenticity checking. Among them, there are on-line authentication systems that check in real time. In this case, however, the consumer must wait a long time for authentication, or it becomes impossible due to difficulty or impossibility of communication at the moment of authentication.

Authenticating machines limited to giving the consumer only "yes" or "no" answers, i.e. "authentic" or "fake," are also subject to fraud, and do not guarantee the veracity of the information to the consumer as they can be tampered with to always give a positive answer. Even when not tampered with, such machines cannot identify if the product comes from theft, contraband or illicit reuse of disposed packaging, i.e. they are subject to giving the user the

false impression of purchasing a product conveyed through a legitimate supply chain. This is typically the case of machines such as those that emit violet or ultraviolet light onto some visual element that is embedded in the product.

Therefore, the existing means of the state of the art to promote the  
5 verification of the authenticity of a product are inefficient and subject to flaws. The need exists for a process that enables consumers to reliably check the authenticity of a product and that solves the abovementioned problems.

It is, therefore, an object of the present invention to provide a  
process and system for the authentication of products whereby the authenticity  
10 of a product can be easily recognized by the consumer.

Another object of the present invention is to provide a product authentication process and system in which copying of the verification element is impossible.

It is another object of the present invention to provide a product  
15 authentication process and system in which it is possible to detect and prohibit the illegitimate reuse of an authentic verification element.

It is another object of the present invention to provide a product authentication process and system that allows the authenticity of the product to be verified off-line.

20 It is another object of the present invention to provide a product authentication process and system that is tamper-proof.

It is another object of the present invention to provide a product authentication process and system that gives the manufacturer and/or distributor means to combat theft and contraband by preventing stolen or  
25 smuggled authentic products from being authenticated.

Finally, it is another object of the present invention to provide a system that promotes the process of the present invention.

#### **BRIEF DESCRIPTION OF THE INVENTION**

For this specification, the following definitions are used:

30 Product: a unit of any product, or a product lot, or a package of any product containing one or more product units.

**Product Identity:** a string of characters that identifies the product exclusively. Each identity corresponds to only one product.

**Off-line:** defines the non-existence of data exchange with, or data processing by, a remote server at the moment of authenticity verification, be it  
5 by means of a network or through a dedicated communication channel.

**Remote server:** an element that is capable of processing data and exchanging it, through a dedicated communication channel or a network other than a local-area network (LAN), with another element significantly distant from the first.

10 **Manufacturer:** the manufacturer of the product, or one that adds value to the product, or the manufacturer's representative, distributor, or anyone interested in keeping the authenticity of the product.

**Consumer:** any person interested in checking the authenticity of a product, whether buying it or not.

15 **Checker:** a device that assists the consumer in verifying the authenticity of the product.

**Message:** any message containing information comprehensible to humans, such as a visual sign, a sentence within the language that the customer can understand, audio signals, tactile patterns, and so forth.

20 **Sale:** defined as any commercial transaction involving a product, including transactions for which there is no immediate payment.

According to a first embodiment of the present invention, the product authentication process involves the steps of:

- 25 i. Selecting for each product a string of characters to identify it;
- ii. Fixing said string of characters on the product;
- iii. Retrieving the information contained in said string of characters at the moment of checking the product's authenticity;
- iv. Checking the validity of said retrieved string of characters;
- 30 v. Exhibiting a message dependent on the result of said validity checking;

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).

10 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.

15 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.

25 Another example is a string of characters which is a function of the contents of the ID, such as a digital signature or the output 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 value will only be considered formally

consistent if the latter are valid for that ID.

The ID may also contain characters used for exhibiting a message, herein referred to simply as message characters. In this case, the ID provides the means to choose the message that will be exhibited to the consumer as a consequence of the validation of the ID. The ID may contain any message, such as a description of the main characteristics of the product or, as another example, a number that serves as an index for picking a message from a table of messages.

The ID may also contain characters that are used both to check formal consistency and to determine what message will be exhibited. For example, the output of a hash function may be used as index for selection from a table of messages. In another example, part of the ID may be used to test consistency by comparison with the digital signature while another part is used as index for that table. In another example, the ID can be the very message, or part of it.

The product's ID having been chosen, it is then (ii) fixed on the product. Fastening can be by physical means, such as marking a string of characters or a bar code onto the product, as well as by inserting information into a digital means fixed to the product, such as a magnetic strip or an electronic chip of the kind known as RFID or Smart Tag, or by any other suitable means. The choice of the means by which the ID is fixed on the product is not relevant for the scope of the present invention. Preferably, the ID thus fastened to the product becomes inseparable from it in order to prevent the use of the ID in other products. However, the ID can also be fastened to other places that accompany and/or are directly associated with the product. The ID must be fixed on the product in a manner that allows its information to be retrieved.

Subsequently, generally at the point of sale or distribution of the product, the person interested in checking the authenticity of the product submits it to the device herein referred to as off-line checker, or simply checker. The checker then (iii) retrieves the information in the ID fixed on the product; (iv)

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 value,  
25       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-

storage unit, the table of valid or invalid IDs does not have to store the full contents of each ID, but only the minimum that is needed to unambiguously individualize the reference to each ID.

If the checker concludes that the ID is valid, it exhibits (v) a  
5 comprehensible message on a display or a video screen, and/or via audio signals, and/or via tactile patterns and so on. If the checker concludes that the ID is invalid, it produces (v) a warning of counterfeit product or some information incomprehensible to humans.

The message exhibited to the consumer in case the ID is valid can  
10 be a standard message. Preferably, however, said message is linked to the message characters contained in the ID. More preferably, said message characters are related to the properties or characteristics of the product. Based on the message exhibited, the consumer decides whether or not to accept the product as authentic.

15 If the consumer decides to purchase the product, the validity indication of its ID is updated in the data-storage unit (vi), after the sale is registered, so as to prevent that ID from being considered valid in future authentications.

Alternatively, the consumer may decide not to purchase the  
20 product after authentication, even if considered authentic. In this case, the data-storage unit can register (vi) that the product has been submitted one more time to an authenticity check, and invalidate its ID after a certain pre-defined number of times is exceeded.

The data-storage unit is subjected to periodic updates (vii) to  
25 receive new lists of valid or invalid IDs. These updates bring information about IDs whose validity was cancelled since the latest update, about IDs that from then on will be considered valid, for example because they correspond to new products placed on the market. These updates (vii) may also collect from the data-storage unit information that can be sent to other data-storage units.  
30 Optionally, these updates alter other information contained in the data-storage unit, such as the contents of a table of messages. Optionally, information on IDs

that ceased being valid may be sent to the product manufacturer or to third parties. These updates (vii) take place as often as the manufacturer wishes, and may also be triggered by events that justify validation of certain IDs, such as the arrival of new products on the market or at the point of sale or distribution, or by events that warrant invalidation of certain IDs, such as theft or robbery of products or a product recall. The means of update is indifferent. On-line means such as the Internet, intranets, private networks or dedicated channels can be used, as well as off-line means, such as the distribution of CD-ROMs. The periodicity and the means of updating the data-storage unit are not relevant to the scope of the present invention.

In a second embodiment of the present invention, the product ID is encrypted and the result of the encryption is fixed on the product. According to this second embodiment, a public-key cryptography system, also known as asymmetric cryptography, is used.

In public-key cryptography, two mutually related keys are used, one public and another private. The public key can be made available to the public and may be known by any interested party. The private key, on the other hand, is kept secret by its owner.

In the practice known as cryptographic signature, the private key is employed to encrypt the data. Only the bearer of the private key is able to convert comprehensible data into totally incomprehensible data that can, however, be retrieved by the use of the corresponding public key. Since decryption is accomplished with the public key, anyone can retrieve the original data previously encrypted.

There are several public-key cryptography systems considered secure. One example is the system known as RSA, from RSA Security, Bedford, Massachusetts, USA. Other examples include the McEliece and the El Gamal systems. The choice of the public-key cryptography system to be employed is not relevant for the scope of this invention.

The product authentication process according to the second embodiment of the present invention additionally comprises the step of

encrypting said string of characters that identifies the product using a private key of a public-key cryptography system before step (ii) and after step (i). The second embodiment of the process includes an additional step of disclosing the public key that corresponds to the private key used to encrypt the ID, at any moment before step (iii). The second embodiment of the process also includes, as part of the step (iii) of retrieving the information contained in said string of characters, the decryption, by means of said public key, of the encrypted data fixed on the product.

Therefore, according to the second embodiment of the present invention, the product ID is encrypted with the private key before it is fixed (ii) on the product. The public key corresponding to the private key must be disclosed to allow decryption at the moment of retrieving the information contained in the ID. Disclosure of the public key may occur at any time provided it takes place before (iii) the information contained in the encrypted ID is retrieved.

