(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 728 680**

(51) Int. CI.:

G05B 19/418 (2006.01)
G06F 9/445 (2008.01)
G06F 21/30 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **31.01.2015 E 15153386 (6)**

(97) Fecha y número de publicación de la concesión europea: **06.03.2019 EP 3051372**

(54) Título: **Identificación y verificación seguras de productos**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.10.2019

(73) Titular/es:

INEXTO SA (100.0%)
Avenue Edouard-Dapples 7
1006 Lausanne, CH

(72) Inventor/es:

BORLET-HOTE, ALAIN LAURENT ROBERT;
FRADET, ERWAN y
GAUTHIER, YANNICK GEORGES CHARLES

(74) Agente/Representante:

CURELL SUÑOL, S.L.P.

DESCRIPCIÓN

Identificación y verificación seguras de productos.

La presente invención se refiere, en general, a técnicas para marcar productos con códigos de identificación seguros y para la verificación de dichos códigos, y se refiere, más particularmente, a sistemas y métodos para gestionar la distribución de instrucciones seguras de configuración de producción y para generar identificadores de producto seguros.

Los métodos existentes para la identificación de productos conllevan, típicamente, la aplicación de un identificador exclusivo a un producto en el momento de su envasado. El documento US-2013/226326 describe un sistema de gestión de procesado de lentes. Estos sistemas no se ajustan eficientemente a escala en organizaciones que disponen de múltiples instalaciones de producción, o en líneas de producción con capacidad de envasado a una velocidad muy alta. Adicionalmente, los métodos de identificadores existentes no son suficientemente seguros ya que no están asociados a instrucciones seguras de configuración de producción y no llevan información adicional de producto beneficiosa para las autoridades reguladoras y los comerciantes.

Existe una necesidad de un método y un aparato mejorados para controlar y autorizar de manera segura la producción de artículos fabricados, así como para marcar artículos fabricados con identificadores de productos seguros, particularmente uno que se pueda usar para la verificación de impuestos, la verificación de volúmenes de producción y la autenticación de artículos fabricados.

Se proporciona un método para inicializar un proceso destinado a controlar de manera segura una instalación de producción según la reivindicación 1.

En un aspecto de la divulgación, se proporciona un método para autenticar una producción de productos, incluyendo el método almacenar electrónicamente los datos de configuración para una tirada de producción, especificando los datos de configuración para la tirada de producción unos parámetros usados en la producción de productos; determinar si los datos de configuración para la tirada de producción están autorizados; si la tirada de producción está autorizada: generar un testigo de seguridad y asociar el testigo a los datos de configuración; y firmar digitalmente los datos de configuración generando una firma digital y asociando la firma digital a los datos de configuración; recibir los datos de configuración firmados digitalmente y la firma digital en una máquina de producción; en la máquina de producción, verificar la firma digital asociada a los datos de configuración firmados digitalmente; calcular un conjunto de identificadores de productos seguros sobre la base de los datos de configuración firmados digitalmente; producir unos productos en una tirada de producción según los datos de configuración firmados digitalmente; e imprimir el conjunto de identificadores de productos seguros en los productos según los datos de configuración firmados digitalmente.

En la descripción sucesiva de formas de realización, se hace referencia a los dibujos adjuntos que forman parte de las mismas, los cuales muestran, a título ilustrativo, formas de realización específicas de la materia en cuestión reivindicada. Debe entenderse que pueden usarse otras formas de realización, y que pueden realizarse cambios o modificaciones, tales como cambios estructurales. Dichas formas de realización, cambios o modificaciones no constituyen necesariamente desviaciones del alcance con respecto a la materia en cuestión reivindicada pretendida. Aunque las etapas posteriores se pueden presentar en un cierto orden, en algunos casos la ordenación se puede cambiar de manera que ciertas entradas se proporcionen en momentos diferentes o en un orden diferente sin cambiar la función de los sistemas y métodos descritos. No es necesario que los diversos cálculos que se describen posteriormente, tales como aquellos que se encuentran dentro de los procedimientos de inicialización, generación y autenticación de código, se lleven a cabo en el orden dado a conocer, y podrían implementarse fácilmente otras formas de realización que usen ordenaciones alternativas de los cálculos. Además de su reordenación, los cálculos también se podrían descomponer en subcálculos con los mismos resultados.

Tal como se usa en la presente invención, entidad puede referirse a: i) una persona, tal como un consumidor de un producto; ii) un grupo, tal como un grupo que tenga un interés común, tal como minoristas; iii) un dispositivo informático; iv) un nodo informático en un sistema en red; v) una ubicación de almacenamiento, tal como una unidad de almacenamiento de memoria que almacena un documento; vi) un punto virtual en una red, tal por ejemplo que represente una función comercial dentro de una impresa, y similares. Adicionalmente, una entidad puede representar un punto en un flujo de trabajo, por ejemplo, para autorización, que puede ser llevada a cabo por una persona responsable de ese aspecto del flujo de trabajo o un dispositivo informático que proporcione un procesado automatizado. El término entidad no está destinado a limitarse a uno cualquiera de estos ejemplos y puede extenderse a otras situaciones congruentes con los conceptos que se describen en la presente.

A continuación, se describirán formas de realización de la invención, únicamente a título de ejemplo, haciendo referencia a los dibujos adjuntos, en los cuales:

la figura 1 ilustra un método de ejemplo para la inicialización de código.

La figura 2 ilustra un método de ejemplo para la generación de código.

La figura 3 ilustra un método de ejemplo para la autorización de código.

Módulos del sistema

A continuación, se describen varios módulos. Cualesquiera de los módulos pueden estar ubicados conjuntamente de manera física, o pueden estar ubicados remotamente uno con respecto a otro. Adicionalmente, cualesquiera de los módulos se podrían combinar en términos lógicos o físicos, en un módulo único, sin desviarse con respecto al alcance de la invención.

