



No. 13-153978- -00007-0000

Fecha: 2014-10-31 15:42:56

Dep. 2020 DIR.NUEVASCR

Tra. 11 PATENTEIYII

Eve: 378 FASENACIONALI

Act. 523 RESPUESTA

Folios: 56

Clarke, Modet & Cº

COLOMBIA

P-3848

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
DIVISION DE NUEVAS CREACIONES

E. S. D.

JF

Re: Expediente No. 13-153.978

Solicitud de patente a nombre de **DIGITAL CODING AND TRACKING ASSOCIATION**

Yo, SILVANA MARIA LOPEZ DIAZ identificada como aparece al pie de mi firma, domiciliada en la Carrera 11 No. 86-53, piso 6, obrando como apoderada sustituta de acuerdo con la sustitución adjunta de la sociedad **DIGITAL CODING AND TRACKING ASSOCIATION**, domiciliada en Suiza, solicitante de la patente de la referencia, en respuesta al oficio No. 7342 notificado por fijación en lista el 24 de junio de 2014, para dar respuesta al referido oficio y teniendo en cuenta el memorial presentado el 17 de septiembre de 2014 mediante el cual se solicitó una prórroga de 30 días para dar respuesta al referido oficio me permito manifestar:

1. Con fundamento en la facultad que confiere el artículo 34 de la Decisión 486 al solicitante para modificar la solicitud de patente en cualquier momento del trámite, presento junto con este memorial nuevo capítulo reivindicatorio, el cual consta de 15 reivindicaciones y reemplaza completamente el capítulo presentado anteriormente.

2. **Usos y segundos usos**

En dicho respecto, se le informa al presente Despacho que se han eliminado las expresiones de las reivindicaciones 6, 8, 11, 12, 14 y 15 que hacían alusión a uso, por tanto se ve superada ésta objeción.

3. **Claridad**

- 3.1 Se solicita amablemente cambiar el título de la invención por “APARATO Y MÉTODO QUE COMPRENDE PROPORCIONAR UNA CLAVE CRIPTOGRÁFICA Y UN CÓDIGO DE IDENTIFICACIÓN PARA LA MARCACIÓN DE ARTICULOS FABRICADOS”, ya que por un error en la traducción quedó mal escrito.
 - 3.2 Como primera medida, se modificó la antigua reivindicación 1 (nueva reivindicación 1), incluyendo las características de la antigua reivindicación

P-3848

1/56

Clarke, Modet & C^o

COLOMBIA

3 con el fin de definir y dar mayor claridad al método reclamado. Estas modificaciones se encuentran debidamente sustentadas en el capítulo descriptivo.

- 3.3 Se realizaron las correcciones de traducción en la reivindicación 7 y de igual forma en el capítulo descriptivo, el cual se anexa a este memorial.
- 3.4 Se modificaron las expresiones que hacían referencia a resultados a obtener en la reivindicación 13. Sin embargo
- 3.5 Con respecto a la objeción por falta de concisión, la solicitante respetuosamente manifiesta su desacuerdo ya que las reivindicaciones 14 y 15 tienen dependencia de la reivindicación 13 que se refiere a un aparato. En cuanto a las reivindicaciones 6 y 9 se modificaron con el fin de superar la objeción realizada por el señor examinador.
- 3.6 Se colocaron los números de referencia de los elementos que conforman el artículo de la presente invención de acuerdo a las figuras presentadas.

En cuanto a estas modificaciones, me permito decir que las mismas no amplían de ninguna manera la materia objeto de la presente solicitud y se realizaron con el ánimo de superar las objeciones de claridad y novedad planteadas por el examinador en su concepto técnico.

En consecuencia, nos permitimos informar que las nuevas reivindicaciones 1 a 15 se ajustan a las disposiciones del artículo 30 de la Decisión 486.

En cuanto al número de reivindicaciones, atentamente nos permitimos decir que no se adjunta tasa por reivindicaciones adicionales, toda vez que el nuevo capítulo reivindicatorio tiene el mismo número de cláusulas que el originalmente presentado y en esencia es el mismo objeto pero más limitado.

4. Novedad

El señor examinador establece en su concepto técnico que las antiguas reivindicaciones 1 a 7, 9, 10 y 13 a 15 carecen de novedad a la luz del documento EP 1 645 992 (D1).

En este sentido, me permito decir que el artículo 16 de la Decisión 486 de la Comisión de la Comunidad Andina establece que la invención se considera nueva cuando no está comprendida en el estado de la técnica. Si de acuerdo con el espíritu de la norma legal indicada, la invención no se considera como nueva si está "comprendida" en el estado de la técnica, dicha norma se está refiriendo, naturalmente, a la totalidad del invento y no a alguno o a algunos de los

Clarke, Modet & C^o

COLOMBIA

componentes. Para que la invención pierda su calidad de novedosa, es claro que ella, **TODA ELLA**, ha de estar contenida en el “conjunto de conocimientos existentes que son aplicables al proceso industrial” como define el estado de la técnica el Tribunal de justicia del Acuerdo de Cartagena (Proceso No. 6-IP-89, sentencia de 31 de octubre de 1989, publicada en Jurisprudencia del Tribunal de Justicia del Acuerdo de Cartagena, Tomo 11, BID-INTAL, Buenos Aires, 1994, página 60).

Lo anterior significa que, para que las razones que aduce ese despacho para desvirtuar la novedad fuesen ciertas, sería forzoso que se demostrara que la invención de mi mandante esté comprendida en el estado de la técnica de forma **TOTAL**, lo cual no sucede con la materia reclamada en las nuevas reivindicaciones.

Teniendo en cuenta lo anterior, es deseo de la solicitante presentar argumentos en contra de estas declaraciones, con el fin de demostrar que la invención reclamada en la presente solicitud posee características técnicas que no están contenidas en su totalidad en el estado de la técnica.

En este sentido, la solicitante quiere señalar que la nueva reivindicación 1 describe nuevas características “...proporcionar el código de activación (213) al punto en la cadena de suministro en respuesta al punto en la cadena de suministro que transmite la información relacionada con la clave criptográfica recibida, en donde el código de activación (213) permite que la clave criptográfica en el estado inactivo en el punto en la cadena de suministro se active para formar la clave criptográfica en el estado activo y (...) encriptar, por medio del centro de verificación (114), el código de activación (213) con una clave pública de un par de claves asimétricas asociado con un certificado de la clave criptográfica de manera que el código de activación (213) puede ser descifrado por el punto de la cadena de suministro utilizando una clave privada del par de claves asimétricas asociado con el certificado de la clave criptográfica (...)”, lo cual no se encuentra divulgado en D1.

En conclusión, la presente invención es, por tanto, novedosa y tiene nivel inventivo a la luz de D1.

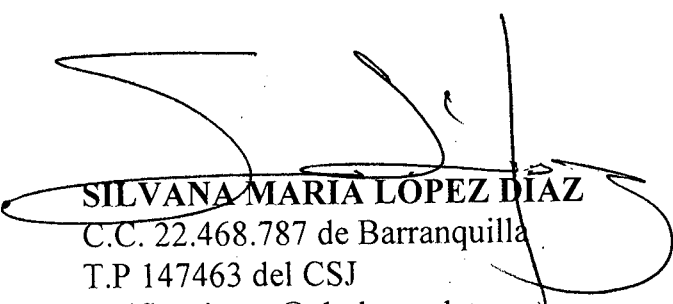
En este sentido, y siguiendo el Manual Andino de Patentes, la presente invención tal y como se encuentra definida en las nuevas reivindicaciones 1 a 15, tiene diferencias con el estado del arte e implicó un nivel inventivo durante su desarrollo, por lo cual debe ser considerada como novedosa e inventiva según las disposiciones de los artículos 16 y 18 de la Decisión 486.

5. Conclusiones

Habiendo atendido cabalmente las objeciones presentadas por ese despacho, atentamente solicitamos se conceda el privilegio de patente de invención a la solicitud en estudio o si el señor examinador considera que subsisten razones para objetar la presente invención, rogamos expedir otro examen de fondo con los debidos motivos y razones que sustenten su objeción con el fin de que nuestro mandante tenga la posibilidad de exponer sus argumentos con base en la interpretación de los artículos 45 de la Decisión 486 -el cual otorga la facultad al examinador para emitir los exámenes de fondo-, 35 y 59 del Código Contencioso Administrativo que señala que: *“habiéndose dado oportunidad a los interesados para expresar sus opiniones, y con base en las pruebas e informes disponibles, se tomará la decisión que será motivada al menos en forma sumaria si afecta a particulares”* y *“(.) deberá proferirse la decisión definitiva. Esta se motivará en sus aspectos de hecho y de derecho, y en los de conveniencia si es el caso”*, respectivamente (El subrayado es nuestro).

En consecuencia, solicitamos a ese despacho pronunciarse en relación con todos los argumentos presentados en este memorial dando estricta aplicación al principio del debido proceso consagrado en el artículo 29 de la Constitución Nacional

Señor Superintendente,



SILVANA MARIA LÓPEZ DÍAZ

C.C. 22.468.787 de Barranquilla

T.P 147463 del CSJ

notificaciones@clarkemodet.com.co

Clarke, Modet & C^o

COLOMBIA

ANEXO

- Nuevo capítulo de reivindicaciones
- Nuevo capítulo descriptivo

P-3848
Rvs modificadas
Octubre 24, 2014

REIVINDICACIONES

1. Un método para marcar artículos fabricados, caracterizado porque comprende:

proporcionar una clave criptográfica en un estado inactivo a un punto en la cadena de suministro para los artículos fabricados;

proporcionar la clave criptográfica en un estado activo y un código de activación (213) para activar la clave criptográfica en el estado activo para formar la clave criptográfica en el estado activo, a un centro de verificación (114);

proporcionar el código de activación (213) al punto en la cadena de suministro en respuesta al punto en la cadena de suministro que transmite la información relacionada con la clave criptográfica recibida, en donde el código de activación (213) permite que la clave criptográfica en el estado inactivo en el punto en la cadena de suministro se active para formar la clave criptográfica en el estado activo y

enviar el código de activación (213) del centro de verificación (114) al punto en la cadena de suministro;

encriptar, por medio del centro de verificación (114), el código de activación (213) con una clave pública de un par de claves asimétricas asociado con un certificado de la clave criptográfica de manera que el código de activación (213) puede ser descifrado por el punto de la cadena de suministro utilizando una clave privada del par de claves asimétricas asociado con el certificado de la clave criptográfica;

generar, en el punto en la cadena de suministro, un

6

P-3848
Rvs modificadas
Octubre 24, 2014

código de identificación (ID) para cada artículo fabricado, el código ID siendo derivado de la clave criptográfica en el estado activo y una clave dinámica generada para cada lote de artículos fabricados;

proporcionar la clave dinámica para cada lote de artículos fabricados al centro de verificación;

marcar cada artículo fabricado con el código ID;
and

contar el número de códigos ID marcados en los artículos fabricados.

