(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 738 415**

(51) Int. CI.:

H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **13.08.2016 PCT/EP2016/069316**

(87) Fecha y número de publicación internacional: **16.02.2017 WO17025645**

(96) Fecha de presentación y número de la solicitud europea: **13.08.2016 E 16751297 (9)**

(97) Fecha y número de publicación de la concesión europea: **01.05.2019 EP 3335370**

(54) Título: **Ofuscación o aleatorización mejorada para una identificación y verificación seguras de productos**

(30) Prioridad:

13.08.2015 US 201562204753 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.01.2020

(73) Titular/es:

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

(72) Inventor/es:

FRADET, ERWAN;
CHATELAIN, PHILIPPE y
CHANEZ, PATRICK

(74) Agente/Representante:

CURELL SUÑOL, S.L.P.

DESCRIPCIÓN

Ofuscación o aleatorización mejorada para una identificación y verificación seguras de productos.

Esta solicitud reivindica el beneficio de la solicitud provisional US n.º de serie 62/204,753, presentada el 13 de agosto de 2015.

La presente invención se refiere, en general, a técnicas para cifrar caracteres alfanuméricos en relación con el marcaje de productos con códigos de identificación seguros y la verificación de esos códigos, y también a sistemas y procedimientos para gestionar la distribución de instrucciones seguras de configuración de producción y generar identificadores de productos seguros.

Los procedimientos existentes para la identificación de productos conllevan, típicamente, la aplicación de un identificador único a un producto en el momento de su embalaje. Estos sistemas no se adaptan a escala eficientemente en organizaciones que presentan múltiples instalaciones de producción, o en cadenas de producción con capacidad de embalar a una velocidad muy alta. Adicionalmente, los procedimientos 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 vendedores.

Existe una necesidad de un procedimiento 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 producto seguros, en particular uno que se pueda usar para la verificación de impuestos, la verificación de volúmenes de producción y la autenticación de artículos fabricados.

Los sistemas existentes cifran caracteres alfanuméricos usados como identificadores de producto de carácter en carácter. Esto limita dichos sistemas, por ejemplo en relación con los números, en general de 0 a 9 o, si se usan únicamente letras, limita los sistemas al número de letras en el alfabeto usado, multiplicado por dos (incluyendo letras mayúsculas y letras minúsculas). Esta invención hace frente a estos inconvenientes. Se divulgan sistemas existentes en los documentos US-2013/02979, 29, US-2013/0099901 y en el documento de GIUSEPPE ATENIESE ET AL., “Untraceable RFID tags via insubvertible encryption”, *PROCEEDINGS OF THE 12TH. ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY*. (CCS’05). ALEXANDRIA, VA, 7 a 11 de NOVIEMBRE de 2005; NUEVA YORK, NY: ACM, US, (20051107), doi:10.1145/1102120.1102134, ISBN 978-1-59593-226-6, páginas 92 a 101,

Las siguientes formas de realización de la invención son a título de ejemplo y no están destinadas a limitar el alcance de la invención, el cual queda definido por las reivindicaciones.

Aunque se han descrito una o más formas de realización de la presente invención, en el alcance de la misma se incluyen diversas modificaciones, adiciones, permutaciones y equivalentes de dichas formas de realización. En la siguiente descripción de formas de realización, se hace referencia a los dibujos adjuntos que forman parte de la misma, los cuales muestran, a título de ilustración, 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 son, necesariamente, desviaciones con respecto al alcance en relación con la materia en cuestión pretendida y reivindicada. Aunque las etapas siguientes 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 los procedimientos descritos. No es necesario que los diversos cálculos que se describen a continuación, tales como aquellos incluidos en los procedimientos de inicialización, generación y autenticación de código, se lleven a cabo en el orden divulgado, y podrían implementarse fácilmente otras formas de realización usando ordenaciones alternativas de los cálculos. Además de reordenarlos, los cálculos también se podrían descomponer en subcálculos con los mismos resultados.

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

la figura 1 ilustra un procedimiento de ejemplo para calcular un identificador de máquina.

La figura 2 ilustra un procedimiento de ejemplo para ofuscar datos.

La figura 3 ilustra un ejemplo de procedimiento para la inicialización de código.

La figura 4 ilustra un ejemplo de procedimiento para la generación de código.

La figura 5 ilustra un ejemplo de procedimiento para la autorización de código.

De acuerdo con una forma de realización de la invención para un procedimiento destinado a ofuscar datos almacenados en una red, el procedimiento comprende: definir y almacenar información descriptiva del estado de una máquina informática como número de máquina (*MNUM*), incluyendo la información descriptiva del estado el número de bases que comprenden la información descriptiva del estado; generar un identificador único y seguro de producto de máquina (*MSUPI*), como transformación matemática reversible de un identificador único de producto de máquina (*MUPI*), basándose en información descriptiva del estado de una máquina informática, comprendiendo la etapa de cálculo del *MSUPI*: definir el número de etapas de manera que sea *imax*, para cada etapa generar un primer número aleatorio Clave de Ofuscación para Generación de Código ($CGOK_{i,1}$) y un segundo número aleatorio Clave de Ofuscación para Generación de Código ($CGOK_{i,2}$), comprendiendo dicha acción de generar: calcular un primer número aleatorio ($CGOK_{i,1}$) coprimo con un número basado en la información descriptiva del estado de la máquina informática (*MNUM*); calcular un segundo número aleatorio ($CGOK_{i,2}$) que presenta un tamaño de bits igual o menor que (*MNUM*); definir $m_{0,2} = MUPI$; calcular para cada elemento *i*, desde *i* = 1 a *imax* – 1*:* $m_{i,1} = (m_{i\text{-}1,2} \times CGOK_{i,1}) \bmod (MNUM)$; $m_{i,2} = (m_{i,1} \bmod CGOK_{i,2})$; si ($m_{i,2} > MNUM) \rightarrow m_{i,2} = m_{i,1}$; definir $MSUPI = m_{imax,2}$; y almacenar el identificador único y seguro de producto de máquina (*MSUPI*) en unos medios electrónicos de almacenamiento de datos. La forma de realización antes descrita, así como las formas de realización alternativas adicionales que se describen en la presente memoria, se pueden materializar en una invención implementada por ordenador, un sistema de ordenador, o un soporte de datos informatizado.

