

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 674 421**

51 Int. Cl.:

G06Q 10/00 (2012.01)

G06K 19/08 (2006.01)

G06Q 30/00 (2012.01)

G06Q 10/08 (2012.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **24.02.2016** **E 16157121 (1)**

97 Fecha y número de publicación de la concesión europea: **25.04.2018** **EP 3065091**

54 Título: **Sistema de autenticación de productos**

30 Prioridad:

05.03.2015 IT UB20150077

45 Fecha de publicación y mención en BOPI de la traducción de la patente:

29.06.2018

73 Titular/es:

**ISTITUTO POLIGRAFICO E ZECCA DELLO
STATO S.P.A. (100.0%)
Via Salaria 691
00138 Roma (RM), IT**

72 Inventor/es:

**GHISA, GIUSEPPE;
LUCIANI, LAURA y
INFORTUNA, FRANCESCO**

74 Agente/Representante:

ISERN JARA, Jorge

ES 2 674 421 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Sistema de autenticación de productos

5 La presente invención se refiere a un sistema para verificar la autenticidad de un producto.

De manera más precisa, la presente invención se refiere a un sistema que está basado en una etiqueta que tiene un PRIMER CÓDIGO DE VERIFICACIÓN, un segundo CÓDIGO DE VALIDACIÓN, posiblemente un tercer CÓDIGO DE ACCESO para acceder a una base de datos y un GRÁFICO que no es legible ópticamente.

10 A través de un procedimiento basado en los elementos anteriores (PRIMER CÓDIGO DE VERIFICACIÓN, CÓDIGO DE VALIDACIÓN, CÓDIGO DE ACCESO, GRÁFICO), el usuario es capaz de determinar si el producto que ha comprado es auténtico.

15 En caso de inconsistencia de los elementos anteriores, el sistema determina un fallo en el proceso de autenticación de los artículos y el comprador tiene la opción de activar una ALERTA a las autoridades pertinentes, conectándose a un lugar de referencia o implementando cualquier otra acción dirigida a aclarar la incongruencia del producto a través del punto de venta.

20 Estado de la técnica

Las soluciones disponibles en el mercado para la protección de artículos contra el fraude son múltiples, algunas son adecuadas para garantizar la autenticidad de unos productos específicos del tipo de los de alto coste, otras son adecuadas para el seguimiento y verificación de productos ampliamente accesibles, otras más se pueden utilizar para una amplia variedad de productos.

25 Las tecnologías más comunes se basan en la verificación por medio de la adquisición automática de la información de una etiqueta (sin codificar y/o en forma de un código de barras mono o bidimensional) y su transmisión a un sistema de procesamiento de datos remoto (una base de datos), capaz de manejar una información incalculable sobre las características del artículo.

30 En los últimos años, también las tecnologías de RFID se han desarrollado considerablemente, lo que permite una rápida verificación de información compleja.

35 Una amplia variedad de soluciones le permite al usuario final verificar directamente la autenticidad del producto por medio de teléfonos inteligentes, tanto en modo de adquisición como de decodificación de un código Q/código de barras o usando NFC o una tecnología similar.

40 Partiendo de una visión general de las soluciones patentadas y de las disponibles, por tipo, encontramos:

- 45 - Etiquetas con códigos de barras realizadas con soportes garantizados por medio de una marca de agua, elementos impresos o aplicaciones especiales (por ejemplo, hologramas, fibrillas de seguridad, etc.). En estas, se usa un elemento con una peculiaridad física para certificar la autenticidad de un producto (documentos US 2006/0244253 A1, US 2009/0080760 A1, US 2010/0012728, US 2013/8533075 B, GB 23.837.768).
- 50 - Etiquetas que están basadas en códigos de barras mono o bidimensionales, chips RFID o similares. Estas, una vez asociadas a un producto, le permiten al comprador verificar que son genuinas leyendo el código, usando para ello dispositivos automáticos comunes en el mercado tales como teléfonos inteligentes, en los que se ha instalado un programa informático dedicado, es decir, una "app" que puede conectarse a una base de datos y efectuar las consultas necesarias para comprobar la autenticidad del producto.

55 A continuación, se citan las patentes que reivindican las soluciones más interesantes: WO 2012/020291, US 2013/0193200 A1, US 2012/0187185 A1, US 2014/0122889, WO 2013/157017 A1, WO 2014/055356, GB 2383776, WO 2010 / 050 928 A1, WO 94/22580, JP 4591216 B2, EP 2736035 A2, EP 2096851 A1, 2012 CN 10047466, CN 2012 10049530, 10029851 CN 2013, CN 2010 10199867 y WO 2014/014401.

Las soluciones basadas en etiquetas que contienen elementos con una peculiaridad (primer punto) tienen la desventaja de tener que usar, para su validación, un instrumento específico, que, en general, tiene una influencia considerable en el coste de la solución o requiere expertos para la verificación de su autenticidad.

60 Las indicadas en el segundo punto a veces no son capaces de interceptar el fraude en caso de que se duplique o reutilice un código válido. Los productos no genuinos pueden estar entonces provistos con códigos aparentemente válidos que podrían autenticar estos primeros como genuinos (falso positivo) y esto pondría en peligro a todo el sistema de validación.

65 En particular, la patente WO 2012/020291 prevé el uso de información impresa en la etiqueta como un código QR o contenida en un microprocesador y de una base de datos específica, de tal manera que el consumidor pueda,

leyendo el código, consultar la base de datos y acceder a información detallada sobre el producto. El punto crítico de la solución propuesta es la imposibilidad de interceptar el fraude que surge del uso de etiquetas reales que se reutilizan aplicándolas sobre productos falsos.