2. El método de conformidad con la reivindicación 1, caracterizado porque la clave criptográfica se genera en un generador de claves (115) separado del punto en la cadena de suministro.

3. El método de conformidad con la reivindicación 1 o reivindicación 2, caracterizado porque el código de activación (213) puede ser descifrado por un código generador en el punto de la cadena de suministro utilizando una clave privada del par de claves asimétricas asociado con el certificado de la clave criptográfica.

4. El método de conformidad con cualquier reivindicación precedente, caracterizado porque el paso de del punto en la cadena de suministro que transmite la información relacionada con la clave criptográfica recibida comprende enviar información relacionada con la clave criptográfica recibida del punto en la cadena de suministro al centro de verificación (114).

5. El método de conformidad con cualquier reivindicación precedente, caracterizado porque los códigos ID generados no se almacenan.

7

P-3848
Rvs modificadas
Octubre 24, 2014

6. El método de conformidad con cualquier reivindicación precedente, caracterizado porque además comprende:

reportar a una autoridad gubernamental (301) el número de códigos ID marcados en los artículos fabricados;

almacenar la información, por medio del centro de verificación, conectando los código ID marcados en los artículos fabricados con la información específica de esos artículos fabricados de tal forma que los impuestos pagados o que se deben pueden verificarse contra el número actual de artículos fabricados; y

llevar a cabo una verificación de impuestos.

7. El método de conformidad con la reivindicación 6, caracterizado porque el reporte se lleva a cabo por embarque y por depósito de impuestos sobre consumo de tal forma que los impuestos pagados pueden verificarse o calcularse por embarque y por depósito de impuestos sobre consumo.

8. El método de conformidad con cualquier reivindicación precedente, caracterizado porque además comprende, antes del paso de generar un código ID para cada artículo fabricado, el paso de

recibir la autorización de la autoridad gubernamental (301) del punto en la cadena de suministro para generar un número definido de códigos ID; y

llevar a cabo una verificación de impuestos.

9. El método de conformidad con la reivindicación 8, caracterizado porque además comprende, antes del paso de la autorización de la autoridad gubernamental (301) del punto en la cadena de suministro para generar un número definido de

8

P-3848
Rvs modificadas
Octubre 24, 2014

códigos ID, el paso de solicitar la autorización de la autoridad gubernamental (301).

10. El método de conformidad con la reivindicación 8 o reivindicación 9, caracterizado porque además comprende reportar a la autoridad gubernamental (301) el número de códigos ID marcados en los artículos fabricados.

11. El método de conformidad con cualquier reivindicación precedente, caracterizado porque además comprende reportar a un tercero el número de códigos ID marcados en los artículos fabricados; y

llevar a cabo una verificación del volumen de producción.

12. El método de conformidad con cualquier reivindicación precedente, caracterizado porque además comprende que:

un usuario transmita los código ID marcados en un artículo fabricado seleccionado al centro de verificación (114);

el centro de verificación derive del código ID, la clave criptográfica y la clave dinámica utilizadas para generar el código ID;

el centro de verificación (114) derive de la clave criptográfica y la clave dinámica información relacionada con la artículos fabricados seleccionados;

el centro de verificación (114) transmita al menos algo de la información relacionada con los artículos fabricados seleccionados al usuario; y

llevar a cabo una autenticación del artículo fabricado seleccionado .

9

P-3848
Rvs modificadas
Octubre 24, 2014

13. Un aparato para marcar artículos fabricados, caracterizado porque comprende:

un generador de claves (115) generando una clave criptográfica, en donde la clave criptográfica presenta un estado activo y un estado inactivo;

al menos un punto en una cadena de suministro para los artículos fabricados, en donde el generador de claves (115) envía la clave criptográfica, en el estado activo al punto en la cadena de suministro, en donde el punto en la cadena de suministro recibe un código de activación (213) en respuesta al punto en la cadena de suministro transmitiendo la información relacionada con la clave criptográfica recibida , y en donde el código de activación (213) permite que la clave criptográfica en el estado inactivo se active para formar la clave criptográfica en el estado activo;

un centro de verificación (114) para verificar las propiedades de los artículos fabricados, en donde el generador de claves (115) proporciona la clave criptográfica en el estado activo y el código de activación (213) al centro de verificación;

el centro de verificación proporciona el código de activación (213) al punto en la cadena de suministro por medio del envío del código de activación (213) del centro de verificación al punto en la cadena de suministro;

un generador de código (111), en el punto en la cadena de suministro generando un código de identificación (ID) para cada artículo fabricado, el código ID siendo derivado de la clave criptográfica en el estado activo y una clave dinámica generada para cada lote de artículos fabricados, en donde la clave dinámica para cada lote de

P-3848
Rvs modificadas
Octubre 24, 2014

artículos fabricados es provista al centro de verificación (114);

un marcador (113) en el punto en la cadena de suministro marcando cada artículo fabricado con el código ID; y

un contador contando el número de códigos ID marcados en los artículos fabricados,

en donde el centro de verificación (114) encripta el código de activación (213) con una clave pública de un par de claves asimétricas asociado con un certificado de la clave criptográfica de manera que el código de activación (213) puede ser descifrado por el punto de la cadena de suministro utilizando una clave privada del par de claves asimétricas asociado con el certificado de la clave criptográfica.

14. Un método adecuado caracterizado porque comprende:

generar una pluralidad de códigos de identificación (ID) para artículos fabricados;

marcar cada artículo fabricado con un código ID de la pluralidad de códigos ID por medio de un aparato de acuerdo con la reivindicación 13;

contar el número actual de códigos ID de la pluralidad de códigos ID marcados en los artículos fabricados, en donde el número actual de códigos ID es el mismo como o menor que a pluralidad de códigos ID;

reportar a una autoridad gubernamental (301) el número actual de códigos ID marcados en los artículos fabricados; y

almacenar la información conectando los ID de código marcados en los artículos fabricados con la

P-3848
Rvs modificadas
Octubre 24, 2014

información específica de esos artículos fabricados, de tal forma que los impuestos pagados o que se deben pueden verificarse contra el número actual de artículos marcados; y llevar a cabo una verificación de impuestos.

15. El método de conformidad con la reivindicación 14, caracterizado porque además comprende, antes del paso de generar una pluralidad de códigos ID para los artículos fabricados:

solicitar autorización de una autoridad gubernamental (301) para generar códigos ID para los artículos fabricados; y recibir la autorización de la autoridad gubernamental (301) para generar un número definido de códigos ID para los artículos fabricados.

**APARATO Y MÉTODO QUE COMPRENDE PROPORCIONAR UNA CLAVE
CRIPTOGRÁFICA Y UN CÓDIGO DE IDENTIFICACIÓN PARA LA MARCACIÓN
DE ARTICULOS FABRICADOS**

5

Campo de la Invención

La presente invención se refiere a métodos y aparatos para marcar artículos fabricados. En particular, la presente invención se refiere al marcado de productos empacados, por ejemplo, paquetes o cartones de cigarrillos y
10 otros productos del tabaco.

Antecedentes de la Invención

Los productos de contrabando y falsificados causan una significativa pérdida de utilidades a los productores y las autoridades gubernamentales. Los productos falsificados
15 de calidad inferior que se venden ilegalmente también son perjudiciales para el consumidor y el fabricante. Los consumidores se afectan porque pueden obtener productos de inferior calidad que puede ser peligroso. Esto es particularmente importante para productos tales como
20 farmacéuticos. Los fabricantes se ven afectados porque pueden sufrir una pérdida de reputación, un aumento en la competencia con sus propios productos, y la infracción de otros derechos legales. Los productos de contrabando, que son productos fabricados con el propósito de evadir impuestos o
25 las regulaciones gubernamentales, también son un problema considerable para los productores y las autoridades gubernamentales. Estos productos se comercian e importan ilegalmente y puede dar como resultado pérdidas significativas en ingresos.

30

Los problemas de contrabando y falsificación también son particularmente graves para productos que se someten a tributación, por ejemplo, los productos del tabaco.

13

También existen problemas para muchas otras clases de productos comercializados que llevan un fuerte valor de marca. Estos incluyen muchos productos internacionalmente comercializados tales perfumes, alcoholes, relojes y productos de lujo. Por lo tanto, los fabricantes, consumidores, distribuidores, mayoristas, importadores, autoridades gubernamentales y otras partes autorizadas necesitan ser capaces de verificar fácilmente que los productos particulares son genuinos. Además, las autoridades gubernamentales y otras partes autorizadas necesitan ser capaces de verificar fácilmente que el volumen de artículos fabricados se adhiere a los volúmenes autorizados, particularmente para productos sujetos a tributación. Las autoridades gubernamentales y otras partes autorizadas además necesitan ser capaces de verificar el estado de los impuestos para productos sujetos a tributación y proteger los ingresos derivados de tal tributación.

Breve Descripción de la Invención

Existe la necesidad de un método y aparato mejorados para marcar artículos fabricados, particularmente uno que pueda utilizarse para verificación de impuestos, verificación de volumen de producción y autenticación de los productos fabricados.

