(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 774 708**

(51) Int. CI.:

G06F 21/30 (2013.01)
G06Q 10/08 (2012.01)
G06F 16/955 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **10.10.2008 PCT/EP2008/063634**

(87) Fecha y número de publicación internacional: **15.04.2010 WO10040415**

(96) Fecha de presentación y número de la solicitud europea: **10.10.2008 E 08805227 (9)**

(97) Fecha y número de publicación de la concesión europea: **08.01.2020 EP 2350912**

(54) Título: **Método para autenticar un producto en un contenedor, y método asociado para verificar la autenticidad de producto y su contenedor**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.07.2020

(73) Titular/es:

OI EUROPE SÀRL (100.0%)
Route de Buyère 2
1030 Bussigny-près-Lausanne, CH

(72) Inventor/es:

DANGMANN, OLIVIER y
DESHERAUD, GILLES

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Método para autenticar un producto en un contenedor, y método asociado para verificar la autenticidad de producto y su contenedor

La presente invención se refiere al campo técnico general de autenticación y trazabilidad de producto.

La invención encuentra una aplicación especializada en el envasado de productos líquidos de alto valor, particularmente vinos, bebidas espirituosas y fragancias, que se someten cada vez más a falsificación, o bien mediante reenvasado (o llenado) desde contenedores originales a unos falsos o mediante la sustitución de productos genuinos por productos falsos en contenedores originales o falsos.

Diversos métodos y tecnologías ya se han propuesto e implementando para mejorar la trazabilidad y/o autenticidad de productos líquidos envasados (o llenados) en botellas. Estos métodos generalmente implican fijar una etiqueta al cuello, corcho o cápsula de una botella que contiene un producto, llevando la etiqueta un código de trazabilidad o autenticidad, o un dispositivo (chip electrónico) que habilita la autenticación del producto envasado desde el productor hasta el consumidor final. La etiqueta se diseña y coloca en la botella de tal forma que debe romperse, o al menos alterarse, para abrir la botella y poder usar el producto.

Otros métodos implican imprimir o grabar un código de autenticación o trazabilidad directamente en el material de botella para autenticar al menos el propio contenedor.

Tales métodos permiten la autenticación de un producto y/o su contenedor siempre que ambos sean originales desde su producción hasta su venta al usuario final sin reenvasado. Sin embargo, puede surgir una situación en la que el producto envasado originalmente ya es un producto falso. O un producto genuino puede haberse reenvasado entre la producción y venta. En tal caso, el producto se volverá completamente imposible de rastrear para el consumidor final, cuya seguridad puede estar, por lo tanto, en riesgo si el producto y/o su contenedor son falsificaciones.

El documento US 2003/0070394 A1 describe un sistema para imprimir etiquetas de envasado de producto farmacéutico que evita etiquetado impreciso en un sistema de envasado de producto farmacéutico automatizado. Sin embargo, este sistema evita errores en el etiquetado de productos farmacéuticos y no soluciona los problemas asociados con falsificación y de productos/contenedores falsos.

La publicación de Solicitud de Patente de Estados Unidos US 2003/0116629 A1 describe una disposición de código de barras que permite determinar posiciones a lo largo de un eje. Incluye una pluralidad de símbolos de código de barras, teniendo cada uno caracteres iniciales y finales y datos codificados entre los mismos. Escanear el símbolo de código de barras que corresponde a una posición particular entre la pluralidad de símbolos de código de barras en la columna puede permitir la identificación de la posición particular a lo largo del eje. En otra realización en forma de una cinta, esta disposición de código de barras puede detectar un nivel de líquido en una botella de líquido.

Existe, en consecuencia, una necesidad de un nuevo método de autenticación, por el cual puede asegurarse tanto la autenticidad como la trazabilidad de un producto y su contenedor por productores a los consumidores.

Existe también una necesidad de un método de autenticación que mejore la prevención de falsificación del producto envasado mediante reenvasado o sustitución del producto genuino.

Estos objetivos se satisfacen, de acuerdo con un primer aspecto de la presente invención, mediante un método para habilitar la autenticación de un producto acondicionado en un contenedor, y de dicho contenedor, de acuerdo con la reivindicación 1.

El método de la invención proporciona una solución completa y totalmente segura para autenticar y rastrear un producto desde la producción hasta el consumidor final. Habilita una autenticación de producto y su contenedor separada por medio de primer y segundo medios de autenticación de los que se extraen primera y segunda claves de autenticación respectivamente y registran en dos bases de datos separadas. Cada par asociado de primera y segunda claves de autenticación se asegura a continuación mediante una tercera clave de autenticación derivada mediante un programa informático a partir de dicha primera y segunda claves de autenticación.