Según una forma de realización alternativa o adicional, la información descriptiva del estado de la máquina informática comprende una combinación de información de tiempo y número de producto. De acuerdo con una forma de realización alternativa o adicional, la información de tiempo incluye año juliano, día juliano, hora de producción y minuto de producción. De acuerdo con una forma de realización alternativa o adicional, la información descriptiva del estado incluye el valor de un contador incremental reinicializado sobre una base periódica. De acuerdo con una forma de realización alternativa o adicional, el número basado en la información descriptiva del estado de la máquina informática se calcula como 10 x 366 x 24 x 60 x *Identificador de Tiempo*. De acuerdo con una forma de realización alternativa o adicional, *Identificador de Tiempo* se define como el entero 2210. De acuerdo con una forma de realización alternativa o adicional, se obtiene un Identificador Único y Seguro de Producto (*SUPI*), un código alfanumérico de 12 caracteres, de tal manera que *SUPI = (p* x *m)* mod *(MNUM* x *mRuido* x *RunLim)*.

Según una forma de realización alternativa o adicional para generar un código con el fin de identificar, de manera segura, productos producidos en una instalación de producción, el procedimiento comprende: recibir electrónicamente datos de configuración de unos medios electrónicos de almacenamiento de datos; 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 productos autorizados, y un testigo (*token*) 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, llevándose a cabo la generación del identificador de producto: definiendo y almacenando información descriptiva del estado de una máquina informática como número de máquina (*MNUM*), incluyendo la información descriptiva del estado el número de bases que comprenden la información descriptiva del estado; generando un identificador único y seguro de producto de máquina (*MSUPI*), como una transformación matemática reversible de un identificador único de producto y máquina (*MUPI*), sobre la base de información descriptiva del estado de una máquina informática, comprendiendo la etapa de cálculo de *MSUPI*: definir el número de etapas de manera que sea *imax*, para cada etapa generar un primer número aleatorio Clave de Ofuscación para Generación de Código ($CGOK_{i,1}$) y un segundo número aleatorio Clave de Ofuscación para Generación de Código ($CGOK_{i,2}$), comprendiendo dicha acción de generar: calcular un primer número aleatorio ($CGOK_{i,1}$) coprimo con un número basado en la información descriptiva del estado de la máquina informática (*MNUM*); calcular un segundo número aleatorio ($CGOK_{i,2}$) que presenta un tamaño de bits igual o menor que (*MNUM*); definir $m_{0,2} = MUPI$; calcular para cada elemento *i*, desde *i* = 1 a *imax* – 1*:* $m_{i,1} = (m_{i\text{-}1,2} \times CGOK_{i,1}) \bmod (MNUM)$; $m_{i,2} = (m_{i,1} \bmod CGOK_{i,2})$; si ($m_{i,2} > MNUM) \rightarrow m_{i,2} = m_{i,1}$; definir $MSUPI = m_{imax,2}$; almacenar el identificador único y seguro de producto de máquina (*MSUPI*) en unos medios electrónicos de almacenamiento de datos como identificador de producto; transmitir el identificador de producto desde el módulo de identificación hasta 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.

De acuerdo con una forma de realización alternativa o adicional, el procedimiento comprende, además: recibir electrónicamente datos de configuración de unos medios electrónicos de almacenamiento de datos; 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 productos 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.

Según una forma de realización alternativa o adicional, la solicitud es de un intervalo de identificadores. De acuerdo con una forma de realización alternativa o adicional, el procedimiento comprende, además, 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.

Según una forma de realización alternativa o adicional, el identificador único de producto y máquina (*MUPI*) se transforma sin rellenar el identificador único de producto y máquina (*MUPI*), de tal manera que la longitud en bits del identificador único de producto y máquina (*MUPI*) es igual a la longitud en bits del identificador único y seguro de producto de máquina (*MSUPI*).

En una forma de realización alternativa o adicional, el procedimiento para la verificación de un identificador único de producto y máquina seguro comprende: recibir, por parte de un módulo de verificación, para su verificación, un *MSUPI*; asignar *MSUPI* como $m_{0,2}$; recuperar, por parte del módulo de verificación, un primer número aleatorio $CGOK_{i,1}$ y un segundo número aleatorio, $CGOK_{i,2}$ y el *imax* asociado a los números aleatorios recuperados y el *MSUPI* recibido; calcular para cada elemento *i*, desde *i = 1* a *imax - 1*: $m_{i,1} = (m_{i-1,2} \bmod CGOK_{i,2})$; si $(m_{i,2} > MNUM) \rightarrow m_{i,1} = m_{i-1,2}$; $m_{i,2} = (m_{i,1} \times CGOK^{-1}{}_{i,1}) \bmod (MNUM)$; $m_{cg} = m_{imax,2}$; y verificar $MUPI = m_{cg} / mRuido$ y valor de ruido = $m_{cg} \bmod mRuido$, basándose *MUPI* en información descriptiva del estado de una máquina informática.

Según una forma de realización alternativa o adicional, el identificador único y seguro de producto de máquina (*MSUPI*) se transforma sin haber rellenado el identificador único de producto y máquina (*MUPI*), de tal manera que la longitud en bits del identificador único de producto y máquina (*MUPI*) es igual a la longitud en bits del identificador único y seguro de producto de máquina (*MSUPI*). Según una forma de realización alternativa o adicional, las autorizaciones que se reciben de un módulo de autorización se pueden transmitir a un módulo de verificación, de manera que posteriormente se pueden procesar solicitudes de verificación con respecto a dichas autorizaciones, y pudiendo incluir datos transmitidos al módulo de verificación el identificador único y seguro de producto de máquina (*MSUPI*).

Los procedimientos descritos se pueden usar de manera adicional o alternativamente al cifrado, y se pueden usar como procedimiento para ofuscar números usando una base definida. El procedimiento se puede usar para cualquier base definida finita. Los procedimientos se pueden usar sobre una base numérica predefinida, tal como 0 a 9 cuando se usen números, o cero a F para hexadecimal. Este procedimiento trabaja sobre una base definida que no se limita al número de caracteres usados en el intervalo normal de caracteres correspondiente a esa base.

Para este procedimiento, se define un grupo a partir del cual se seleccionarán caracteres alfanuméricos; a cada uno de estos grupos se le denomina base. Un ejemplo sería 0 → 52 (0 y 52 incluidos). Cada uno de estos números sería un “carácter” individual que sería cifrado. Alternativamente, se podría definir una base de 0 → 932. Alternativas permitirían una combinación de letras y números. Como ejemplos no limitativos, esto puede incluir los correspondientes del alfabeto inglés, el alfabeto cirílico, o cualquier otro alfabeto además de números. El sistema permite una definición de la base usando cualquier conjunto finito o combinación de conjuntos como bases para que cada uno de ellos se cuente como un “carácter” individual cuando se ofusca el número. Puede usarse cualquier conjunto de caracteres alfanuméricos siempre que se asigne un valor numérico para cada carácter. Esto se puede usar para combinar, por ejemplo, conjuntos de números hexadecimales y un alfabeto.