Módulo de control

Haciendo referencia a la figura 1, el Módulo de Control (conocido también como “Orquestador”) (110) puede recibir entradas de cualesquiera de los otros módulos o fuentes exteriores, y puede proporcionar instrucciones a los otros módulos del sistema sobre la base de programas preconfigurados y/o las entradas de operarios en el mismo. También puede generar un resumen de panel de control del estado del sistema.

La entrada para el Módulo de Control puede incluir cualesquiera o la totalidad de los datos de configuración (105). Los datos de configuración suministrados pueden indicar cualesquiera o la totalidad de los parámetros incluyendo, aunque sin carácter limitativo, la máquina correspondiente a la producción, la línea de producción, la fábrica, el producto que se debe producir, y el volumen de producto. Los datos de configuración pueden indicar qué artículos (por ejemplo, productos) se van a marcar con los identificadores seguros, y cómo pueden producirse esos artículos. Los datos de configuración pueden indicar un intervalo de productos, tales como identificadores de producto de inicio y finales. En algunas formas de realización, el intervalo puede ser un conjunto de identificadores de producto. Los datos de configuración pueden ser proporcionados por un operario del sistema o se pueden generar de manera dinámica o automática. Los datos de configuración pueden incluir, además, instrucciones ejecutables o un algoritmo interpretable. Los datos de configuración se pueden basar en entradas del operario o la salida de un sistema de ejecución de fabricación, u otro sistema centralizado destinado a ordenar cómo y qué producir.

El Módulo de Control (110) puede transmitir los datos de configuración a cualquier módulo, incluyendo, aunque sin carácter limitativo, al Módulo de Autorización (130), al Módulo de Identificación (140) y al Módulo de Firma (145).

El Módulo de Control puede solicitar autorización del Módulo de Autorización para ejecutar una operación de producción. Este proceso conlleva transmitir una solicitud (que incluye parte o la totalidad de los datos de configuración) al Módulo de Autorización, y recibir datos de configuración firmados o cifrados. En algunas formas de realización, el Módulo de Autorización puede devolver los datos de configuración al Módulo de Control, incluyendo una firma digital aplicada a esos datos de configuración. El Módulo de Autorización determina si autorizar la solicitud del Módulo de Control sobre la base de los datos que recibe. Adicionalmente, la información devuelta por el Módulo de Autorización incluida en los Datos de Configuración se puede usar para delimitar los códigos generados con la autorización proporcionada. Puesto que los datos son firmados por el Módulo de Autorización, se puede evitar que el sistema modifique los datos de configuración. Como ejemplo no limitativo, se puede controlar, permitir o denegar una modificación de una solicitud para producir una marca en lugar de otra.

Las autorizaciones recibidas del Módulo de Autorización también se pueden transmitir al Módulo de Verificación de manera que, posteriormente, solicitudes de verificación se pueden procesar con respecto a esas autorizaciones. Los datos transmitidos al Módulo de Verificación pueden incluir un identificador seguro, así como cualesquiera de los datos de configuración. En algunos ejemplos, los datos de configuración enviados al Módulo de Autorización pueden incluir información de intervalo de productos.

Los datos de configuración firmados o validados pueden ser la parte o la totalidad del conjunto de parámetros de entrada del Módulo de Control, verificados y validados por el Módulo de Autorización, que permanece en vigor durante una producción. Un testigo de seguridad puede ser una salida del Módulo de Autorización y/o un parámetro de entrada del Módulo de Control. El testigo de seguridad puede ser una prueba de que el identificador de producto se corresponde con datos de configuración validados y, por lo tanto, con una producción autorizada. El testigo de seguridad puede ser una entrada para el Módulo de Firma con el fin de generar una firma para un identificador de producto individual, o la firma de un identificador de producto individual, o un identificador de producto en sí mismo, o un intervalo de productos o identificadores de producto. El testigo de seguridad puede ser un código exclusivo, un código aleatorio, o un código seudoaleatorio. El testigo de seguridad puede ser cualquier carácter numérico, o alfabético, o combinación de caracteres numéricos y alfabéticos.

Módulo de autorización

El Módulo de Autorización funciona de manera que valida solicitudes de autorización con el fin de realizar una acción en el sistema de identificación. En algunas formas de realización, puede funcionar como un administrador de licencias.

El Módulo de Autorización puede recibir los datos de configuración. El Módulo de Autorización también puede recibir información de intervalo y/o algoritmo. En algunas formas de realización, el Módulo de Autorización puede recibir datos de configuración de entrada del Módulo de Control. El intervalo de salida puede identificar, opcionalmente, un intervalo de productos, máquinas, fábricas, intervalos o volúmenes de producto que están autorizados. La salida también puede incluir información de intervalo y/o puede incluir un algoritmo que comprende un conjunto de instrucciones ejecutables o interpretables que se usarán para generar el testigo de seguridad. El Módulo de Autorización puede estar centralizado a nivel de fábrica o puede estar descentralizado en cada línea de producción, o una combinación de ambas opciones.

El Módulo de Autorización puede almacenar y/o generar una o más claves de cifrado. En algunas formas de realización, la clave almacenada por el Módulo de Autorización puede ser una clave de cifrado privada pública de acuerdo con una infraestructura de clave pública (PKI). En algunas formas de realización, el Módulo de Autorización almacena la única copia de la clave privada. En otras formas de realización, el Módulo de Autorización se distribuye sobre varias instancias que reproducen las claves entre ellas. En el caso de la PKI, el Módulo de Autorización puede dar salida a datos de configuración firmados. En algunas formas de realización, el Módulo de Autorización puede cifrar los datos de configuración y/o firmar la salida de datos de configuración.

En algunas formas de realización, el sistema está configurado de manera que solamente el Módulo de Autorización puede leer los parámetros de entrada protegidos del Módulo de Control, requeridos para la generación del testigo de seguridad. En algunas formas de realización, la clave se proporciona al Módulo de Autorización desde otra fuente.

