(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 724 877**

(51) Int. CI.:

G09C 5/00 (2006.01)
H04L 9/00 (2006.01)
H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **16.12.2013 PCT/EP2013/076725**

(87) Fecha y número de publicación internacional: **26.06.2014 WO14095737**

(96) Fecha de presentación y número de la solicitud europea: **16.12.2013 E 13821800 (3)**

(97) Fecha y número de publicación de la concesión europea: **13.02.2019 EP 2932494**

(54) Título: **Método y aparato para marcar artículos manufacturados usando una característica física**

(30) Prioridad:

17.12.2012 EP 12197525

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.09.2019

(73) Titular/es:

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

(72) Inventor/es:

CHANEZ, PATRICK y
FRADET, ERWAN

(74) Agente/Representante:

CURELL SUÑOL, S.L.P.

DESCRIPCIÓN

Método y aparato para marcar artículos manufacturados usando una característica física.

La presente invención se refiere a métodos y aparatos para marcar artículos manufacturados. En particular, la presente invención se refiere al marcaje de bienes envasados.

Los bienes falsificados y de contrabando son un problema mundial para clientes, fabricantes y autoridades gubernamentales. Los bienes falsificados, que son producciones no autorizadas de bienes, habitualmente de calidad inferior, se venden de manera ilegal por todo el mundo. Estos bienes son perjudiciales para el cliente ya que podrían ser de calidad inferior lo cual puede resultar peligroso (esto es en particular importante para productos tales como productos farmacéuticos u otros bienes consumidos). Los bienes falsificados son perjudiciales para los fabricantes ya que estos pueden sufrir una pérdida de reputación, un incremento de la competencia por parte de fabricantes ilegales que producen sus productos, e infracciones de otros derechos legales. Los bienes de contrabando, que son bienes manufacturados con la finalidad de evadir impuestos o regulaciones gubernamentales, constituyen también un problema considerable para los fabricantes y las autoridades gubernamentales. Estos bienes son desviados, comercializados o importados de manera ilegal lo cual da como resultado pérdidas significativas de ingresos para las autoridades gubernamentales debido a una recaudación incorrecta de tasas o impuestos.

Es ventajoso poder autenticar artículos manufacturados usando marcas exclusivas sobre los artículos sin necesidad de almacenar cada marca exclusiva en la ubicación en la que se van a autenticar los artículos. También es deseable poder detectar artículos falsificados, o artículos para los cuales se ha copiado la marca exclusiva de un producto auténtico, sin necesidad de almacenar un registro de autenticación de cada marca exclusiva.

La publicación de solicitud de patente internacional WO 01/43086 divulga el marcaje de productos usando una imagen generada para cada muestra de producto en una textura modificada específica.

La publicación de solicitud de patente internacional WO 97/24699 divulga la autenticación de mercancías por medio de una codificación cifrada de una característica física o química de las mismas.

La patente US nº 6.212.638 divulga la generación de una secuencia impredecible de símbolos para identificar un producto.

M. Lehtonen, N. Oertel, H. vogt, “Features, Identity, Tracing and Cryptography in Product Autentication”, *13th International Conference on Concurrent Enterprising*, 4 de junio de 2007, divulga una visión general de la autenticación de productos de la técnica.

En un aspecto de la divulgación, se proporciona un método de marcaje de un artículo manufacturado según la reivindicación 1.

Tal como se usa en la presente memoria, “identificador de producto único” significa un identificador que identifica de forma exclusiva un artículo manufacturado. A cada artículo manufacturado se le proporciona un identificador de producto único diferente. El identificador de producto único es, típicamente, una secuencia o valor numérico o alfanumérico.

Tal como se usa en la presente, “cifrado” significa el proceso de transformar información usando un algoritmo para conseguir que esa información sea ilegible para todos excepto aquellos que poseen un conocimiento especial en forma de una clave de cifrado. El descifrado es el proceso inverso. Una “clave de cifrado” es un elemento de información que se usa junto con un algoritmo de cifrado para cifrar o descifrar información. Una clave de cifrado es, típicamente, una secuencia o valor numérico o alfanumérico.

Tal como se usa en la presente memoria, la expresión “clave secreta” se usa para describir una clave usada en un *hash* con clave que se genera usando un identificador de producto único y una o más claves o elementos de datos adicionales. En el momento en el que es generada, la clave secreta no es conocida por ninguna otra parte más que la parte que creó la clave secreta. En este contexto, la expresión “clave secreta” no se limita a significar una clave privada en el contexto de un esquema de cifrado asimétrico.

Tal como se usa en la presente memoria, una “función *hash*” es una función que mapea datos de entrada con una salida de tamaño fijo (habitualmente menor que los datos de entrada) denominada valor *hash*. Típicamente, una función *hash* sustituye o transpone, o sustituye y transpone, la información para crear el valor *hash* o valor de ruido. Preferentemente, la función *hash* es una función *hash* criptográfica. La función *hash* criptográfica produce una huella digital o suma de comprobación de los datos de entrada. Puede considerarse que dos elementos de datos son idénticos si, usando la misma función *hash* criptográfica, producen el mismo valor *hash*. Ventajosamente, la función *hash* es una función *hash* unidireccional lo cual significa que es imposible

computacionalmente obtener los datos de entrada a partir del valor *hash*. Estas propiedades se pueden usar en un proceso de autenticación, tal como se describirá. Una función *hash* se puede codificar combinando una clave secreta y un mensaje de entrada con el fin de crear un ruido o valor *hash* con clave.

Tal como se usa en la presente, la expresión “valor de ruido” significa un valor *hash*, o un valor *hash* con clave, o una secuencia de valores o caracteres derivada directamente de un valor *hash* y una clave secreta.

La propiedad física medida del artículo manufacturado puede ser cualquier propiedad física medida y se puede basar en la masa, el tamaño, la forma, la textura o estructuración superficial, el color, la composición química o la respuesta a un estímulo, tal como una respuesta a estímulos eléctricos, magnéticos u ópticos. Preferentemente, la propiedad física medida se selecciona y mide a una resolución tal que sea probable que sea exclusiva para cada artículo manufacturado, o al menos que sea más probable que sea diferente que igual para cualesquiera dos artículos manufacturados. Preferentemente, la propiedad física medida proporciona una firma física para el artículo manufacturado. En una forma de realización preferida, la propiedad física medida es una imagen de una porción del envasado del artículo manufacturado.

El identificador seguro puede ser cualquier tipo de identificador aunque, preferentemente, es una secuencia o valor numérico o alfanumérico. La marca también puede ser una secuencia de caracteres o números o puede ser una representación gráfica, tal como un código de barras unidimensional o bidimensional.

En una forma de realización, la etapa de generación del identificador seguro comprende generar un primer identificador cifrando el identificador de producto único junto con el valor de ruido del sistema y generar el identificador seguro cifrando el primer identificador junto con el valor de ruido físico.