A través del método de la invención ahora es posible garantizar que el par asociado formado por un producto y su contenedor es genuino, y que ni el producto ni el contenedor se ha falsificado. De hecho, las tres claves de autenticación separadas proporcionan tres diferentes niveles de seguridad que deben satisfacerse para garantizar la autenticidad de producto y su contenedor.

Adicionalmente, el contenedor para el producto envasado es un contenedor de vidrio o cristal, y el primer medio de autenticación se graba con láser en el contenedor en el "extremo caliente" del proceso de fabricación. Por lo tanto, el

primer medio de autenticación es prácticamente imposible de copiar o falsificar.

De acuerdo con otra realización preferida del método de la invención, el primer y segundo medios de autenticación son ópticamente legibles. Esto facilita la comprobación y lectura de los medios de autenticación a lo largo de la producción y comercialización del producto envasado.

Para mejorar adicionalmente el nivel de seguridad del método de la invención contra falsificación, es particularmente ventajoso que el segundo medio de autenticación comprenda al menos un código aleatorio bidimensional del que se extrae ópticamente dicha segunda clave de autenticación.

Adicionalmente, el segundo medio de autenticación puede comprender ventajosamente al menos una firma física aleatoria tridimensional del que se extrae ópticamente dicha segunda clave de autenticación. En este caso, la firma física aleatoria tridimensional se implementa preferentemente de tal forma que es visible en una etiqueta aplicada al contenedor.

Adicionalmente, la firma física aleatoria tridimensional se genera, de acuerdo con la invención, aleatoriamente en un material transparente, que puede ser, por ejemplo, un polímero termoestable.

En otra realización preferida de la invención, la etiqueta de contenedor comprende una película a prueba de manipulación y se aplica en dicho contenedor como un sello de apertura.

De acuerdo con la invención, el segundo medio de autenticación ventajosamente también comprende un código de trazabilidad.

En una realización preferida de la invención, el primer medio de autenticación comprende un código de matriz de datos, y el segundo medio de autenticación comprende una etiqueta de burbujas.

En una realización preferida adicional de la invención, la primera, segunda y tercera claves de autenticación comprenden cada una un código numérico o alfanumérico.

En un segundo aspecto, la presente invención también se refiere a un método de verificación de la autenticidad y originalidad de un producto envasado en un contenedor, habilitándose el contenedor y el producto individualmente para autenticación por el primer y segundo medios de autenticación respectivamente, de acuerdo con el método anteriormente descrito.

Un método de verificación de este tipo incluye al menos las etapas de:

a) leer ópticamente el primer medio de autenticación para el contenedor por medio de un lector óptico, comprendiendo dicho lector óptico que medios para extraer una clave de autenticación de contenedor de la señal óptica leída de dicho primer medio de autenticación y conectándose a una primera base de datos en la que se registran las primeras claves de autenticación originales de cada contenedor autenticado original,

b) comparar la clave de autenticación extraída por dicho lector óptico con cada primera clave de autenticación original en la primera base de datos, y

c) si la clave de autenticación de contenedor extraída por dicho lector óptico corresponde a una de las primeras claves de autenticación originales registradas en la primera base de datos, leer ópticamente el segundo medio de autenticación para el producto envasado en dicho contenedor con un lector óptico, comprendiendo dicho lector óptico que medios para extraer una clave de autenticación de producto de la señal óptica leída de dicho segundo medio de autenticación y conectándose a una segunda base de datos en la que se graban las segundas claves de autenticación originales de cada producto autenticado original, y

d) comparar la clave de autenticación de producto extraída por dicho lector óptico con cada segunda clave de autenticación original en la segunda base de datos, y

e) si la clave de autenticación de producto extraída por dicho lector óptico corresponde a una de las segundas claves de autenticación originales registradas en la segunda base de datos, evaluar la autenticidad del par asociado de dicho contenedor y dicho producto acondicionado en el mismo generando una clave de autenticación de seguridad a partir de una combinación implementada por ordenador de dichas claves de autenticación de contenedor y producto extraídas con dicho lector óptico, y comparar dicha clave de autenticación de seguridad con cada dicha tercera clave de autenticación única original registrada en dicha tercera base de datos para la clave de autenticación del par producto contenedor asociado, en el que la tercera clave de autenticación es un identificador único de la primera y segunda clave de autenticación asociada.

La presente invención se presentará ahora en detalle en la siguiente descripción, con referencia a la Figura 1 y 2 que representan esquemáticamente, en forma de bloque, el método de autenticación de la presente invención en dos implementaciones preferidas.