El Módulo de Autorización se puede materializar en forma de un módulo de seguridad de *hardware* (HSM), u otro tipo de dispositivo informático físico que salvaguarde y gestione claves digitales para una autenticación fuerte y que proporciona procesado criptográfico. La funcionalidad del Módulo de Autorización la puede realizar un ordenador con una placa incorporada, con una clave de cifrado o clave privada PKI. El módulo puede estar equipado con características tales que intentos de acceder a los datos den como resultado que el mismo se vuelva ilegible o inaccesible.

Si la entrada para el Módulo de Autorización es un intervalo y un algoritmo, el Módulo de Autorización puede dar salida a una identidad en el intervalo de autorización y un testigo de seguridad del identificador. Por ejemplo, la identidad de salida puede ser un intervalo de 0 a 1.000 con un testigo de seguridad para cada artículo del intervalo.

El Módulo de Autorización puede generar una clave a partir de cualquier parámetro usado en el Módulo de Control. En algunas formas de realización, el Módulo de Autorización puede generar u obtener una clave a partir de una clave existente de cualquier parámetro usado en el Módulo de Control de tal manera que solamente un Módulo de Autorización específico pueda usar esta clave. El equipo y el *software* que implementan esta técnica de clave pública se pueden materializar en un criptosistema asimétrico.

La salida del Módulo de Autorización puede ser información, tal como los datos de configuración y, opcionalmente, uno o más testigos de seguridad, con una firma digital proporcionada por el Módulo de Seguridad. Alternativamente, la salida del Módulo de Autorización puede ser los datos de configuración cifrados para una clave poseída por el Módulo de Autorización. La salida del Módulo de Autorización se puede proporcionar al Módulo de Control.

Según una forma de realización, el método para autenticar una producción de productos incluye almacenar electrónicamente datos de configuración para una tirada de producción, especificando los datos de configuración para la tirada de producción unos parámetros usados en la producción de productos; determinar si los datos de configuración para la tirada de producción están autorizados; si la tirada de producción está autorizada: generar un testigo de seguridad y asociar el testigo a los datos de configuración; y firmar digitalmente los datos de configuración generando una firma digital y asociando la firma digital a los datos de configuración; recibir los datos de configuración firmados digitalmente y la firma digital en una máquina de producción; en la máquina de producción, verificar la firma digital asociada a los datos de configuración firmados digitalmente; calcular un conjunto de identificadores de productos seguros sobre la base de los datos de configuración firmados digitalmente; producir unos productos en una tirada de producción según los datos de configuración firmados digitalmente; e imprimir el conjunto de identificadores de productos seguros en los productos según los datos de configuración firmados digitalmente.

En otras formas de realización, los datos de configuración representan un intervalo de productos que se deben

producir. En otras formas de realización, los datos de configuración representan un intervalo de productos, máquinas, fábricas, intervalos, o volúmenes de producto que están autorizados. Otras formas de realización incluyen recibir una solicitud de verificación, comprendiendo la solicitud un identificador de producto y determinar si los datos de configuración para la tirada de producción están autorizados por referencia a un administrador de licencias. Otras formas de realización incluyen generar un testigo de seguridad para un intervalo de productos; y asociar el testigo de seguridad al intervalo de productos.

Módulo de firma

El Módulo de Firma puede recibir los datos de configuración, una clave de autorización, un testigo de seguridad o cualquier combinación de los mismos, así como un identificador de producto exclusivo o generado por el Módulo de Identificación. En algunas formas de realización, el Módulo de Firma puede recibir, adicionalmente, una o más características intrínsecas de máquina y/o producto, y/o características de artículo de producto. El Módulo de Firma puede crear una firma digital sobre la base de cualesquiera o la totalidad de esas entradas, a las que se hace referencia, en general, en la presente, como datos de configuración.

Para generar la firma digital, en algunas formas de realización, en primer lugar, el Módulo de Firma puede generar un compendio u otra representación de los datos de configuración. En algunas formas de realización, el compendio se puede generar calculando un valor *hash* criptográfico de los datos de configuración según un algoritmo de firma digital proporcionado por el Módulo de Firma que ejecuta el algoritmo de firma digital. Como ejemplos no limitativos, el valor *hash* se puede calcular según funciones MD5, SHA-1, SHA-2, SHA-3/Keccak. A continuación, el compendio se puede descifrar usando una clave privada obtenida por el Módulo de Firma para generar la firma digital.

En algunas formas de realización, una firma digital puede usar una tecnología de Infraestructura de Clave Pública (PKI) para establecer la autenticidad de datos de configuración. Los sistemas de PKI usan certificados y claves para identificar entidades, individuos u organizaciones. El Módulo de Autenticación usa una clave privada para firmar los datos de configuración y asocia los datos de configuración a un certificado incluyendo la clave pública usada por el Módulo de Autenticación.

Un módulo destinatario usa una clave pública para verificar la firma digital y, de este modo, la autenticidad de los datos de configuración firmados. Pueden utilizarse tecnologías de soporte para establecer otras características de no repudio, tales como el momento de la firma y el estado de las claves de firma. La clave pública se puede proporcionar directamente a la entidad destinataria, o mediante publicación en un directorio o repositorio en línea.

Módulo de identificación

El Módulo de Identificación puede recibir los datos de configuración y generar identificadores para artículos a marcar. El Módulo de Identificación puede recibir una firma digital generada por el Módulo de Firma que se combinará con el identificador exclusivo para generar un identificador exclusivo compuesto.

Los identificadores pueden incluir, o pueden basarse en, la fecha y/o la hora de producción de un producto a marcar y la firma digital recibida desde el Módulo de Firma. En algunas formas de realización, los identificadores seguros generados pueden ser exclusivos o sustancialmente exclusivos. En algunas formas de realización, los identificadores seguros pueden ser el testigo de seguridad.