De acuerdo con un primer aspecto de la invención, se proporciona un método para marcar artículos fabricados, que comprende: proporcionar una clave criptográfica en un estado inactivo a un punto en una cadena de suministro para los artículos fabricados; proporcionar la clave criptográfica en un estado activo y un código de activación para activar la clave criptográfica en el estado inactivo para formar la

clave criptográfica en el estado activo, a un centro de verificación; proporcionar el código de activación al punto en la cadena de suministro en respuesta al punto en la cadena de suministro que transmite la información relacionada con la clave criptográfica recibida, el código de activación permite que la clave criptográfica en el estado inactivo en el punto en la cadena de suministro se active para formar la clave criptográfica en el estado inactivo en el punto en la cadena de suministro a ser activada para formar la clave criptográfica en el estado activo; generar, en el punto en la cadena suministro, un código de identificación (ID, por sus siglas en inglés) para cada artículo fabricado, el código ID siendo derivado de la clave criptográfica en el estado activo y una clave dinámica generada para cada lote de artículos fabricados; proporcionar la clave dinámica para lote de artículos fabricados al centro de verificación; marcar cada artículo fabricado con el código ID; y continuar el número de códigos ID marcados en los artículos fabricados.

La invención proporciona un método mejorado para marcar artículos fabricados. Este método puede utilizarse para verificación de impuestos (para artículos fabricados que se someten a tributación), para la verificación del volumen de producción y para la autenticación de los artículos fabricados. Un código ID se marca en cada artículo fabricado, de tal forma que cada artículo fabricado puede identificarse singularmente. El conteo del número de códigos ID marcados en los artículos fabricados asegura que los artículos fabricados rechazados o eliminados no se identifiquen. Es decir, el número correcto o actual de artículos fabricados marcados se cuenta.



Los artículos fabricados pueden ser cualquier artículo fabricado, incluyendo productos de tabaco, tales como paquetes de cigarrillos o cartones de cigarrillos, u otros artículos que llevan un fuerte valor de marca o se someten a tributación. El punto en la cadena de suministro puede comprender cualquier ubicación, sitio, lugar o posición dentro de una cadena de suministro para los artículos fabricados. Por ejemplo, el punto en la cadena de suministro puede comprender un punto de importación, un punto de distribución, un comprador, un mayorista o cualquier otro enlace en la cadena de suministro. Más preferiblemente, sin embargo, el punto en la cadena de suministro comprende un centro de producción o línea de producción para los artículos fabricados.

El paso de marcar cada artículo fabricado puede comprender impresión de chorro de tinta, impresión holográfica, impresión láser o cualquier otra impresión o marcación que permita la impresión o la marcación de los códigos ID en cada artículo. El paso de marcar cada artículo fabricado puede comprender imprimir o marcar cada artículo, imprimir o marcar el empaque externo, imprimir o marcar las etiquetas adhesivas o marbetes o cualquier otra impresión o marcación apropiada. El punto en la cadena de suministro puede comprender un sensor para detectar los códigos ID marcados en los artículos fabricados. El sensor puede confirmar que cada código ID ha sido apropiadamente marcado en el artículo fabricado. El sensor puede contar solamente el número de códigos ID apropiadamente marcados en los artículos fabricados.

En una modalidad, la clave criptográfica se genera

en un generador de claves separado del punto en la cadena de suministro.

La clave criptográfica es simplemente cualquier pieza de información (por ejemplo, un número) que puede utilizarse en combinación con otros parámetros para formar un código. La clave criptográfica en el estado activo es preferiblemente la clave criptográfica en un estado no codificado. La clave criptográfica en el estado inactivo es preferiblemente la clave criptográfica en un estado codificado. De esta forma, el código de activación es preferiblemente un mecanismo de descodificación para convertir la clave codificada en una clave no codificada. La clave criptográfica puede incluir un número porciones que incluyen una pluralidad de códigos secretos.

El paso de proporcionar la clave criptográfica en un estado activo a un punto en una cadena de suministro puede comprender enviar la clave criptográfica en el estado inactivo desde el generador de claves al punto en la cadena de suministro en un soporte de datos no volátil. El soporte de datos no volátil es un soporte de datos que incluye memoria de computadora no volátil, es decir, memoria de computadora que puede retener la información almacenada aun cuando no está activada. Los ejemplos, incluyen, pero no se limitan a, un CD-ROM, un DVD-ROM o un disco duro removible. Alternativamente, el paso de proporcionar la clave criptográfica en un estado inactivo a un punto en la cadena de suministro puede comprender proporcionar la clave criptográfica en el estado inactivo a través de una conexión en red segura.

El generador de claves preferiblemente forma parte

del centro de verificación. En este caso, el paso de proporcionar la clave criptográfica en un estado activo y el código de activación al centro de verificación puede comprender almacenar la clave criptográfica en el código de activación en una base de datos accesible al centro de verificación. No se requiere ninguna transferencia de la clave criptográfica o del código de activación

El paso de proporcionar el código de activación al punto en la cadena de suministro preferiblemente comprende enviar el código de activación desde el centro de verificación al punto en la cadena de suministro.

El paso del punto en la cadena de suministro que transmite la información relacionada con la clave criptográfica recibida preferiblemente comprende enviar la información relacionada con la clave criptográfica recibida desde el punto en la cadena de suministro al centro de verificación.

Preferiblemente, el paso de proporcionar el código de activación al punto en la cadena de suministro en respuesta al punto en la cadena de suministro que transmite la información con relación a la clave criptográfica recibida constituye el registro del punto en la cadena de suministro. Preferiblemente, la información relacionada con la clave criptográfica recibida y el código de activación se transmiten por medio de un intercambio de par de claves asimétricas. En este caso, la clave criptográfica puede incluir un certificado criptográfico digital y el par claves asimétricas puede comprender una clave pública y una clave privada asociadas con el certificado criptográfico digital. El punto en la cadena de suministro puede proporcionar

información relacionada con la clave criptográfica recibida
codificada utilizando la clave pública del par de claves
asimétricas. Esto permite al receptor, por ejemplo, el centro
de verificación, descodificar la información relacionada con
5 la clave criptográfica recibida utilizando la clave privada
del par de claves asimétricas. La información relacionada con
la clave criptográfica recibida puede enviarse junto con la
información que identifica el punto en la cadena de
suministro, por ejemplo, el centro de producción. También
10 puede codificarse utilizando una clave pública del par de
claves asimétricas. De esta forma, una clave particular se
enlaza a un centro de producción particular u otro punto en
la cadena de suministro. El punto en la cadena de suministro
puede recibir el código de activación, por ejemplo, del
15 centro verificación, codificarse a través de la clave pública
del par de claves asimétricas. Esto permite que el punto de
la cadena de suministro descodifique el código de activación
utilizando la clave privada del par de claves asimétricas.

La información relacionada con la clave
20 criptográfica preferiblemente se almacena en una base de
datos accesible para el centro de verificación.
Preferiblemente, la información relacionada con la clave
criptográfica se almacena junto con la información que
identifica el punto en la cadena de suministro asociada con
25 la clave. Preferiblemente, la información que identifica el
punto en la cadena de suministro se almacena junto con la
clave criptográfica.

El paso de proporcionar la clave dinámica para cada
lote y artículos fabricados al centro de verificación puede
30 comprender enviar la clave dinámica desde el punto en la

cadena de suministro al centro de verificación. La clave dinámica puede enviarse a través de una conexión de Internet segura. Preferiblemente la clave dinámica para un lote de artículos fabricados se envía junto con la información relacionada con el lote de los artículos fabricados. Las claves dinámicas preferiblemente se almacenan en una base de datos accesible al centro de verificación. Preferiblemente, cada clave dinámica se almacena junto con la información acerca del lote asociado de los artículos fabricados.

La clave dinámica es simplemente cualquier pieza de información (por ejemplo, un número) que puede utilizarse en combinación con otros parámetros para formar un código. En una modalidad, la clave dinámica es un código secreto que se define a través de un lote particular de artículos. El código ID de artículo fabricado puede derivarse de la clave criptográfica en el estado activo y la clave dinámica puede ser cualquier número de mecanismos. En una modalidad, la clave dinámica y la clave criptográfica se combinan para formar un código de ruido pseudo-aleatorio que puede utilizarse como una firma digital para el código ID. El código de ruido puede derivarse adicionalmente del código ID mismo.

En una modalidad preferida, los códigos ID generados no se almacenan. Esto reduce las posibilidades de falsificaciones para acceder códigos ID válidos.

El método puede utilizarse para verificación de impuestos y el método además puede comprender reportar a una autoridad gubernamental el número de códigos ID marcados en los artículos fabricados; y el centro de verificación almacena la información que se conecta con los códigos ID

20

marcados en los artículos fabricados para la información específica de aquellos artículos fabricados tales como aquellos que pagaron o deben impuestos que pueden verificarse contra el número actual artículos fabricados.

5 De esta forma, el conteo de los códigos marcados en los artículos fabricados puede utilizarse para propósitos de verificación o recolección de impuestos. Es decir el conteo del número correcto actual de artículos fabricados marcados puede utilizarse para propósitos de verificación, o
10 recolección de impuestos. Esto proporciona medios enteramente electrónicos para que una autoridad gubernamental evalúe si ha sido pagada la cantidad correcta de impuestos. Por supuesto, el reporte puede ser para cualquier tercera parte interesada también, para verificación de impuestos, la
15 tercera parte usualmente comprenderá una autoridad gubernamental. La recolección de impuestos potencial, con base en el número de códigos ID reportados, puede compararse y reconciliarse con los impuestos actuales pagados, por ejemplo con base en las recepciones de impuestos actuales. El
20 centro de verificación puede administrarse a través de una parte confiable independiente del fabricante de los artículos fabricados. Por ejemplo, el centro de verificación puede administrarse a través de una autoridad gubernamental. Esto es particularmente ventajoso para la verificación de
25 impuestos.