En esta forma de realización, el método puede comprender, además, autenticar el artículo manufacturado en un centro de verificación, comprendiendo la etapa de autenticación: identificar la marca en el artículo; descifrar la marca para obtener el primer identificador y el valor de ruido físico; descifrar el primer identificador para obtener el identificador de producto único y el valor del ruido del sistema; generar una clave física nueva a partir de una propiedad física medida del artículo manufacturado; generar una copia nueva del valor de ruido físico ejecutando una función *hash* sobre la clave física nueva y el identificador de producto único derivado; comparar la copia nueva del valor de ruido físico con el valor de ruido físico derivado; y proporcionar una indicación de si el valor de ruido físico derivado es idéntico a o está correlacionado con la copia nueva del valor de ruido físico.

La etapa de comparación puede comprender obtener una puntuación de correlación y la etapa de proporcionar una indicación comprende proporcionar una indicación de si la puntuación de correlación es mayor que un valor de umbral.

En esta forma de realización, la etapa de autenticación puede comprender, además: generar una copia nueva de la clave secreta a partir del identificador de producto único y dicha una o más claves de cifrado; generar una copia nueva del valor de ruido del sistema ejecutando una función *hash* sobre la copia nueva de la clave secreta y el identificador de producto único; comparar la copia nueva del valor de ruido del sistema con el valor de ruido derivado del sistema; y proporcionar una indicación de si la copia nueva del valor de ruido del sistema y el valor de ruido derivado del sistema son idénticos.

En otra forma de realización, la etapa de generación del identificador seguro comprende generar un primer identificador seguro cifrando el identificador de producto único junto con el valor de ruido del sistema; generar un segundo identificador seguro cifrando el identificador de producto único junto con el valor de ruido físico; y poner una marca en el artículo manufacturado, comprendiendo la marca el primer y el segundo identificadores seguros o un identificador o identificadores derivados del primer y segundo identificadores seguros.

En esta forma de realización, el método puede comprender, además, autenticar el artículo manufacturado en un centro de verificación, comprendiendo la etapa de autenticación: identificar la marca en el artículo; descifrar la marca para obtener el identificador de producto único, el valor de ruido del sistema y el valor de ruido físico; generar una copia nueva de la clave secreta a partir del identificador de producto único y de dicha una o más claves de cifrado; generar una copia nueva del valor de ruido del sistema ejecutando una función *hash* sobre la copia nueva de la clave secreta y el identificador de producto único; comparar la copia nueva del valor de ruido del sistema con el valor de ruido derivado del sistema; generar una clave física nueva a partir de una propiedad física medida del artículo manufacturado; generar una copia nueva del valor de ruido físico ejecutando una función *hash* sobre la clave física nueva y el identificador de producto único derivado; comparar la copia nueva del valor de ruido físico con el valor de ruido físico derivado; y proporcionar una indicación tanto de si la copia nueva del valor de ruido del sistema es idéntica al valor de ruido derivado del sistema como de si la copia nueva del valor de ruido físico es idéntica a o está correlacionada con el valor de ruido físico obtenido.

En cualquiera de las formas de realización, la etapa de generar el primer identificador seguro puede comprender cifrar el identificador de producto único y el valor de ruido del sistema usando una clave de un generador de códigos, comprendiendo la etapa de generación del segundo identificador seguro combinar el primer identificador

seguro y el valor de ruido físico junto con un ID de generador de código, y en donde la clave de generador de código se puede derivar u obtener a partir de una tabla de consulta en un centro de verificación usando el ID de generador de códigos.

En cualquiera de las formas de realización, el método puede comprender, además, la etapa de almacenar dicha una o más claves de cifrado en un centro de verificación. Dicha una o más claves de cifrado pueden comprender una clave estática y una clave dinámica, y en donde se crea una clave dinámica nueva para cada lote de artículos manufacturados mientras que se usa la misma clave estática para diversos lotes de artículos manufacturados.

El identificador de producto único puede incluir información que identifica un lote de artículos al cual pertenece el artículo.

La invención proporciona la capacidad de realizar autenticaciones tanto sobre la base de información del fabricante, es decir, las diversas claves de cifrado, como sobre la base de una propiedad física del artículo. Esto proporciona dos capas de autenticación, y permite la detección de clonación de identificadores sobre artículos genuinos, pero no requiere un almacenamiento a gran escala de códigos de autenticación.

En otro aspecto de la invención, se proporciona un aparato para marcar un artículo manufacturado, según la reivindicación 15:

En una forma de realización, los medios de procesado están configurados para: generar un primer identificador para cada artículo manufacturado, cifrando el identificador de producto único junto la clave secreta o el valor de ruido del sistema; y generar el identificador seguro para cada artículo manufacturado, cifrando el primer identificador junto con el valor de ruido físico.

En otra forma de realización, los medios de procesado están configurados para: generar un primer identificador seguro para cada artículo manufacturado, cifrando el identificador de producto único junto con la clave secreta o el valor de ruido del sistema y generar un segundo identificador seguro para cada artículo manufacturado, cifrando el identificador de producto único junto con la clave física o el valor de ruido físico; y el marcador está configurado para marcar cada artículo manufacturado, con el primer identificador seguro y el segundo identificador seguro o un identificador o identificadores derivados del primer y del segundo identificadores seguros.

El artículo manufacturado puede ser un recipiente de embalaje que contiene un producto tabacalero. Los ejemplos de productos tabacaleros son cigarrillos, tabaco en hojas sueltas, puros, y cartuchos o recargas para sistemas para fumar calefactados eléctricamente u otros sistemas de cigarrillos electrónicos.

La invención permite autenticar artículos manufacturados sin requerir el almacenamiento de grandes volúmenes de información. Esto es importante para cualquier sistema práctico adecuado para autenticar artículos producidos con altos volúmenes. Además, el uso de una clave física en combinación con un identificador de producto único (UPI) hace que aumente la seguridad y hace que resulte más difícil la producción de bienes falsificados y de contrabando. La adición de una clave física proporciona un sistema que puede detectar la clonación y resulta difícil de duplicar. Incluso si un falsificador tuviera conocimiento de la herramienta en particular usada para generar la clave física, la combinación de la clave física con un UPI para producir un identificador hace que la clonación resulte casi imposible. La invención también permite llevar a cabo una autenticación en línea, es decir, conectada a un centro de verificación a través de una red de comunicaciones sobre la base del valor de ruido del sistema, al mismo tiempo que permite llevar a cabo una autenticación fuera de línea sobre la base del valor de ruido físico. El marcaje requerido sobre cada artículo es simplemente uno o más códigos y, por lo tanto, añade gastos muy reducidos a cada artículo en comparación con algunas otras soluciones, que se basan en etiquetas caras que son técnicamente difíciles de reproducir.