En el caso de intervalos, el Módulo de Identificación puede generar un identificador de intervalo y un conjunto de identificadores dentro del intervalo generado.

A los identificadores creados se les puede dar salida hacia un módulo de control de impresión para su impresión directa sobre un producto o los mismos se pueden introducir en un procesado adicional para generar otro código que se imprime en el envase del producto.

Módulo de verificación

Haciendo referencia a la figura 3, el Módulo de Verificación (150) puede recibir los datos de configuración verificados y, sobre la base de esos datos de configuración validados, validar una solicitud de autorización (305) para una fábrica, máquina, producto o volumen de producción notificado. Las entradas para el Módulo de Verificación pueden incluir cualesquiera o la totalidad de los datos de configuración verificados, la salida del módulo de firma, identificadores, testigos de seguridad y/o información de intervalos. El Módulo de Verificación puede generar información para un Módulo de Autorización con estos parámetros con el fin de verificar/validar un identificador de producto.

El Módulo de Verificación puede generar un descifrado (320) de la solicitud, que incluye uno o más identificadores o intervalos de identificadores (315) y datos de firma (310) que incluyen uno o más testigos de

seguridad.

Si se introduce un testigo de seguridad en el Módulo de Verificación, el Módulo de Verificación puede devolver información referente a la autorización, los datos de configuración y/o intervalos. Si se usa un testigo de seguridad individual para un intervalo de productos, el testigo de seguridad se puede proporcionar al Módulo de Verificación con el fin de verificar parámetros asociados al intervalo de productos, más que productos individuales. Esta forma de realización puede ser particularmente útil en el contexto de la regulación de exportaciones.

Procesos del sistema

Inicialización del código de identificación

La Inicialización del Código de Identificación se puede llevar a cabo para validar la autorización y los parámetros. En algunas formas de realización, por motivos de rendimiento, esto se puede realizar una vez en el comienzo de la producción. Haciendo referencia a la figura 1, el Módulo de Control (110) puede acceder a un almacén de datos (115) en relación con parámetros adicionales, o pueden proporcionarse parámetros adicionales al módulo. Los parámetros y los datos de configuración, una vez firmados por el Módulo de Autorización (130), forman los datos de configuración validados (135). El Módulo de Control recibe datos de configuración verificados, según se ha descrito anteriormente, como respuesta a su solicitud al Módulo de Autorización (130).

La autorización puede ser una autorización para producir un producto, o para marcar un producto con una cierta ID, o ambas opciones. Los datos de configuración y los parámetros adicionales se transmiten al Módulo de Autorización y son usados por el Módulo de Autorización para generar el testigo de seguridad. El Módulo de Autorización puede firmar los datos de configuración y los parámetros adicionales, formando los datos de configuración firmados. Tal como se ha descrito anteriormente, los datos de configuración pueden especificar una cierta tirada de producción u otros productos y actividades. El Módulo de Autorización puede generar un bloque de autorización que incluye una clave, identificadores autorizados, y un testigo de seguridad. En algunas formas de realización, la clave puede ser generada por el Módulo de Autorización, o puede ser proporcionada al mismo. El Módulo de Autorización puede transmitir el bloque de autorización al Módulo de Control. El Módulo de Control puede transmitir los datos de configuración validados y otra información, tal como una lista de identificadores, un intervalo de identificadores y/o uno o más testigos de seguridad, al Módulo de Firma (145). El Módulo de Firma puede firmar los datos y enviar los datos firmados y la firma al Módulo de Control. A continuación, el Módulo de Identificación (140) puede recibir del Módulo de Control un bloque de inicialización que incluye los identificadores y/o intervalos de identificadores para productos.

Una forma de realización de la invención incluye un método para inicializar un proceso para controlar de manera segura una instalación de producción, que comprende: recibir electrónicamente unos datos de configuración de un almacén de datos electrónicos; almacenar electrónicamente los datos de configuración para una tirada de producción, especificando los datos de configuración para la tirada de producción unos parámetros usados en la producción de productos; transmitir los datos de configuración a un módulo de autorización; en el módulo de autorización: determinar si la tirada de producción está autorizada; generar datos de configuración validados que comprenden una clave, una representación de una pluralidad de identificadores de producto autorizados, y un testigo de seguridad; transmitir los datos de configuración validados a un módulo de firma; y, en el módulo de firma, firmar los datos de configuración validados.

Otras formas de realización pueden incluir determinar si los datos de configuración para la tirada de producción están autorizados; si la tirada de producción está autorizada: generar un testigo de seguridad y asociar el testigo a los datos de configuración; y firmar digitalmente los datos de configuración generando una firma digital y asociando la firma digital a los datos de configuración.

Otras formas de realización pueden incluir recibir los datos de configuración firmados digitalmente y la firma digital en una máquina de producción; en la máquina de producción, verificar la firma digital asociada a los datos de configuración firmados digitalmente; y calcular un conjunto de identificadores de producto seguros sobre la base de los datos de configuración firmados digitalmente.

Otras formas de realización pueden incluir producir unos productos en una tirada de producción según los datos de configuración firmados digitalmente; e imprimir el conjunto de identificadores de producto seguros en los productos según los datos de configuración firmados digitalmente.

Otras formas de realización pueden incluir que la determinación de si la tirada de producción está autorizada comprenda asimismo recuperar datos de licencia de un servidor de licencias.