A cada carácter se le asigna un valor numérico, con un valor mínimo y un valor máximo, y los mismos a continuación se combinan. Por ejemplo, si se combinan un número hexadecimal y el alfabeto finlandés el cual tiene 29 letras, se pueden asignar los valores 0 a 15 para los números hexadecimales, de tal manera que 15 se corresponde con 0, 14 se corresponde con 1, hasta 1 que se corresponde con B y 0 que se corresponde con A. Con el alfabeto finlandés, de manera similar los números correspondientes pueden ser 1 con A a 29 con Å (suponiendo que se usan solamente letras mayúsculas), o se puede asignar 1 con L y contar hasta donde 18 se corresponde con Å, 19 se corresponde con A y 29 se asigna a K.

No es necesario que la asignación sea lineal, siempre que se almacene qué carácter o número se asigna a qué valor numérico. Esto además se puede realizar dinámicamente, también si se desea una ofuscación adicional, siempre que las asignaciones se graben para un posterior descifrado. Con el ejemplo del uso de un hexadecimal y un alfabeto de 29 caracteres, el intervalo podría ser MAX = Hex(max) * Alfabeto(max) + Alfabeto(max) mientras que el mínimo MIN = Hex(min) * Alfabeto(min) + Alfabeto(min). En ambos ejemplos mencionados, hay dos bases. Este ejemplo proporciona una base de intervalo de [1, 464]. Esto es debido a que los números del Alfabeto discurren desde 1 a 29, por contraposición a 0 a 28 correspondientes a los 29 caracteres. Alternativamente, los mismos conjuntos se pueden combinar como *MAX = Alfabeto(max) * Hex(max) + Hex(max)* y *MIN = Alfabeto(min) * Hex(min) + Hex(min)*, y proporciona una base de intervalo de [0, 450]. Por lo tanto, usando las

mismas bases componentes, es posible crear diversos intervalos para ofuscar mejor los números que se usarán en el proceso.

En otro ejemplo en el que debe crearse la base de intervalo, la base de intervalo puede ser descriptiva del estado de una máquina informática, tal como una combinación de identificadores de tiempo y numéricos. En este ejemplo, la base de intervalo se puede crear usando múltiples bases. En este ejemplo, la misma está compuesta por cinco bases diferentes y sería una combinación de año juliano truncado (*JY*) [0-10], combinado con fecha juliana (*JD*) [0-366], hora del día (*HY*) [0-24], minuto de la hora (*Mins*), [0-60] y un Identificador de Tiempo (*TI*) [0-2210] y un contador incremental adicional reinicializado cada minuto. El número de bases que se usan para crear la base de intervalo se define como *imax*. En la figura 1 se ilustra un ejemplo de esta forma de realización.

El intervalo se determina convirtiendo los caracteres alfanuméricos en un único intervalo. Por ejemplo, en este caso, los años se convierten en días, a continuación los días totales en horas, las horas totales en minutos y, a continuación, en contadores incrementales. Una manera de lograr esto es usar los números máximos para cada uno con el fin de obtener el extremo superior del intervalo y los números mínimos de cada uno para determinar el extremo inferior del intervalo. Por ejemplo, valor máximo *MAX = (((JY(max) * JD(max) + JD(max)) * HR(max) + HR(max)) * Mins(max) + Mins(max)) * TI(max) + TI(max)*. El mínimo del intervalo es *MIN = (((JY(min) * JD(min) + JD(min)) * HR(min) + HR(min)) * Mins(min) + Mins(min)) * TI(min) + TI(min)*. En este ejemplo el intervalo es [0,12815659610].

Usando los intervalos del ejemplo anterior, se puede definir un Identificador único de producto y máquina (*MUPI*). Definiéndolo para que se sitúe dentro del valor tal que *MUPI = (((JY * JD(max) + JD) * HR(max) + HR) * Mins(max) + Mins) * TI(max) + TI*. Para ofuscar mejor el número, puede añadirse un componente aleatorio. Este número aleatorio se puede generar de cualquier manera siempre que se conozca el intervalo del número aleatorio. Este número aleatorio puede ser una firma digital que se genera usando un conjunto de clave secreta y dinámica. Esto se puede realizar, por ejemplo, usando un código de autenticación de mensaje *hash* con clave. Por ejemplo, un *MUPI* combinado con clave dinámica, cuando se usa una función de extracción, produciría la clave secreta, y el *MUPI* combinado con la clave secreta usando una función *hash* se usaría para calcular el valor de Noise (Ruido*)*. Esto permite definir un valor m_{cg} = *MUPI * mRuido* + Ruido. Este valor *MUPI* se cifrará usando la Clave de Ofuscación para Generación de Código (*CGOK*).

Pueden usarse dos valores de *CGOK*, el primero $CGOK_{i,1}$, es un número que es coprimo con el valor máximo del intervalo correspondiente a *MUPI*. *MNUM = JY(max) * JD(max) * HR(max) * Mins(max) * TI(max)*, que es 10*366*24*60*2210 en este ejemplo. El segundo $CGOK_{i,1}$, $CGOK_{i,2}$, es un número en el intervalo [*MIN, MNUM-1*] con un tamaño en bits igual o menor que $CGOK_{i,1}$. Para efectuar los cálculos, $m_{0,2}$ se define de manera que sea igual a *MUPI* y se define *MSUPI* de manera que sea el elemento máximo de $m_{i,2}$, que es $m_{imax,2}$. Si hay 8 bases que comprenden la base de intervalo, entonces el elemento *MSUPI* = $m_{8,2}$. A continuación, *MSUPI* se puede combinar con un ID de Generador de Código, *CGID*. Esto se efectúa desplazando el *CGID* según la dimensión de *MSUPI*, de tal manera que *m = CGID x (MNUM x mRuido) + MSUPI*, donde *mRuido* es el valor posible máximo de Ruido. El código final, Identificador Único y Seguro de Producto (*SUPI*), se obtiene cifrando *m* con el uso de un código de ofuscación global, *p*, que puede ser igual para todos los generadores de código. *SUPI* se define como (*p x m*) mod (*MNUM x mRuido x RunLim*), y *SUPI* se convierte a un código alfanumérico de 12 caracteres. En la figura 2 se ilustra un ejemplo de esta forma de realización.