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 es una vista esquemática de un sistema de marcaje de acuerdo con una forma de realización de la invención;

la Figura 2 ilustra cómo se obtienen el valor de ruido del sistema y el valor de ruido físico;

la Figura 3 es un diagrama de flujo que muestra un método de marcaje de una forma de realización de la invención, que se puede llevar a cabo sobre el sistema de la Figura 1;

la Figura 4 es un diagrama de flujo que muestra un método de autenticación para la forma de realización de la invención mostrada en la Figura 3, que se puede llevar a cabo sobre el sistema de la Figura 1;

la Figura 5 es un diagrama de flujo que muestra un método de marcaje de otra forma de realización de la invención, que se puede llevar a cabo sobre el sistema de la Figura 1; y

la Figura 6 es un diagrama de flujo que muestra un método de autenticación para la forma de realización de la invención mostrada en la Figura 5, y que se puede llevar a cabo sobre el sistema de la Figura 1.

Las marcas exclusivas sobre artículos manufacturados se pueden usar para realizar un seguimiento de los artículos. Por ejemplo, un pedido de un cliente se puede vincular a la etiqueta o etiquetas identificativas de una caja o cajas de transporte particulares que contienen bienes pedidos. “Bienes” en este contexto, significa artículos manufacturados u otras mercancías destinadas a su distribución o venta a clientes. Esto permite que el cliente, el fabricante y todos los intermediarios realicen de manera constante un seguimiento de la ubicación de los bienes requeridos. Esto se puede lograr usando escáneres para escanear los identificadores y comunicarse con un centro de verificación. Alternativamente, los identificadores pueden ser leídos por un humano, el cual, a continuación, puede comunicar manualmente con un centro de verificación. Los identificadores también pueden ser usados por clientes, autoridades nacionales y otras partes, con el fin de verificar que un artículo particular contiene productos genuinos. Por ejemplo, una parte puede usar un escáner para leer el identificador que se encuentra en una caja de transporte (o el identificador puede ser leído por un humano, según se ha descrito anteriormente). Los detalles del identificador se pueden enviar a un centro de verificación. A continuación, el centro de verificación puede consultar, o procesar de otro modo, los detalles del identificador, determinar los detalles de producción de la caja de transporte y enviar esos detalles al escáner, permitiendo, así, que la parte verifique la caja de transporte, y los productos contenidos en la misma, como genuinos. En caso de que la base de datos central no reconozca el identificador, la parte puede suponer que las mercancías en cuestión son falsificadas. Los identificadores también se pueden usar para rastrear artículos. Por ejemplo, si el fabricante necesita recordar los productos de un número seleccionado de cajas de transporte, esas cajas de transporte se pueden rastrear usando sus identificadores.

La Figura 1 es una vista esquemática de un sistema de marcaje de acuerdo con una forma de realización de la invención. En esta forma de realización, el sistema 101 comprende uno o más centros de producción 103, 105, 107 para producir artículos manufacturados 109. Cada centro de producción puede comprender una cadena o instalación de producción la cual puede ser una cadena de fabricación y envasado de cigarrillos. Preferentemente, la producción se lleva a cabo en lotes, dedicándose cada lote a la producción de un cierto número de artículos manufacturados individuales. Si hay dos o más centros de producción, estos pueden estar ubicados físicamente en el mismo emplazamiento de fabricación o en uno diferente. En esta forma de realización preferida, el sistema incluye centros de producción 103, 105, 107, aunque, de hecho, la invención se puede realizar en un punto de importación, un punto de distribución, las instalaciones de un comprador, las instalaciones de un mayorista o cualquier otro punto de la cadena de suministro.

Cada centro de producción incluye un generador de códigos 111 para generar códigos correspondientes a los artículos manufacturados 109. Preferentemente, el generador de códigos 111 es un microcontrolador u ordenador totalmente autónomo dedicado a un centro de producción particular. Cada centro de producción incluye, también, un generador de claves físicas 112, que mide o codifica una propiedad física de cada artículo manufacturado y convierte la misma en una clave física 207. El generador de códigos 111 usa las claves físicas para generar códigos con vistas a su marcaje en los artículos.

En esta forma de realización, el generador de claves físicas es del tipo descrito en el documento WO 2007/071788. Una porción del envasado de cada artículo se ilumina y una imagen de la porción iluminada es capturada por un sensor digital de imágenes. La porción del envasado se selecciona por su microestructura caótica, estable en el tiempo. Los materiales tales como el papel y el cartón tienen una microestructura caótica que se puede usar como “huella dactilar” del artículo. La imagen de la microestructura de la porción del artículo se convierte en una clave física o firma, según se describe en el documento WO2 007/071788, en forma de un valor o matriz alfanumérico. Un generador de claves físicas de este tipo está disponible en Signoptic Technologies, Savoie Technolac, 5 allée Lac d’Aiguebelette BP340 F-73375, LE BOURGET-DU-LAC, Francia. No obstante, puede usarse cualquier tipo de generador de claves físicas y el mismo podría basarse en otras propiedades físicas del artículo, tales como la masa o la forma, o incluso podría basarse en propiedades químicas o biológicas del artículo.

En esta forma de realización, cada centro de producción incluye también un marcador 113 para marcar los códigos generados en los artículos manufacturados 109. El marcador 113 puede comprender cualesquiera medios de marcaje adecuados, por ejemplo, aunque sin carácter limitativo, una impresora de chorros de tinta continua, una impresora de chorros de tinta por goteo bajo demanda, una impresora holográfica, una impresora por láser, o cualquier otra impresora o marcador que permita la impresión o marcaje de los códigos generados en los artículos manufacturados individuales. La impresión o marcaje de los códigos generados puede ser sobre cada artículo, sobre un envase externo, sobre etiquetas o de cualquier otra manera adecuada. En una forma de realización, los códigos generados se imprimen en etiquetas o rótulos adhesivos que se aplicarán a los artículos manufacturados, preferentemente de manera no separable. En una forma de realización, los códigos generados se imprimen por medio de un haz de láser sobre una capa de material sensible al láser, depositado sobre el

artículo manufacturado o sobre el envasado del artículo. Este método permite imprimir un código a través de una capa de envoltura transparente.

El sistema 101 comprende, además, un centro de verificación 114 que incluye un generador de claves 115 para generar claves 209, 211 con vistas a su uso en el marcaje y la autenticación de los artículos manufacturados y un servidor central 117. En esta forma de realización, el generador de códigos 111 se puede comunicar con el centro de verificación 114 por medio de una conexión de internet 119 y un servidor 121 local con respecto al centro de producción, o a través de otros medios de comunicación de datos. Alternativamente, el generador de códigos 111 se podría comunicar con el centro de verificación por medio de un portal de fabricación dedicado a uno o más centros de producción.

El generador de claves 115 genera una clave criptográfica, a la que se hace referencia en la presente como clave estática. El generador de claves 115 genera una versión no cifrada de la clave estática y una versión cifrada de la clave estática. La versión no cifrada de la clave estática, a la que se hace referencia, en la presente, como clave estática activa 209, se muestra con un borde continuo en la Figura 1. La versión cifrada de la clave estática, a la que se hace referencia, en la presente, como clave estática inactiva 211, se muestra con un borde de trazos en la Figura 1. La clave estática activa 209, es decir, la versión no cifrada de la clave estática, se genera en el generador de claves 115 y, por lo tanto, es accesible para el servidor central 117. El generador de claves 115 envía la clave estática inactiva 211 al generador de códigos 111 en el centro de producción 103, 105, 107.