Generación de códigos de identificación

Haciendo referencia a la figura 2, el proceso de Generación de Código genera los códigos durante el proceso de producción. El proceso de generación del código de identificación puede comenzar con una solicitud para el Módulo de Identificación (140) en relación con un identificador o un intervalo de identificadores, los cuales, a continuación, se devuelven al Módulo de Control (110). A continuación, los identificadores se envían al Módulo de Firma (145), el cual firma los identificadores y devuelve los identificadores firmados al Módulo de Control. El Módulo de Firma puede recibir un testigo de seguridad. En algunas formas de realización, no es necesario que el Módulo de Firma sea controlado por medio de instrucciones externas y, si debe considerarse cualquier código de identificación, el código se puede vincular a un testigo de seguridad individual. El Módulo de Firma puede ser controlado por el Módulo de Autorización. A continuación, el Módulo de Control puede enviar los datos de salida al control de impresión en el Módulo de Impresora (210). Los datos de salida enviados al control de impresión se pueden cifrar antes de la transmisión. Los datos de configuración se pueden transmitir al Módulo de Verificación (150) para la gestión de solicitudes de verificación subsiguientes.

Una forma de realización de la invención incluye un método para generar un código con vistas a identificar de manera segura productos producidos en una instalación de producción, que incluye recibir electrónicamente los datos de configuración de un almacén de datos electrónicos; almacenar electrónicamente los datos de configuración para una tirada de producción, especificando los datos de configuración para la tirada de producción unos parámetros usados en la producción de productos; transmitir los datos de configuración a un módulo de autorización; en el módulo de autorización: determinar si la tirada de producción está autorizada; generar datos de configuración validados que comprenden una clave, una representación de una pluralidad de identificadores de producto autorizados, y un testigo de seguridad; transmitir los datos de configuración validados a un módulo de firma; en el módulo de firma, firmar los datos de configuración validados; en un módulo de identificación, recibir una solicitud de un identificador de producto y generar un identificador de producto como respuesta a la solicitud; transmitir el identificador de producto desde el módulo de identificación a un módulo de firma; firmar digitalmente el identificador de producto en el módulo de firma; y transmitir el identificador de producto firmado digitalmente a un módulo de impresora.

Otras formas de realización pueden incluir recibir electrónicamente datos de configuración de un almacén de datos electrónicos; almacenar electrónicamente los datos de configuración para una tirada de producción, especificando los datos de configuración para la tirada de producción unos parámetros usados en la producción de productos; transmitir los datos de configuración a un módulo de autorización; en un módulo de autorización: determinar si la tirada de producción está autorizada; generar datos de configuración validados que comprenden una clave, una representación de una pluralidad de identificadores de producto autorizados, y un testigo de seguridad; transmitir los datos de configuración validados a un módulo de firma; en el módulo de firma, firmar los datos de configuración validados.

En otras formas de realización, la solicitud es para un intervalo de identificadores. Otras formas de realización pueden incluir determinar si los datos de configuración para la tirada de producción están autorizados; si la tirada de producción está autorizada: generar un testigo de seguridad y asociar el testigo a los datos de configuración; y firmar digitalmente los datos de configuración generando una firma digital y asociando la firma digital a los datos de configuración.

Verificación del código de identificación

El Módulo de Verificación puede recibir una solicitud de verificación. La solicitud puede incluir uno o más códigos de identificación. El módulo de verificación puede descifrar o desenmarañar de otra manera el código de identificador recibido. La información resultante, tras su descifrado, puede incluir un componente de firma y un identificador. A continuación, el identificador resultante se puede vincular con respecto a los datos de configuración originales previamente almacenados en asociación con el identificador. Los datos vinculados pueden incluir otros identificadores en un intervalo, un testigo de seguridad, y otra información almacenada en relación con la producción del producto que lleva ese código de identificación.

Algunas formas de realización pueden incluir una funcionalidad adicional para procesar identificadores que se proporcionan al Módulo de Verificación sobre la base de la parte que solicita la verificación del código. A diferentes partes se les pueden proporcionar medios diferentes para acceder al Módulo de Verificación. Por ejemplo, a un minorista u otra forma de comerciante, se le puede proporcionar un portal o canal de comunicaciones diferente al de un consumidor. También se puede requerir al minorista que se autentique en el Módulo de Verificación.

En algunas formas de realización, el sistema se puede configurar de manera que una verificación por parte de un consumidor dé como resultado la marcación de un identificador como verificado. El sistema se puede configurar además para almacenar aquellos códigos para los cuales un consumidor solicita verificación. Todas las solicitudes subsiguientes de verificación de aquellos códigos ya verificados pueden ser denegadas o procesadas de otra manera diferencialmente.

Funciones de exportación

Formas de realización de la invención se pueden aplicar en el contexto de la exportación de código a terceros. Esas formas de realización pueden incluir una función de exportación configurada para generar un código aparte con este fin. El código exportado se puede generar recopilando uno o más identificadores de producto y/o testigos de seguridad, y firmando esos identificadores y/o testigos. Los identificadores y/o testigos se pueden recopilar en cualquier punto del proceso de producción. Los identificadores firmados y/o testigos en forma de códigos exportados se pueden proporcionar a un tercero el cual los puede almacenar y llevar a cabo una verificación de la validez de los identificadores y/o testigos.

Arquitecturas del sistema

Los sistemas y métodos descritos en la presente se pueden implementar en *software* o *hardware* o cualquier combinación de los mismos. Los sistemas y métodos descritos en la presente se pueden implementar usando uno o más dispositivos informáticos los cuales pueden ser o no independientes entre sí en términos físicos o lógicos. Adicionalmente, varios aspectos de los métodos descritos en la presente se pueden combinar o fusionar en otras funciones. En algunas formas de realización, los elementos del sistema ilustrados se podrían combinar en un único dispositivo de *hardware* o se podrían separar en múltiples dispositivos de *hardware*. Si se usan múltiples dispositivos de *hardware*, los dispositivos de *hardware* podrían estar ubicados próximos físicamente o alejados entre sí.