When the second embodiment of the invention is employed, a suitable way of disclosing the public key is to record it in a data-storage unit to which the off-line checker has access. If there is more than one public key kept in the data-storage unit, a non-encrypted identifier must be present on the product to allow selection of the adequate public key. Another way of disclosing the public key is to fix it on the very product, explicitly, thus making it unnecessary to use other means of disclosure. The way the public key is disclosed is not relevant for the scope of the present invention.

After decryption, the information contained in the ID can be retrieved (iii) and the process of the present invention follows the subsequent steps as described above.

According to a third embodiment of the present invention, the product ID is encrypted by means of a symmetric cryptography system, also known as private-key cryptography. In this type of cryptography the same key is employed both for encrypting and decrypting the data and therefore the key must be secret. An example of symmetric cryptography is the system known as DES, but there are many others. The choice of the symmetric cryptography

system to be employed is not relevant for the scope of the present invention.

The authentication process according to the third embodiment of the present invention additionally comprises the step of encrypting said string of characters that identifies the product using a private-key cryptography system before step (ii) and after step (i). The third embodiment of the process of the present invention also comprises the step of decrypting the encrypted data with the same key used for encryption, when (iii) retrieving the information.

Therefore, according to the third embodiment of the present invention the ID is encrypted before it is fastened to the product. However, according to this third embodiment, there is need to disclose the decryption key. The checker has access to the key, but it must be kept secret from the public.

In any embodiment of the present invention, the information contained in the ID can be protected by additional layers of encryption. For example, after step (i) and before step (ii), an additional encryption is done with a key corresponding to the point of sale/distribution. That destination-dependent key may be chosen by the manufacturer or, alternatively, chosen and informed to the manufacturer by those responsible for the point of sale/distribution.

In any of the embodiments of the present invention, the ID can be compressed before (ii) fixing it on the product. In this case, the step (iii) of retrieving the information contained in the ID includes decompression of the data.

The present invention also refers to an off-line product authentication system comprising:

- a data storage unit that can store at least one list of valid or invalid strings of characters;
- a checker that can verify the validity of said string of characters that identifies the product; and
- a message-delivery element.

The system of the present invention may also comprise:

- a sales register capable of recording a commercial transaction involving said product and of indicating to the data-storage unit that the string of

characters that identifies that product should no longer be considered valid.

When the second or third embodiment of the process of the present invention is used, the system must also comprise means of encrypting and decrypting a string of characters that identifies the product.

5           Such means for encrypting and decrypting the ID is preferably software. Manual means may also be employed, but less preferably because they are much more burdensome and costly.

          The data-storage unit is preferably a database capable of storing a list of IDs. There are no restrictions on the type of database employed. Physical  
10   spreadsheets may be used, although less preferably.

          The checker, according to the present invention, is preferably a computer capable of retrieving information from the ID fixed on the product, processing it and checking the validity of the ID in said data-storage unit. A personal computer with an adequate data-input device is fully able to run the  
15   steps of the process of the present invention.

          The message-delivery element may be a display or video screen in the checker unit, such as the video monitor of a personal computer, or a display or video employed specifically to output messages. The message-delivery element may also be a speaker that outputs an audio signal. The  
20   message-delivery element may also combine both visual and sound output devices. The message-delivery element may, as well, be a tactile interface, such as a Braille display or a thermal output device. Any element capable of conveying a message to a person can be employed in the process of the present invention.

25           The sales register, herein referred to simply as register, may be a computer or point-of-sale cash register, provided it combine the functions of registering the sale of a product and updating the information regarding the validity of the product ID in the data-storage unit.

          In another embodiment of the system of the present invention, the  
30   checker is combined with the register in a single unit that can check the validity of the ID, output a message, register the sale and update the ID validity

Indication in the data-storage unit or, in case the ID is considered invalid, block the transaction.

In yet another embodiment of the system of the present invention, the checker is portable in order to allow checking authenticity in a remote site.

5

#### **BRIEF DESCRIPTION OF THE FIGURES**

These and other objectives, improvements and effects of the process and system of the present invention will become clear to those skilled in the art from the detailed description presented below, making reference to the following figures. The purpose of the figures is to illustrate specific embodiments of the invention. Said figures are schematic, with dimensions and proportions that may not correspond to reality, since they aim to illustrate the invention didactically, without imposing any limitations other than those specified in the attached claims, wherein:

10

- Figure 1 is a block diagram that schematically represents the first embodiment of the process of the present invention;

15

- Figure 2 is a block diagram that schematically represents the second embodiment of the process of the present invention;

- Figure 3 is a block diagram that schematically represents the third embodiment of the process of the present invention;

20

- Figure 4 is a schematic diagram that represents the system of the present invention; and

- Figure 5 is an enlarged image of the PDF-417 bar code created according to the example of the present invention.

#### **DETAILED DESCRIPTION OF THE INVENTION**

25

Figs. 1 and 4 illustrate the process and system according to one embodiment of the present invention. A manufacturer (10) initially selects (100) a string of characters that identifies a product (20). As mentioned above, the string of characters that identifies the product is defined as identity (ID).

Next, the ID is fixed (102) on the product (20). Preferably, the ID is fixed in such manner that it becomes fully associated with the product. More preferably, fastening is on the product itself. Fastening may be by any physical

30

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 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, such  
15 as MD-5 and SHA, among others.

Inclusion of a site identifier, or of a digital signature, or of a hash 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.

At the sale or distribution site (30), or at any time deemed  
30 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

adequate data-input device. Retrieval of the information contained in the ID fixed on the product can be accomplished by typing in the characters that compose it, by reading a bar code or a magnetic strip, by receiving radio-frequency signals, or by any other suitable means. Having retrieved (103) the  
5 information in the ID, the off-line checker (31) processes it in order to verify if said ID is valid (104).

If the checker detects any formal inconsistency in the retrieved ID, it is considered invalid. Otherwise, the ID will only be considered valid if the contents of the data-storage unit indicate it is valid. Thus, verification (104) of  
10 the ID's validity can involve two criteria. First, if the ID has characters that allow for checking of its consistency and integrity, the checker does the appropriate computations to conduct such verification. Without rejection in the consistency and integrity criterion, the checker confers the validity of the ID by consulting (C) a table of valid or invalid identities in the data-storage unit (34). In this case, the  
15 answer (D) to this consultation will determine the validity of the ID.

The data-storage unit (34) is, for example, a database that runs in said personal computer, or which the latter has local or off-line access to.

A message that depends on the validity of the ID is exhibited (105) to the consumer on a display (33). The display (33) can be, for instance, a  
20 liquid-crystal screen or a video monitor. Optionally, the message is exhibited by means of an audio signal or some other form of delivery means especially useful for people with reading difficulties.

The message displayed helps the person interested in authenticating the product to decide whether it is authentic or not. In case the  
25 checker (31) considers (104) the ID invalid, an alert message or an incomprehensible message is displayed (105). If, otherwise, the checker (31) considers (104) the ID valid, a comprehensible message is displayed (105). There are no restrictions to what the comprehensible message should be. Preferably, however, it is related to the contents of the ID.

30 After the message is displayed (105), information related to the validity of said ID is updated (106) in the data-storage unit (34). This update

(106) registers the fact that the validity of that ID has just been checked, and may also record the date and time when this occurred. In case the ID has been considered (104) valid, this update (106) makes a move towards cancelling its validity. This cancellation of validity can be immediate or, alternatively, mediated  
5 by a few conditioners such as making the ID invalid only after a certain period of time has passed since verification, or counting how many times the validity of that ID has been checked so far and cancelling it only after a certain number of times is exceeded. On the other hand, if the ID has been considered (104) invalid, this update (106) may record that a counterfeit product with that ID was  
10 submitted to an authenticity check.

Registering the sale of the product (20) also provokes an update (106) of the validity status of its ID in the data-storage unit (34). The sales register (35) is capable of retrieving (103) the information contained in the ID and verifying (104) its validity in a manner analogous to that of the checker (31).  
15 In case the ID is Invalid (H), the sales register (35) blocks the sale. If the ID is valid (H) and the product is sold, the sales register (35) provokes (G) an update (106) of the data-storage unit (34) in such manner that from then on that ID be considered Invalid.

Checker (31) and sales register (35) may be dissociated from one  
20 another, in separate units. In this embodiment the customer can, for example, check the authenticity of the product at the shelf or counter before deciding to buy it. Later on, when the cashier registers the sale, the sales register (35) updates (106) the data-storage unit (34), cancelling the validity of that product's ID. In another embodiment, the checker (31) and the sales register (35) are  
25 associated in a single unit. This way the customer can check the authenticity and purchase the product at one and the same time at the cashier.