En el siguiente ejemplo, el método de la invención se describirá en relación con la autenticación de un producto líquido tal como vino envasado en botellas de vidrio. Sin embargo, el método de la invención no se limita a la autenticación de productos líquidos, ni a contenedores hechos de vidrio.

De acuerdo con una primera variante de la invención mostrada en la Figura 1, una primera etapa del proceso de autenticación propuesto consiste en proporcionar un contenedor, por ejemplo una botella de vidrio para envasar vino, con un primer medio de autenticación para autenticar la botella de vidrio. Por lo tanto, en la planta de producción de vidrio, se producen botellas de vidrio en una fila en una máquina de formación de botellas 1 (habitualmente una máquina de SI) en la que se moldean botellas de vidrio a partir de un lote de vidrio fundido caliente. Las botellas, una vez moldeadas, directamente salen de la máquina de SI 1 en un estado caliente y se graban con láser con un primer medio de autenticación AM1 antes de entrar en un túnel de recocido 2.

De acuerdo con la invención, el primer medio de autenticación AM1 es preferente y ventajosamente un código de matriz de datos, que se graba con láser dentro del material de vidrio de la botella directamente a la salida de la máquina de SI, es decir, en extremo caliente.

Tal grabado en extremo caliente de un código de matriz de datos AM1 puede efectuarse ventajosamente por medio de un sistema de grabación con láser, tal como en sistema de grabación con láser de extremo caliente comercializado por la empresa MSC Inspection Worldwide.

La grabación de un código de matriz de datos AM1 en extremo caliente en el material de vidrio de las botellas proporciona un código de identificación/autenticación único para las botellas. Este código comprende toda información requerida acerca de la sección de la máquina de SI 1 o el molde en el que se forma una botella, la fecha de producción así como el código de la empresa, código de la línea y código de la planta. Las botellas formadas y grabadas en extremo caliente comprenden de este modo un medio de autenticación AM1 seguro y resistente, que es irreproducible, pero fácilmente legible por medio de lectores ópticos estándar.

Por lo tanto, es posible verificar la autenticidad de las botellas a lo largo de toda su vida, no únicamente dentro de la planta de vidrio durante producción de las botellas, sino también después de que las botellas hayan abandonado la planta de producción en la planta de llenado y, a continuación, cuando las botellas llenas se lanzan a la venta en el mercado.

Después de pasar el túnel de recocido 2, las botellas se comprueban a continuación, y un lector óptico en la línea lee su código de matriz de datos AM1 para verificar el grabado correcto del código en el material de vidrio de las botellas. Al leer dicho código de matriz de datos, se extrae una primera clave de autenticación AC1. Esta primera clave de autenticación AC1 es una clave o código numérico o alfanumérico automáticamente derivado por un programa informático a partir de la lectura del código de matriz de datos grabado en la botella.

Una vez obtenida, la primera clave o código de autenticación AC1 para la botella, es decir, para el contenedor, se registra en una primera base de datos DB1, que de este modo acumula la clave de autenticación individual para cada botella producida. Por lo tanto, es posible mantener un rastro constante de cada botella producida comercializada de modo que puede escanearse e identificarse mediante una simple lectura óptica de la matriz de datos en cualquier sitio después de que se haya producido. Después de leer los códigos de matriz de datos AM1, las botellas se apilan en palés a continuación en la etapa 3 mostrada en la Figura 1 antes de enviarse a plantas de llenado.

La segunda etapa del método de autenticación de la invención consiste en, después de autenticar las botellas por su primer medio de autenticación AM1, autenticar el producto. En el presente ejemplo, el producto es vino, a envasarse en las botellas autenticadas.

La autenticación del producto envasado de acuerdo con el método de la invención incluye la etapa de aplicación de un segundo medio de autenticación AM2 para el producto en las botellas ya autenticadas.

Para este fin, las botellas autenticadas se suministran a una línea de llenado 4 en la que se llenan en fila. Después del llenado, un sistema de lectura lee una segunda vez el medio de autenticación AM1 de cada botella así llenada, que también se conecta a la primera base de datos DB1 en la que se han registrado las primeras claves de autenticación AC1 para las botellas. De este modo se comprueba que todas las botellas usadas para el llenado del vino son botellas auténticas de su proveedor. Tras la comprobación satisfactoria de la primera clave de autenticación AC1, el sistema de lectura a continuación desencadena la aplicación de un segundo medio de autenticación AM2 para el vino en la botella que se acaba de comprobar.

Como alternativa, la comprobación del código AC1 en la planta de llenado también puede efectuarse justo después del llenado y taponado de las botellas como se representa en la Figura 1 mediante una flecha discontinua.