La clave estática inactiva 211 se puede enviar desde el generador de claves 115 al generador de códigos 111 en un soporte de datos no volátil, por ejemplo, un CD-Rom, un DVD-Rom o un disco duro extraíble. El soporte de datos se transfiere físicamente al generador de códigos 111 en el centro de producción 103, 105, 107. Alternativamente, la clave estática inactiva 211 se puede enviar desde el generador de claves 115 al generador de códigos 111 por medio de una conexión en red segura, por ejemplo, una que conlleve un cifrado. Esto se puede producir a solicitud del generador de códigos 111. Esto garantiza la autenticidad, la confidencialidad y la integridad de la clave estática.

El generador de claves 115 genera también el código de activación 213, el cual comprende la clave o código para descifrar la clave estática inactiva 211 con el fin de formar la clave estática activa 209. Este código de activación 213 es también accesible para el servidor central 117. Preferentemente, la clave estática activa 209 y el código de activación 213 se almacenan junto con la identificación del centro de producción 103, 105, 107 al cual están asignados.

En una forma de realización, la clave estática comprende una serie de porciones. La porción principal puede ser una pluralidad de códigos secretos, por ejemplo, una matriz de sal. Una matriz de sal puede ser, por ejemplo, una cadena larga de dígitos aleatorios o seudoaleatorios de caracteres. La serie de porciones puede incluir, además, un identificador único para la clave estática, un código serializado que defina cómo se va a combinar la clave estática con una clave dinámica (lo cual se describe posteriormente), un certificado criptográfico digital asociado al identificador único de la clave estática y una licencia o política de claves estáticas que contiene el certificado criptográfico digital generado anteriormente.

Preferentemente, la clave estática inactiva, es decir, la versión cifrada de la clave estática y, en particular, la pluralidad de códigos secretos, se cifra usando un cifrado fuerte. Un ejemplo de cifrado adecuado es el cifrado por bloques Triple DES (Norma de Cifrado de Datos) o el cifrado por bloques Triple DES/Rijandel. Los dos aplican tres veces el algoritmo de cifrado de Norma de Cifrado de Datos a cada bloque de datos, y el Triple DES/Rijandel es una variante menor del Triple DES que ha sido desarrollado por IBM. En ese caso, la clave del Triple DES o Triple DES/Rijandel comprende el código de activación 213. Así, en una forma de realización preferida, la clave estática activa 209 no está cifrada, la clave inactiva 211 se cifra usando la clave del Triple DES o Triple DES/Rijandel, y el código de activación 213 comprende esa clave del Triple DES o Triple DES/Rijandel.

En la siguiente etapa 203, se registra la clave estática inactiva 211 recibida por el generador de códigos 111. Esto lo lleva a cabo el generador de códigos 111 que envía al centro de verificación 114 información 215 sobre la clave estática recibida y cualquier información relevante de la máquina (no mostrada). Esta se envía, preferentemente, por medio de una conexión de internet segura 119, tal como se muestra en la Figura 1, aunque se puede enviar por cualquier otra vía adecuada. El centro de verificación 114 devuelve al generador de códigos 111 el código de activación 213. El código de activación 213 permite activar la clave estática inactiva 211, y esto se muestra esquemáticamente en la referencia 217. Preferentemente, el código de activación 213 se envía también por medio de la conexión de internet segura 119, tal como se muestra en la Figura 1. Preferentemente, el procedimiento de registro está dispuesto de tal manera que la clave estática activa 209 no se transfiere nunca a través de internet.

El procedimiento de registro puede adoptar la forma de un mecanismo de intercambio convencional de par de claves pública/privada. Este puede usar un par de claves asimétricas asociado al certificado criptográfico digital que forma parte de la clave estática, según se ha descrito anteriormente. En ese caso, la clave pública del par de claves asimétricas puede presentarse en forma de una clave emitida por un tercero, por ejemplo, una autoridad

gubernamental. La información 215 sobre la clave estática recibida que se envía desde el generador de códigos 111 al centro de verificación 114 puede comprender el identificador único correspondiente a la clave estática que forma parte de la clave estática, según se ha descrito anteriormente. La información relevante de la máquina (no mostrada) que se envía también desde el generador de códigos 111 al centro de verificación 114 puede comprender un identificador único o certificado para el generador de códigos 111 o el centro de producción. Ese identificador único puede incluir información sobre la ubicación e identidad del generador de códigos o centro de producción, el cual ha sido autorizado previamente para la producción. Preferentemente, el identificador único de clave estática y el identificador de generador de códigos o de centro de producción se cifran usando la clave pública del par de claves asimétricas asociado al certificado de la clave estática.

Una vez que el centro de verificación 114 recibe el identificador único de clave estática cifrado y el identificador de generador de códigos o de centro de producción, el centro de verificación 114 puede realizar un descifrado usando la clave privada del par de claves asimétricas asociado al certificado de la clave estática. A continuación, el centro de verificación puede comprobar que el identificador único de clave estática y el identificador de generador de códigos o de centro de producción son válidos. A continuación, el centro de verificación 114 devuelve al generador de códigos 111 el código de activación 213. Tal como ya se ha mencionado, preferentemente, el código de activación 213 se presenta en forma de un cifrado de Triple DES o Triple DES/Rijandel. El centro de verificación cifra el código de activación (por ejemplo, el cifrado de Triple DES o Triple DES/Rijandel) con la clave pública del par de claves asimétricas asociado al certificado de la clave estática. Esto permite que el código de activación (por ejemplo, el cifrado de Triple DES o Triple DES/Rijandel) sea descifrado por el generador de códigos usando la clave privada del par de claves asimétricas asociado al certificado de la clave estática. A continuación, la clave estática inactiva 211 se puede activar usando el código de activación descifrado 213 con el fin de formar la clave estática activa 209.

Una vez que se ha activado la clave estática inactiva 211 en el generador de códigos 111, el centro de producción puede fabricar artículos y producir códigos para los artículos manufacturados en el generador de códigos 111.

El generador de códigos 111 genera una clave nueva, a la que se hace referencia, en la presente, como clave dinámica 219, para cada lote de artículos manufacturados. Preferentemente, la clave dinámica 219 es un código secreto aleatorio, tal como un número aleatorio. El generador de códigos usa la clave dinámica 219 para un lote, junto con la clave estática activa 209, con el fin de generar una clave secreta 223. La clave secreta 223 es la n usada en combinación con las claves físicas y un identificador de producto único (UPI) para cada artículo con el fin de generar códigos 221 (por ejemplo, códigos alfanuméricos) que se marcarán en los artículos manufacturados en ese lote. En esta forma de realización, el UPI para cada artículo comprende detalles de producción que identifican el momento de producción junto con un valor de contador incremental para distinguir artículos producidos dentro de un periodo de tiempo individual por el mismo centro de producción.