Checker and data-storage unit may also be portable (40). Thus, they can be transported to the site of consumption or distribution instead of having the consumer or distributor go to the point of sale. This embodiment is  
30 especially useful when the consumer places an order for delivery of a product or a lot. The product or lot shipped to the consumer or distributor is submitted to

authenticity check at the point of destination. The checker and data-storage unit having been taken to the same location, off-line authenticity check is done in a manner completely analogous to that described above. The portable checker can be, for example, a laptop computer equipped with the adequate data-input device, while its magnetic disk plays the role of portable data-storage device.  
5 For the same reasons, the sales register may be portable to allow registering a sale at the point of destination of the product.

Those skilled in the art will understand that the same results can be obtained by updating the validity of the ID (106) in the data-storage unit before or at the same time the message is displayed (105). The exact temporal  
10 order of those two steps is not relevant for the scope of the present invention.

The data-storage unit (34) is periodically updated with remote information (107) that validates certain IDs, for instance as new products are produced and put on the market, and with information that invalidates other IDs, for example as products are subjected to authentication checks and sold  
15 elsewhere, or as theft, robbery or a recall justify cancellation of certain IDs. These updates (107) also upload from the data-storage unit information to be sent to other data-storage units. Optionally, these updates (107) also change other data in the data-storage unit, such as the contents of a table of messages.  
20 The exact frequency of these updates is not relevant for the scope of this invention.

Figure 4 shows information exchange involving a central administration hereafter referred to simply as administrator (50). The manufacturer (10) sends (A) to the administrator a list of identities that correspond to authentic products (20) about to be put on the market. Said list is,  
25 in turn, updated (B) into the data-storage unit (34). Optionally, the data-storage unit (34) sends (E) to the administrator a list of IDs that have become invalid, or that have been subjected to validity checks more than a certain number of times, or a list of IDs apparently corresponding to counterfeit products that have  
30 been subjected to authentication. The list sent (E) to the administrator may also be sent (F) to the manufacturer (10) as a report for statistical control or other

ends.

Administration of the system of the present invention may be done by an administrator (50) other than the manufacturer, such as the one in Fig. 4, as well as by the manufacturer (10) itself. Those skilled in the art will understand that the administration can be done in a distributed manner, by several data processors. In this case, the administrator can be understood as being the set of all pieces of software that, acting together but in a distributed way, implement the steps described above. The exact means by which system administration is accomplished is not relevant for the scope of the present invention.

The administrator and the data-storage unit (34) can exchange information (107) through a dedicated communication channel, a private network, or the Internet. In case no telecommunication means is available, the update (107) may be carried out with the help of a portable data-storage element, such as diskettes or CDs transported to and from the points of sale/distribution. The exact means of exchanging information (107) between the administrator and the data-storage unit and the frequency with which it is done are not relevant to the scope of this invention.

Figure 2 illustrates the second embodiment of the process according to the present invention, where the ID is encrypted using a public-key cryptography system. According to this embodiment, after the ID is selected (100) it is subjected to encryption (101) using a public-key cryptography system.

Optionally, the manufacturer may compress the ID before encrypting, or compress the encrypted ID before. Should this be the case, the data ought to be decompressed during the information retrieval step (103).

The ID is encrypted (101) with a private key of a public-key cryptography system. The result is a sequence of characters not comprehensible to humans. Said private key is not disclosed, and is of exclusive property of the manufacturer (10) or administrator (50).

The encrypted ID is then fixed (102) on the product (20). Preferably, the encrypted ID is fully associated to the product. With greater

preference, fastening is on the product itself. Fastening may be by any physical means, such as a printed bar code, or by any digital means, such as a magnetic strip or an RFID chip, as long as the information contained in the ID be retrievable. The exact means by which the encrypted ID is fastened to the product is not relevant for the scope of the present invention. The encrypted ID may also be fastened onto a product lot or onto several products at the same time in the case of those sold in more than one unit in the same package.

The public key corresponding to the private key is disclosed (108) to allow decryption of the encrypted ID. Disclosure of the public key may be at any time: before selecting (100) the ID; or after selecting and before encrypting it (101); as well as after encryption and before fastening (102) of the encrypted ID onto the product; or even after fastening (102); as long as it occurs before the retrieval (103) of the information contained in the encrypted ID, because only in possession of the public key it is possible to run the verification step (104). The means by which the public key is disclosed is not relevant for the scope of the present invention. The process then follows the steps of the first embodiment of the invention, but including in step (iii) the decryption of the encrypted data.

According to this second embodiment, the data-storage unit (34) optionally has the capacity to store the public key(s) disclosed by the manufacturer(s). Preferably, the checker (31) is able to recognize the manufacturer and select the adequate public key.

Optionally, the public key is fixed on the product. In this case, it is neither necessary to store that public key in the data-storage unit (34) nor to disclose it by other means.

Figure 3 illustrates a third embodiment of the process of the present invention, where instead of employing a public-key cryptography system, a private-key cryptography system is used. The process runs the steps described for the second embodiment of the present invention, but not including the step of disclosing the key, since the key used for ID encryption is the same as the key used for decryption and, therefore, must be kept secret.

The present invention also refers to a product authentication system, as illustrated in Figure 4, comprising:

- a means of fixing a string of characters that identifies the product on the product (20) in such manner that the string of characters can be  
5 retrieved;
- a data-storage unit (34) for storing at least one list of valid or invalid strings of characters;
- a checker (31) to check the validity of the string of characters that identifies the product; and
- 10 - a message-delivery element (33).

The system of the present invention may additionally comprise a sales register (35) to record and process a commercial transaction involving said product and to update the data-storage unit so that the string of characters that identifies said product be no longer considered valid.

- 15 The means employed for fixing the string of characters that identifies the product is preferentially a physical means such as printing the string itself or a bar code representation of it. Electronic means can also be employed, such as RFID chips, magnetic strips, or any other suitable means.

- 20 When either the second or the third embodiment of the process of the present invention is employed, the system must also comprise a means of encrypting and decrypting a string of characters that identifies the product. Said means of encrypting and decrypting the ID is preferably software, such as an RSA-based software. Manual means can also be employed, but less preferably.

- 25 The data-storage unit (34) is preferably a database capable of storing ID information. There are no restrictions regarding the type of database employed. Spreadsheets in physical format can also be used, but less preferably.

- 30 The checker (31), according to the system of the present invention, is preferably a computer able to retrieve the ID and to check its validity in said data-storage unit. A personal computer with suitable peripheral equipment is fully able to run the steps of the process of the present invention.

The sales register (35) may be a computer or point-of-sale cash register, as long as it combines the functions of registering the sale of the product and updating the data-storage unit.

In another embodiment of the system of the present invention, checker (31) and sales register (35) are combined in a single unit that can verify the authenticity of a product, deliver a message, register the sale of the product and update the data-storage unit (34).

In another embodiment of the system of the present invention, the checker is portable (40), thus permitting authentication of a product at a site where a checker is otherwise unavailable.

In another embodiment of the system of the present invention, the sales register is portable, thus permitting the sale of a product to be registered at a site where a sales register is otherwise unavailable.

According to the specification above, it will be evident for those skilled in the art that the present invention solves the problems of the state of the art by providing a process and system for product authentication that promotes easy recognition of product authenticity by the consumer by virtue of the exhibition of a message, visual, auditory or otherwise. Nonetheless, the present invention renders useless the duplication of the authentication element, as well as makes the reuse of product ID impossible. In addition, authenticity check is off-line, waiving the need for on-line connection with a remote server at authentication time. Furthermore, the present invention gives manufacturers great advantage in inhibiting illicit actions such as contraband, robbery and piracy.

25

#### EXAMPLE

The present invention will now be described in a practical example of the application of one of the embodiments presented above, given only as an illustration, without imposing any limitations beyond those contained in the attached claims.

30

In this example, a drugs manufacturer prints on the package of one of its products a code which will allow the consumer to check that the

product is authentic. This authenticity check is done off-line at the drugstore before the product is purchased.

This manufacturer is catalogued as No. 01 in a registry of manufacturers. At a certain moment, the manufacturer selects a pair of keys of the RSA cryptographic system, one public and the other private.

In order to generate that pair of keys, the manufacturer uses software that runs on a conventional computer. Initially, the manufacturer chooses four random numbers, called R1, R2, R3 and R4, to be given as input to that software:

10               - R1=123456789  
                - R2=235619181  
                - R3=126171819  
                - R4=121256171

Based on the four inputs R1, R2, R3 and R4, the software produces as outputs two long prime numbers P and Q, whose values in decimal notation are as follows:

P=7730063972416833541332074347972555699484007996936627505136892  
8424940196293451  
Q=9002600512219211542746605816952425698540062197104387541  
20 5635710094429895131083

That same software calculates the product of P and Q, called N, so that  $N=P \times Q$ , whose value in decimal notation is as follows:

N=6959067787756705876553835596165330393095183089839319075724666  
375734801686354559138532426783559571765453427537120582295229823  
25 306581086097206402868379437433

The manufacturer's public key consists of two numbers: one of them is the number N above, and the other is the number 3, which will serve as exponent in the decryption procedure.