En otra variante mostrada en la Figura 2, también es posible efectuar el método de la invención con una primera clave de autenticación AC1 que se extrae únicamente en la planta de llenado mediante la lectura del código de matriz de datos AM1 grabado en las botellas directamente en la línea de llenado, y registrando las primeras claves de autenticación AC1 en una primera base de datos DB1'. A continuación, una vez que cada primera clave de autenticación AC1 se ha registrado en base de datos DB1', se desencadena la asignación de un segundo medio de autenticación AM2 para la botella que se acaba de leer y llenar con vino.

El segundo medio de autenticación AM2 preferentemente comprende un código o firma aleatoria de dos o tres dimensiones o que se forma, imprime o implementa de otra manera en una etiqueta. El código o firma aleatoria de dos o tres dimensiones es visible directamente y legible ópticamente en la etiqueta, que se aplica a la botella después de que se ha llenado con el producto, por ejemplo, el vino, en la etapa 4, y después de que la botella se ha taponado en la estación de taponado 5. Como en la Figura 1, pero no representada en la Figura 2, la lectura de AM1 y la extracción del código AC1 puede producirse directamente después del llenado 4 y taponado de las botellas en 5.

En una realización preferida del método de la invención, el segundo medio de autenticación para el producto es una firma aleatoria tridimensional implementada en una etiqueta. Una firma aleatoria 3D de este tipo es un autenticador único o no reproducible que consta de una estructura 3D visible formada, como se prefiere en la presente invención, mediante la generación aleatoria de burbujas dentro de un material transparente tal como un polímero termoestable.

La firma aleatoria 3D es visible en dicha etiqueta de modo que puede leerse mediante medios ópticos especializados para extraer una segunda clave de autenticación AC2 que se registra a continuación en una segunda base de datos DB2 para almacenar las claves de autenticación para el vino envasado en las botellas.

Preferentemente, la clave de autenticación AC2 que corresponde al segundo medio de autenticación AM2 se extrae o atribuye directamente por el productor de firma una vez que se ha creado, y se imprime directamente en la etiqueta de modo que un consumidor puede usar la clave impresa para verificar por sí mismo la autenticidad de un vino que compró introduciendo la clave de autenticación directamente en un sitio web de internet conectado a la base de datos DB2 de segundas claves de autenticación. Si la clave introducida corresponde a una registrada en la base de datos, entonces el consumidor sabe que su vino es genuino.

Una solución particularmente eficiente y segura para aplicar firmas aleatorias 3D en etiquetas se proporciona por la empresa francesa PROOFTAG S.A.S que usa la tecnología BUBBLE TAG®, que es la preferida de acuerdo con la invención para formar el segundo medio de autenticación.

Las etiquetas que llevan la firma aleatoria 3D para autenticación del vino llenado en las botellas se fijan preferentemente en el cuello de las botellas para formar un sello de apertura. Para este fin, las etiquetas pueden comprender ventajosamente una película a prueba de manipulación aplicada al cuello de cada botella, y al menos parcialmente sobre el tapón de cada botella. Las etiquetas que llevan la firma aleatoria 3D también pueden comprender preferentemente un código de trazabilidad tal como un código de matriz de datos.

Como alternativa, la etiqueta que lleva la etiqueta de burbujas también puede insertarse dentro del tapón de la botella y retraerse en el cuello de la botella después del llenado y encorchado de la botella.

Por lo tanto, usando códigos de matriz de datos AM1 grabados en las botellas en extremo caliente, y usando AM2 de etiquetas 3D implementadas en etiquetas aplicadas en los cuellos de las botellas después del llenado y cerrado de las botellas, tanto las botellas como el vino dentro de las mismas se autentican y se pueden autenticar individualmente.

Las botellas se envasan a continuación en una estación de envasado 6 y envían a minorista para su venta a los consumidores finales 7.

El método de la invención comprende además una tercera etapa para autenticar el par asociado formado por el vino y su botella para garantizar que, incluso si el vino y la botella son ambos genuinos, corresponde exactamente a un par original asociado como se formó originalmente en la planta de producción, y que no se ha producido ninguna separación o alteración de o bien el contenedor o bien el producto envasado en el mismo entre producción y venta al consumidor final.

Por esta razón, el método de la invención comprende una tercera etapa en la que se genera una tercera clave de autenticación AC3 para autenticar el par asociado formado por el producto, por ejemplo, vino, y su contenedor, por ejemplo, una botella, a partir de una combinación implementada por ordenador de dicha primera y segunda claves de autenticación, registrándose dicha tercera clave de autenticación en una tercera base de datos DB3.