El procedimiento de ofuscación es reversible para la verificación del proceso y los productos. Esto se logra ejecutando el proceso de ofuscación a la inversa. Esto es posible debido a que *CGOK* es coprimo con *MNUM*, y se usa una función Indicatriz de Euler con respecto a *MNUM*. Esto permite el cálculo del *MUPI* y *MNUM* a partir de *MSUPI*. El descifrado de *SUPI*, por lo tanto, requiere las siguientes etapas, $m = \left(p^{16\times 34^{11-1}} \times SUPI\right) \bmod (MNUM \times mNoise \times RunLim)$. A partir de *m*, pueden extraerse el *MSUPI* y el *CGID*, *MSUPI = m* mod *(MNUM* x *mRuido)* y *CGID = m / (MNUM* x *mRuido*). A partir de aquí, *MSUPI* se desofusca usando el inverso de *CGOK*. Puesto que se conoce *CGID*, el mismo se puede usar para recuperar, a partir de una base de datos, los *CGOK* apropiados. *MUPI = m_{cg} / mRuido*, y el valor de ruido se puede comprobar también ya que ruido = m_{cg} mod *mRuido*.

Implementación de ejemplo

En otro aspecto de la exposición, los procedimientos descritos en la presente memoria se pueden implementar en un entorno informático según se describe en la presente memoria usando instrucciones ejecutables. Un conjunto de ejemplo de instrucciones para generar un identificador seguro y ofuscado de producto es el siguiente:

```
//codeGenID
int id = 122334;
int noise = 345;
var gr = new int[12];
int noiseSize = 1;
for (int i = 0; i < 12; i++)
{
   gr[i] = (id % numberOfGroups);
   noiseSize = noiseSize * Groups[id % numberOfGroups].Length;
   id = id / numberOfGroups;
}
```

```
var usedNoise = noise % noiseSize;
StringBuilder stb = new StringBuilder(12);
for (int i = 0; i < 12; i++)
{
   stb.Append(Groups[gr[i]][noise % Groups[gr[i]].Length]);
   noise = noise / Groups[gr[i]].Length;
}
Console.WriteLine("Code = " +stb.ToString());
string code = "GFL1BARARARA";
id = 0;
usedNoise = 0;
int carryOver = 0;
for (int i = 11; i >= 0; i--)
{
   var ch = code[i];
   for (int j = 0; j < numberOfGroups; j++)
   {
      var index = Groups[j].IndexOf(ch);
      if (index >= 0)
      {
         id = id * numberOfGroups + j;
         usedNoise = usedNoise * carryOver + index;
         carryOver = Groups[j].Length;
      }
   }
}
Console.WriteLine("Id = " + id);
}
```

Los algoritmos de clave simétrica tales como 3DES, AES y otros actúan sobre bloques de datos de entrada. Para que ocurra esto, la longitud de los datos de entrada debe ser exactamente igual a la longitud de los bloques o un múltiplo entero de la longitud de los bloques para ese algoritmo. En el ejemplo del cifrado AES de 128 bits, la longitud de los bloques puede ser 128 bits o 16 bytes. Los datos de entrada que se deben cifrar podrían tener, por ejemplo, un tamaño de 20 bytes, 4 bytes más allá de la longitud de los bloques en este ejemplo. Con el fin de conseguir que la longitud de los datos de entrada sea un múltiplo de la longitud de los bloques, es necesario

rellenar los datos de entrada. En este caso, el relleno se calcularía como: 20 bytes requieren (16 – (20-16)) = 12 bytes de relleno. De este modo, este relleno puede incrementar significativamente el tamaño del conjunto de datos cifrado, incrementando de manera similar la cantidad de almacenamiento físico de datos requerido para almacenar los datos cifrados. Tal como resulta evidente a partir de la implementación del ejemplo anterior, el procedimiento de ofuscación de la invención se puede configurar para ofuscar datos, tales como identificadores de producto, sin requerir un relleno de los datos de los identificadores de producto de entrada.

Integración con sistemas seguros de producción

Los sistemas y procedimientos descritos antes para ofuscar datos se pueden usar, de manera ventajosa, en combinación con sistemas para autenticar una producción de productos. En otro aspecto de la exposición, se proporciona un procedimiento para autenticar una producción de productos, incluyendo el procedimiento 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 productos en una tirada de producción de acuerdo con los datos de configuración firmados digitalmente; e imprimir el conjunto de identificadores de productos seguros sobre los productos de acuerdo con los datos de configuración firmados digitalmente.

Tal como se usa en la presente memoria, una entidad puede referirse a: (i) una persona, tal como un consumidor de un producto; (ii) un grupo, tal como un grupo que tiene 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 que represente una función comercial dentro de una empresa y similares. Adicionalmente, una entidad puede representar un punto en un flujo de trabajo, tal como para una autorización, la cual 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 pretende limitarse a ninguno de estos ejemplos y se puede ampliar a otras situaciones congruentes con los conceptos descritos en la presente memoria.

Módulos del sistema

A continuación se describen varios módulos. Cualquiera de los módulos puede estar ubicado de manera conjunta físicamente, o puede estar ubicado remotamente uno con respecto a otro. Adicionalmente, cualquiera de los módulos se podría combinar en términos lógicos o físicos en un único módulo sin desviarse con respecto al alcance de la invención.

Módulo de control

En referencia a la figura 3, el Módulo de Control (conocido también como “Orquestador”) (110) puede recibir una entrada de cualquiera de los otros módulos o de fuentes exteriores, y puede proporcionar instrucciones a los otros módulos del sistema basándose en programas preconfigurados y/o las entradas del operador en el mismo. También puede generar un resumen de panel de control del estado del sistema.

La entrada destinada al 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 va a 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 en 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, el Módulo de Autorización (130), el Módulo de Identificación (140) y el 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 basándose en 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, se pueden procesar solicitudes de verificación 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 intervalos 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 para 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 proporcione procesado criptográfico. La funcionalidad del Módulo de Autorización la puede llevar a cabo un ordenador con una placa incorporada con una clave de cifrado o clave privada PKI. El módulo puede estar equipado con características de tal manera que intentos de acceder a los datos darán 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 Firma. 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.

De acuerdo con una forma de realización, el procedimiento 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 productos en una tirada de producción de acuerdo con los datos de configuración firmados digitalmente; e imprimir el conjunto de identificadores de productos seguros en los productos de acuerdo con los datos de configuración firmados digitalmente.