The numbers that constitute the public key are stored in the data-storage unit to which the authenticity checker has off-line access, such as the magnetic storage medium of a personal computer at the point of sale.

The private key consists of the pair of numbers P and Q. The private key is available as input to an encryption software that runs on the manufacturer's computer and serves to generate the code that will be printed on the package of the product. The manufacturer does not disclose the private key.

5           Given P and Q as input, the encryption software generates two other values: one called "Phi", which is the product  $(P - 1) \times (Q - 1)$ ; and the other called D, which is the multiplicative inverse of 3, modulo Phi. Only the manufacturer is privy to the values of Phi and D.

10           The encryption software also receives as inputs the number by which the manufacturer is catalogued in the registry, in this case the number 01, the product's serial number, and some text chosen by the manufacturer.

15           In the present example, the manufacturer produces a box containing capsules of the antibiotic Amoxicillin, and gives that box the serial number 1234567890. The encryption software aggregates the binary representation of the number 01 as a prefix to the binary representation of that serial number. The result is then aggregated, also as a prefix, to the binary ASCII representation of the text "AMOXICILLIN 750 MG CAPSULES – EXPIRES 03 MAY 2009". The resulting string of bits is the ID of the product. It is regarded by the software as a numerical value M.

20           Next, the software does the mathematical calculation: M raised to the power D, modulo N. The result X is the encrypted ID, and its numerical value is shown below in hexadecimal notation:

25           X= 71 5B F1 81 5C 1D FE BF 14 BC 4F 3B 0D AF 6F 42 34 78  
BA 51 47 41 D1 F9 83 1B 93 DD 1B 15 A9 C4 6C 8E 40 B6 AD E2 14 8B 03 C9  
1D 30 8E D1 B6 E1 E8 BB 96 38 4F 59 99 8B 6C D2 F1 CA E3 5F B6 E0

          The binary representation of the number 01, which identifies the manufacturer, is then aggregated as a prefix to the binary representation of the value of X. The resulting string of bits is, in hexadecimal notation:

30           01 71 5B F1 81 5C 1D FE BF 14 BC 4F 3B 0D AF 6F 42 34 78 BA  
51 47 41 D1 F9 83 1B 93 DD 1B 15 A9 C4 6C 8E 40 B6 AD E2 14 8B 03 C9 1D  
30 8E D1 B6 E1 E8 BB 96 38 4F 59 99 8B 6C D2 F1 CA E3 5F B6 E0

This string of bits is then converted into a kind of representation that will make it retrievable by electronic means in the future. In this example, the chosen representation is a bar code. Among many existing bar-code representations, the manufacturer chooses the bi-dimensional one known as PDF-417. The resulting bar code is shown in Figure 5, greatly enlarged to allow easy visualization of the details. The manufacturer affixes that bar code onto the box that contains the medicine.

As previously mentioned, the manufacturer discloses the public key that corresponds to the private key used to encrypt the ID. In other words, the numbers N and 3 are disclosed at some moment before decryption takes place.

The consumer, who is in the drugstore where that box of medicine is for sale and is interested in checking its authenticity before buying it, submits the box to the bar-code reader that is part of the checker, a device with data-processing capability. The checker retrieves the information contained in the bar code and gives it as input to software that runs on a CPU at the drugstore.

The software initially finds out who the manufacturer is by reading the first byte of the string of bits. This enables the software to select, from a table of public keys, the correct public key it will use to decrypt the encrypted ID, since other manufacturers may have chosen to use other keys. Next, disregarding the first byte, all the remainder is the value of X. According to the cryptographic method employed, the information M contained in X is recovered by performing the mathematical calculation  $M = X^3 \text{ modulo } N$ .

Having calculated M, which is the identity of the product, the software separates the serial number from the message. If the serial number contained in the ID is not among those listed in a table of valid serial numbers pertaining to manufacturer 01, a table which is stored in the drugstore's data-storage unit, the ID will be considered invalid and, as a consequence, the equipment will warn the consumer that the product is a counterfeit by means of showing the word "COUNTERFEIT" on its display and simultaneously having its voice synthesizer utter it aloud. The same will happen if that serial number is

listed as valid but this is, for instance, the tenth time it is submitted to the checker. In this instance, ten times is the limit the manufacturer has chosen to signal to the software that something odd is going on which deserves investigation and, in the interim, to invalidate that serial number.

5           If the serial number is considered valid, the checker will show on its display the text "AMOXICILLIN 750 MG CAPSULES – EXPIRES 03 MAY 2009" contained in M. Simultaneously, that text will be uttered aloud by the checker's voice synthesizer.

10           When the consumer reads and/or hears clearly the name of the medicine and other comprehensible information contained in that text, he/she becomes convinced that the product is authentic.

          Once satisfied that the contents of the box are authentic, the consumer takes it to the cashier, pays for it and receives the sales ticket. As the cashier's terminal registers the transaction, it updates the table of valid serial  
15           numbers in the drugstore's data storage unit, invalidating that particular serial number so that no other product with the same serial number may be considered authentic.

          During the next on-line update of the data-storage unit, which in the present example will take place two days later, the fact that the  
20           aforementioned serial number was invalidated will be uploaded to the administrator, which in turn transmits this information to all other data-storage units. During the same on-line update, the data-storage unit receives information about serial numbers that from then on ought to be considered invalid, as well as about other serial numbers that from then on should be  
25           considered valid.

          It should be understood that, although the present invention has been described in relation to its preferred embodiments, those skilled in the art may develop numerous variations of details and expand the processes and system described above to cover other types of applications without, however,  
30           deviating from the principles of the invention. For example, several of the elements described for the different embodiments may be combined in a

manner not illustrated above. Therefore, the attached claims should be interpreted as covering all equivalents that are within the scope and character of the present invention.

**CLAIMS**

1. Off-line product authentication process comprising the steps of:
- 5 It;
- i. Selecting for each product a string of characters to identify
- 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;
- 10 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
- 15 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.
- 20 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.
- 25 6. The process of claim 1, 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 1, characterized in that said string of characters comprises a digital signature or the result of a hash function.
- 30 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 claim 1, characterized in that said string of characters is compressed.

11. The process of claim 1, 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 claim 1, characterized in that said string of characters fixed on the product is inseparable from the product.

17. The process of claim 1, 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

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

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 claim 1, characterized by additionally comprising the steps of:

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

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.

21. The system of claim 20, characterized by additionally  
10 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.

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

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

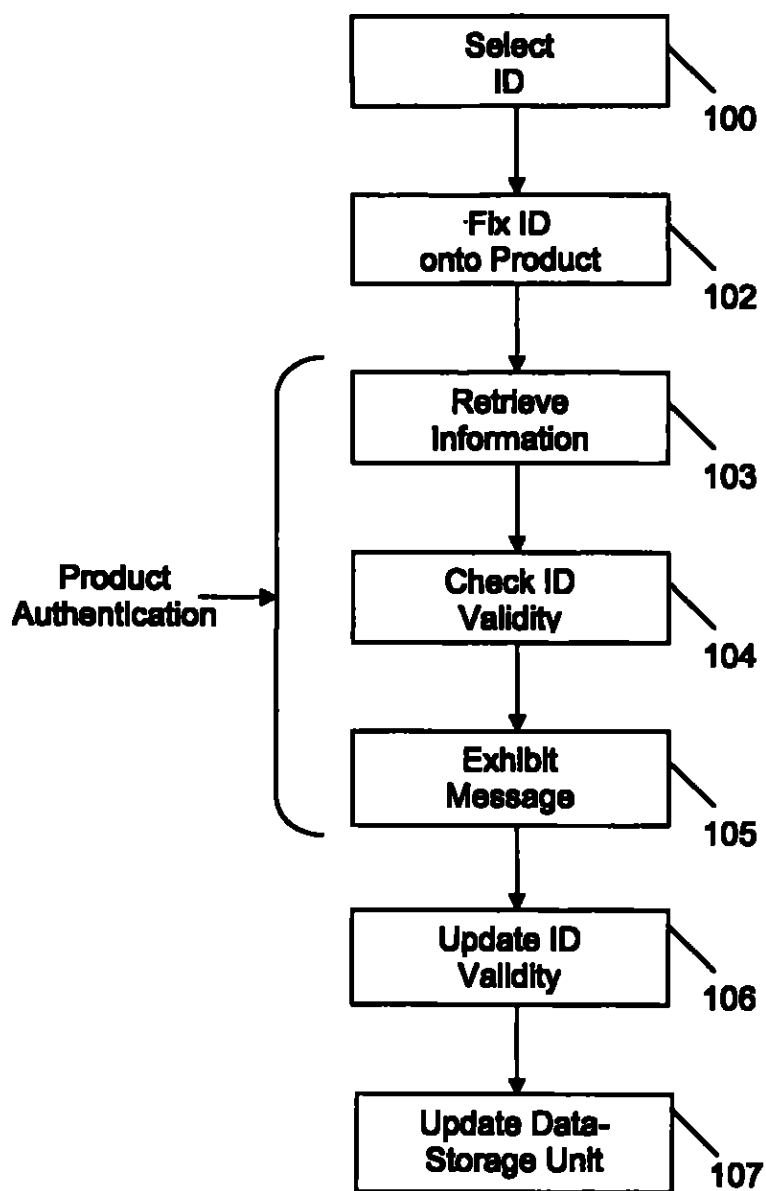
28. The system of claim 20 or 21, characterized in that said checker and said sales register are combined in one single unit.