5 En la patente WO 2014/014401, en su lugar, se reivindica un sistema de al menos dos etiquetas, conteniendo, cada una de ellas, una serie de caracteres que se pueden leer alterando de manera irreversible el soporte físico. En este caso, la información contenida se construye de tal manera que se satisfaga un algoritmo predeterminado y se produzca un resultado de validación que garantice la autenticidad del producto. El método propuesto, sin embargo, requiere un proceso complejo de generación y un emparejamiento incorrecto de las etiquetas (desajustadas) 10 invalidaría todo el sistema de verificación. También es difícil, pero no imposible, la duplicación de etiquetas. El documento WO2014/014508 se refiere a un sistema RFID que está protegido por una etiqueta que lo preserva contra lecturas no autorizadas. El documento WO2009/086368 se refiere a un sistema RFID en el que se aplica una etiqueta conductora para protegerlo contra lecturas. El documento US2006/0244253 se refiere a la generación de un gráfico único en una etiqueta de identificación del artículo. Los problemas indicados anteriormente, en particular, en las patentes WO 2012/020291 y WO 2014/014401, se resuelven mediante el nuevo método concebido que combina 15 una simplicidad de producción con una tecnología avanzada y que tiene una aplicación práctica y un uso seguro.

El objetivo de la presente invención consiste en proporcionar un sistema efectivo de autenticación de productos que resuelva los problemas y supere los inconvenientes de la técnica anterior.

20 La materia objeto de la presente invención es un sistema de acuerdo con las reivindicaciones adjuntas. A continuación, la invención se describirá a modo de ejemplo, pero no a modo de limitación, con referencia particular a las figuras de los dibujos adjuntos, en los que:

- 25 - la Figura 1 muestra una realización de la etiqueta de acuerdo con la invención, en sus diversas capas;
- la Figura 2 muestra un diagrama de flujo de la gestión del producto de autenticación de acuerdo con el sistema de la invención;
- la Figura 3 muestra un diagrama de bloques que ilustra el flujo de información entre los diversos dispositivos, que en una realización, forman parte del sistema de acuerdo con la invención;
- 30 - la Figura 4 muestra un diagrama de flujo que ilustra el proceso de verificación de la autenticidad de un producto de acuerdo con una realización de la invención.

Descripción detallada de la invención

35 *Etiqueta y códigos numéricos*

Con referencia a la Figura 1, la etiqueta 100 puede ser de tipo adhesivo u otro tipo dependiendo de su uso final y también puede contener información (impresa) relativa al producto o bien elementos comerciales o de seguridad adicional o de identificación, tales como por ejemplo, tiras holográficas, logotipos, marcas comerciales, etc. Con esta 40 tecnología se pueden realizar etiquetas, que sean capaces de garantizar la autenticidad de vinos, licores, medicamentos, piezas de repuesto de vehículos motorizados, relojes, equipos de alta fidelidad, productos electrónicos o cualquier otro producto. Pueden estar hechos con cualquier material (papel, medios sintéticos, etc.) y debe estar equipado con un microprocesador RFID u otro dispositivo que pueda ser interrogado electrónicamente y que tenga una memoria para almacenar datos, posiblemente provisto con un sistema de seguridad para evitar imitaciones/clonaciones, así como la interceptación fraudulenta de información durante la comunicación.

La etiqueta 100 se compone de dos capas 110 y 120, como se muestra en la Figura 1. En dicha primera capa 110 se fija un microprocesador RFID u otro dispositivo 140, que puede ser interrogado electrónicamente y tiene una memoria para almacenar datos, que se usan para grabar los siguientes códigos:

- 50 - un PRIMER CÓDIGO DE VERIFICACIÓN, adaptado para la evaluación de la primera interrogación de etiqueta;
- un CÓDIGO DE VALIDACIÓN, calculado usando un algoritmo especial; y opcionalmente:
- un CÓDIGO DE ACCESO, que es la clave de acceso para poder consultar una base de datos (opcional).

55 En la misma primera capa 110 también estará presente un GRÁFICO 150 sin codificar (impreso o aplicado de otra manera), que no es legible ópticamente y se predetermina mediante un algoritmo específico. El posicionamiento de tal GRÁFICO 150 en la primera capa 110 y no en la segunda capa 120, permite mejorar la eficiencia de las fases de producción, evitando al mismo tiempo problemas de "desajuste" debido al acoplamiento de las dos capas, dado que toda la información que contribuye a la validación de la etiqueta está contenida en la primera capa 110.

60 Por el término "no legible ópticamente" se debe entender que no puede interpretarse con dispositivos de reconocimiento óptico, como sucede con el código CAPTCHA.

El GRÁFICO 150 deberá estar cubierto con la parte removible 160 de la segunda capa.

65

En la segunda capa 120 se deposita lo siguiente: una tinta conductora, una película metálica u otros medios, al menos sobre la parte removible 160, con la función de evitar el funcionamiento de la antena del microprocesador (RFID), presente en la primera capa 110, siempre que esta última no se retire (la función de antena se puede interrumpir con un cortocircuito, un blindaje electromagnético u otro). Para facilitar la retirada de la parte 160, está equipada con microcortes o troquelados 165 ("cortes superficiales" a saber, que cortan solo la capa 120). De esta manera, solo retirando la parte 160 de la antena RFID se puede recibir señales del dispositivo de interrogación (un teléfono inteligente u otro). El uso de microcortes hace que la retirada de la capa de protección 160 altere, de forma irreversible, la etiqueta 100, mostrando a cualquier usuario que es una etiqueta ya usada y obstaculice su reutilización como etiqueta virgen. La realización particular del troquelado para estos efectos es posible de muchas formas conocidas. En general, por lo tanto, cualquier medio que permita mostrar la retirada irreversible será adecuado para este propósito. En otras palabras, la parte removible estará configurada de manera que muestre, cuando está en uso, que se ha producido la retirada de forma irreversible.