En una forma de realización alternativa o adicional, los datos de configuración representan un intervalo de productos que van a ser producidos. En una forma de realización alternativa o adicional, los datos de configuración representan un intervalo de productos, máquinas, fábricas, intervalos o volúmenes de producto que están autorizados. Formas de realización alternativas o adicionales pueden incluir 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. Formas de realización alternativas o adicionales pueden incluir 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 memoria, 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 de acuerdo con 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 de acuerdo con funciones MD5, SHA-1, SHA-2, SHA-3/Keccak. A continuación, el compendio se puede cifrar 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 único para generar un identificador único 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 llevar a un procesado adicional para generar otro código que se imprime en el envase del producto.

Módulo de verificación

En referencia a la figura 5, 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. En referencia a la figura 3, el Módulo de Control (110) puede acceder a unos medios de almacenamiento 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 se puede proporcionar 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 puede incluir un procedimiento para inicializar un proceso con el fin de controlar de manera segura una instalación de producción, que comprende: recibir electrónicamente datos de configuración de unos medios electrónicos de almacenamiento de datos; 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.

Formas de realización alternativas o adicionales 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.

Formas de realización alternativas o adicionales 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.

Formas de realización alternativas o adicionales pueden incluir producir productos en una tirada de producción de acuerdo con los datos de configuración firmados digitalmente; e imprimir el conjunto de identificadores de producto seguros en los productos de acuerdo con los datos de configuración firmados digitalmente.

Formas de realización alternativas o adicionales pueden incluir que determinar si la tirada de producción está autorizada comprenda, además, recuperar datos de licencia de un servidor de licencias.

Generación de códigos de identificación

En referencia a la figura 4, 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 al Módulo de Identificación (140) de 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 procedimiento para generar un código con vistas a identificar de manera segura productos producidos en una instalación de producción, que incluye recibir electrónicamente datos de configuración de unos medios electrónicos de almacenamiento de datos; 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 hasta 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.

Formas de realización alternativas o adicionales pueden incluir recibir electrónicamente datos de configuración de unos medios electrónicos de almacenamiento de datos; 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 formas de realización alternativas o adicionales, la solicitud es de un intervalo de identificadores. Formas de realización alternativas o adicionales 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 almacenados previamente 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. Diferentes partes pueden estar provistas de medios diferentes para acceder al Módulo de Verificación. Por ejemplo, un minorista u otra forma de comerciante puede proveerse de 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 independiente 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 y/o testigos firmados 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 procedimientos descritos en la presente memoria se pueden implementar en *software* o *hardware* o cualquier combinación de los mismos. Los sistemas y procedimientos descritos en la presente memoria 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 procedimientos descritos en la presente memoria 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 uno de otro.

Los procedimientos se pueden implementar en un producto de programa informático 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 adecuado 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 informatizados 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, etc.). 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 informático puede ser un conjunto de instrucciones que se pueden usar, de manera directa o indirecta, en un ordenador. Los sistemas y procedimientos descritos en la presente memoria se pueden implementar usando lenguajes de programación tales como Flash™, JAVA™, C++, C, C#, Visual Basic™, JavaScript™, PHP, XML, HTML, etc., 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 adecuada para su uso en un entorno informático. El *software* puede incluir, aunque sin carácter limitativo, firmware, *software* residente, microcódigo, etc. En la implementación de interfaces entre módulos de programación se pueden usar protocolos tales como el SOAP/HTTP. Los componentes y la funcionalidad descritos en la presente memoria se pueden implementar en cualquier sistema operativo de escritorio que se ejecute en un entorno virtualizado o no virtualizado, utilizando cualquier lenguaje de programación adecuado para desarrollo de *software*, incluyendo, aunque sin carácter limitativo, diferentes versiones de Microsoft Windows™, Apple™ Mac™, iOS™, Unix™/X-Windows™, Linux™, etc.

Los procesadores adecuados 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 informatizado de almacenamiento de datos, tal como una memoria de solo lectura, una memoria de acceso aleatorio, ambas, o cualquier combinación de los dispositivos de almacenamiento de datos descritos en la presente memoria. 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 medios de almacenamiento *flash*. Los dispositivos de almacenamiento adecuados para incorporar de manera tangible instrucciones de programa informático 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 procedimientos descritos en la presente memoria se pueden implementar usando cualquier combinación de elementos de *software* o *hardware*. Los sistemas, módulos y procedimientos descritos en la presente memoria 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 procedimientos descritos en la presente memoria se pueden implementar en un sistema de ordenador que incluya un componente de fondo (*back-end*), tal como un servidor de datos, o que incluya un componente de software intermedio (*middleware*), tal como un servidor de aplicación o un servidor de Internet, o que incluya un componente de presentación (*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, etc. 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, transformaciones y equivalentes de ella.

REIVINDICACIONES

1. Procedimiento para ofuscar datos almacenados en una red, comprendiendo el procedimiento:

definir y almacenar información descriptiva del estado de una máquina informática como número de máquina, MNUM, incluyendo la información descriptiva del estado el número de bases que comprenden la información descriptiva del estado;

generar un identificador único y seguro de producto de máquina, MSUPI, como transformación matemática reversible de un identificador único de producto de máquina, MUPI, basándose en información descriptiva del estado de una máquina informática, comprendiendo la etapa de cálculo del *MSUPI*:

definir el número de etapas de manera que sea *imax*, para cada etapa generar un primer número aleatorio Clave de Ofuscación para Generación de Código, $CGOK_{i,1}$, y un segundo número aleatorio Clave de Ofuscación para Generación de Código, $CGOK_{i,2}$, comprendiendo dicha acción de generar:

calcular un primer número aleatorio $CGOK_{i,1}$, coprimo con un número basado en la información descriptiva del estado de la máquina informática, MNUM;

calcular un segundo número aleatorio $CGOK_{i,2}$, que presenta un tamaño de bits igual o menor que MNUM;

definir $m_{0,2} = MUPI$;

calcular para cada elemento *i*, desde *i* = 1 a *imax* – 1*:*

$m_{i,1} = (m_{i-1,2} \times CGOK_{i,1}) \bmod (MNUM);$
$m_{i,2} = (m_{i,1} \bmod CGOK_{i,2});$
si $(m_{i,2} > MNUM) \rightarrow m_{i,2} = m_{i,1}$;

definir $MSUPI = m_{imax,2}$;

almacenar el identificador único y seguro de producto de máquina, MSUPI, en unos medios electrónicos de almacenamiento de datos.

2. Procedimiento según una o más de las reivindicaciones anteriores, en el que la información descriptiva del estado de la máquina informática comprende una combinación de información de tiempo y número de producto.

3. Procedimiento según una o más de las reivindicaciones anteriores, en el que la información de tiempo incluye año juliano, día juliano, hora de producción y minuto de producción.