El generador de códigos usa una función *hash* criptográfica sobre una combinación del UPI con la clave secreta y una combinación del UPI con la clave física. Esto crea huellas dactilares digitales, a las que se hace referencia, en la presente, como “valores de ruido”, para el artículo, y estos valores de ruido se usan para generar los códigos 221 que se marcan en los artículos por parte del marcador 113. Además de funciones *hash* criptográficas usadas comúnmente, hay disponible una variedad de técnicas para generar los valores *hash* o valores de ruido, incluyendo, aunque sin carácter limitativo: transposición, sustitución, sustitución por tablas e indexación.

La Figura 2 ilustra el método de generación de los valores de ruido llevado a cabo por el generador de códigos 111. Para generar el valor de ruido de sistema 225, en primer lugar se deriva la clave secreta a partir de la clave estática activa 209, la clave dinámica 219 y el UPI 221. La clave dinámica 219 y la clave estática activa 209 son conocidas únicamente para el centro de verificación 114 y el generador de códigos 111. En la etapa 301, la clave dinámica y el UPI se usan para extraer la clave secreta de la matriz de sal contenida en la clave estática, de acuerdo con el código serializado dentro de la clave estática. A continuación, a la clave secreta 223 y el UPI 221 se les aplica una función *hash* en la etapa 303 con el fin de producir el ruido de sistema para el artículo. Para generar el valor de ruido físico 227, a la clave física 207 se le aplica una función *hash* con el UPI 221 en la etapa 305. La función *hash* usada para generar el valor de ruido de sistema puede ser igual o diferente de la función *hash* usada para generar el valor de ruido físico.

La Figura 3 ilustra un método de uso del valor de ruido de sistema y el valor de ruido físico para generar un identificador seguro para cada artículo de acuerdo con una primera forma de realización de la invención. En la etapa 311, se combinan el valor de ruido de sistema 225 y el UPI 221. En la etapa 313, el valor de ruido del sistema y el UPI combinados se cifran por medio de la clave de ofuscación de generador de códigos (CGOK) 231 para producir un primer identificador 241. La CGOK es particular del generador de códigos y se precarga en el generador de códigos. A continuación, el primer identificador 241 se combina con el valor de ruido físico 227 y un identificador de generador de códigos 233. El identificador de generador de códigos (CGID) 233 permitirá obtener la CGOK durante la autenticación. A continuación, la combinación del primer identificador, el valor de ruido físico y el CGID se cifra usando una clave global 235 en la etapa 317 para producir el identificador seguro 251. La clave global 235 es común para todos los centros de producción, y puede formar parte de un par de claves

simétricas o asimétricas conocido por el centro de verificación. A continuación, el identificador seguro 251 se marca en el artículo en la etapa 319 por medio del marcador 113.

El generador de códigos 111 o el centro de producción 103, 105, 107 mantiene un recuento de los códigos que se marcan sobre los artículos manufacturados. Además, el generador de códigos 111 envía la clave dinámica 219 para cada lote, junto con información sobre el lote (no mostrada), al centro de verificación 114. Esto se puede llevar a cabo por medio de una conexión de internet 119. La información sobre el lote puede incluir diversos elementos de información, por ejemplo, aunque sin carácter limitativo, marca comercial, mercado pretendido o destino pretendido. No es necesario que las claves dinámicas 219 se envíen al centro de verificación 114 en tiempo real, y se pueden comunicar al centro de verificación en cualquier momento adecuado, por ejemplo mensualmente. Las claves dinámicas 219 enviadas al centro de verificación 114 se almacenan en una base de datos (por ejemplo, en el servidor central 117) en o accesible desde el centro de verificación 114. Preferentemente, la clave dinámica 219 para cada lote se almacena junto con la información de lote enviada al centro de verificación 114 al mismo tiempo.

Preferentemente, la clave estática activa 209 se elimina cuando el generador de códigos 111 en un centro de producción particular 103, 105, 107 se sitúa fuera de servicio. Esto evita que un usuario malicioso obtenga acceso a la clave estática activa 209 sin un registro adecuado. Pueden proporcionarse medios adicionales para deshabilitar el generador de códigos 111 y evitar un uso no autorizado del generador de códigos 111 y el centro de producción.

La Figura 4 ilustra las etapas llevadas a cabo por el centro de verificación 114 y por el usuario 601 cuando un usuario 601 desea autenticar un artículo manufacturado individual marcado de acuerdo con el proceso de la Figura 3. El usuario 601 lee el código 621 sobre el artículo y lo envía al centro de verificación 114. Esto se muestra en la Figura 1. El usuario 601 puede enviar el código al centro de verificación 114 por cualesquiera medios adecuados, tales como una conexión de Internet segura o no segura.

El centro de verificación recibe el identificador seguro en la etapa 321. El identificador seguro se descifra usando la clave global 235 (o la clave correspondiente del par de claves en caso de que se usen claves asimétricas) en la etapa 323 para desvelar el valor de ruido físico 227 y el primer identificador 241. Se desvela también el CGID. Usando una tabla de consulta, a continuación, a partir del CGID, se obtiene la CGOK 231. A continuación, el primer ID se descifra en la etapa 325 usando la CGOK 231 con el fin de desvelar el ruido de sistema 225 y el UPI 221. Con esta información, junto con la clave estática activa 209 y la clave dinámica 219 y una clave física nueva, pueden reproducirse tanto el valor de ruido físico como el valor de ruido de sistema para autenticar el artículo.

Para reproducir el valor de ruido físico, el usuario 601 debe obtener una clave física nueva en la etapa 327 registrando una imagen de la porción del artículo de la misma manera y bajo las mismas condiciones que las usadas para generar la clave física original 207. A continuación, al UPI y a la clave física nueva se les aplica una función *hash* para generar un valor de ruido físico nuevo en la etapa 329. En la etapa 331, el ruido físico nuevo se compara con el valor de ruido físico extraído desvelado en la etapa 323. Si el valor de ruido físico nuevo es suficientemente similar al valor de ruido físico extraído, entonces se completa una parte del proceso de autenticación. Si el valor de ruido físico nuevo no es suficientemente similar al valor de ruido físico extraído, entonces se determina que el artículo no es auténtico en la etapa 339.

Puede que se requiera que el valor de ruido físico nuevo sea idéntico al valor de ruido físico extraído con el fin de que el artículo sea considerado auténtico. No obstante, es posible prever algunas diferencias entre el valor de ruido físico nuevo y el valor de ruido físico extraído usando una puntuación de correlación y requiriendo una puntuación de correlación de umbral con el fin de considerar el artículo auténtico. El documento US 2005/0257064 describe un método estadístico adecuado para calcular un grado de correlación o similitud entre dos firmas digitales derivadas de propiedades físicas medidas de un medio fibroso.