La cubierta 160 del microprocesador u otros medios de almacenamiento de datos con un elemento de cribado o de cortocircuitado evita tanto lecturas súbitas como inadecuadas, haciendo que sea imposible intentar cambiar la información contenida en el microprocesador, que pondría en peligro al sistema de validación de productos.

En la segunda capa 120, también se pueden imprimir elementos gráficos o se pueden aplicar elementos de seguridad, que distingan al producto o se puede imprimir un "código QR" 130, que se vaya a usar para acceder a un sitio de referencia que contenga información sobre el producto.

Las dos capas 110 y 120 están acopladas permanentemente entre sí para obtener una etiqueta 100 como un único elemento, que incorpora en su interior el microprocesador RFID u otros medios de almacenamiento de datos 140 y el elemento gráfico 150. La parte inferior de la etiqueta así formada puede ser adhesiva o libre, dependiendo de la especificación específica a la que esté dedicada.

Sistema de verificación

Con referencia a la Figura 3, el sistema de verificación 300 se compone de una etiqueta 100, un programa informático dedicado (no mostrado), una posible interfaz de red 380, unos lectores inteligentes 320 que tengan una gran difusión en el mercado (por ejemplo, un teléfono inteligente) y una "app" 350, que sea adecuada para verificar los códigos mencionados.

El teléfono inteligente 320 lee por interacción (protocolo NFC) 330 con un RFID, incluido en una etiqueta 100, los códigos anteriores. El sistema 300 (concretamente el teléfono inteligente 320) verifica la exactitud del PRIMER CÓDIGO DE VERIFICACIÓN para garantizar que es una primera lectura.

Si el PRIMER CÓDIGO DE VERIFICACIÓN es correcto, la "app" cambia en la memoria RFID el estado de tal código de "primera lectura" a "lectura" y bloquea la capacidad de escribir adicionalmente en el RFID (u otros medios de almacenamiento de datos). Posteriormente, la "app" también verifica que el CÓDIGO DE VALIDACIÓN sea correcto y posiblemente usa el ACCESO uno para acceder a una base de datos remota (y/o autenticación en el servidor remoto).

Si la verificación de cumplimiento del CÓDIGO DE VALIDACIÓN en la etapa 370 es positiva, se produce un mensaje de RESULTADO 322 en la etapa 375 en la pantalla 321 del lector inteligente 320 (teléfono inteligente), cuyo contenido gráfico debe corresponderse al menos parcialmente con el GRÁFICO 150 declarado sin codificar en la etiqueta 100 (por ejemplo, comparación visual por parte del usuario).

A modo de ejemplo, la correspondencia se puede realizar de las siguientes maneras:

- el GRÁFICO es un dibujo con la forma de un objeto y el resultado es al menos el nombre del objeto;
- el GRÁFICO es un nombre escrito con elementos gráficos accesorios y el resultado es al menos una cadena de texto correspondiente al nombre;
- el GRÁFICO es un dibujo y el resultado es al menos el mismo o un dibujo muy similar.

Este último, no reconocible mediante una lectura automática, evita imitaciones del sistema a través de una "app" desarrollada a efectos de prevenir usos fraudulentos.

Si la verificación de cumplimiento del CÓDIGO DE VALIDACIÓN 370 es negativa, el proceso de verificar fallará y el comprador será capaz de conectar con el sitio de referencia 380 y activar en la etapa 376 una ALERTA a las autoridades pertinentes o implementar cualquier otra acción para aclarar la incongruencia del producto a través de la tienda.

La información resultante de la verificación, junto con cualquier dato adicional, se puede grabar, como funciones opcionales, en una base de datos para la estructuración de información útil tanto para el operador del sistema como para el usuario (identificación, seguimiento, etc.).

Programas informáticos

Con referencia a la Figura 3, el sistema 300, de acuerdo con la invención, en una realización, implica el uso de los siguientes tres módulos de programas informáticos:

- SW1 - Programa informático para la generación de los códigos contenidos en las etiquetas. Hace uso de un algoritmo de encriptación específico;
- SW2 - Programa informático para la generación de ficheros gráficos de impresión y programación de los medios de almacenamiento electrónicos (RFID). También puede tener una función para intercomunicarse/poblar una base de datos;
- SW3 - Programa informático para la validación y autenticación automáticas del producto ("app" de verificación de códigos).

Lectores inteligentes

Para la lectura de los datos indicados en la etiqueta 100 y para la ejecución del proceso de validación, se necesita el uso de un lector "inteligente" (teléfono inteligente), que, a través de una "app" dedicada de verificación de códigos, sea capaz de realizar el proceso de verificación de la autenticidad del producto.

Tal dispositivo podría ser, por ejemplo, un teléfono inteligente 320 equipado con un lector NFC (no mostrado), un posible dispositivo de georreferenciación (no mostrado) u otro (por ejemplo, una cámara, no mostrada).

Funcionamiento del sistema de autenticación de productos

En la Fig. 2 se muestra un diagrama de flujo 200 con las diversas partes implicadas en la autenticación en una configuración preferente de la invención.

Una autoridad designada 201 genera en la etapa 210 los códigos anteriores, un número de veces en función del tamaño del lote de producto que uno quiera proteger y produce una reserva de etiquetas.