Los métodos se pueden implementar en un producto de programa de ordenador accesible desde un soporte de almacenamiento utilizable por ordenador o legible por ordenador que proporcione código de programa para su uso por parte de o en relación con un ordenador o cualquier sistema de ejecución de instrucciones. Un soporte de almacenamiento utilizable por ordenador o legible por ordenador puede ser cualquier aparato que pueda contener o almacenar el programa para su uso por parte del o en relación con el ordenador o sistema, aparato o dispositivo de ejecución de instrucciones.

Un sistema de procesado de datos apto para almacenar y/o ejecutar el código de programa correspondiente puede incluir por lo menos un procesador acoplado de manera directa o indirecta a dispositivos computarizados de almacenamiento de datos, tales como elementos de memoria. Al sistema se le pueden acoplar dispositivos de entrada/salida (I/O) (que incluyen, aunque sin carácter limitativo, teclados, pantallas, dispositivos señaladores, etcétera). Al sistema también se le pueden acoplar adaptadores de red para permitir que el sistema de procesado de datos llegue a acoplarse a otros sistemas de procesado de datos o impresoras remotas o dispositivos de almacenamiento a través de redes privadas o públicas intermedias. Para proporcionar interacción con un usuario, las características se pueden implementar en un ordenador con un dispositivo de pantalla, tal como un CRT (tubo de rayos catódicos), una LCD (pantalla de cristal líquido), u otro tipo de monitor para visualizar información al usuario, y un teclado y un dispositivo de entrada, tal como un ratón o un control de *trackball* por medio de los cuales el usuario puede proporcionar entradas al ordenador.

Un programa de ordenador puede ser un conjunto de instrucciones que se pueden usar, de manera directa o indirecta, en un ordenador. Los sistemas y métodos descritos en el presente se pueden implementar usando lenguajes de programación, tales como Flash™, JAVA™, C++, C, C#, Visual Basic™, JavaScript™, PHP, XML, HTML, etcétera, o una combinación de lenguajes de programación, incluyendo lenguajes compilados o interpretados, y se pueden desplegar en cualquier formato, incluyendo en forma de un programa autónomo o en forma de un módulo, componente, subrutina u otra unidad apta para su uso en un entorno informático. El *software* puede incluir, aunque sin carácter limitativo, microprogramas, *software* residente, microcódigo, etcétera. En la implementación de interfaces entre módulos de programación se pueden usar protocolos tales como el SOAP/HTTP. Los componentes y las funcionalidades descritos en la presente se pueden implementar en cualquier sistema operativo de escritorio que se ejecute en un entorno virtualizado o no virtualizado, utilizando cualquier lenguaje de programación apto para desarrollo de *software*, incluyendo, aunque sin carácter limitativo, diferentes versiones de Microsoft Windows™, Apple™ Mac™, iOS™, Unix™/X-Windows™, Linux™, etcétera.

Los procesadores aptos para la ejecución de un programa de instrucciones incluyen, aunque sin carácter limitativo, microprocesadores de propósito general y especial, y el procesador único o uno de los múltiples procesadores o núcleos, de cualquier tipo de ordenador. Un procesador puede recibir y almacenar instrucciones y datos de un dispositivo computarizado de almacenamiento de datos, tal como una memoria de solo lectura, una memoria de acceso aleatoria, ambas, o cualquier combinación de los dispositivos de almacenamiento de datos descritos en la presente. Un procesador puede incluir cualquier circuitería de procesado o circuitería de control operativa para controlar las operaciones y el rendimiento de un dispositivo electrónico.

El procesador también puede incluir, o puede estar acoplado operativamente para comunicarse con, uno o más dispositivos de almacenamiento de datos para almacenar datos. Dichos dispositivos de almacenamiento de datos pueden incluir, como ejemplos no limitativos, discos magnéticos (incluyendo discos duros internos y discos extraíbles), discos magnetoópticos, discos ópticos, memoria de solo lectura, memoria de acceso aleatorio, y/o

almacenamiento *flash*. Los dispositivos de almacenamiento aptos para incorporar de manera tangible instrucciones de programa de ordenador y datos también pueden incluir todas las formas de memoria no volátil, incluyendo, por ejemplo, dispositivos de memoria de semiconductores, tales como EPROM, EEPROM y dispositivos de memoria *flash*; discos magnéticos tales como discos duros internos y discos extraíbles; discos magnetoópticos; y discos CD-ROM, y DVD-ROM. El procesador y la memoria se pueden suplementar con, o incorporar en, ASIC (circuitos integrados de aplicación específica).

Los sistemas, módulos y métodos descritos en la presente se pueden implementar usando cualquier combinación de elementos de *software* o *hardware*. Los sistemas, módulos y métodos descritos en la presente se pueden implementar usando una o más máquinas virtuales que funcionen de manera individual o en combinación mutua. Para encapsular una plataforma de máquina informática física en una máquina virtual que se ejecuta bajo el control de software de virtualización que funciona en un anfitrión o plataforma informática de *hardware* se puede usar cualquier solución de virtualización aplicable. La máquina virtual puede tener tanto *hardware* de sistema virtual como *software* de sistema operativo invitado.

Los sistemas y métodos descritos en la presente se pueden implementar en un sistema de ordenador que incluya un componente de fondo (del inglés, *back-end*), tal como un servidor de datos, o que incluya un componente de software intermedio (del inglés, *middleware*), tal como un servidor de aplicación o un servidor de Internet, o que incluya un componente de presentación (del inglés, *front-end*) tal como un ordenador de cliente que tenga una interfaz de usuario gráfica o un navegador de Internet, o cualquier combinación de los mismos. Los componentes del sistema se pueden conectar mediante cualquier forma o soporte de comunicación de datos digitales, tal como una red de comunicaciones. Los ejemplos de redes de comunicaciones incluyen, por ejemplo, una LAN, una WAN, y los ordenadores y redes que forman Internet.