Cabe la posibilidad de que o bien el usuario 601 o bien el centro de verificación 114 lleve a cabo la etapa 329 y 331. Si al usuario 601 se le proporciona el UPI por parte del centro de verificación, el usuario final puede autenticar el artículo basándose en el valor de ruido físico. De manera similar, si la clave física nueva se proporciona al centro de verificación 114, el centro de verificación puede autenticar el artículo basándose en el valor de ruido físico.

Para reproducir el valor de ruido de sistema, debe regenerarse la clave secreta. En la etapa 333, usando el UPI y el CGID, el centro de verificación 114 puede recuperar la clave dinámica 219 y la clave estática activa 209 a partir de registros mantenidos en el centro de verificación. A continuación, puede regenerarse la clave secreta usando el UPI 221, la clave dinámica 219 y la clave estática activa 209. En la etapa 335, se reproducen un valor de ruido de sistema nuevo ejecutando una función *hash* al UPI y a la clave secreta. En la etapa 337, el valor de ruido de sistema nuevo se compara con el valor de ruido de sistema extraído en la etapa 325. Si el valor de ruido de sistema nuevo y el valor de ruido de sistema extraído son idénticos, puede determinarse, en la etapa 339, que el artículo es auténtico.

En una forma de realización, se requieren comparaciones tanto del valor de ruido físico como del valor de ruido de sistema con el fin de que un artículo sea considerado auténtico. No obstante, es posible permitir una autenticación sobre la base de solamente una de estas comprobaciones, si así se desea.

A partir de la clave estática activa derivada 209, puede determinarse el centro de producción 103, 105, 107 en el cual se fabricó el artículo, ya que las claves estáticas activas se almacenan preferentemente en el centro de verificación junto con detalles de sus centros de producción asociados. A partir de la clave dinámica derivada 219, puede determinarse la información de lote correspondiente al artículo ya que las claves dinámicas se almacenan, preferentemente, en el centro de verificación junto con la información de lote asociada. De este modo, el centro de verificación 114 puede obtener, a partir del código 221 enviado desde el usuario 601, varios elementos de información 603 sobre el artículo individual así como la comprobación de la autenticidad del artículo. A continuación, todas las porciones de la información 603, o porciones seleccionadas de la misma, que incluyen una indicación de si el artículo es o no auténtico se pueden enviar al usuario 601. Esto se muestra en la Figura 1. La información 603 se envía, preferentemente, al usuario 601 a través de los mismos medios por los que se envió el código original.

La Figura 5 ilustra un proceso de marcaje de acuerdo con una segunda forma de realización de la invención. En el método de la Figura 5, se producen dos identificadores seguros, uno basado en el valor de ruido de sistema 225 y otro basado en el valor de ruido físico 227. El valor de ruido de sistema 225 se combina con el UPI 221 en la etapa 341. A continuación, la combinación del valor de ruido de sistema y el valor de ruido físico se cifra con la CGOK 231 en la etapa 343 para producir el primer ID 241, como en la primera forma de realización de la Figura 3. A continuación, el primer ID 241 se combina con el CGID en la etapa 345 y se cifra con la clave global 235 en la etapa 347 para producir un primer ID seguro 271. El valor de ruido físico 227 se combina con el UPI en la etapa 221 para producir un segundo ID 261. El segundo ID se cifra con la clave global 235 en la etapa 353 para producir un segundo ID seguro. A continuación, el artículo se puede marcar, en la etapa 355, con el primer ID seguro 271 y el segundo ID seguro 281, o con una marca o marcas derivadas de una combinación del primer ID seguro 271 y el segundo ID seguro 281.

La Figura 6 ilustra las etapas llevadas a cabo para autenticar un artículo marcado usando el proceso ilustrado en la Figura 5. En la etapa 401, la marca o marcas son leídas por el usuario y este último obtiene el primer identificador seguro 271 y el segundo identificador seguro 281. En la etapa 403, la clave global 235 se usa para obtener el valor de ruido físico 227, una primera copia del UPI 221, el primer ID 241 y el CGID 233. Si el usuario tiene la clave global 235, el usuario puede autenticar el artículo basándose en el segundo identificador seguro fuera de línea, es decir, sin necesitar una conexión con el centro de verificación. El usuario genera una clave física nueva en la etapa 407, y a esta se le aplica una función *hash* con el UPI para generar un valor de ruido físico nuevo en la etapa 409. El usuario puede comparar el valor de ruido físico nuevo con el valor de ruido físico extraído en la etapa 403, en la etapa 411. Tal como se ha descrito en referencia a la Figura 3, el artículo puede considerarse auténtico en la etapa 419 si el valor de ruido físico nuevo es igual, o suficientemente similar, al valor de ruido físico extraído.

En la etapa 405, el CGID es usado por el centro de verificación para recuperar la CGOK 231, y la CGOK se usa para descifrar el primer ID 241 con el fin de desvelar el ruido de sistema y una segunda copia del UPI. En la etapa 408, la segunda copia del UPI se puede comparar, opcionalmente, con la segunda copia del UPI en forma de una comprobación. En la etapa 423, el centro de verificación 114 recupera la clave dinámica 219 y la clave estática activa 209 usando el CGID y el UPI. En la etapa 415, se genera un valor de ruido de sistema nuevo en primer lugar regenerando una clave secreta a partir del UPI, la clave dinámica y la clave estática, y, a continuación, ejecutando una función *hash* a la clave secreta con el UPI. En la etapa 417, el valor de ruido de sistema nuevo se compara con el valor de ruido de sistema extraído en la etapa 405. Si son idénticos, el artículo puede autenticarse en la etapa 419. Igual que con la forma de realización de la Figura 3, puede ser necesaria una autenticación basada tanto en el valor de ruido de sistema como en el valor de ruido físico para que un artículo sea considerado auténtico.

Aunque la invención se ha descrito en referencia a la fabricación de cigarrillos, debe quedar claro que la misma es aplicable a cualesquiera productos que requieran autenticación, tales como productos farmacéuticos, bebidas alcohólicas y bienes de lujo.

REIVINDICACIONES

1. Método de marcaje de un artículo manufacturado, que comprende:

crear un identificador de producto único (UPI) para un artículo manufacturado;

crear una o más claves de cifrado (209, 219);

generar una clave secreta (223) usando el identificador de producto único y dicha una o más claves de cifrado;

generar un valor de ruido de sistema (225) usando la clave secreta y el identificador de producto único;

generar una clave física a partir de (207) una propiedad física medida del artículo manufacturado;

generar un valor de ruido físico (227) usando la clave física y el identificador de producto único;

en el que, para crear el valor de ruido de sistema y el valor de ruido físico, el método usa transposición, sustitución, sustitución por tablas e indexación, o una función *hash* criptográfica sobre una combinación del identificador de producto único con la clave secreta y una combinación del identificador de producto único con la clave física;

generar un identificador seguro derivado (251, 271, 281) de o que incorpora la clave secreta, y la clave física, siendo el identificador seguro derivado de o incorpora el valor de ruido de sistema, y siendo el identificador seguro derivado de o incorpora el valor de ruido físico; y

poner (319, 355) una marca en el artículo manufacturado, comprendiendo la marca el identificador seguro o un identificador derivado del identificador seguro.