Estos códigos, como función accesoria 204, se envían en la etapa 216 a una base de datos 230 para la grabación de los códigos.

La reserva de etiquetas 210 fabricadas se envía en la etapa 215 al fabricante/distribuidor 202 para su aplicación, en la etapa 220, sobre el envase/partida/palé individual y, como función complementaria 204, toda la información relacionada con el producto y la lista de etiquetas canceladas se envían, en la etapa 225, a una base de datos para la grabación, en la etapa 240, de la información de producto y de la lista negra de las etiquetas canceladas.

Posteriormente, el fabricante/distribuidor 202 realiza la distribución de los productos en la etapa 250, sobre los que se han aplicado previamente las etiquetas 220 y, como función accesoria 204, los datos de distribución del producto en los comercios se envían en la etapa 255 y se graban en la etapa 260.

El consumidor 203 compra el producto distribuido en la etapa 270 y, a través de la etiqueta, verifica la autenticidad con un teléfono inteligente y puede, como prestación opcional 204, preguntar, en la etapa 275, en el sitio web 280 información adicional sobre el producto y en la etapa 275 puede proporcionar información relevante para la autenticación del producto (tal como información de georreferenciación). El sitio web 280 proporciona la información adicional solicitada sobre el producto por el consumidor 203 a través de la interacción 276.

Como funciones adicionales 204, los códigos grabados en la base de datos 230, la información del producto, la "lista negra" de las etiquetas anuladas en la etapa 240 y los datos sobre la distribución del producto en los comercios de la etapa 260, se envían, respectivamente, a través de las interacciones 235, 245 y 265, al sitio web 280, para una actualización de datos.

El diagrama de flujo 400 ilustrado en la Figura 4 muestra el funcionamiento del sistema en una configuración preferente, a través de las siguientes etapas:

- efectuar en la etapa 410 la activación del sistema de validación al retirar la protección del microprocesador;
- efectuar en la etapa 420 la adquisición de los códigos;
- ejecutar en la etapa 430 la lectura del PRIMER CÓDIGO DE VERIFICACIÓN (verificar su consistencia con respecto a las especificaciones de generación de códigos o de cualquier otra forma conocida o futura);
- si en la etapa 440 la verificación descubre que el PRIMER CÓDIGO DE VERIFICACIÓN es correcto, el flujo emite la orden 446 de ejecutar en la etapa 450 el cambio de estado de "Primera lectura" a "Leído" y procede a bloquear la escritura en la memoria del microprocesador;
- si en la etapa 440 la verificación no es satisfactoria (se trata de una etiqueta que ya se ha leído o el PRIMER CÓDIGO DE VERIFICACIÓN es incorrecto), la "app" puede enviar en la etapa 445 una ALERTA;
- efectuando una prueba 460, que consiste en verificar al menos el CÓDIGO DE VALIDACIÓN;

- en respuesta a la prueba de la etapa 460, se obtiene la generación de un resultado (conjunto de símbolos en pantalla) en la etapa 470;
- ejecutar en la etapa 480 la comparación entre el resultado generado en la etapa 470 y el GRÁFICO presente en la etiqueta;
- 5 - si en la etapa 490 la comparación arroja un resultado positivo en la etapa 496, el usuario obtiene la información de que el producto que ha comprado es auténtico;
- si en la etapa 490 la comparación (por ejemplo, visual) del usuario arroja un resultado negativo (etiqueta alterada, etiqueta falsa, etc.) el usuario puede activar un procedimiento de reclamación o una ALERTA en el sistema remoto de la etapa 495.

10 Después de la verificación del CÓDIGO DE VALIDACIÓN, se pueden grabar las coordenadas geo-temporales del evento (el lugar y la fecha de la inspección) y esto puede suponer, en un servidor remoto, la activación del certificado de garantía del producto asociado con la etiqueta o, directamente, puede aportar una prueba documental de la fecha de inicio del periodo de garantía. Esta última fase se puede iniciar con la orden del usuario o automáticamente,

15 inmediatamente después de la lectura del PRIMER CÓDIGO DE VERIFICACIÓN (sujeto a la conclusión satisfactoria del proceso) y también puede basarse en otra información de identificación del producto (por ejemplo, una indicación del número de serie del producto).

20 *Ventajas de la invención*

El sistema de acuerdo con la invención, es una herramienta simple y efectiva para verificar la autenticidad de un producto y contrarrestar la introducción de productos falsificados en el mercado, que, si están bien fabricados, los consumidores comprarían pensando que son auténticos.

25 La construcción de la etiqueta resulta particularmente innovadora y ventajosa con todos los elementos fundamentales (códigos, elementos gráficos, microprocesador) en la primera capa, no visible, lo que facilita la producción de la misma a un bajo coste y al mismo tiempo la inhibición del funcionamiento de la antena del microprocesador por una segunda capa de material (configurada para producir un cortocircuito en la antena o su blindaje electromagnético), y que una vez retirada ya no puede volver a restaurarse a su estado original.

30 Este mecanismo de inhibición también protege al microprocesador frente a cualquier lectura/escritura inadecuada.

Además, la innovación aparece en el uso de un PRIMER CÓDIGO DE VERIFICACIÓN que se altera de manera permanente tras la primera lectura de la etiqueta, haciendo que sea imposible volver a utilizar la misma etiqueta. Por

35 último, dado que el momento de la modificación se pueden grabar las coordenadas geo-temporales del evento (el lugar y la fecha de compra/validación y otra información complementaria tal como el número de serie del producto), esto puede constituir la activación del certificado de garantía del producto.