El reporte puede llevarse a cabo por embarque o por depósito de impuestos al consumo tales como los impuestos pagados o que se deben, pueden verificarse o calcularse por embarque y por depósito de impuestos al consumo. Esto es
30 ventajoso porque, en muchas jurisdicciones el embarque de los

productos de un depósito de impuestos al consumo es el activador del pago de impuestos. El reporte puede llevarse a cabo solamente por embarque. El reporte puede llevarse solamente por depósito de impuestos al consumo. El reporte
5 puede llevarse a cabo para cualquier unidad deseada. El método puede además comprender calcular automáticamente los impuestos que se deben por embarque y por depósito de impuestos al consumo. El método además puede comprender automáticamente recolectar los impuestos que se deben por
10 embarque y por depósito de impuestos al consumo. El método puede comprender monitorear el pago de los impuestos que se deben por embarque y por depósito de impuestos al consumo.

El método puede utilizarse para verificación de impuestos y el método además puede comprender, antes del paso
15 de generar un código ID para cada artículo fabricado, el paso de que una autoridad gubernamental autorice el punto en la cadena de suministro para generar un número definido de códigos ID.

La autorización puede transmitirse desde la
20 autoridad gubernamental al punto en la cadena de suministro. Alternativamente, la autorización puede transmitirse desde la autoridad gubernamental a un portal de fabricación en comunicación con el punto en la cadena de suministro. La autorización puede transmitirse desde la autoridad
25 gubernamental a través de un canal de comunicación seguro. El canal de comunicación seguro puede dedicarse a la comunicación entre la autoridad gubernamental y el punto en la cadena de suministro o portal de fabricación.

Preferiblemente, el número definido de códigos ID
30 corresponde a un lote de artículos fabricados.

22

Preferiblemente, la autorización corresponde a un número definido de artículos fabricados que tienen restricciones en cuanto a impuestos comunes.

El método además puede comprender, antes del paso 5 de que la autoridad gubernamental autorice el punto en la cadena de suministro generar un número definido de códigos ID, el paso de solicitar la autorización de la autoridad gubernamental.

La solicitud puede transmitirse a la autoridad 10 gubernamental desde el punto en la cadena de suministro. Alternativamente, la solicitud puede transmitirse a la autoridad gubernamental desde un portal de fabricación en comunicación con el punto en la cadena de suministro. Preferiblemente, la solicitud se transmite a través de un 15 canal de comunicación seguro. El canal de comunicación puede dedicarse a la comunicación entre la autoridad gubernamental y ese punto en la cadena de suministro o portal de fabricación.

El método puede además comprender reportar a la 20 autoridad gubernamental el número de códigos ID marcados en los artículos fabricados.

El reporte puede llevarse a cabo a través del punto en la cadena de suministro. Alternativamente, el reporte puede llevarse a cabo a través de un portal de fabricación en 25 comunicación con el punto en la cadena de suministro. Este paso permite a la autoridad gubernamental verificar que el número actual de códigos ID marcados en los artículos fabricados cumple con el número definido de códigos ID autorizados por la autoridad gubernamental. El reporte 30 también puede ser para cualquier tercera parte interesada sin

embargo, para la verificación de impuestos, la tercera parte usualmente comprenderá una autoridad gubernamental. El centro de verificación puede almacenar información conectando los códigos ID marcados en los artículos „fabricados con información específica para esos artículos fabricados, tales como los impuestos pagados o que se deben que pueden verificarse contra el número actual o correcto de artículos fabricados. De esta forma, el conteo de los códigos ID marcados en los artículos fabricados puede utilizarse para propósitos de verificación de recolección de impuestos. Esto proporciona medios completamente electrónicos para que una autoridad gubernamental evalúe si se ha pagado la correcta cantidad de impuestos. El punto en la cadena de suministro también puede reportar a la autoridad gubernamental el índice de impuestos para cada artículo fabricado. Si el número definido de códigos ID corresponde a un lote de artículos fabricados, preferiblemente cada artículo fabricado en el lote de los artículos fabricados se asocia con un solo índice de impuestos.

El método además puede comprender un usuario que transmite el código ID marcado a un artículo fabricado seleccionado al centro de verificación; el centro de verificación, deriva del código ID, la información de impuestos relacionada con el artículo fabricado seleccionado; el centro de verificación transmite por lo menos algo de la información de impuestos relacionada con el artículo fabricado seleccionado al usuario. El usuario puede comprender una autoridad gubernamental u otro cuerpo oficial.

Utilizando el método de la invención para verificación de impuestos proporciona un número ventajas. Los

métodos y sistemas de la técnica anterior típicamente utilizan sellos fiscales o calcomanías fiscales para verificación de impuestos. Ambos están usualmente en la forma de etiquetas adhesivas directamente acopladas al empaque del consumidor en los artículos fabricados. La etiqueta adhesiva típicamente incluye características de seguridad visibles e invisibles. Los sellos de impuestos se utilizan para recolección de impuestos y la verificación del estado pagado del impuesto. Usualmente, los sellos fiscales llevan el valor del impuesto al consumidor actual que se debe en el artículo específico en el cual se aplica el sello fiscal. Las calcomanías fiscales también se utilizan para la recolección de impuestos y la verificación del estado pagado del impuesto pero esto usualmente es a través de la verificación del volumen de producción. En general, el número de calcomanías fiscales vendidas o enviadas al fabricante necesitará corresponder al número actual o correcto de artículos fabricados vendidos o distribuidos para ventas. Usualmente, las calcomanías fiscales no llevan un valor de impuesto al consumidor particular sino que el fabricante necesitará pagar un precio por calcomanía fiscal emitida.

A pesar de que existe una amplia creencia de que las calcomanías fiscales y los sellos de fiscales aún proporcionarán medios seguros y efectivos para proteger los ingresos por impuestos al consumo, los recientes desarrollos han demostrado que aún los sellos en papel más sofisticados han sido falsificados exitosamente. Tal falsificación solamente aumentará según la tecnología de la falsificación y las técnicas aumentan. Además, los sellos válidos pueden desviarse, por ejemplo, de un centro de fabricación

25

autorizado a otro centro de fabricación no autorizado. De esta forma, el sitio de fabricación no autorizado parece estar autorizado porque los sellos fiscales son válidos.

Utilizando el método de la invención para la
5 verificación de impuestos proporciona un número de ventajas. En primer lugar, no existe la necesidad de distribución de marcadores físicos (por ejemplo, etiquetas adhesivas), que podrían fácilmente interceptarse. Esto también da como resultado un menor impacto ambiental. En segundo lugar,
10 preferiblemente los códigos ID no se almacenan, lo cual reduce las posibilidades de falsificación para acceder códigos ID válidos. El método es extremadamente seguro para la falsificación y alteración de códigos válidos y para el robo de códigos. Esto también evita que los falsificadores
15 pirateen la base de datos de códigos ID válidos e inserten códigos no autorizados, de esta forma haciendo imposible distinguir entre códigos válidos e inválidos. En tercer lugar, comparado con otra tecnología de verificación de impuestos, el método de la invención no es costoso de
20 implementar, lo cual permite que se utilice más ampliamente que los sistemas existentes, particularmente para fabricantes de tamaño pequeño y medio. Además, muchos fabricantes ya están utilizando un sistema de códigos ID para identificar artículos fabricados. Tal sistema puede fácilmente adaptarse
25 para ser utilizado con el método de la invención para propósitos de verificación de impuestos. Finalmente, si se desea, los usuarios, las autoridades gubernamentales u otros terceros pueden fácilmente acceder la información de impuestos acerca de un artículo fabricado particular en
30 tiempo real. No se requiere de sistemas o entrenamiento

especializado y cualquier parte interesada como por ejemplo importadores, entidades de punto de venta y otros miembros de la cadena de suministro, pueden acceder la información de impuestos.

5 El centro de verificación puede administrarse a través de un tercero confiable independientemente del fabricante de los artículos fabricados. Por ejemplo, el centro de verificación puede administrarse a través de una autoridad gubernamental. Esto es particularmente ventajoso
10 para verificación de impuestos.

El método puede utilizarse para verificación de volumen de producción y el método además puede comprender reportar a un tercero el número de códigos ID marcados en los artículos fabricados.

15 La verificación del volumen de producción es la verificación de los volúmenes actuales producidos, por ejemplo, el número actual de artículos fabricados. El reporte puede llevarse a cabo a través del punto en la cadena de suministro. Alternativamente, el reporte puede llevarse a
20 cabo a través de un portal de fabricación en comunicación con el punto en la cadena de suministro. Preferiblemente, el reporte comprende reportar de manera segura, por ejemplo, sobre un canal de red segura. Preferiblemente, el centro de verificación almacena información que conecta los códigos ID
25 marcados en los artículos fabricados con la información específica de esos artículos fabricados. De esta forma, los códigos ID marcados en los artículos fabricados puede enlazarse a la información específica al número actual o correcto de artículos fabricados marcados. El número de
30 códigos ID marcados en los artículos fabricados puede

27

reportarse por nivel de impuestos, por unidad de tiempo o por Unidad de Identificación de Existencias (SKU, por sus siglas en inglés).

Esto permite al tercero verificar el número de artículos fabricados producidos y distribuidos. El reporte puede tomar lugar en periodos de tiempo regulares. El reporte no necesita tomar lugar inmediatamente después de que los artículos fabricados se marcan. El tercero puede ser una autoridad gubernamental u otro tercero que tiene interés en el número de artículos fabricados, por ejemplo fabricados en un centro de producción particular. El reporte puede comprender enviar los códigos ID marcados en los artículos fabricados a un tercero.

El reporte puede llevarse a cabo por embarque, o por depósito de impuestos de consumo, tal como los volúmenes de producción pueden verificarse o calcularse por embarque o por depósito de impuestos de consumo. Esto es ventajoso porque, en muchas jurisdicciones, el embarque de los productos de un depósito de impuestos al consumo se activa a través del pago de los impuestos, de tal forma que el volumen de los productos que salen de un depósito particular es crítico.

El uso del método de la invención para verificación de volumen de producción proporciona un número de ventajas. Por ejemplo, muchos fabricantes ya utilizan un sistema de códigos ID para identificar artículos fabricados. Tal sistema puede fácilmente adaptarse para ser utilizado con el método de la invención para propósitos de verificación de volumen de producción. Además, los volúmenes de producción pueden reportarse a un tercero, por ejemplo una autoridad

gubernamental, regularmente y en tiempo real.