4. Procedimiento según una o más de las reivindicaciones anteriores, en el que la información descriptiva del estado incluye el valor de un contador incremental reinicializado sobre una base periódica.

5. Procedimiento según una o más de las reivindicaciones anteriores, en el que el número basado en la información descriptiva del estado de la máquina informática se calcula como 10 x 366 x 24 x 60 x *Identificador de Tiempo*.

6. Procedimiento según una o más de las reivindicaciones anteriores, en el que el *Identificador de Tiempo* se define como el entero 2210.

7. Procedimiento según una o más de las reivindicaciones anteriores, en el que un Identificador Único y Seguro de Producto, SUPI, un código alfanumérico de 12 caracteres, se obtiene de tal manera que $SUPI = (p \times m) \bmod (MNUM \times mRuido \times RunLim)$.

8. Procedimiento para generar un código con el fin de identificar de manera segura productos producidos en una instalación de producción, que comprende:

recibir electrónicamente datos de configuración de unos medios electrónicos de almacenamiento de datos;

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 productos 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, llevándose a cabo la generación del identificador de producto con un procedimiento según cualquier reivindicación anterior que incluye almacenar el identificador único y seguro de producto de máquina, MSUPI, en los medios electrónicos de almacenamiento de datos como identificador de producto;

transmitir el identificador único y seguro de producto de máquina desde el módulo de identificación hasta un módulo de firma;

firmar digitalmente el identificador único y seguro de producto de máquina en el módulo de firma; y

transmitir el identificador único y seguro de producto de máquina firmado digitalmente a un módulo de impresora.

9. Procedimiento según una o más de las reivindicaciones 1 a 7, que comprende, además:

recibir electrónicamente datos de configuración de unos medios electrónicos de almacenamiento de datos;

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 productos 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.

10. Procedimiento según la reivindicación 8, en el que la solicitud es de un intervalo de identificadores.

11. Procedimiento según una o más de las reivindicaciones 8 a 10, que comprende, además:

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.

12. Procedimiento según una o más de las reivindicaciones anteriores, en el que el identificador único de producto de máquina, MUPI, se transforma sin rellenar el identificador único de producto de máquina, MUPI, de tal manera que la longitud en bits del identificador único de producto de máquina, MUPI, es igual a la longitud en bits del identificador único y seguro de producto de máquina, MSUPI.

13. Procedimiento para verificar un identificador seguro y exclusivo de producto y máquina, que comprende:

recibir, por parte de un módulo de verificación, para su verificación, un *MSUPI*;

asignar *MSUPI* como $m_{0,2}$;

recuperar, por parte del módulo de verificación, un primer número aleatorio $CGOK_{i,1}$ y un segundo número aleatorio, $CGOK_{i,2}$ y el *imax* asociado a los números aleatorios recuperados y el *MSUPI* recibido;

calcular para cada elemento *i*, desde *i* = 1 a *imax* - 1:

$m_{i,1} = (m_{i-1,2} \bmod CGOK_{i,2})$;
si $(m_{i,2} > MNUM) \rightarrow m_{i,1} = m_{i-1,2}$;
$mi,2 = (m_{i,1} \times CGOK^{-1}{}_{i,1}) \bmod (MNUM)$;

$m_{cg} = m_{imax,2}$;

verificar $MUPI = m_{cg} / mRuido$ y valor de ruido = m_{cg} mod *mRuido*, donde *MUPI* se basa en información descriptiva del estado de una máquina informática.

14. Procedimiento según la reivindicación 13, en el que el identificador único y seguro de producto de máquina, MSUPI, se transforma sin haber rellenado el identificador único de producto de máquina, MUPI, de tal manera que la longitud en bits del identificador único de producto de máquina, MUPI, es igual a la longitud en bits del identificador único y seguro de producto de máquina, MSUPI.

15. Procedimiento según una o más de las reivindicaciones anteriores, en el que las autorizaciones que se reciben de un módulo de autorización se pueden transmitir a un módulo de verificación, de manera que posteriormente se pueden procesar solicitudes de verificación con respecto a dichas autorizaciones, y, en el que los datos transmitidos al módulo de verificación pueden incluir el identificador único y seguro de producto de máquina, MSUPI.

16. Sistema para ofuscar datos almacenados en una red, comprendiendo el sistema:

un procesador informático configurado para:

definir y almacenar información descriptiva del estado de una máquina informática como número de máquina, MNUM, incluyendo la información descriptiva del estado el número de bases que comprenden la información descriptiva del estado;

generar un identificador único y seguro de producto de máquina, MSUPI, como transformación matemática reversible de un identificador único de producto de máquina, MUPI, basándose en información descriptiva del estado de una máquina informática, comprendiendo la etapa de cálculo del *MSUPI*:

definir el número de etapas de manera que sea *imax*, para cada etapa generar un primer número aleatorio Clave de Ofuscación para Generación de Código, $CGOK_{i,1}$, y un segundo número aleatorio Clave de Ofuscación para Generación de Código, $CGOK_{i,2}$, comprendiendo dicha acción de generar:

calcular un primer número aleatorio, $CGOK_{i,1}$, coprimo con un número basado en la información descriptiva del estado de la máquina informática, MNUM;

calcular un segundo número aleatorio, $CGOK_{i,2}$, que presenta un tamaño de bits igual o menor que MNUM;

definir $m_{0,2} = MUPI$;

calcular para cada elemento *i*, desde *i* = 1 a *imax* – 1:

$m_{i,1} = (m_{i-1,2} \times CGOK_{i,1}) \bmod (MNUM)$;
$m_{i,2} = (m_{i,1} \bmod CGOK_{i,2})$;
si $(m_{i,2} > MNUM) \rightarrow m_{i,2} = m_{i,1}$;

definir $MSUPI = m_{imax,2}$; y

unos medios electrónicos de almacenamiento de datos configurados para almacenar el identificador único y seguro de producto de máquina, MSUPI, en los medios electrónicos de almacenamiento de datos.