40 En lo que precede, se han descrito realizaciones preferentes y se han sugerido variantes de la presente invención, pero se debe entender que los expertos en la materia podrán efectuar modificaciones y cambios, sin desviarse por ello del correspondiente ámbito de protección, como se ha definido en las reivindicaciones adjuntas.

REIVINDICACIONES

1. Etiqueta (100) de verificación de la autenticidad de un producto, que comprende al menos una primera capa (110) y una segunda capa (120) anclada a dicha primera capa, estando fijados sobre dicha primera capa (110) unos medios electrónicos interrogables inalámbricamente (140), que están equipados con una memoria, incluyendo dicha segunda capa (120) una parte removible (160), estando provistos, al menos en dicha parte removible (160), unos medios de interrupción de interrogación, que están adaptados para interrumpir la interrogación de dichos medios electrónicos interrogables inalámbricamente (140); estando la etiqueta caracterizada por que:
- dicha parte removible (160) está configurada para mostrar de manera irreversible, cuando está en uso, que se ha retirado;
 - en dichos medios electrónicos interrogables inalámbricamente (140), se almacena al menos un PRIMER CÓDIGO DE VERIFICACIÓN, para la verificación de la primera lectura de la etiqueta y al menos un CÓDIGO DE VALIDACIÓN, para la verificación de la autenticidad de la etiqueta;
 - en dicha primera capa está presente un GRÁFICO (150), que está cubierto por la parte removible (160), no legible por ningún dispositivo de reconocimiento óptico y que está generado por un algoritmo basado en dicho al menos un CÓDIGO DE VALIDACIÓN.
2. Etiqueta de acuerdo con la reivindicación 1, caracterizada por que dichos medios de interrupción de interrogación están constituidos por unos medios de blindaje electromagnético o unos medios de cortocircuitado.
3. Etiqueta de acuerdo con la reivindicación 1 o 2, caracterizada por que en dichos medios electrónicos interrogables inalámbricamente (140) además se almacena un CÓDIGO DE ACCESO, que está adaptado para acceder a una base de datos remota.
4. Etiqueta de acuerdo con cualquiera de las reivindicaciones 1 a 3, caracterizada por que dichos medios electrónicos interrogables inalámbricamente (140) están constituidos por o incluyen una RFID.
5. Etiqueta de acuerdo con cualquiera de las reivindicaciones 1 a 4, caracterizada por que en dicha segunda capa (120) está provisto un código QR (130).
6. Etiqueta de acuerdo con la reivindicación 5, caracterizada por que el código QR (130) está provisto fuera de dicha parte (160).
7. Etiqueta de acuerdo con cualquiera de las reivindicaciones 1 a 6, caracterizada por que comprende un troquelado (165) para permitir la retirada de dicha parte removible (160), estando dicho troquelado adaptado para mostrar de manera irreversible, cuando está en uso, que se ha producido la retirada.
8. Etiqueta de acuerdo con cualquiera de las reivindicaciones 1 a 7, caracterizada por que dicho al menos un CÓDIGO DE VALIDACIÓN incluye un número de serie de dichos medios electrónicos interrogables inalámbricamente (140).
9. Un método (300) de autenticación de etiquetas, caracterizado por el hecho de usar una etiqueta (100) para la autenticación de un producto como la que se define en una cualquiera de las reivindicaciones 1 a 8 y por el hecho de efectuar las siguientes etapas:
- A. retirar la parte removible (160) de dicha etiqueta (100);
 - B. interrogar, mediante un dispositivo de lectura (320), dichos medios electrónicos interrogables inalámbricamente (140), para obtener dicho al menos un PRIMER CÓDIGO DE VERIFICACIÓN y dicho al menos un CÓDIGO DE VALIDACIÓN;
 - C. verificar, mediante un procesador, que dicho al menos un PRIMER CÓDIGO DE VERIFICACIÓN es válido;
 - D. en caso de un resultado positivo en la etapa C, almacenar, en la memoria de dichos medios electrónicos interrogables inalámbricamente (140), la información sobre la lectura satisfactoria de dicho al menos un PRIMER CÓDIGO DE VERIFICACIÓN;
 - E. generar, mediante dicho procesador, basándose al menos en dicho al menos un CÓDIGO DE VALIDACIÓN, un conjunto de símbolos;
 - F. mostrar, en una pantalla de visualización, dicho conjunto de símbolos de la etapa E;
 - G. verificar, por parte de un usuario, que dicho conjunto de símbolos mostrados en dicha pantalla de visualización se corresponde al menos parcialmente con el contenido gráfico de dicho GRÁFICO (150).
10. Método de acuerdo con la reivindicación 9, caracterizado por que se activa una alarma o indicación de imposibilidad de proceder dado que la etiqueta ya ha sido usada en caso de que el resultado de la etapa G sea negativo.

11. Método de acuerdo con la reivindicación 10, caracterizado por que la alarma o indicación de imposibilidad de proceder se activa a través de una interfaz WEB (380).

5 12. Método de acuerdo con cualquiera de las reivindicaciones 9 a 11, caracterizado por realizar la siguiente etapa adicional:

H. comunicar, mediante dicho procesador, dicho al menos un PRIMER CÓDIGO DE VERIFICACIÓN, y opcionalmente otra información asociada con el producto, a un servidor remoto, que en consecuencia activa una garantía de un producto asociada con dicha etiqueta.

10 13. Método de acuerdo con cualquiera de las reivindicaciones 9 a 12, caracterizado por que en la etapa B también se lee dicho CÓDIGO DE ACCESO y se efectúa una etapa adicional para conectarse a un servidor remoto y acceder a una base de datos basándose en dicho CÓDIGO DE ACCESO.