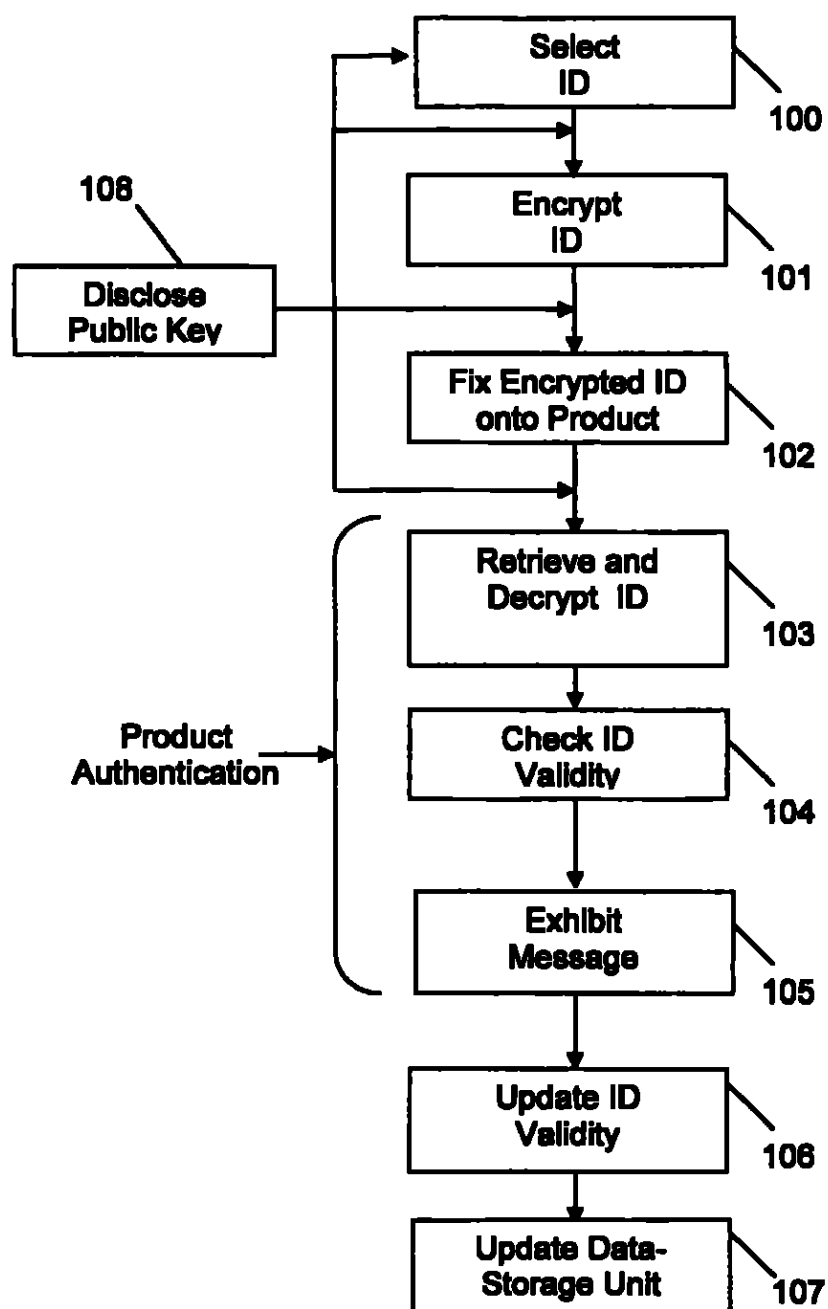
29. The system of claim 20, characterized in that said checker is portable.

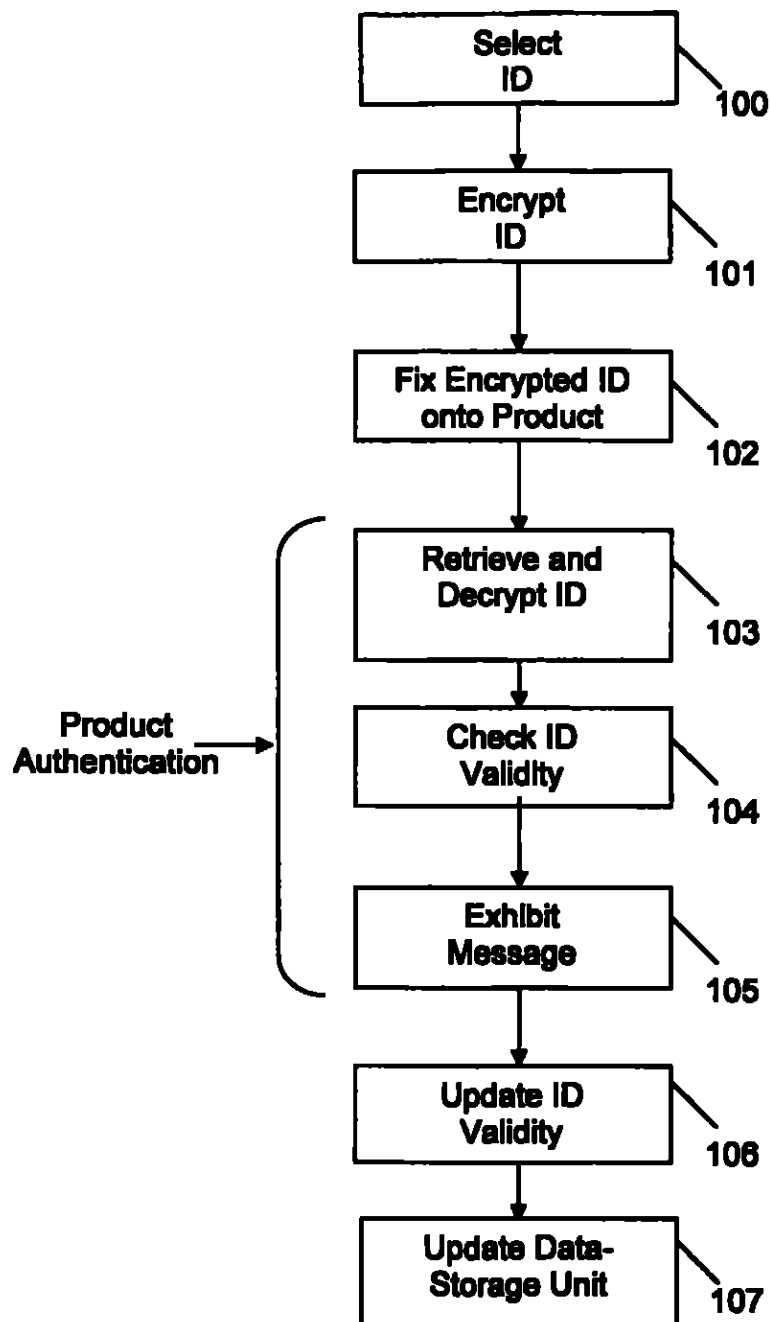
30 30. The system of claim 21, 26 or 27, characterized in that said sales register is portable.

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.