El centro de verificación puede administrarse a través de un tercero independiente del fabricante de los artículos fabricados. Por ejemplo, el centro de verificación
5 puede administrarse a través de una autoridad gubernamental. Esto es particularmente ventajoso para la verificación del volumen de producción.

El método puede utilizarse para autenticar un artículo fabricado seleccionado y el método puede además
10 comprender: un usuario que transmite el código ID marcado en el artículo fabricado seleccionado al centro de verificación; el centro de verificación deriva del código ID, la clave criptográfica y la clave dinámica utilizada para generar el código ID; el centro de verificación deriva de la clave
15 criptográfica y la clave dinámica la información relacionada con el artículo fabricado seleccionado; y el centro de verificación transmite por lo menos algo de la información relacionada con el artículo fabricado seleccionado al usuario.

20 Esto permite al usuario verificar que el artículo fabricado seleccionado sea genuino. Esto también permite al usuario obtener información seleccionada acerca del artículo fabricado. La información puede incluir información con respecto al centro de producción o el sitio de fabricación
25 del artículo fabricado, información relacionada con el generador de códigos que generó el código ID en el artículo fabricado, información acerca del tiempo (por ejemplo, fecha, hora, minutos) de la producción y otra información que pueda estar asociada con el código ID. El usuario puede comprender
30 una autoridad gubernamental u otro cuerpo oficial, un

importador, una de punto de venta o un miembro de la cadena de suministro, y un consumidor final, o cualquier otra parte interesada.

Preferiblemente, la clave criptográfica se almacena
5 en una base de datos accesible al centro de verificación. Preferiblemente, la clave criptográfica se almacena junto con la información que identifica el punto en la cadena de suministro, por ejemplo, el centro de producción. En este caso, el paso del centro de verificación de derivar de clave
10 criptográfica la información relacionada con el artículo fabricado seleccionado puede comprender que el centro de verificación acceda a la base de datos y obtenga información que identifique el punto en la cadena de suministro asociada con la clave criptográfica.

15 Preferiblemente, la clave dinámica se almacena en una base de datos accesible al centro de verificación. Preferiblemente, la clave dinámica se almacena junto con la información acerca del lote asociado de artículos fabricados. En este caso, el paso del centro de verificación de derivar
20 de la clave dinámica la información relacionada con el artículo fabricado seleccionado puede comprender que el centro de verificación acceda a la base de datos y obtenga información acerca del lote de los artículos fabricados asociados con la clave dinámica. Si la clave dinámica y la
25 clave criptográfica se combinan para formar un código de ruido pseudo-aleatorio utilizado con una firma digital para el código ID, el código ID sin asignar puede derivarse del código ID digitalmente firmado. Entonces, el centro de verificación puede determinar la clave dinámica y la clave
30 criptográfica de la base de datos e independientemente

30

derivar el código de ruido para comparación con el código ID digitalmente firmado recibido.

El código ID transmitido desde el usuario al centro de verificación puede transmitirse a través de una conexión
5 de Internet segura o no segura. La información transmitida desde el centro de verificación al usuario puede transmitirse a través de una conexión de Internet segura o no segura.

El centro de verificación puede administrarse a través de un tercero independiente del fabricante de los
10 artículos fabricados. Por ejemplo, el centro de verificación puede administrarse a través de una autoridad gubernamental.

De acuerdo con la invención, también se proporciona un aparato para marcar artículos fabricados, que comprende:
un generador de claves para generar una clave criptográfica,
15 la clave criptográfica tiene un estado activo y un estado inactivo; por lo menos un punto en la cadena de suministro para los artículos fabricados, el generador de claves estando configurado para enviar la clave criptográfica, en el estado inactivo, al punto en la cadena de suministro, en donde el
20 punto en la cadena de suministro se configura para recibir, en respuesta al punto en la cadena de suministro que transmite la información relacionada con la clave criptográfica recibida, un código de activación para activar la clave criptográfica, el código de activación permite que
25 la clave criptográfica en el estado activo se active para formar la clave criptográfica en el estado activo; un centro de verificación para verificar las propiedades de los artículos fabricados, el generador de claves configurado para proporcionar una clave criptográfica en el estado activo, y
30 el código de activación al centro de verificación; un

generador de códigos, en el punto en la cadena de suministro, para generar un código de identificación (ID) para cada artículo fabricado, el código ID siendo derivado de la clave criptográfica en el estado activo y una clave generada para cada lote de artículos fabricados, en donde la clave dinámica para cada lote de artículos fabricados es provista al centro de verificación; un marcador en el punto en la cadena de suministro para marcar cada artículo fabricado con un código ID; y contador para contar el número de códigos ID marcados en los artículos fabricados.

El aparato es un aparato para marcar artículos fabricados, que puede utilizarse para verificación de impuestos (para artículos fabricados que se someten a tributación), para verificación de volumen de producción y para autenticación de los artículos fabricados. El número correcto o actual de artículos fabricados marcados se cuenta. Un código ID se marca en cada artículo fabricado, en tal forma que cada artículo fabricado puede identificarse singularmente.

El aparato además puede comprender una base de datos accesible a, o que forma parte del centro de verificación. La clave criptográfica puede almacenarse en la base de datos. La clave criptográfica puede almacenarse en la base de datos junto con la información que identifica el punto en la cadena de suministro asociada con la clave. La clave dinámica puede almacenarse en la base de datos. Cada clave dinámica puede almacenarse en la base de datos junto con la información acerca del lote asociado de artículos fabricados. El generador de claves puede formar parte del centro de verificación.

32

Además se describe con relación al método de la invención que también puede ser aplicable al aparato de la invención.

De acuerdo con la invención, también se proporciona
5 un método para marcar artículos fabricados, el método
utilizado para verificación de impuestos y comprende: generar
una pluralidad de códigos de identificación (ID) para los
artículos fabricados; marcar cada artículo fabricado con un
código ID de la pluralidad de códigos ID; contar el número
10 actual de códigos ID de la pluralidad de códigos ID marcados
en los artículos fabricados, en donde el número actual de
códigos ID es igual a o menor que la pluralidad de códigos
ID; reportar a una autoridad gubernamental el número actual
de códigos ID marcados en los artículos fabricados; y
15 almacenar la información que conecta los códigos ID marcados
con los artículos fabricados con la información específica de
esos artículos fabricados, tales como los impuestos pagados o
que se deben que pueden verificarse contra el número actual
de artículos marcados.

20 Los códigos ID pueden generarse y marcarse sobre
los artículos en cualquier punto en la cadena de suministro
para los artículos fabricados, por ejemplo, en un punto de
importación, un punto de distribución, un comprador, un
mayorista o cualquier otro enlace en la cadena de suministro.
25 Más preferiblemente, sin embargo, el punto en la cadena de
suministro en el cual se generan los códigos ID y se marcan
sobre los artículos fabricados comprende un centro de
producción o línea de producción para artículos fabricados.

El método además puede comprender, antes del paso
30 de generar una pluralidad de códigos ID para los artículos

fabricados: solicitar autorización de una autoridad gubernamental para generar códigos ID para los artículos fabricados; y recibir la autorización de la autoridad gubernamental para generar un número definido de códigos ID para los artículos fabricados.

El paso de solicitar autorización de una autoridad gubernamental puede comprender transmitir una solicitud de la autoridad gubernamental a través de un canal de comunicación seguro. La solicitud puede transmitirse desde cualquier punto en la cadena de suministro, por ejemplo un centro de producción. Alternativamente, la solicitud puede transmitirse desde un portal de fabricación en comunicación con el punto en la cadena de suministro. El canal de comunicación seguro puede dedicarse a la comunicación entre la autoridad gubernamental y el punto en la cadena de suministro o el portal de fabricación.

El paso de recibir la autorización de la autoridad gubernamental puede comprender recibir la autorización de la autoridad gubernamental a través de un canal de comunicación seguro. La autorización puede transmitirse a cualquier punto en la cadena de suministro. Alternativamente, la autorización puede transmitirse al portal de fabricación en comunicación con el punto en la cadena de suministro. El canal de comunicación seguro puede dedicarse a la comunicación entre la autoridad gubernamental y ese punto en la cadena de suministro o portal de fabricación. Preferiblemente, el número definido de códigos ID corresponde a un lote de artículos fabricados.

El paso de reportar a la autoridad gubernamental el número de códigos marcados en los artículos fabricados puede

34

comprender reportar a la autoridad gubernamental a través de un canal de comunicación seguro. El reporte puede llevarse a cabo a través de cualquier punto en la cadena de suministro para los artículos fabricados. Alternativamente, el reporte
5 puede llevarse a cabo a través de portal de fabricación en comunicación con un punto en la cadena de suministro. El canal de comunicación seguro puede dedicarse a la comunicación entre la autoridad gubernamental y ese punto en la cadena de suministro o portal de fabricación. Este paso
10 permite a la autoridad gubernamental verificar el número de códigos ID marcados en los artículos fabricados. La información que conecta los códigos ID marcados en los artículos fabricados con la información específica de esos artículos fabricados puede almacenarse, tal como los
15 impuestos pagados o que se deben, pueden verificarse contra el número actual o correcto de artículos fabricados. De esta forma, el conteo de los códigos ID marcados en los artículos fabricados puede utilizarse para propósitos de verificación o recolección de impuestos. Esto proporciona medios
20 completamente electrónicos para que una autoridad gubernamental evalúe si se ha pagado la correcta cantidad de impuestos. El índice de impuestos para cada artículo fabricado también puede reportarse a la autoridad gubernamental. Si el número actual de códigos ID corresponde
25 a un lote artículos fabricados, preferiblemente cada artículo fabricado en el lote de artículos fabricados está asociado con un solo índice de impuestos.

El método además puede comprender que un usuario transmita el código ID marcado en el artículo fabricado
30 seleccionado a un centro de verificación; el centro de

35

verificación deriva del código ID, información de impuesto relacionado con el artículo fabricado seleccionado; y el centro de verificación transmite por lo menos algo de la información de impuestos relacionada con el artículo fabricado seleccionado al usuario. El usuario puede comprender una autoridad gubernamental u otro cuerpo oficial. El centro de verificación puede administrarse a través de un tercero confiable independiente del fabricante de los artículos fabricados. Por ejemplo el centro de verificación puede administrarse a través de una autoridad gubernamental.