15 14. Método de acuerdo con cualquiera de las reivindicaciones 9 a 13, caracterizado por que, si el resultado de la etapa C es negativo, una alarma o indicación de etiqueta ya usada o no utilizable se envía a dicha pantalla de visualización.

20 15. Un sistema (300) de autenticación de productos, que comprende:

- al menos una etiqueta (100) de autenticación de un producto, que comprende unos medios electrónicos interrogables inalámbricamente que están equipados con una memoria (140);
- al menos un dispositivo de lectura (320), en particular, un teléfono inteligente, para leer dichos medios electrónicos interrogables inalámbricamente (140) para obtener uno o más códigos, estando el dispositivo de
- 25 lectura provisto de una pantalla de visualización;
- un procesador que ejecuta un programa de verificación de la autenticidad de la etiqueta (100) basándose en dicho uno o más códigos,

estando el sistema caracterizado por que:

- 30 - dicha etiqueta es la etiqueta de acuerdo con una cualquiera de las reivindicaciones 1 a 8;
- dicho programa está configurado para realizar las etapas B, C, E, F del método de acuerdo con una cualquiera de las reivindicaciones 9 a 14.

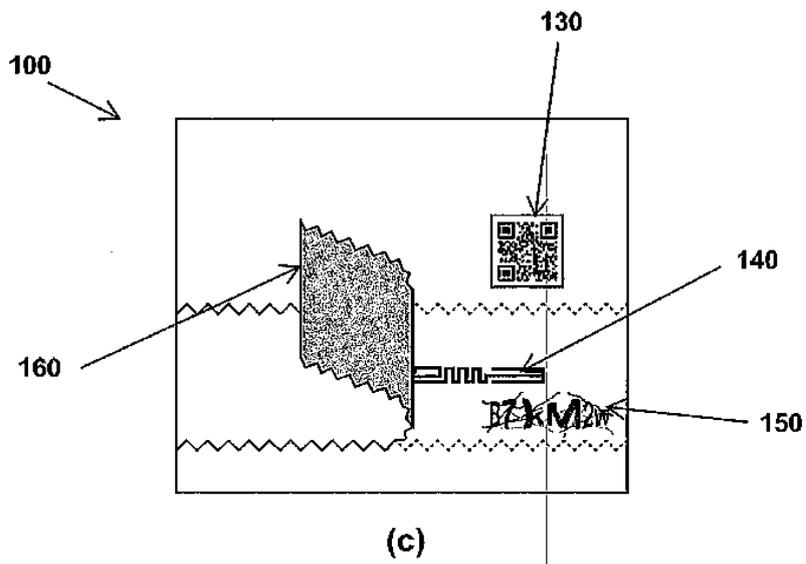
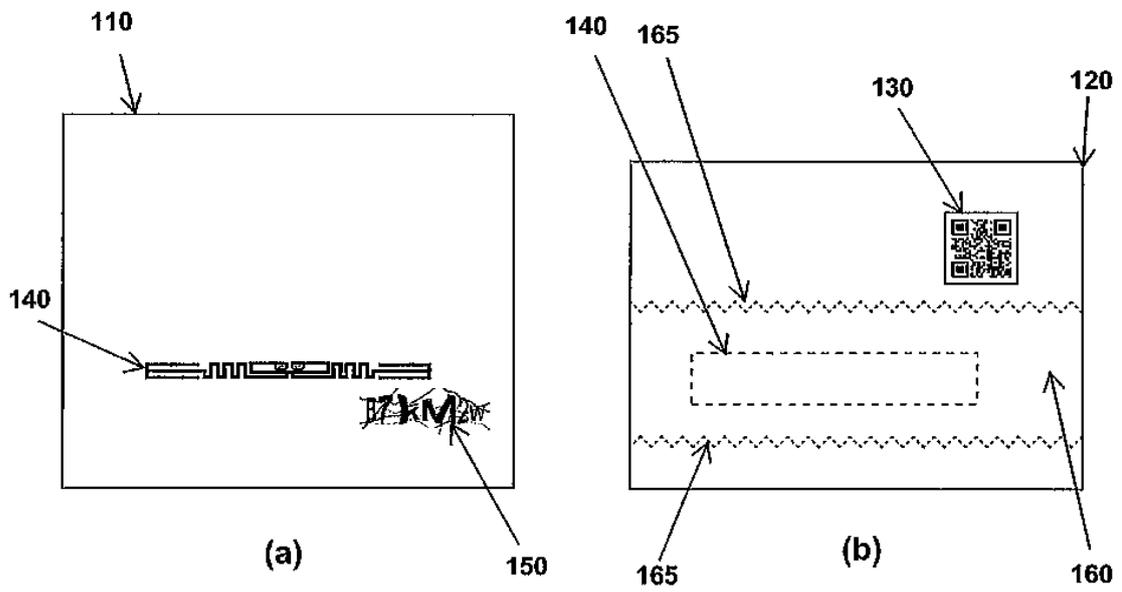