17. Sistema para generar un código con el fin de identificar de manera segura productos producidos en una instalación de producción, que comprende un procesador informatizado configurado para ejecutar instrucciones con el fin de:

recibir electrónicamente datos de configuración de unos medios electrónicos de almacenamiento de datos;

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 productos 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, llevándose a cabo la generación del identificador de producto con un sistema según la reivindicación 16, almacenándose el identificador único y seguro de producto de máquina, MSUPI, en los medios electrónicos de almacenamiento de datos como identificador de producto;

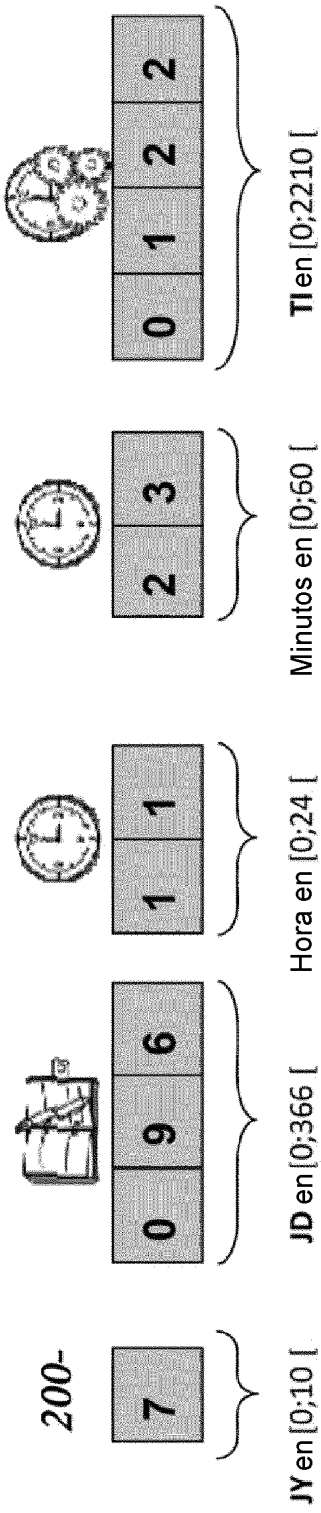
y estando configurado el procesador, además, para:

transmitir el identificador único y seguro de producto de máquina desde el módulo de identificación hasta un módulo de firma;

firmar digitalmente el identificador único y seguro de producto de máquina en el módulo de firma; y

transmitir el identificador único y seguro de producto de máquina firmado digitalmente a un módulo de impresora.

Fig. 1



$$MUPI = (((JY \times 366 + JD) \times 24 + Hora) \times 60 + Minutos) \times 2210 + TI$$

Fig. 2

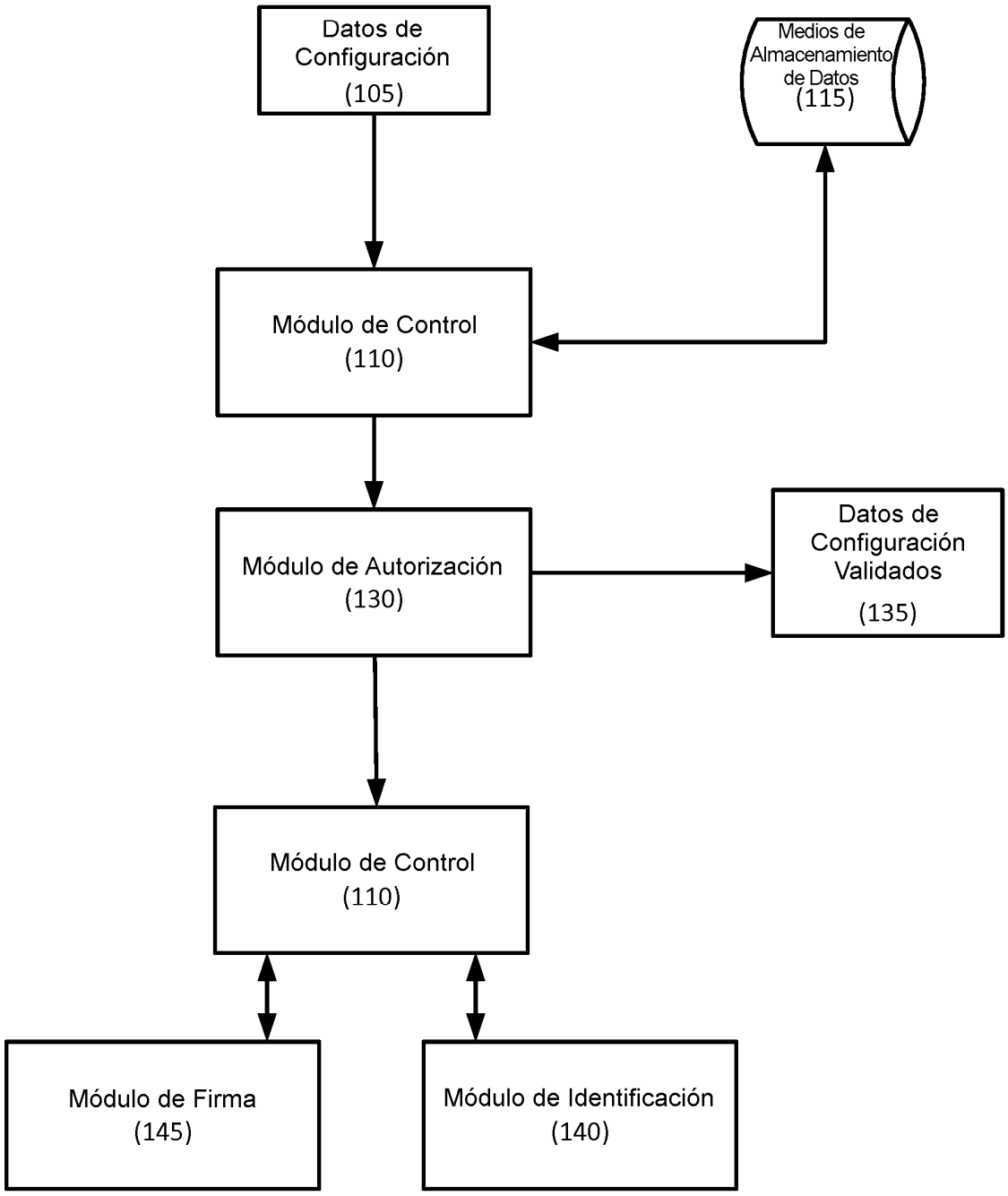
$$m_{0,2} = MUPI$$

$$\begin{cases} m_{i,1} = \left(m_{i-1,2} \times CGOK_{i,1}\right) \bmod \left(10 \times 366 \times 24 \times 60 \times 2210\right) \\ m_{i,2} = \left(m_{i,1} \oplus CGOK_{i,2}\right) \\ SI\left(m_{i,2} > 10\text{x}366\text{x}24\text{x}60\text{x}1100\text{x}2210\right) \rightarrow m_{i,2} = m_{i,1} \end{cases}$$

$$MSUPI = m_{8,2}$$

ES 2 738 415 T3

Fig. 3


Datos de Configuración (105)
Medios de Almacenamiento de Datos (115)
Módulo de Control (110)
Módulo de Autorización (130)
Datos de Configuración Validados (135)
Módulo de Control (110)
Módulo de Firma (145)
Módulo de Identificación (140)