El método de este aspecto de la invención proporciona un número ventajas. Como ya explicó, los métodos y sistemas de la técnica anterior utilizan típicamente sellos fiscales o calcomanías fiscales para verificación de impuestos. A pesar de que existe una amplia creencia de que las calcomanías fiscales y los sellos fiscales aún proporcionan medios seguros y efectivos para proteger los ingresos de impuestos al consumo, los recientes desarrollos han demostrado que aún los sellos en papel más sofisticados han sido exitosamente falsificados. Tal falsificación solamente aumentará según la tecnología de la falsificación y el conocimiento aumenta. Además, los sellos válidos pueden desviarse, por ejemplo, de un centro de fabricación autorizado a otro centro de fabricación no autorizado.

El método de este aspecto de la invención proporciona un número de ventajas. En primer lugar, no existe la necesidad de distribución de marcadores físicos (por ejemplo, etiquetas adhesivas) que podrían fácilmente interceptarse. Esto también da como resultado un menor impacto ambiental. En segundo lugar, preferiblemente los

códigos ID no se almacenan, lo que reducen las posibilidades de que los falsificadores accedan a los códigos ID válidos. El método es extremadamente seguro para falsificación y alteración de códigos válidos y para el robo de códigos. En
5 tercer lugar, comparado con una alta tecnología de verificación de impuestos, el método de la invención no es costoso de implementar, lo cual permite que sea más ampliamente utilizado que los sistemas existentes, particularmente para fabricantes de tamaño pequeño y medio.
10 Además, muchos fabricantes ya están utilizando un sistema de códigos ID para identificar artículos fabricados. Tal sistema puede fácilmente adaptarse para ser utilizado con el método de la invención para propósitos de verificación de impuestos. Finalmente, si se desea, los usuarios, la autoridad
15 gubernamental u otras partes pueden fácilmente acceder la información de impuestos acerca de un artículo fabricado en particular en tiempo real. No se requieren sistemas o entrenamiento especializado y cualquier parte interesada, por ejemplo importadores, entidades de punto de venta y otros
20 miembros de la cadena de suministro, pueden acceder la información de impuestos.

En modalidad particular, el paso de generar la pluralidad de códigos ID para los artículos fabricados comprende generar los códigos ID de una clave criptográfica
25 en un estado activo y por lo menos clave dinámica, cada clave dinámica estando asociada de artículos fabricados. La clave criptográfica puede generarse en un generador de claves. La clave criptográfica en el estado activo puede ser provista al centro de verificación, junto un código de activación para
30 activar la clave criptográfica en un estado inactivo para

37

formar la clave criptográfica en el estado activo. La clave criptográfica en el estado inactivo puede ser provista al generador de código. El centro de verificación puede proporcionar el código de activación al generador de códigos en respuesta al generador de códigos que transmite la información con relación a la clave criptográfica recibida, por lo tanto registrando el generador de códigos para generación de códigos. Las claves criptográficas pueden almacenarse en una base de datos. Las claves dinámicas pueden almacenarse en una base de datos. Preferiblemente, los códigos ID no se almacenan.

Las características de un aspecto de la invención pueden aplicarse a otro aspecto de la invención. Además, las características descritas con relación a la verificación de impuestos puede aplicarse a la verificación del volumen de producción y la autenticación, las características descritas con relación a la verificación del volumen de producción pueden ser aplicables a la verificación de impuestos de la autenticación, y las características descritas con relación a la autenticación pueden ser aplicadas a la verificación de impuestos y a la verificación del volumen de producción.

Breve Descripción de las Figuras

Las modalidades de la invención ahora se describirán, a manera de ejemplo solamente, con referencia a las figuras anexas, en donde:

La Figura 1 es una vista esquemática de un sistema marcador de acuerdo con una modalidad de la invención;

La Figura 2 es un diagrama de flujo que muestra tres pasos del método de una modalidad de la invención que

puede llevarse a cabo en el sistema de la Figura 1;

La Figura 3 muestra un paso más del método de la Figura 2 cuando el sistema de la Figura 1 se utiliza para una primera modalidad de verificación de impuestos;

5 La Figura 4 muestra un paso más del método de la Figura 2 cuando el sistema de la Figura 1 se utiliza para una segunda modalidad de verificación de impuestos;

La Figura 5 muestra un paso más del método de la Figura 2 cuando el sistema de la Figura 1 se utiliza para
10 verificar un volumen de producción; y

La Figura 6 muestra un paso más del método de la Figura 2 cuando el sistema de la Figura 1 se utiliza para autenticar un artículo fabricado.

Descripción Detallada de la Invención

15 La Figura 1 es una vista esquemática de un sistema marcador de acuerdo con una modalidad de la invención. En esta modalidad, un sistema 101 comprende uno o más centros de producción 103, 105, 107 para producir artículos fabricados 109. Cada centro de producción puede comprender una línea de
20 producción o instalación que puede ser la fabricación de cigarrillos o una línea de empaque. Preferiblemente, la producción se lleva a cabo en lotes, cada lote estando dedicado a la producción de un cierto número de artículos fabricados individuales. Si existen uno o más centro de
25 producción, estos pueden estar físicamente localizados en el mismo o diferentes sitios de fabricación. En esta modalidad preferida, el sistema incluye centro de producción 103, 105, 107, pero la invención de hecho puede llevarse a cabo en cualquier punto de importación, un punto de distribución, un
30 comprador, un mayorista o cualquier otro punto en la cadena

de suministro.

Cada centro de producción incluye un generador de código 111 para generar códigos para los artículos fabricados 109. Preferiblemente, el generador de código 111 es una 5 computadora completamente autónoma o un micro-controlador dedicado a un centro de producción particular. En esta modalidad, cada centro de producción también incluye un marcador 113 para marcar los códigos generados sobre los artículos fabricados 109. El marcador 113 puede comprender 10 cualquier medio de marcación adecuado, por ejemplo, pero no limitándose a, una impresora de chorro de tinta continuo, una impresora de chorro de tinta de gota sobre demanda, una impresora holográfica, una impresora láser, o cualquier otra impresora o marcador que permita la impresión y marcación de 15 los códigos generados en artículos fabricados individuales. La impresión o marcación de los códigos generados puede ser en cada artículo, o un paquete externo, o en etiquetas, o en cualquier otra forma conveniente. En una modalidad, los códigos generados se imprimen en etiquetas o marbetes 20 adhesivos a ser aplicados a los artículos fabricados, preferiblemente de forma no removible. En una modalidad, los códigos generados se imprimen a través de un rayo láser en una capa de material sensible al láser depositado en el artículo fabricado o en el empaque del artículo. Este método 25 permite que un código sea impreso a través de una capa de envoltura transparente.

El sistema 101 además comprende un centro de verificación 114 que incluye un generador de claves 115 para generar claves 209, 211, para utilizarse en la marcación y 30 autenticación de los artículos fabricados y un servidor

central 117. En esta modalidad, el generador de código 111 puede comunicarse con el centro de verificación 114 a través de una conexión de Internet segura 119 y un servidor 121 local al centro de producción, o a través de otros medios de comunicación de datos. Alternativamente, el generador de códigos 111 podría comunicarse con el centro de verificación a través de un portal de fabricación de fabricación dedicado a uno o más centro de producción.

La Figura 2 es un diagrama de flujo que muestra tres pasos del método de una modalidad de la invención que pueden llevarse a cabo en el sistema 101 de la Figura 1. Haciendo referencia a las Figuras 1 y 2, en un primer paso 201 del método, el generador de claves 115 genera una clave criptográfica en la forma de una clave de máquina. El generador de claves 115 genera una versión no codificada de la clave de máquina y una versión codificada de la clave de máquina. La versión no codificada de la clave de máquina, conocida como la clave de máquina activa 209, se muestra como un borde sólido en las Figuras 1 y 2. La versión codificada de la clave de máquina, conocida como la clave de máquina inactiva 211 se muestra con un borde punteado en las Figuras 1 y 2. La clave de máquina activa 209, es decir la versión no codificada de la clave de máquina, se genera en el generador de claves 115 y por consiguiente es accesible al servidor central 117. Esto se muestra en ambas Figuras 1 y 2. El generador de claves 115 envía la clave de máquina inactiva 211 al generador de código 111 en el centro de producción 103, 105, 107. Esto se muestra en ambas Figuras 1 y 2.

La clave de máquina inactiva 211 puede enviarse desde el generador de claves 115 al generador de código 111

en un soporte de datos no volátil, por ejemplo, un CD-ROM, un DVD-ROM o un disco duro removible. El soporte de datos se transfiere físicamente al generador de código 111 en el centro de producción 103, 105, 107. Alternativamente, la
5 clave de máquina inactiva 211 puede enviarse desde el generador de claves 115 al generador de códigos 111 a través de una conexión de red segura, por ejemplo una que involucra la codificación. Esto puede ser en solicitud del generador de códigos 111. Esto asegura a la autenticidad, la
10 confidencialidad y la integridad de la clave de la máquina.

El generador de claves 115 también genera el código de activación 213, que comprende la clave o codificación para descodificar la clave de máquina inactiva 211 para formar la clave de máquina activa 209. Este código de activación 213
15 también es accesible al servidor central 117 y esto también se muestra en las Figuras 1 y 2. Preferiblemente, la clave de máquina activa 209 y el código de activación 213 se almacenan junto con la identificación del centro producción 103, 105, 107 al cual se asignaron.

20 En una modalidad, la clave de máquina comprende un número de porciones. La porción primaria puede ser una pluralidad de códigos secretos, por ejemplo, una matriz salina. Una matriz salina puede ser, por ejemplo, una larga cadena de dígitos aleatorios o pseudo-aleatorios de
25 caracteres. El número de porciones además puede incluir un identificador único para la clave de máquina, un código serializado que define cómo la clave de la máquina se va a combinar con una clave dinámica (explicado más adelante), un certificado criptográfico digital asociado con el
30 identificador único de la clave de la máquina y una política

o licencia de la clave de la máquina que contiene el certificado criptográfico digital generado anteriormente.