2. Método según la reivindicación 1, en el que el identificador seguro incorpora el identificador de producto único.

3. Método según la reivindicación 2, en el que la etapa de generación del identificador seguro comprende generar (311, 313) un primer identificador cifrando el identificador de producto único junto con el valor de ruido de sistema y generar el identificador seguro cifrando (317) el primer identificador junto con el valor de ruido físico.

4. Método según la reivindicación 3, en el que:

- la etapa de generación del primer identificador cifrando el identificador de producto único junto con el valor de ruido de sistema se lleva a cabo mediante cifrado (313) con una clave de ofuscación de generador de códigos (CGOK);

- a continuación, el primer identificador se combina con el valor de ruido físico y un identificador de generador de códigos (233);

- la combinación del primer identificador, el valor de ruido físico y el identificador de generador de códigos se cifra (317), a continuación, usando una clave global (235) para producir el identificador seguro.

5. Método según la reivindicación 4, en el que la clave de ofuscación de generador de códigos es particular de un generador de códigos (111) sobre el cual es precargada, y en el que la clave global es común para la totalidad de uno o más centros de producción.

6. Método según la reivindicación 3, que además comprende autenticar el artículo manufacturado en un centro de verificación, comprendiendo la etapa de autenticación:

identificar (321) la marca en el artículo;

descifrar (323) la marca para obtener el primer identificador y el valor de ruido físico;

descifrar (325) el primer identificador para obtener el identificador de producto único y el valor de ruido de sistema;

generar (327) una clave física nueva a partir de una propiedad física medida del artículo manufacturado;

generar (329) una copia nueva del valor de ruido físico ejecutando una función *hash* sobre la clave física nueva y el identificador de producto único obtenido;

comparar (331) la copia nueva del valor de ruido físico con el valor de ruido físico derivado; y

proporcionar una indicación (339) de si el valor de ruido físico derivado es idéntico a o está correlacionado la copia nueva del valor de ruido físico.

7. Método según la reivindicación 6, comprendiendo además la etapa de autenticación:

generar (333) una copia nueva de la clave secreta a partir del identificador de producto único y dicha una o más claves de cifrado;

generar (335) una copia nueva del valor de ruido de sistema ejecutando una función *hash* sobre la copia nueva de la clave secreta y el identificador de producto único;

comparar (337) la copia nueva del valor de ruido de sistema con el valor de ruido derivado de sistema; y

proporcionar una indicación (339) de si la copia nueva del valor de ruido de sistema y el valor de ruido derivado de sistema son idénticos.

8. Método según la reivindicación 2, en el que la etapa de generación del identificador seguro comprende generar un primer identificador seguro cifrando (241) el identificador de producto único junto con el valor de ruido de sistema;

generar (261) un segundo identificador seguro cifrando el identificador de producto único junto con el valor de ruido físico; y

poner (355) una marca en el artículo manufacturado, comprendiendo la marca el primer y segundo identificadores seguros o un identificador o identificadores derivados del primer y segundo identificadores seguros.

9. Método según la reivindicación 8, en el que:

- el valor de ruido de sistema se combina con el identificador de producto único;

  la combinación del valor de ruido de sistema y el identificador de producto único se cifra (343), a continuación, con una clave de ofuscación de generador de códigos (CGOK) para producir (241) un primer identificador;

- el primer identificador se combina, a continuación, con un identificador de generador de códigos (CGID) y se cifra (347) con una clave global (235) para producir un primer identificador seguro;

- el valor de ruido físico se combina (351) con el producto único para producir un segundo identificador (261);

- el segundo identificador se cifra con la clave global (235) para producir un segundo identificador seguro (281).

10. Método según la reivindicación 8, que además comprende autenticar el artículo manufacturado en un centro de verificación, comprendiendo la etapa de autenticación:

identificar (401) la marca en el artículo;

descifrar (403, 405) la marca para obtener el identificador de producto único, el ruido del sistema y el ruido físico;

generar (413) una copia nueva de la clave secreta a partir del identificador de producto único y de dicha una o más claves de cifrado;

generar (415) una copia nueva del valor de ruido de sistema ejecutando una función *hash* sobre la copia nueva de la clave secreta y el identificador de producto único;

comparar (417) la copia nueva del valor de ruido de sistema con el valor de ruido derivado de sistema;

generar (407) una clave física nueva a partir de una propiedad física medida del artículo manufacturado;

generar (409) una copia nueva del valor de ruido físico ejecutando una función *hash* sobre la clave física

nueva y el identificador de producto único derivado;

comparar (411) la copia nueva del valor de ruido físico con el valor de ruido físico derivado; y

proporcionar (419) una indicación tanto de si la copia nueva del valor de ruido de sistema es idéntica al valor de ruido derivado de sistema como de si la copia nueva del valor de ruido físico es idéntica a o está correlacionada con el valor de ruido físico derivado.

11. Método según cualquiera de las reivindicaciones anteriores, en el que dicha una o más claves de cifrado comprenden una clave estática (209) y una clave dinámica (219), y en el que se crea una clave dinámica nueva para cada lote de artículos manufacturados.

12. Método según cualquiera de las reivindicaciones anteriores, en el que el identificador de producto único incluye información que identifica un lote de artículos al cual pertenece el artículo.

13. Método según cualquiera de las reivindicaciones anteriores, en el que un valor de ruido es un valor *hash*, o un valor *hash* con clave, o una secuencia de valores o caracteres derivada directamente de un valor *hash* y una clave secreta.

14. Método según cualquiera de las reivindicaciones anteriores, en el que la propiedad física medida del artículo manufacturado está basada en la textura superficial del artículo manufacturado.

15. Aparato para marcar un artículo manufacturado, que comprende:

un generador de claves (115) configurado para generar unas claves de cifrado;

un generador de códigos (111) configurado para generar un identificador de producto único para cada artículo manufacturado;

un generador de claves físicas (112) configurado para generar unas claves físicas a partir de una propiedad física medida de cada artículo manufacturado;

unos medios de procesado (111) configurados para:

generar una clave secreta (223) para cada artículo manufacturado usando el identificador de producto único y una o más claves de cifrado;

generar un valor de ruido de sistema (225) para cada artículo manufacturado ejecutando una función *hash* sobre la clave secreta y un identificador de producto único;

generar un valor de ruido físico (227) para cada artículo manufacturado ejecutando una función *hash* sobre la clave física y el identificador de producto único;

generar un identificador seguro (251, 271, 281) derivado de o que incorpora la clave secreta y la clave física, siendo el identificador seguro derivado de o incorpora el valor de ruido de sistema, y siendo el identificador seguro derivado de o incorpora el valor de ruido físico; y

un marcador para marcar (319, 355) cada artículo manufacturado con el identificador seguro o un identificador derivado del identificador seguro.