Una o más formas de realización de la invención se pueden poner en práctica con otras configuraciones de sistemas de ordenador, incluyendo dispositivos de mano, sistemas de microprocesador, electrónica de consumo basada en microprocesadores o programable, miniordenadores, ordenadores centrales, etcétera. La invención también se puede poner en práctica en entornos informáticos distribuidos en los que las tareas son realizadas por dispositivos de procesado remotos que se enlazan a través de una red.

Aunque se han descrito una o más formas de realización de la invención, dentro del alcance de la misma se incluyen diversas modificaciones, adiciones, permutaciones y equivalentes de la misma.

REIVINDICACIONES

1. Método para inicializar un proceso para controlar de manera segura una instalación de producción, que comprende:

- recibir electrónicamente unos datos de configuración (105) para una tirada de producción de un almacén de datos electrónicos;

- almacenar electrónicamente los datos de configuración para la tirada de producción, especificando los datos de configuración para la tirada de producción unos parámetros usados en la producción de productos;

- transmitir los datos de configuración para la tirada de producción a un módulo de autorización (130);

- en el módulo de autorización (130), determinar si la tirada de producción está autorizada;

- recibir los datos de configuración en una máquina de producción y producir unos productos en una tirada de producción según los datos de configuración;

caracterizado por:

- en el módulo de autorización (130), si la tirada de producción está autorizada, generar un testigo de seguridad y asociar el testigo a los datos de configuración y generar unos datos de configuración validados (135) que comprenden una clave de cifrado, una representación de una pluralidad de identificadores de producto autorizados, y el testigo de seguridad;

transmitir los datos de configuración validados a un módulo de firma (145); y

en el módulo de firma (145), firmar digitalmente los datos de configuración validados generando una firma digital con los datos de configuración y asociando la firma digital a los datos de configuración,

estando el método asimismo caracterizado por que:

los datos de configuración recibidos en la máquina de producción son firmados digitalmente y la firma digital es recibida en la máquina de producción;

en la máquina de producción, se verifica la firma digital asociada a los datos de configuración firmados digitalmente; y

se calcula un conjunto de identificadores de productos seguros sobre la base de los datos de configuración firmados digitalmente; y

estando el método asimismo caracterizado por que:

los productos se producen según los datos de configuración firmados digitalmente; y

se imprime el conjunto de identificadores de productos seguros en los productos según los datos de configuración firmados digitalmente.

2. Método según una o más de las reivindicaciones anteriores, en el que la determinación de si la tirada de producción está autorizada comprende asimismo recuperar los datos de licencia de un servidor de licencias.

3. Método según una o más de las reivindicaciones anteriores, que comprende asimismo generar un código para identificar de manera segura los productos producidos en la instalación de producción, que comprende:

en un módulo de identificación (140), recibir una solicitud de un identificador de producto y generar un identificador de producto como respuesta a la solicitud;

transmitir el identificador de producto desde el módulo de identificación (140) a un módulo de firma (145); y

firmar digitalmente el identificador de producto en el módulo de firma (145); y

transmitir el identificador de producto firmado digitalmente a un módulo de impresora (210).

4. Método según la reivindicación 3, en el que la solicitud es para un intervalo de identificadores.

5. Método según una o más de las reivindicaciones anteriores, en el que los datos de configuración representan un intervalo de productos que se deben producir.

6. Método según una o más de las reivindicaciones anteriores, en el que los datos de configuración representan un intervalo de productos, máquinas, fábricas, intervalos o volúmenes de producto que están autorizados.

7. Método según una o más de las reivindicaciones anteriores, que comprende asimismo determinar si los datos de configuración para la tirada de producción están autorizados por referencia a un administrador de licencias.

8. Método según una o más de las reivindicaciones anteriores, que comprende asimismo:

generar un testigo de seguridad para un intervalo de productos; y

asociar el testigo de seguridad al intervalo de productos.