Preferiblemente, la clave de la máquina inactiva, es decir la versión codificada de la clave de la máquina, y particularmente la pluralidad de códigos secretos, se codifican utilizando una cifra fuerte. Un ejemplo de una cifra adecuada es la cifra de bloque Triple DES (siglas en inglés para Estándar de Codificación de Datos) en la cifra de bloques Triple DES/Rijandel. Ambas aplican el algoritmo de la cifra estándar de codificación de datos tres veces a cada bloque de datos y la Triple DES/Rijandel es una variación menor de la Triple DES que ha sido desarrollada por IBM. Este caso, la clave Triple DES o Triple Des/Rijandel comprenden el código de activación 213. De esta forma, en una modalidad preferida, la clave de máquina activa 209 está descodificada, la clave inactiva 211 se codifica utilizando la clave Triple DES o Triple Des/Rijandel, y el código de activación 213 comprende Triple DES o Triple Des/Rijandel.

En el siguiente paso 203, la clave de máquina inactiva 211 recibida por el generador de código se registra. Esto se hace a través del generador de código 111 que envía al centro de verificación 114 información 215 acerca de las claves de máquina recibida y cualquier información de máquina relevante (no mostrado). Preferiblemente se envía a través de una conexión de Internet segura 119, como se muestra en la Figura 1, pero puede enviarse a través de cualquier otra red adecuada. El centro de verificación 114 envía de regreso al generador de código 111 el código de activación 213. El código de activación 213 permite la clave de máquina inactiva 211 se active, y esto se muestra esquemáticamente en 217. El

código de activación 213 preferiblemente también se envía a través de una conexión de Internet segura 119, como se muestra en la Figura 1. El procedimiento de registro preferiblemente se configura de tal forma que la clave de máquina activa 209 nunca se transfiere a través del Internet.

El procedimiento de registro puede tomar la forma de un mecanismo de intercambio de un par de clave pública/privada convencional. Esto puede utilizar un par de claves asimétricas asociado con el certificado criptográfico digital que forma parte de clave de máquina, como se explica anteriormente. En este caso, la clave pública del par de claves asimétricas puede estar en la forma de una clave emitida por tercero, por ejemplo, una autoridad gubernamental. La información 215 acerca de la clave de material recibida que se envía desde el generador de código 111 al centro de verificación 114 puede comprender el identificador único para clave de máquina que forma parte de la clave de máquina, como se explica anteriormente. La información de la máquina relevante (no mostrada) que también se envía desde el generador de código 111 al centro de verificación 114 puede contener un identificador o certificado único para el generador de código 111 o centro de producción. Este identificador único puede incluir información acerca de la ubicación e identidad del generador de código o centro de producción, que ha sido pre-autorizado para la producción. Preferiblemente, el identificador único de clave de máquina y generador de código o el identificador de centro de producción se codifican utilizando la clave pública del par de claves asimétricas asociadas con el certificado de la clave de máquina.

Una vez que el centro de verificación 114 recibe el identificador único de la clave de máquina codificada y el identificador del generador de código o del centro de producción, el centro de verificación 114 puede codificar
5 utilizando la clave privada o un par de claves asimétricas asociadas en el certificado de la clave de máquina. El centro de verificación entonces puede verificar que el identificador único de la clave de máquina y el identificador del generador de código o el centro de producción sean válidos. Después, el
10 centro de verificación 114 envía de regreso al generador de códigos 111 el código de activación 213. Como ya se mencionó, preferiblemente, el código de activación 213 está en la forma de una cifra Triple DES o Triple DES/Rijandel. El centro de verificación codifica el codifica el código de activación
15 (por ejemplo, la cifra Triple DES o Triple DES/Rijandel) con la clave pública del par de claves asimétricas asociadas con el certificado de la clave de máquina. Esto permite que el código de activación (por ejemplo, la cifra Triple DES o Triple DES/Rijandel) a ser descodificada por el generador de
20 código utilizando la clave privada del par claves asimétricas asociadas con el certificado de la clave de máquina. Después, la clave de máquina inactiva 211 puede activarse utilizando el código de activación descodificado 213 con el fin de formar la clave de máquina activa 209.

25 Una vez que la clave de máquina inactiva 211 en el generador de código 111 ha sido activada, el centro de producción es capaz de fabricar artículos y producir códigos para los artículos fabricados en el generador de códigos 111. Como se muestra en el siguiente paso 205, el generador de
30 códigos 111 tiene una clave dinámica 219 por lote de

artículos fabricados. La clave dinámica 209 es preferiblemente un código secreto dinámico aleatorio. El generador de códigos utilizado la clave dinámica 219 para un lote, junto con la clave de máquina 209, para generar códigos 5 221 (por ejemplo, códigos alfa-numéricos) para los artículos fabricados en ese lote. Como se mencionó previamente, el mecanismo particular para combinar la clave dinámica 219 para un lote con clave de máquina activa 209 se define en código serializado que forma parte de la clave de máquina. Los 10 códigos 221 pueden marcarse de los artículos a través del marcador 113. Solamente un código de marca en cada artículo fabricado 109. El generador de código 111 o centro de producción 103, 105, 107 mantiene un conteo 223 de los códigos que se marcan sobre los artículos fabricados.

15 Además, el generador de códigos 111 envía la clave dinámica 219 para cada lote, junto con la información acerca del lote (no mostrado) al centro de verificación 114. Esto puede llevarse a cabo a través de una conexión de Internet segura 119. La información acerca del lote puede incluir 20 viaria información, por ejemplo, pero no limitándose a la marca, el mercado previsto o el destino previsto. La clave dinámica 219 no necesita enviarse al centro de verificación 114 en tiempo real y pueden comunicarse al centro de verificación en cualquier tiempo apropiado, por ejemplo, 25 mensualmente. Las claves dinámicas 219 enviadas al centro de verificación 114 se almacenan en una base de datos (por ejemplo, en el servidor central 117) en o en una forma accesible para el centro de verificación 114. La clave dinámica 219 para cada lote preferiblemente se almacena junto 30 con la información de lotes enviada al centro de verificación

114 al mismo tiempo.

Como ya se explicó, el mecanismo particular para combinar la clave dinámica 219 para un lote con la clave de máquina activa 209 se define en el código serializado que forma parte de la clave de máquina. En una modalidad, la clave dinámica 219 y la clave de máquina activa 209 se combinan por el generador de códigos para formar un código de ruido pseudo-aleatorio que es seguro de ataque criptográfico. El código de ruido no permite la reconstrucción de la clave dinámica 219 y la clave de máquina activa 209 del código de ruido. Una variedad de técnicas conocidas están disponibles para generar el código de ruido, incluyendo, pero no limitándose a, sustitución de tabla, indexación, resumen criptográfico y sus variaciones. El código de ruido preferiblemente se utiliza con una firma digital para el código ID. El código de ruido puede derivarse del código ID mismo. La clave dinámica 219 y la clave de máquina activa 209 son conocidas solamente por el centro de verificación 114 y el generador de código 111.

Preferiblemente, la clave de máquina activa 209 se elimina cuando el generador de código 111 en un centro de producción particular 103, 105, 107 está fuera de servicio. Esto evita que un usuario malicioso gane acceso a la clave de máquina activa 209 sin un registro apropiado. Los medios adicionales para deshabilitar el generador de código 111 y evitar el uso no autorizado del generador de código 111 y el centro de producción pueden ser provistos.

La Figura 3 muestra un paso más 207 del método de la Figura 2 cuando el sistema de la Figura 1 se utiliza para una primera modalidad de verificación de impuestos. En este

caso, los pasos del método se llevan a cabo en el orden 201, 203, 205, 207. Los volúmenes de producción, por ejemplo el número de artículos producidos en cada lote de producción para cada centro de producción, así los datos de producción estadísticos por marca o mercado previsto, pueden obtenerse y almacenarse. Tal información del volumen de producción puede utilizarse para verificar la recolección de impuestos. El sistema puede utilizarse más bien, o además de, un sistema convencional de timbres fiscales o calcomanías fiscales para permitir la verificación del estado de los impuestos pagados, para proteger los ingresos por impuestos al consumo y para evitar la falsificación de los ellos fiscales o de las calcomanías fiscales.

En el tercer paso 205 del método de la Figura 2, el generador de códigos 111 o el centro de producción 103, 105, 107 mantienen un conteo 223 de los códigos que se marcan sobre los artículos fabricados durante el proceso de producción. El conteo puede hacerse a través del generador de códigos 111 y un marcador 113 en cada centro de producción o en otra ubicación apropiada. Si el centro de producción incluye un sensor para detectar los códigos ID marcados en los artículos fabricados, el sensor puede llevar a cabo el conteo. Esto produce el número exacto de códigos 221 que se imprimieron o marcaron y este conteo 223 puede reportarse a un tercero, por ejemplo, una autoridad gubernamental 301. Esto se muestra en las Figuras 1 y 3.

El índice de impuestos para cada artículo fabricado puede enviarse a la autoridad gubernamental 301, u otra parte relevante, junto con el conteo 223. Los impuestos que se deben después pueden calcularse multiplicando todos los códigos

28

impresos asociados con un índice de impuestos específicos por el índice de impuestos mismos. Esto permite a la autoridad gubernamental verificar o calcular los impuestos que se deben o los impuestos que ya se pagaron. El sistema también puede
5 utilizarse con diferentes índices de impuestos si se desea, en cuyo caso los índices pueden capturarse como parte de la información de lotes antes de la producción de un lote de artículos. Preferiblemente, el centro de verificación 114 almacena la información que se conecta a los códigos ID
10 marcados con el número actual o correcto de artículos fabricados a la información específica de los artículos fabricados marcados. Después los impuestos pagados o que se deben pueden verificarse contra los artículos fabricados. El centro de verificación 114 puede administrarse a tercero
15 confiable, por ejemplo, la autoridad gubernamental misma.