De forma práctica, en el ejemplo representado, cuando el vino se llena en una botella y dicha botella se cierra y autentica mediante la aplicación de una etiqueta con una etiqueta 3D, la primera y segunda claves de autenticación AC1, AC2 para la botella y vino se registran en las bases de datos DB1 y DB2 respectivamente. Dicha primera y segunda claves de autenticación también se introducen automáticamente en un sistema informático 8 y combinan para generar una tercera clave de autenticación única AC3 para el correspondiente par asociado de vino y botella.

La tercera clave de autenticación AC3 se registra a continuación en una tercera base de datos DB3.

Esta tercera clave de autenticación es, por lo tanto, el identificador único del par asociado formado por una única botella que se puede autenticar y un único volumen de vino que se puede autenticar envasado en dicha botella.

El método de la invención, por lo tanto, asegura que, desde la producción de un producto acondicionado, por ejemplo, una botella de vino, hasta su venta a consumidores finales, cada botella puede rastrearse, comprobarse y verificarse para determinar la originalidad:

- del contenedor (por ejemplo, botella de vidrio) leyendo el primer medio de autenticación AM1 aplicado a dicho contenedor, para verificar dicha primera clave de autenticación AC1,

- del producto (por ejemplo, vino) envasado en dicho contenedor leyendo el segundo medio de autenticación AM2 aplicado al contenedor, para verificar dicha segunda clave de autenticación AC2,

- del par de contenedor-producto asociado combinando dicha primera y segunda claves de autenticación AC1, AC2 en un sistema informático para comprobar si dicha combinación corresponde a una tercera clave de autenticación AC3 identificada registrada en dicha tercera base de datos DB3.

Gracias al método de la invención, la falsificación de un contenedor original, por ejemplo, en el presente ejemplo una botella de vidrio, puede detectarse fácilmente, así como la falsificación de un producto original, ya que es casi imposible obtener una tercera clave de autenticación registrada sin las dos primera y segunda claves de autenticación AC1, AC2 originales derivadas a partir de dicho primer y segundo medio de autenticación AM1, AM2 de un par de contenedor-producto asociado original.

Como consecuencia, si se falsifica o altera cualquiera del contenedor o el producto, el medio de autenticación ciertamente también será falsificado o alterado y, por lo tanto, será imposible generar la tercera clave de autenticación AC3 requerida para autenticar al 100 % el par de contenedor-producto asociado.

La presente invención también se refiere a un método para verificar la autenticidad y originalidad de un producto acondicionado en un contenedor (tal como vino en una botella de vidrio en el presente ejemplo), autenticándose dicho contenedor y dicho producto individualmente por primer y segundo medios de autenticación AM1, AM2 respectivamente de acuerdo con el método de autenticación de la invención como se ha descrito anteriormente.

El método de verificación de la invención incluye las siguientes etapas:

a) leer ópticamente dicho primer medio de autenticación AM1 para el contenedor por medio de un lector óptico, comprendiendo dicho lector óptico que medios para extraer una clave de autenticación de contenedor de la señal óptica leída de dicho primer medio de autenticación y conectándose a una primera base de datos DB1 en la que se registran las primeras claves de autenticación originales AC1 de cada contenedor autenticado original,

b) comparar la clave de autenticación extraída por dicho lector óptico con cada primera clave de autenticación original AC1 en la primera base de datos, y

c) si la clave de autenticación de contenedor extraída por dicho lector óptico corresponde a una de las primeras claves de autenticación originales AC1 registradas en la primera base de datos DB1, leer ópticamente dicho segundo medio de autenticación AM2 para el producto envasado en dicho contenedor con un lector óptico, comprendiendo dicho lector óptico que medios para extraer una clave de autenticación de producto de la señal óptica leída de dicho segundo medio de autenticación y conectándose a una segunda base de datos DB2 en la que se registran las segundas claves de autenticación originales AC2 de cada producto autenticado original, y

d) comparar la clave de autenticación de producto extraída por dicho lector óptico con cada segunda clave de autenticación original AC2 en la segunda base de datos DB2, y

e) si la clave de autenticación de producto extraída por dicho lector óptico corresponde a una de las segundas claves de autenticación originales AC2 registradas en la segunda base de datos DB2, evaluar la autenticidad del par asociado de dicho contenedor y dicho producto acondicionado en el mismo generando una clave de

autenticación de seguridad a partir de una combinación implementada por ordenador de dichas claves de autenticación de contenedor y producto extraídas por dicho primer y segundo lectores ópticos, y comparar dicha clave de autenticación de seguridad con cada una de dichas terceras claves de autenticación originales AC3 registradas en dicha tercera base de datos DB3 para la clave de autenticación del par producto-contenedor asociado.