Fig. 1

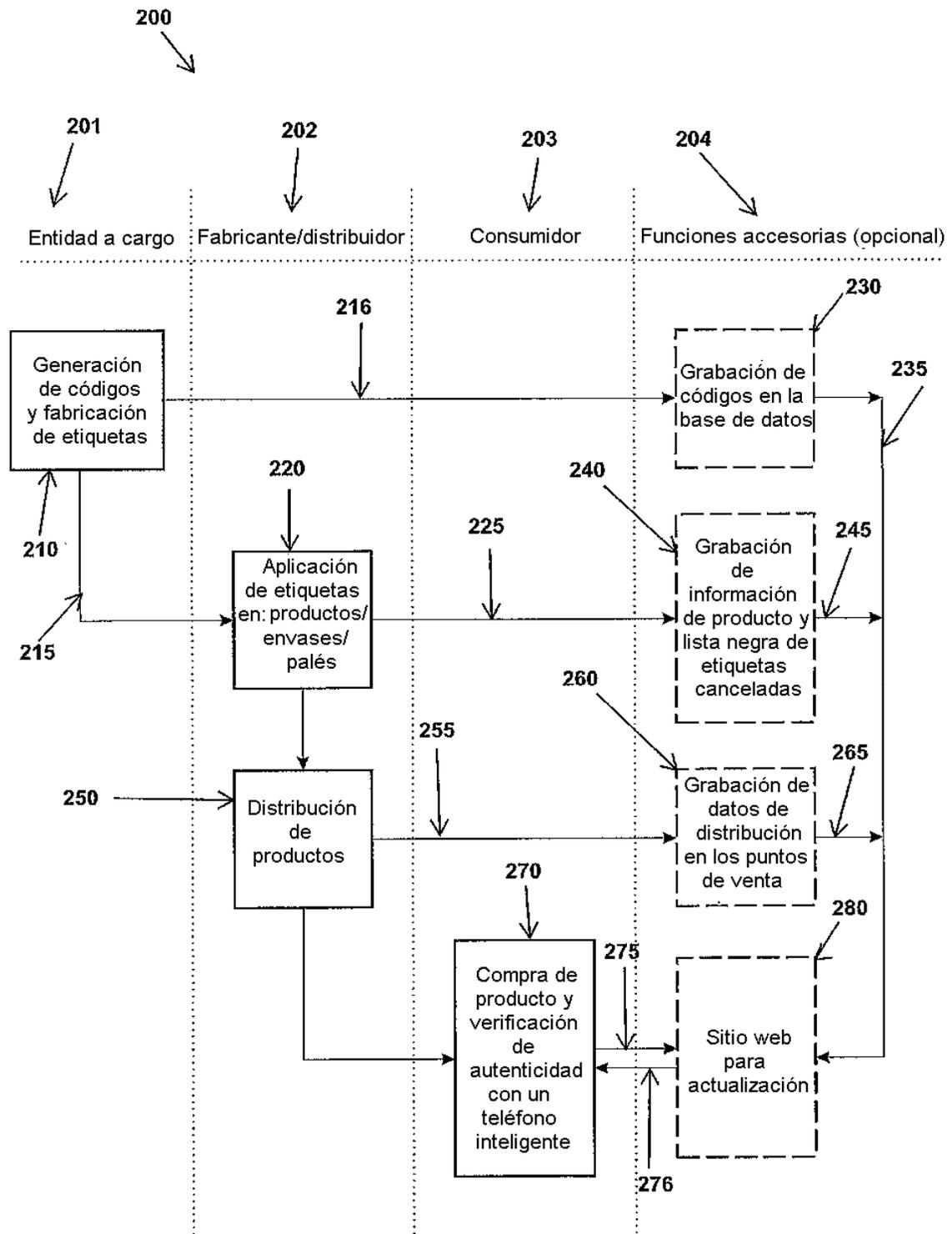


Fig. 2

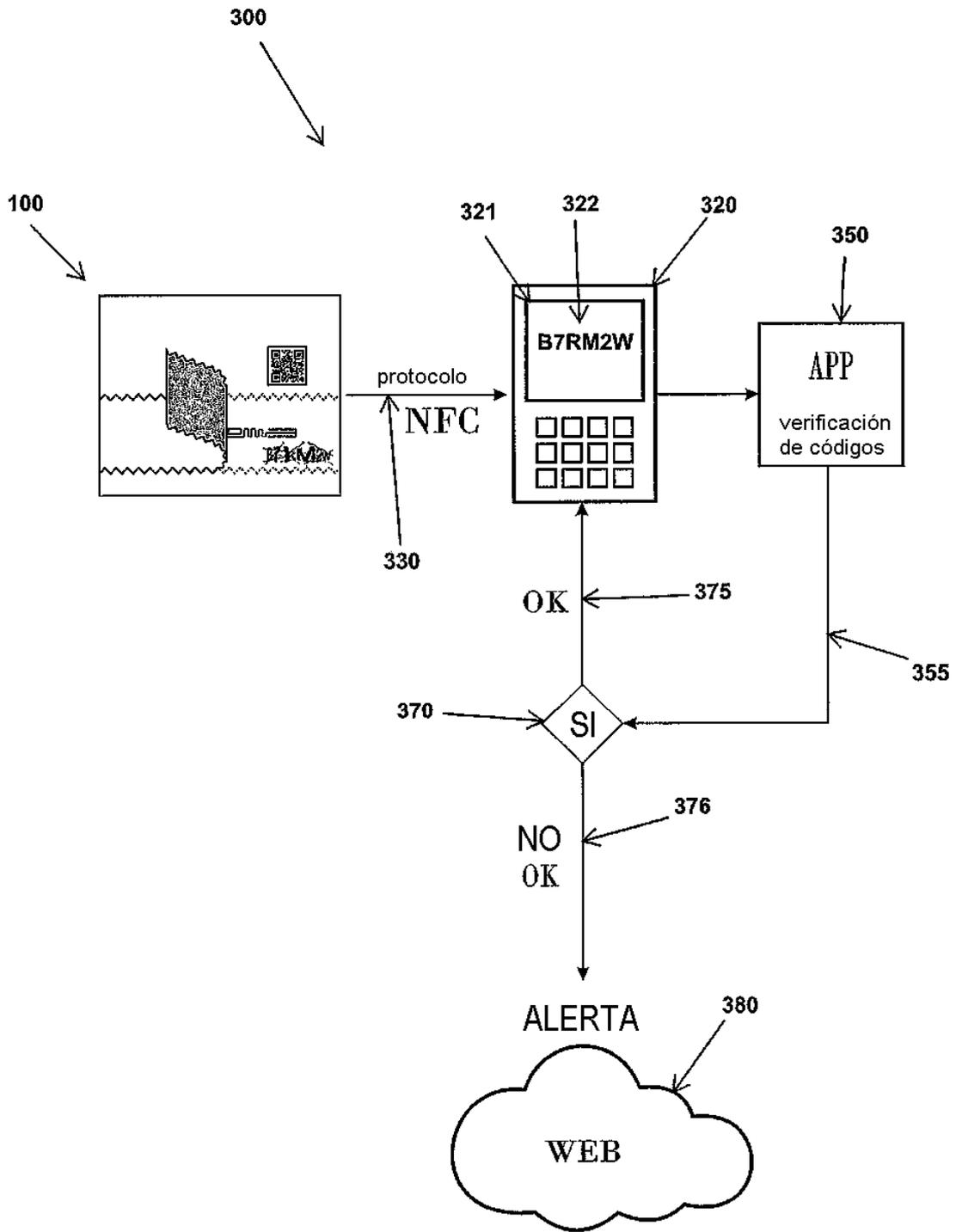