La información del volumen de producción que se reporta a la autoridad gubernamental 301 puede reportar por embarque o por depósito de impuestos al consumo o por embarque y por depósitos de impuesto al consumo. En la información del
20 volumen de producción puede reportarse por categorías tales como por volumen por SKU (siglas en inglés para número de identificación de existencia), volumen por precio al por menor, volumen por producción doméstica, volumen por producción de exportación, volumen sin impuestos. La
25 información del volumen de la producción puede reportarse periódicamente, por ejemplo, cada mes, o en cualquier otro tiempo apropiado.

En algunos casos, la autoridad gubernamental 301 u otra parte, pueden presentar una solicitud al centro de
30 verificación 114 para obtener información de la producción,

tal como el volumen de producción. En este caso, el centro de verificación 114 puede ser mantenido por un tercero confiable independiente del productor de los artículos fabricados. El centro de verificación 114, en respuesta a tal solicitud, después obtener los datos de los centros de producción relevantes 103, 105, 107. Esto puede permitir a las autoridades gubernamentales verificar los volúmenes de producción declarados.

Una de las ventajas de la modalidad de la Figura 3 es que no se requiere autorización preliminar para cada lote de artículos fabricados. Mientras el centro de producción o generador de códigos particular se registre con la autoridad gubernamental, el generador de códigos puede simplemente producir tanto códigos como se requiera. Después, el número actual o corrector de códigos utilizados puede reportarse una vez que los artículos han sido fabricados y marcados.

La Figura 4 muestra un paso más del método de la Figura 2 cuando el sistema de la Figura 1 se utiliza para una segunda modalidad de verificación de impuestos. En este caso, el paso 204 mostrado en la Figura 4 se lleva a cabo antes del paso 205, ya sea después o en paralelo con los pasos 201 y 203. El sistema puede utilizarse en lugar de, o además de, un sistema convencional de sellos fiscales o calcomanías fiscales para permitir la verificación del estado de los impuestos pagados para proteger los ingresos o impuestos al consumo y para evitar la falsificación de los sellos fiscales o calcomanías fiscales.

En el paso 204, el generador de códigos 111 y el marcador 113 en cada centro de producción solicitan la autorización de una autoridad gubernamental 301 para generar

9

un número definido de códigos ID. Esto se muestra esquemáticamente en 403. Alternativamente, la solicitud puede enviarse desde un portal de fabricación dedicado a uno a más de los centros de producción. En respuesta, la autoridad gubernamental 301 autoriza al centro de producción a generar un número definidos de códigos ID. Esto se muestra esquemáticamente en 405.

Preferiblemente, la solicitud 403 activa el pago para la cantidad de códigos ID ordenados. La autorización por consiguiente puede indicar un estado de impuestos pagados. El centro de producción es solamente elegible para fabricar artículos y producir códigos para los artículos fabricados en el generador de códigos 111 una vez que se recibe la autorización. Se puede enviar una solicitud para cada lote de producción de artículos fabricados. Preferiblemente, todos los artículos fabricados en el lote tienen el mismo índice de impuestos asociado.

El paso de la Figura 4 puede combinarse con el reporte a la autoridad gubernamental del número actual o correcto de códigos ID marcados en los artículos fabricados, como se describe con relación a la Figura 3. Esto puede proporcionar confirmación del volumen de producción.

La Figura 5 muestra un paso más 208 del método de la Figura 2 cuando el sistema de la Figura 1 se utiliza para verificar un volumen de producción. En este caso, los pasos del método se llevan a cabo en el orden 201, 203, 205, 208. Los volúmenes de producción, por ejemplo el número de artículos producidos en cada lote de producción a través de cada centro de producción, así como los datos de producción estadística por marca o por mercado previsto, pueden obtenerse

51

y almacenarse. Tal información del volumen de producción puede utilizarse para la administración de la producción o para propósitos oficiales, y puede estar disponibles para usuarios seleccionados.

5 En el tercer paso 205 del método de la Figura 2, el generador de códigos 111 o el centro de producción 103, 105, 107 mantienen el conteo 223 de los códigos que se marcan sobre los artículos fabricados durante de producción. El conteo puede hacerse a través del generador de códigos 111 y el
10 marcador 113 en cada centro de producción o en otra ubicación apropiada. Si el centro de producción incluye un sensor para detectar los códigos ID marcados en los artículos fabricados, el sensor puede llevar a cabo el conteo. Esto produce el número exacto de códigos 221 que se imprimieron o marcaron.
15 Como se muestra en la Figura 5, el cuarto paso 208 del método para la verificación del volumen de producción es reportar el conteo 223 a una parte interesada, por ejemplo una autoridad gubernamental 301. Esto se muestra en las Figuras 1 y 5.

 Preferiblemente, el centro de verificación 114
20 almacena información que conecta los códigos ID marcados en los artículos fabricados con la información específica de los artículos fabricados marcados. En algunos casos, la autoridad gubernamental 301 u otro tercero pueden presentar una solicitud al centro de verificación 114 para obtener
25 información sobre la producción, tal como el volumen de producción. En este caso, el centro de verificación 114 puede ser mantenido por una parte tercera confiable independiente del productor de los artículos fabricados. El centro de verificación 114, en respuesta a tal solicitud, entonces puede
30 obtener los datos de los centros de producción relevantes 103,

105, 107. Esto puede permitir a las autoridades gubernamentales verificarlos volúmenes de producción declarados.

La información de volumen de producción que se
5 reporta a la autoridad gubernamental 301 puede reportarse por
embarque o por depósito de impuestos al consumo o por embarque
y por depósito de impuestos al consumo. La información del
volumen de producción puede reportarse por categoría tal como
volumen por SKU (número de identificación de existencia),
10 volumen por precio al por menor, volumen por producción
doméstica, volumen por producción de exportación, volumen por
producción sin impuestos (si los artículos fabricados se
someten a impuestos especiales). La información del volumen de
producción puede reportarse periódicamente, por ejemplo, cada
15 mes o en cualquier tiempo apropiado.

La Figura 6 muestra un paso más 210 del método de la
Figura 2 cuando el sistema de la Figura 1 se utiliza para
autenticar un artículo fabricado. En este caso, los pasos
del método se llevan a cabo en el orden: 201, 203, 205, 210.
20 En el paso 210, cuando el usuario 601 desea autenticar un
artículo fabricado individual, el usuario envía el código 221
en el artículo al centro de verificación 114. Esto se muestra
en las Figuras 1 y 6. El usuario 601 puede enviar el código al
centro de verificación 114 a través de cualquier medio
25 adecuado tal como una conexión de Internet segura o no segura.
A partir del código 221, el centro de verificación 114 puede
derivar la clave dinámica 119 y la clave de máquina activa 219
utilizada para generar el código 221. Esto se hace a través
de invertir el proceso utilizado para generar el código 221 en
30 el paso 205.

Por ejemplo, si la clave dinámica 219 y la clave de máquina activa 209 se combinan para formar un código de ruido pseudo-aleatorio cuando se utiliza como una firma digital para el código ID, el centro de verificación puede derivar el
5 código ID no asignado del código ID digitalmente asignado. Después, el centro de verificación 114 puede independientemente derivar la clave dinámica 219 y la clave de máquina activa 209 de la información relacionada por el código ID y verificar esto contra el código de ruido recibido.

10 De la clave de máquina activa derivada 209, el centro de producción 103, 105, 107, en el cual el artículo fue fabricado puede determinarse, ya que las claves de máquina activas preferiblemente se almacenan en la base de datos junto con los detalles de sus centros de producción asociados. De
15 clave dinámica derivada 219, la información de lotes para el artículo puede determinarse ya que las claves dinámicas preferiblemente se almacenan en la base de datos junto con la información de lote asociada. De esta forma, el centro de verificación 114 puede derivar, del código 221 enviado del
20 usuario 601, para información 603 acerca del artículo individual. Esto se muestra esquemáticamente en la Figura 6. El centro de verificación también puede experimentar verificaciones de que los varios parámetros (por ejemplo, la máquina activa, la clave dinámica, la información de lotes)
25 tengan valores válidos. Después todos, o porciones seleccionadas de, la información 603 pueden enviarse al usuario 601. Esto se muestra en las Figuras 1 y 6. La información 603 preferiblemente se envía al usuario 601 a través de los mismos medios que envió el código original.

30 Un usuario privilegiado, por ejemplo, un empleado



del fabricante o de una autoridad gubernamental puede recibir información privilegiada adicional no disponible para un usuario genérico. Tal información privilegiada puede incluir información del volumen de producción, información estadística
5 relacionada con centro de producción o acceso al centro de verificación, la fecha expiración, información de garantía, rutas de importación, etc.

Las modalidades descritas proporcionan un método y sistemas mejorados para marcar artículos fabricados, que
10 pueden utilizarse para verificación de impuestos como se muestra en las Figuras 3 y 4, para verificación del volumen de producción como se muestra en la Figura 5 y para la autenticación de artículos fabricados como se muestra en la Figura 6.

15

5-5

RESUMEN DE LA INVENCION

Se proporciona un método y aparato para marcar artículos fabricados. El método comprende proporcionar una clave criptográfica, en un estado inactivo, a un punto en la cadena de suministro, para los artículos fabricados, proporcionar la clave criptográfica, en un estado activo, y un código de activación para activar la clave criptográfica, para un centro de verificación, y proporcionar el código de activación al punto en la cadena de suministro en respuesta al punto en la cadena de suministro que transmite información relacionada con la clave criptográfica recibida. El código de activación permite que la clave criptográfica en el estado inactivo se active para formar la clave criptográfica en el estado activo. El método además comprende generar, en el punto de la cadena de suministro, un código de identificación (ID) para cada artículo fabricado. El código ID se deriva de la clave criptográfica en el estado activo y una clave dinámica generada para cada lote de artículos fabricados. El método además comprende proporcionar la clave dinámica para cada lote de artículos fabricados al centro de verificación, marcando cada artículo fabricado con el código ID, y contando el número actual o correcto de códigos ID marcados en los artículos fabricados. El método y aparato pueden utilizarse para verificación de impuestos (para productos sujetos a tributación), verificación del volumen de producción y autenticación.

56