**Fig. 1**

**Fig. 2**

**Fig. 3**

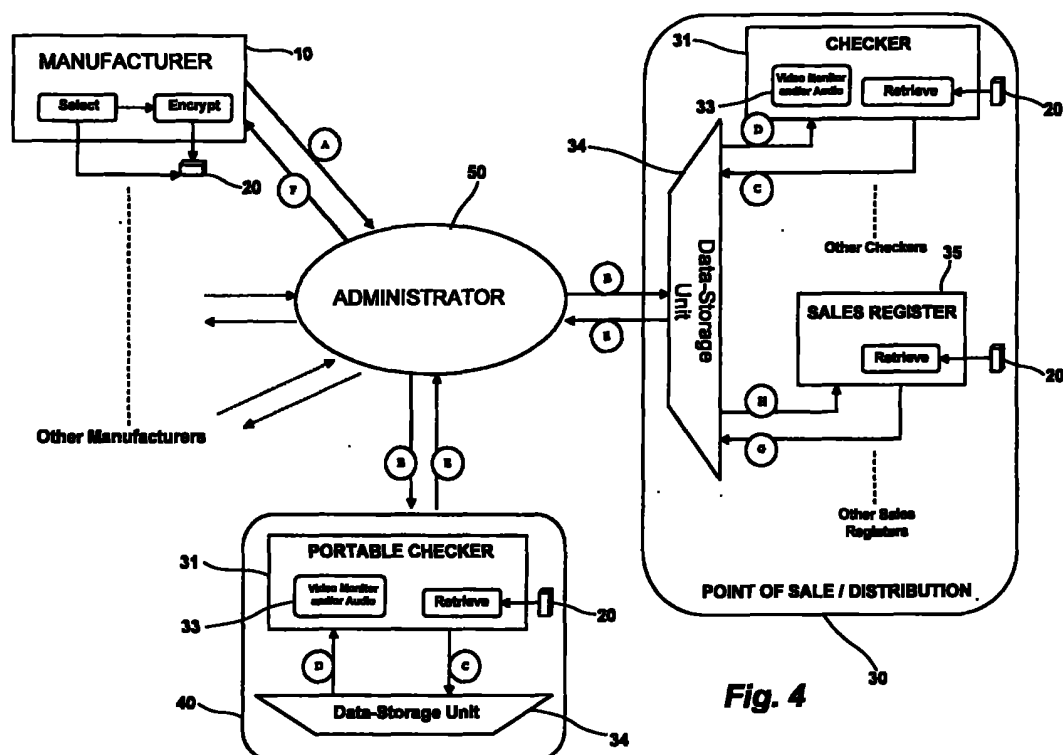


***Fig. 5***

## INTERNATIONAL SEARCH REPORT

International application No.  
PCT/BR 2005/000025

| <b>A. CLASSIFICATION OF SUBJECT MATTER</b><br><b>IPC<sup>7</sup>: G08F 17/80, G07G 1/00</b><br>According to International Patent Classification (IPC) or to both national classification and IPC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                       |                                                                                        |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| <b>B. FIELDS SEARCHED</b><br>Minimum documentation searched (classification system followed by classification symbols)<br><b>IPC<sup>7</sup>: G08F, G07G</b><br>Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched<br>—                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                       |                                                                                        |
| Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)<br><b>Epodoc, WPI, PAJ</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                       |                                                                                        |
| <b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                       |                                                                                        |
| Category*                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Citation of document, with indication, where appropriate, of the relevant passages                                    | Relevant to claim No.                                                                  |
| X                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | US 20040034579 A1 (XU et al) 19 February 2004 (19.02.2004)<br><i>abstract, paragraphs 0007-0010.</i>                  | 1, 11, 12, 20,<br>24, 25, 31                                                           |
| X                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | US 20030085797 A1 (LI) 8 May 2003 (08.05.2003)<br><i>abstract, paragraphs 0016-0021.</i>                              | 1, 11, 18, 20,<br>24, 25, 31                                                           |
| X                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | JP 2003216710 A (DAINIPPON PRINTING) 31 July 2003<br>(31.07.2003)<br><i>abstract, paragraphs 0017-0022, figure 1.</i> | 1, 13, 15, 20,<br>22-25, 31                                                            |
| A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <i>abstract, paragraphs 0017-0022, figure 1.</i>                                                                      | 17-19                                                                                  |
| <input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input checked="" type="checkbox"/> See patent family annex.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                       |                                                                                        |
| * Special categories of cited documents:<br>"A" document defining the general state of the art which is not considered to be of particular relevance<br>"E" earlier application or patent but published on or after the international filing date<br>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)<br>"O" document referring to an oral disclosure, use, exhibition or other means<br>"P" document published prior to the international filing date but later than the priority date claimed<br>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention<br>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone<br>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art<br>"Z" document member of the same patent family |                                                                                                                       |                                                                                        |
| Date of the actual completion of the international search<br><b>1 June 2005 (01.06.2005)</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                       | Date of mailing of the international search report<br><b>15 June 2005 (15.06.2005)</b> |
| Name and mailing address of the ISA/ AT<br><b>Austrian Patent Office</b><br><b>Dresdner Straße 87, A-1200 Vienna</b><br>Facsimile No. +43 / 1 / 534 24 / 535                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                       | Authorized officer<br><b>HARASEK S.</b><br>Telephone No. +43 / 1 / 534 24 / 574        |

# INTERNATIONAL SEARCH REPORT

41

International application No.  
PCT/BR 2005/000025

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages     | Relevant to claim No.       |
|-----------|----------------------------------------------------------------------------------------|-----------------------------|
| X         | JP 2002183270 A (HITACHI) 28 June 2002 (28.06.2002)<br>abstract, paragraphs 0008-0015. | 1, 13, 15, 20,<br>22-25, 31 |
| A         | abstract, paragraphs 0008-0015.                                                        | 17-19                       |

# INTERNATIONAL SEARCH REPORT

42

Information on patent family members

International application No.  
PCT/BR 2005/000025

| Patent document cited<br>in search report |   |                  | Publication<br>date | Patent family<br>member(s) | Publication<br>date |
|-------------------------------------------|---|------------------|---------------------|----------------------------|---------------------|
| JP                                        | A | 20021832<br>70A2 |                     | none                       |                     |
| JP                                        | A | 20032167<br>10A2 |                     | none                       |                     |
| US                                        | A | 20030085<br>797  |                     | none                       |                     |
| US                                        | A | 20040034<br>579  |                     | none                       |                     |

## **MEMORIA DESCRIPTIVA**

### **CAMPO DE LA INVENCION**

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

5 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.

15 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.

25 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 autentique 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 "si" o "no", esto es, "auténtico" o "falso" en relación al producto, también no garantizan completamente al consumidor respecto a la veracidad de la información 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.

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.

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.

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.

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.

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.

**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.

**"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.

**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.

**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.

**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:

- 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 el resultado de la aplicación 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.

5        En el caso que la identidad contenga caracteres de redundancia del tipo 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.

10       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).

15       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.

20       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.

25       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.

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 desencriptación.

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 de 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 desencriptar una secuencia de caracteres que identifica el producto.

El dicho medio para encriptar y desencriptar 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

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  
5 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  
25 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.

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.

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 resultado de la aplicación 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.

La inclusión de un identificador del local a que se destina la venta del producto, o de una firma digital, o de uno Hash junto a la identidad, permite confirmar la consistencia formal e integridad de los datos.

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.

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.

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.

5 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.

10 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  
15 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  
20 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  
25 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

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 desenscriptar la identidad para recuperar las informaciones ahí contenidas.

5 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.

10 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.

15 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 desenscriptación, debiendo, por eso, ser mantenida en secreto por el portador.

20 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;
- 25 - una base de datos (34) para almacenar por lo menos una relación de secuencias de caracteres válidas o no válidas;

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:

P= 77300639724168335413320743479725556994840079969366275051368928  
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:

**N = 6959067787756705876553835596165330393095183089839319075724666  
3757348016863545591338532426783559571765453427537120582295229  
823306581086097206402868379437433**

5 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.

10 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.

15 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.

20 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  
25 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.

5 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 descryptar 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  $M = X^3$  módulo N.

10 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

15 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.

20 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.

25 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.

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.

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 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.

### **REVINDICACIONES**

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 1, 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.

5 7. Un proceso, de acuerdo con la reivindicación 1, 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.

10 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 la reivindicación 1, CARACTERIZADO por el hecho de que dicha secuencia de caracteres es comprimida.

15 11. Un proceso, de acuerdo con la reivindicación 1, CARACTERIZADO por el hecho de que 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.

20 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.

25 16. Un proceso, de acuerdo con la reivindicación 1, CARACTERIZADO por el hecho de que dicha fijación es inseparable del producto.

17. Un proceso, de acuerdo con la reivindicación 1, 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

5 - 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 desenscriptación.

10 19. Un proceso, de acuerdo con la reivindicación 1, CARACTERIZADO porque comprende adicionalmente las etapas de:

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

- desencriptar dicha secuencia de caracteres en la etapa (iii).

15 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;

20 - 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

25 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 desencriptar 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.

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.

28. Un sistema, de acuerdo con la reivindicación 20 o 21, 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.

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 vídeo.

**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.**

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

**RESUMEN**

La presente invención se refiere a un proceso y a un sistema de autenticación de productos donde los dichos productos están provistos de una información que puede ser recuperada en el punto de ventas y/o de distribución para autenticación por medios fuera de línea directamente junto al consumidor y/o distribuidor. De acuerdo con una ejecución de la presente invención, el proceso de autenticación de los productos comprende las etapas de: (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 a otros productos.