Fig. 3

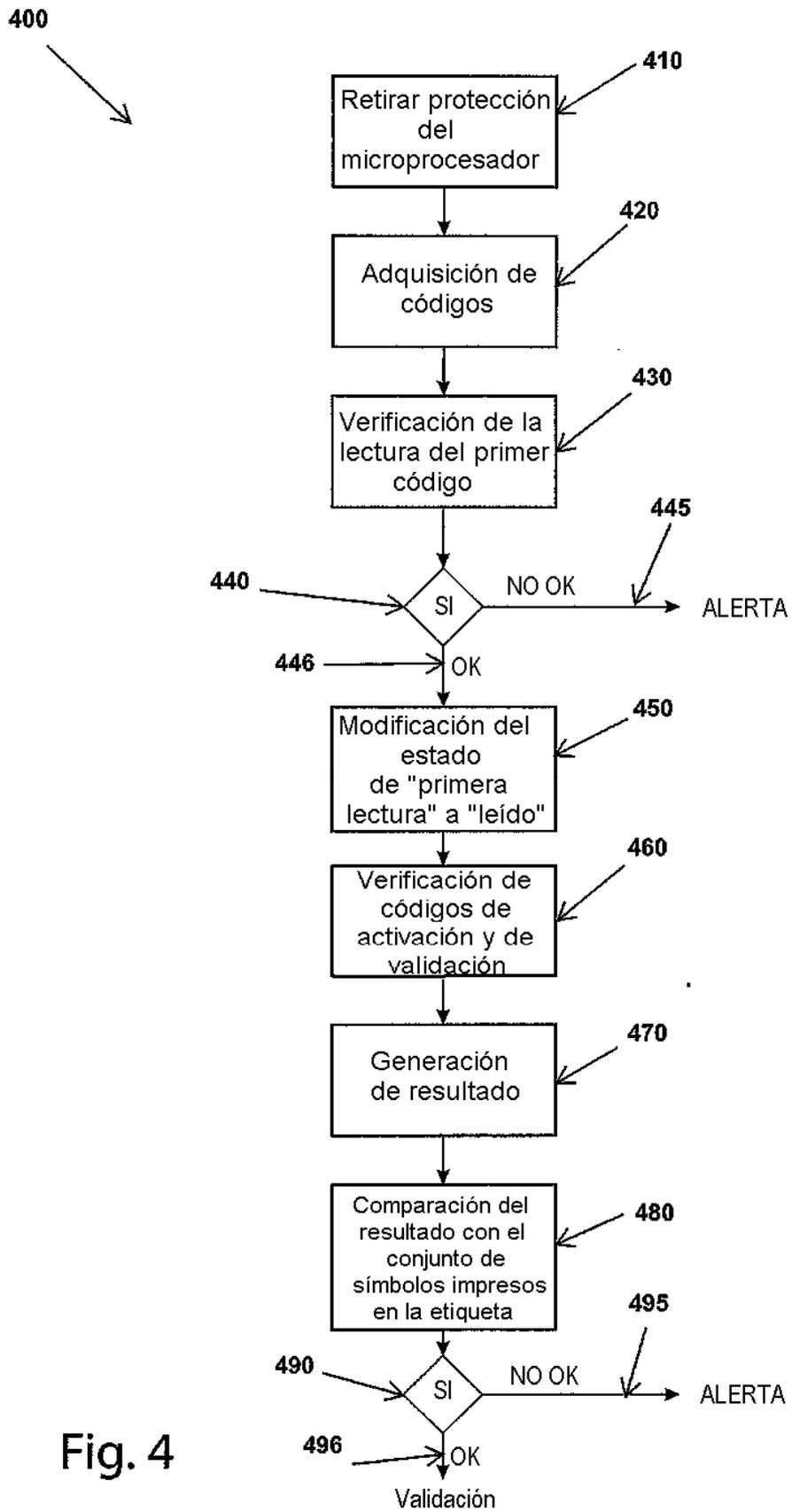


Fig. 4