REIVINDICACIONES

1. Un método de habilitación de autenticación de un producto en un contenedor de vidrio o cristal, y habilitación de autenticación del propio contenedor, que incluye las etapas de:

(a) aplicar al contenedor un primer medio de autenticación (AM1) para asegurar la autenticidad del contenedor,
(b) obtener una primera clave de autenticación (AC1) de dicho primer medio de autenticación y registrar dicha primera clave de autenticación en una primera base de datos (DB1, DB1'),
(c) aplicar al contenedor un segundo medio de autenticación (AM2) independente de dicho primer medio de autenticación para asegurar la autenticidad y originalidad del producto en el contenedor,
(d) obtener una segunda clave de autenticación (AC2) de dicho segundo medio de autenticación y registrar dicha segunda clave de autenticación en una segunda base de datos (DB2) de forma separada de dicha primera clave de autenticación,
(e) generar una tercera clave de autenticación (AC3), para autenticar un par asociado que consta del producto y su contenedor, a partir de una combinación implementada por ordenador de dicha primera y segunda claves de autenticación (AC1, AC2), y
(f) registrar dicha tercera clave de autenticación en una tercera base de datos (DB3); en el que dicho primer medio de autenticación (AM1) se graba con láser en el contenedor en dicha etapa (a) en un extremo caliente de un proceso de fabricación para el contenedor; y

en el que la tercera clave de autenticación es un identificador único de la primera y segunda clave de autenticación asociada.

2. Un método de acuerdo con la reivindicación 1 en el que dicho primer y segundo medios de autenticación (AM1, AM2) son ópticamente legibles.

3. Un método de acuerdo con una de las reivindicaciones 1 o 2 en el que dicho segundo medio de autenticación (AM2) incluye un código aleatorio bidimensional desde el que se lee ópticamente dicha segunda clave de autenticación (AC2) en dicha etapa (d).

4. Un método de acuerdo con una de las reivindicaciones 1 a 2 en el que dicho segundo medio de autenticación (AM2) incluye una firma física aleatoria tridimensional desde la que se lee ópticamente dicha segunda clave de autenticación (AC2) en dicha etapa (d).

5. Un método de acuerdo con la reivindicación 4 en el que dicha firma física aleatoria tridimensional se implementa y es visible en una etiqueta aplicada al contenedor en dicha etapa (c).

6. Un método de acuerdo con la reivindicación 4 o 5 en el que dicha firma física aleatoria tridimensional se genera aleatoriamente en un material transparente y se aplica al contenedor en dicha etapa (c).

7. Un método de acuerdo con la reivindicación 6 en el que dicho material transparente es un polímero termoestable.

8. Un método de acuerdo con una de las reivindicaciones 5 a 7 en el que dicha etiqueta incluye una película a prueba de manipulación y se aplica al contenedor como un sello de apertura.

9. Un método de acuerdo con una de las reivindicaciones 1 a 8 en el que dicho segundo medio de autenticación (AM2) incluye un código de trazabilidad.

10. Un método de acuerdo con una de las reivindicaciones 1 a 7 en el que dicho primer medio de autenticación (AM1) incluye un código de matriz de datos y dicho segundo medio de autenticación (AM2) incluye una etiqueta de burbujas.

11. Un método de acuerdo con una de las reivindicaciones 1 a 8 en el que dicha primera, segunda y tercera claves de autenticación (AC1, AC2, AC3) incluyen cada una un código numérico o alfanumérico.

12. Un método de verificación de la autenticidad y originalidad de un producto en un contenedor de vidrio o cristal, habilitándose el contenedor y el producto individualmente para autenticación de acuerdo con el método expuesto en cualquiera de las reivindicaciones 1 a 11, incluyendo el método las etapas de:

leer ópticamente el primer medio de autenticación (AM1) para el contenedor por medio de un primer lector óptico, incluyendo dicho primer lector óptico medios para extraer una clave de autenticación de contenedor de una señal óptica leída de dicho primer medio de autenticación y conectándose a una primera base de datos (DB1, DB1') en la que se registran primeras claves de autenticación originales (AC1) de cada contenedor de autenticación original, comparar la clave de autenticación obtenida por dicho primer lector óptico en dicha etapa (a) con cada clave de

autenticación original (AC1) en la primera base de datos,
si la clave de autenticación de contenedor leída por dicho lector óptico corresponde a una primera clave de autenticación (AC1) registrada en la primera base de datos (DB1, DB1'), leer ópticamente el segundo medio de autenticación (AM2) para el producto envasado en el contenedor con un segundo lector óptico, incluyendo dicho lector óptico medios para obtener una clave de autenticación de producto de una señal óptica leída de dicho segundo medio de autenticación y conectándose a una segunda base de datos (DB2) en el que se registran segundas claves de autenticación originales (AC2) de cada producto autenticado original,
comparar la clave de autenticación de producto obtenida por dicho segundo lector óptico con cada segunda clave de autenticación original (AC2) en la segunda base de datos (DB2), y
si la clave de autenticación de producto obtenida por dicho segundo lector óptico corresponde a una segunda clave de autenticación (AC2) registrada en la segunda base de datos, evaluar la autenticidad de un par asociado que consta del contenedor y el producto envasado en el contenedor:

- generando una clave de autenticación de seguridad a partir de una combinación implementada por ordenador de dichas claves de autenticación de contenedor y producto extraídas por dichos lectores ópticos, y
- comparando dicha clave de autenticación de seguridad con terceras claves de autenticación (AC3) registradas en una tercera base de datos (DB3) como las claves de autenticación únicas de pares de producto-contenedor asociados, en el que la tercera clave de autenticación es un identificador único de la primera y segunda clave de autenticación asociada.

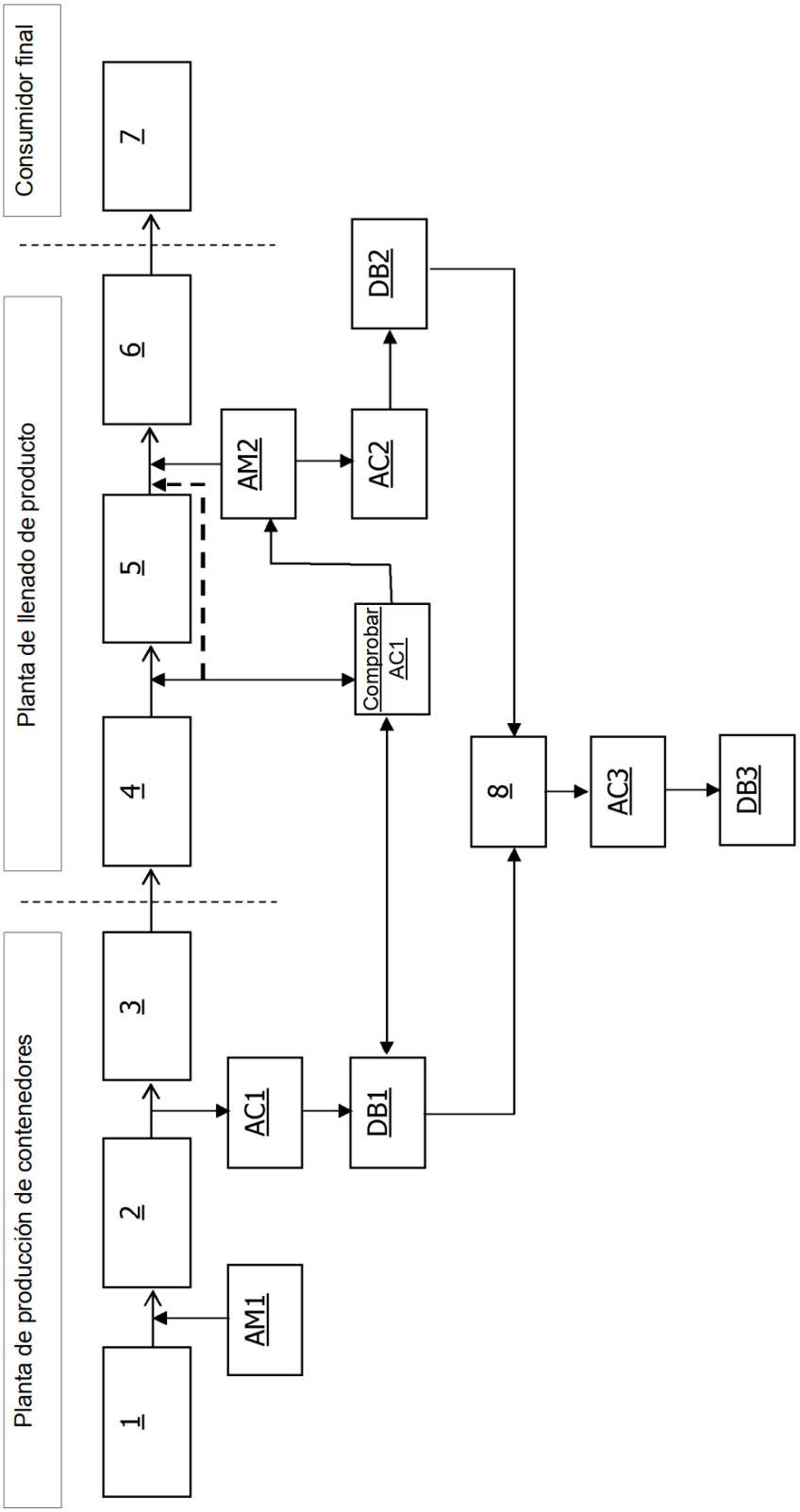
Planta de producción de contenedores
Planta de llenado de producto
Consumidor final
1
2
3
4
5
6
7
AM1
AC1
DB1
AM2
AC2
DB2
Comprobar AC1
8
AC3
DB3