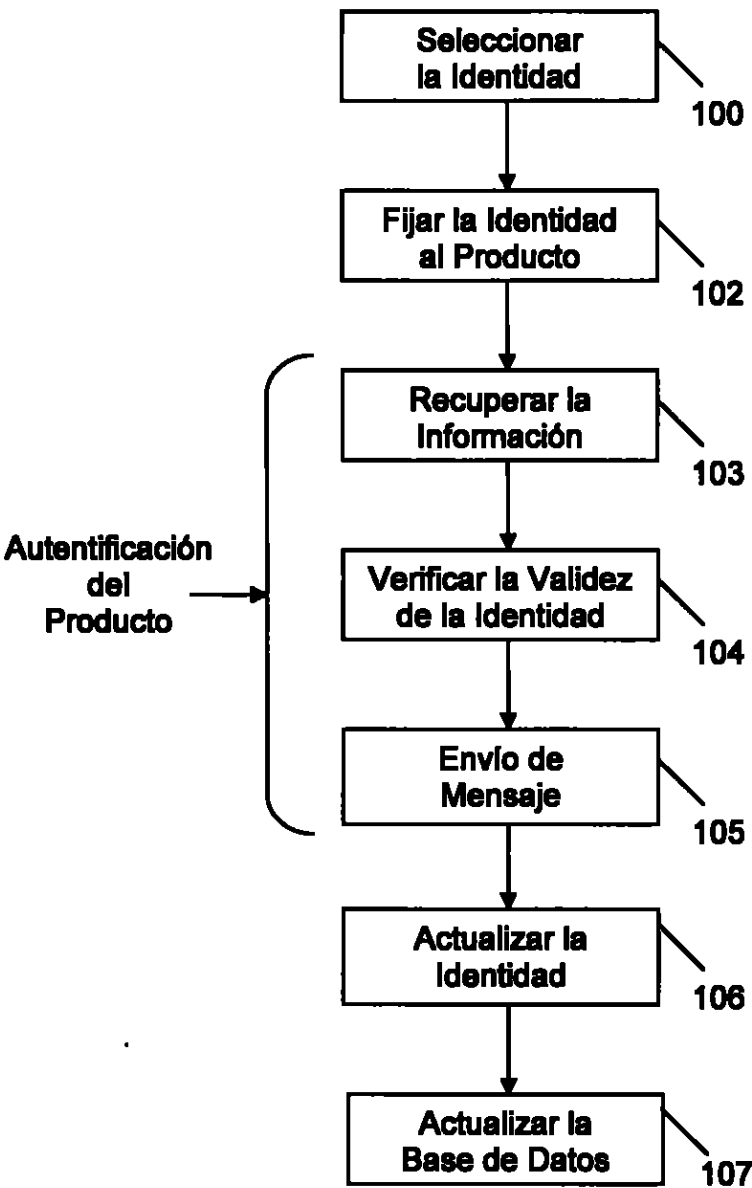


FIG. 1

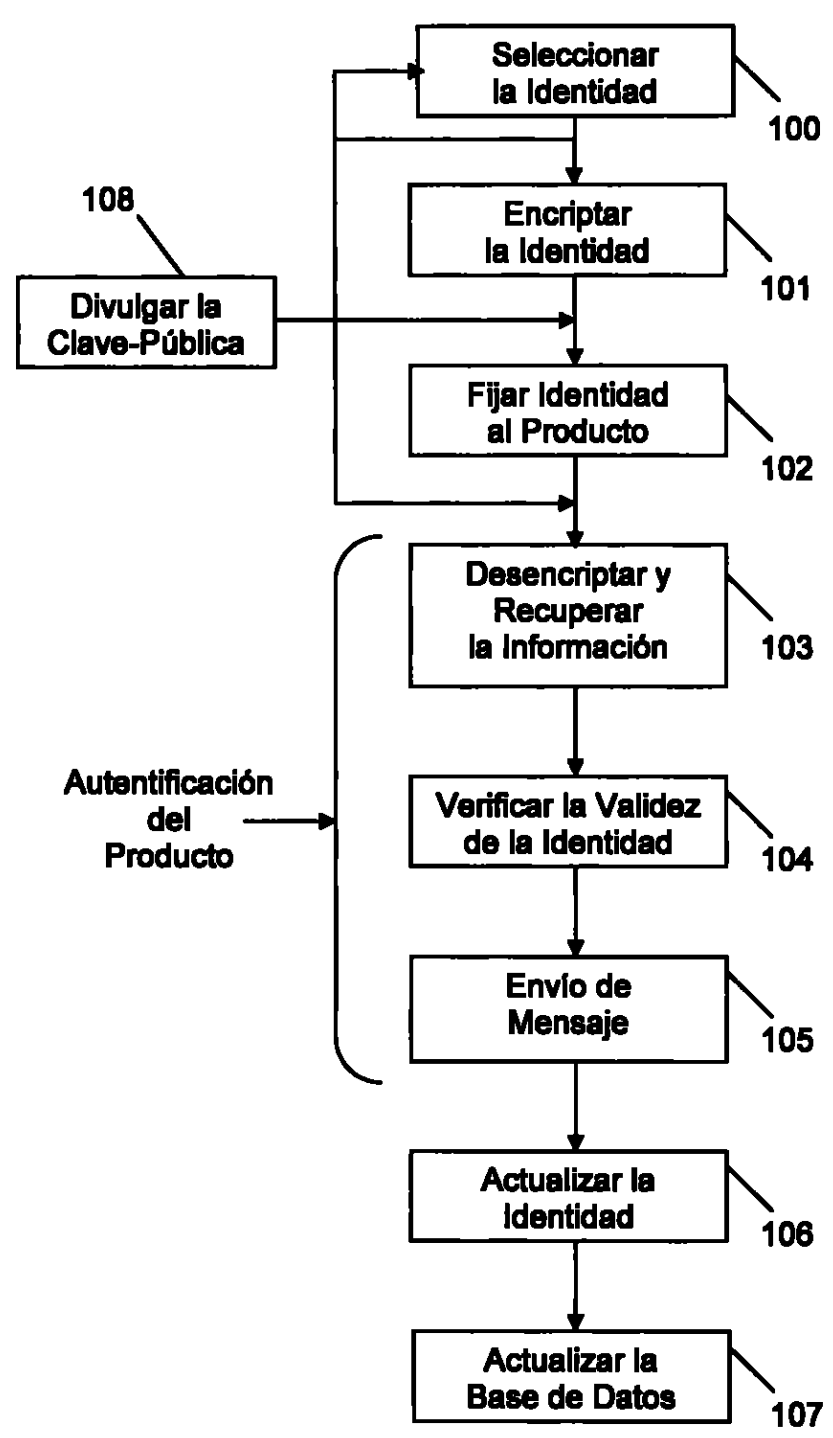


**FIG. 2**

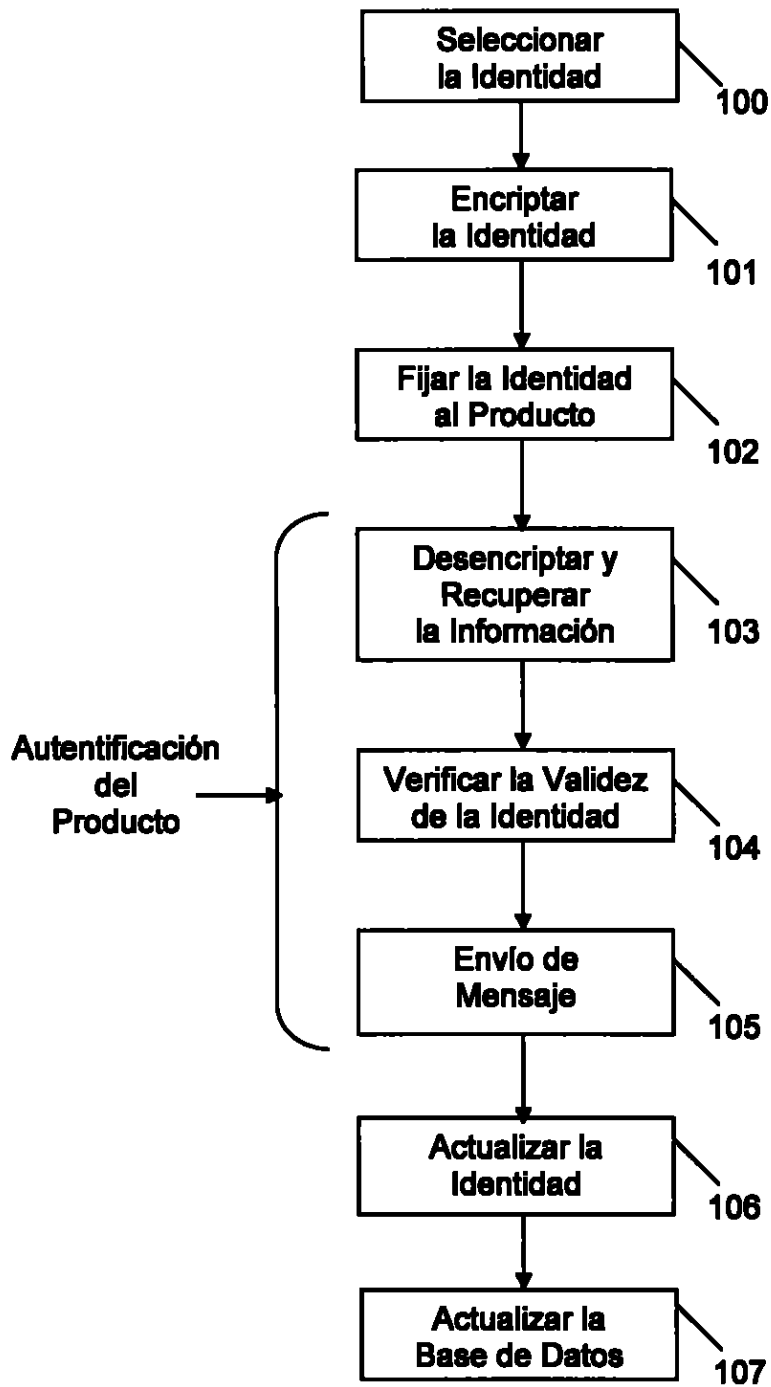


**FIG. 3**

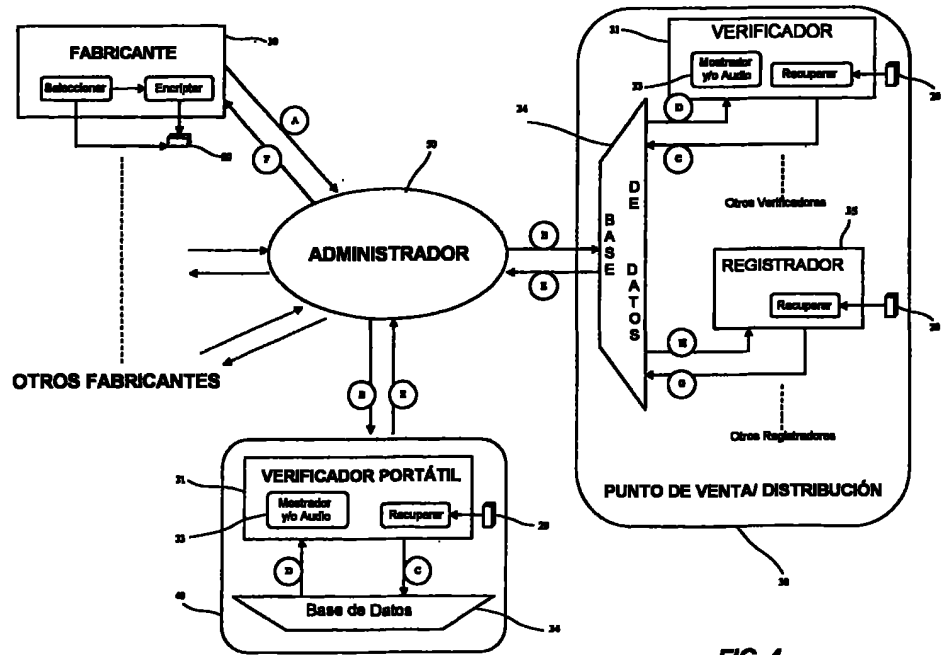
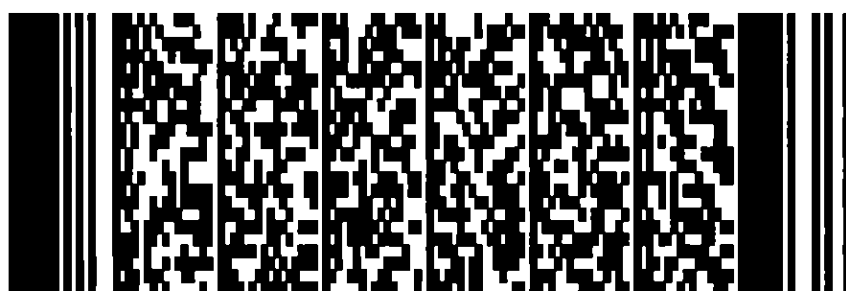


FIG. 4

5/5



Relio folios 82 y 83  
"Tagetur"



Delegatura de Propiedad Industrial  
División de Nuevas Creaciones

## REQUISITOS NECESARIOS PARA PRESENTACION Y AGILIZACION DEL TRÁMITE

|                                                                                     | USUARIO | RADICADOR |
|-------------------------------------------------------------------------------------|---------|-----------|
| <b>PATENTE DE INVENCION ( X ) MODELO DE UTILIDAD ( )</b>                            | ( X )   | ( )       |
| - Indicación de que se solicita la concesión de una patente                         | ( X )   | ( )       |
| - Datos de Identificación del solicitante o de la persona que presenta la solicitud | ( X )   | ( )       |
| - Descripción de la invención                                                       | ( X )   | ( )       |
| - Dibujos de ser estos pertinentes                                                  | ( )     | ( )       |
| - Comprobante de pago de las tasas establecidas                                     | ( X )   | ( )       |

COMPLETA ( ) INCOMPLETA ( X )

### DISEÑO INDUSTRIAL ( )

|                                                                                                             |     |     |
|-------------------------------------------------------------------------------------------------------------|-----|-----|
| - Indicación de que se solicita el registro de Diseño Industrial                                            | ( ) | ( ) |
| - Datos de Identificación del solicitante o de la persona que presenta la solicitud                         | ( ) | ( ) |
| - Representación gráfica y fotográfica del Diseño Industrial o muestra del material que incorpora el diseño | ( ) | ( ) |
| - Comprobante de pago de las tasas establecidas                                                             | ( ) | ( ) |

COMPLETA ( ) INCOMPLETA ( )

### EZQUEMA DE TRAZADO ( )

|                                                                                     |     |     |
|-------------------------------------------------------------------------------------|-----|-----|