Fig. 1
Inicialización de Código

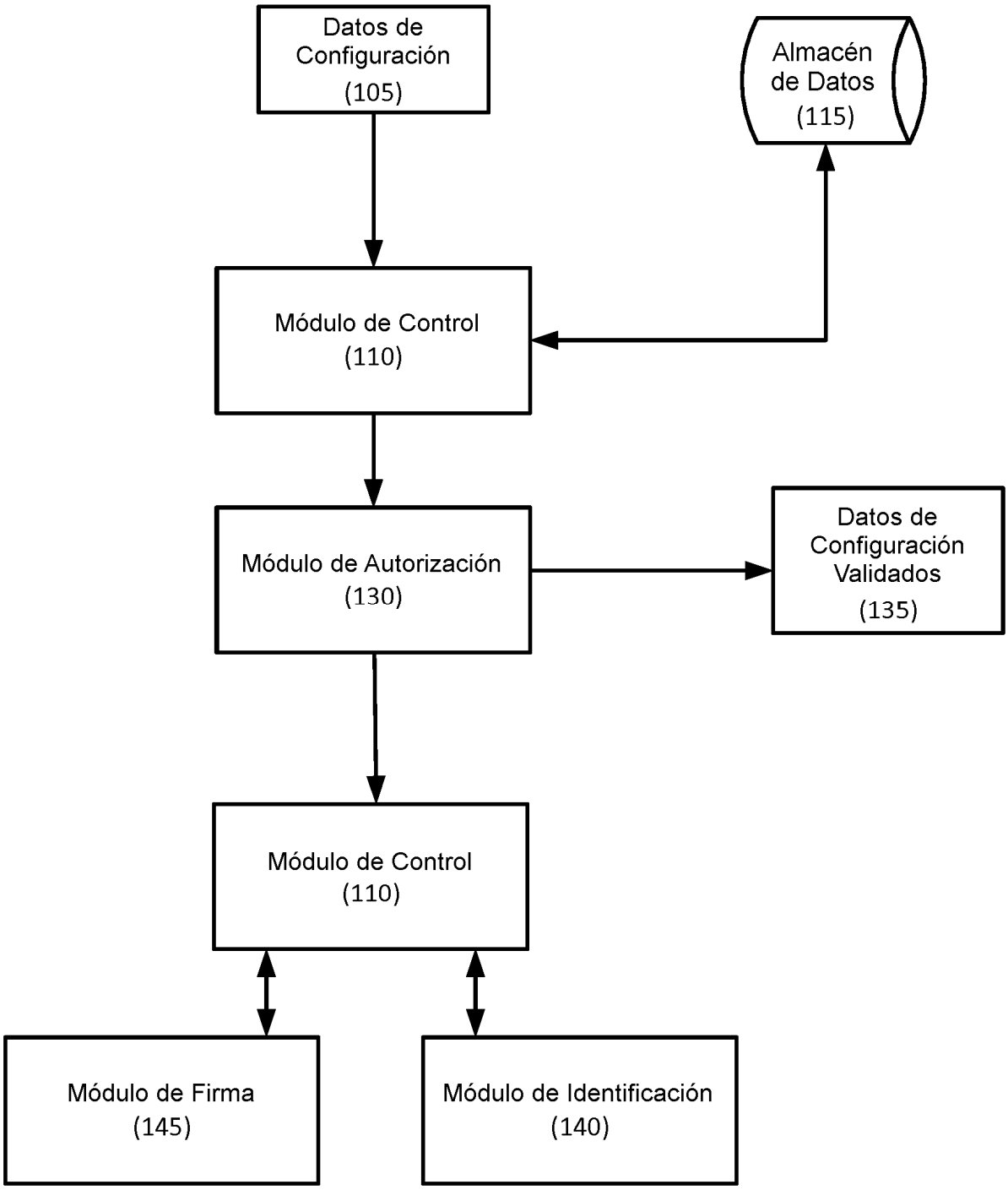

Fig. 2
Generación de Código

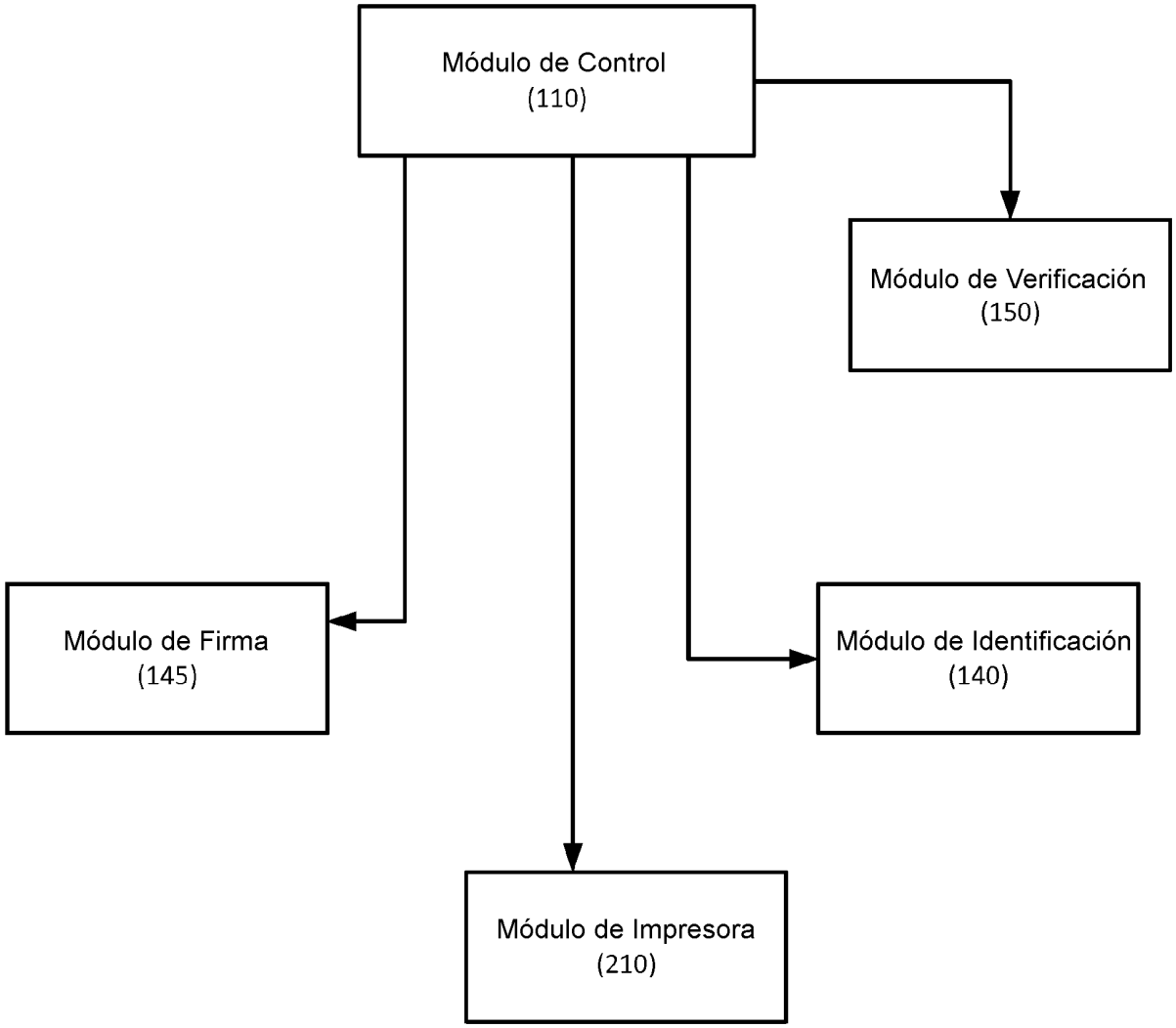

Fig. 3
Autenticación de Código