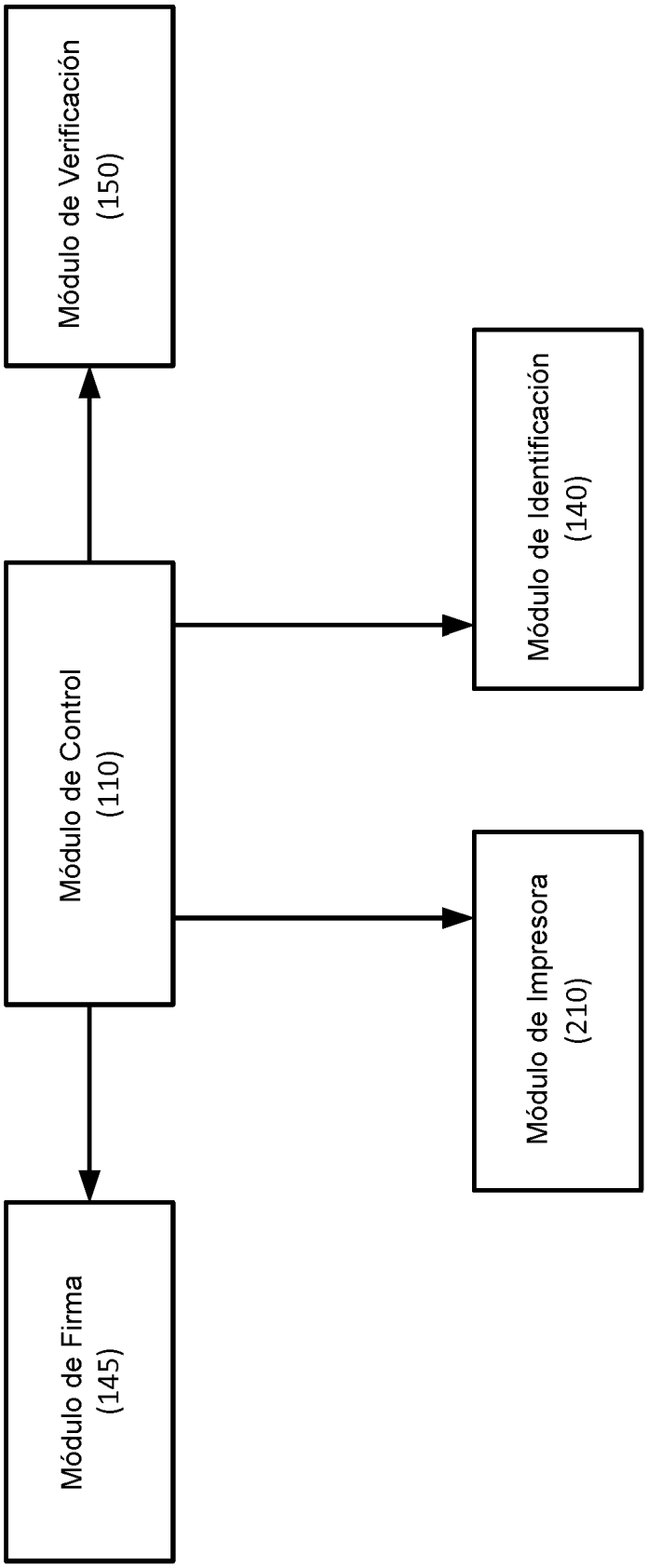
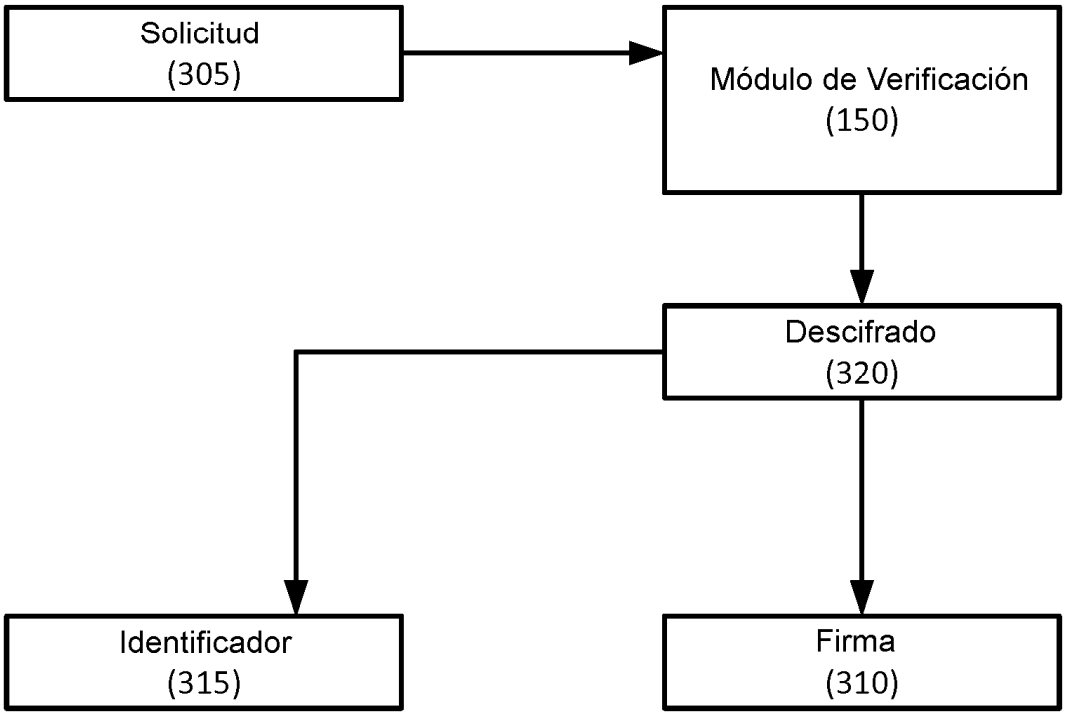

Módulo de Verificación
(150)
Módulo de Identificación
(140)
Módulo de Control
(110)
Módulo de Impresora
(210)
Módulo de Firma
(145)

Fig. 4

Fig. 5


Solicitud
(305)
Módulo de Verificación
(150)
Descifrado
(320)
Identificador
(315)
Firma
(310)