| - Indicación de que se solicita el registro de Diseño Industrial                    | ( ) | ( ) |
| - Datos de Identificación del solicitante o de la persona que presenta la solicitud | ( ) | ( ) |
| - Representación gráfica del Esquema de Trazado                                     | ( ) | ( ) |
| - Comprobante de pago de las tasas establecidas                                     | ( ) | ( ) |

COMPLETA ( ) INCOMPLETA ( )

Firma responsable: Fdo B

Fecha: 1-Dic-06

**REPUBLICA DE COLOMBIA**  
**SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

Bogotá,  
2020

Doctor(a)  
CASTELLANOS ABONDANO MARGARITA

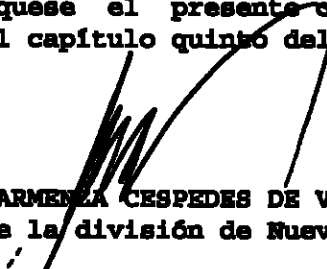
|            |                            |                   |
|------------|----------------------------|-------------------|
| REFERENCIA | Radicación No.             | 6 121494          |
|            | Solicitud internacional    | PCT/BR2005/000025 |
|            | Fecha inicio fase nacional | 04/01/2007        |
|            | Trámite                    | 11                |
|            | Evento                     | 379               |
|            | Actuación                  | 430               |
|            | Oficio No.                 | 825               |

Como resultado del examen de forma, realizado con fundamento en el artículo 38 de la Decisión 486 de la Comisión de la Comunidad Andina, artículo 27 del Tratado de Cooperación en Materia de Patentes (PCT), regla 51 bis del Reglamento y Circular Única de la Superintendencia de Industria y Comercio, se le comunica que:

1. Si fuere el caso, el solicitante debe adjuntar la traducción de los anexos del reporte de examen preliminar internacional (Art. 36.2.b) del tratado PCT.
2. 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.

En cumplimiento de lo dispuesto por el artículo 39 de la Decisión 486, se le requiere para que dentro del término de dos meses siguientes a la fecha de notificación del presente oficio, complete los requisitos anteriormente enunciados. En caso de no dar cumplimiento al presente requerimiento, la solicitud se considerará abandonada y perderá su prelación.

Notifíquese el presente oficio conforme a lo dispuesto en el numeral 5.2, literal e), del capítulo quinto del título primero de la Circular Única No.10 de 2001.

  
ALIX CARMEN CESPEDES DE VERGEL  
Jefe de la división de Nuevas Creaciones

El anterior requerimiento fue notificado por fijación en lista de  
fecha 26 ENE. 2007  
adpall