Fig. 1

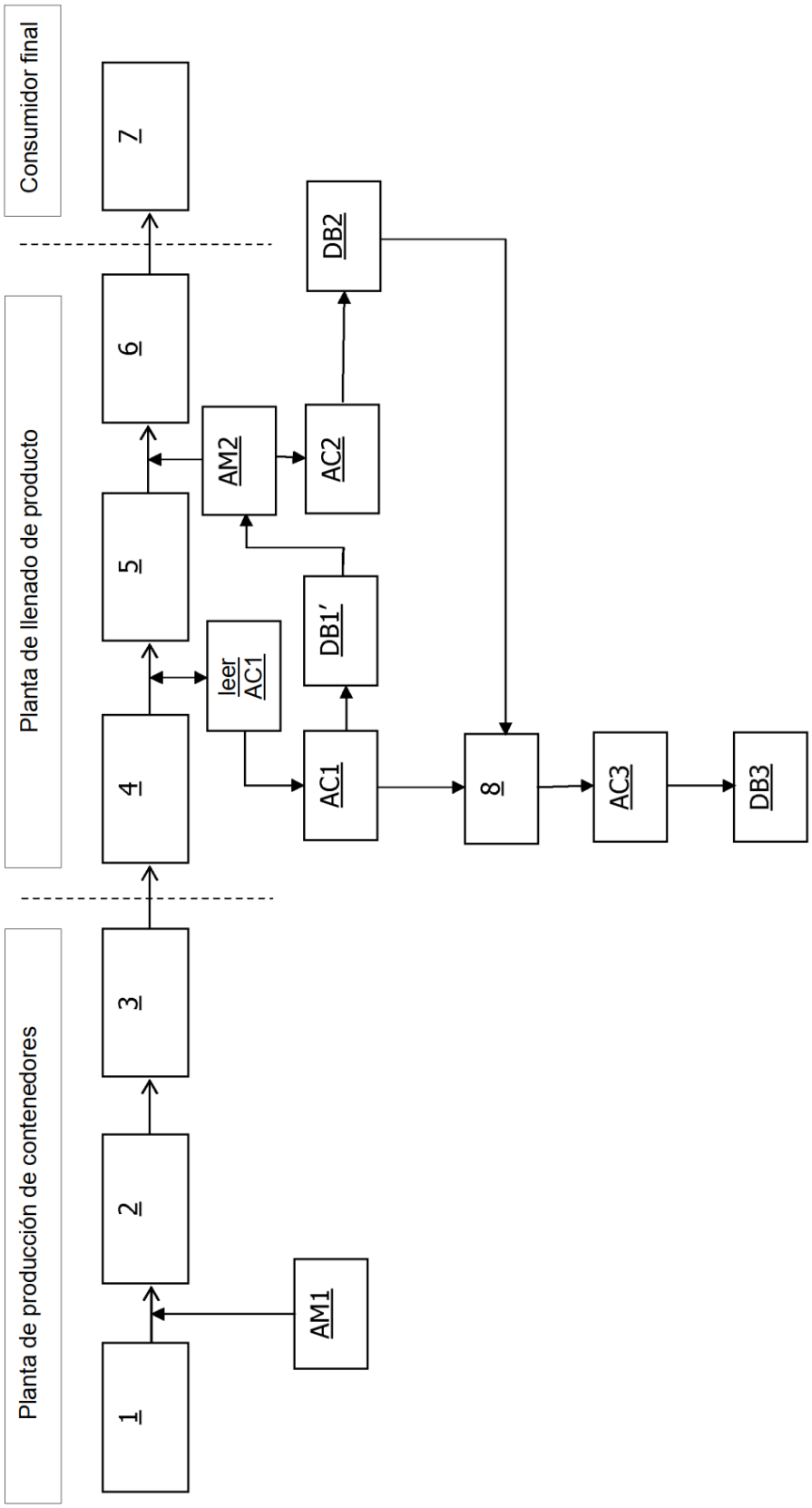
Planta de producción de contenedores
Planta de llenado de producto
Consumidor final
1
2
3
4
5
6
7
AM1
AM2
leer AC1
AC1
AC2
DB1'
DB2
8
AC3
DB3

Fig. 2