16. Aparato según la reivindicación 15, en el que la propiedad física medida del artículo manufacturado está basada en la textura superficial del artículo manufacturado.

Fig. 1

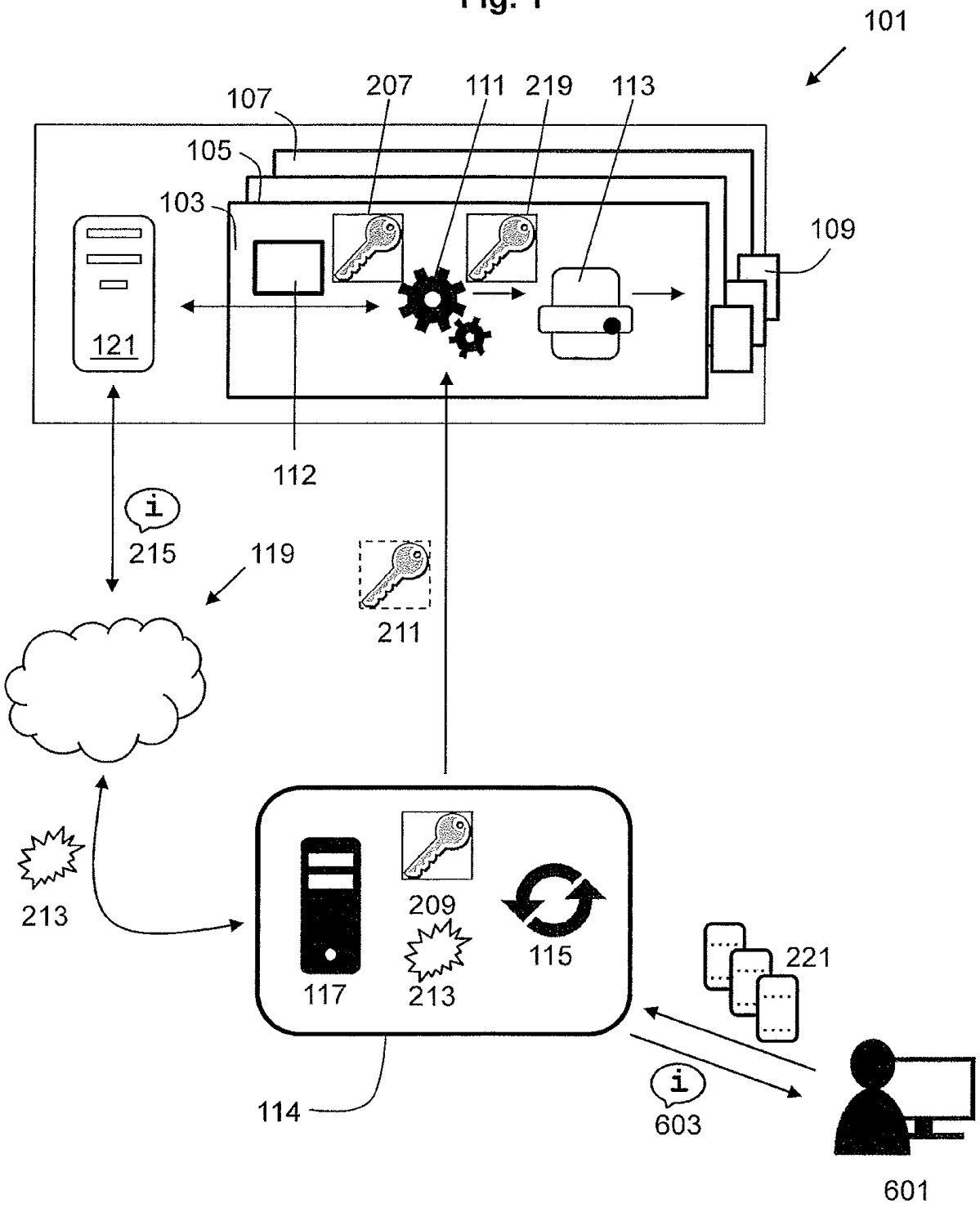
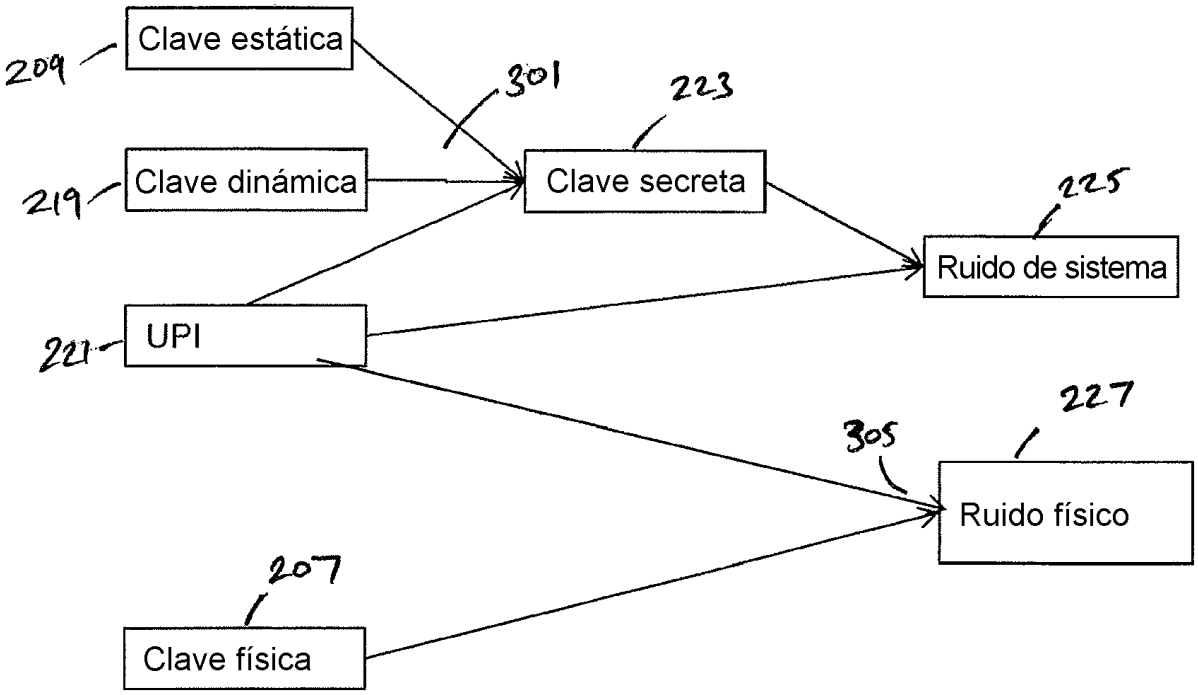

101
107
207
111
219
113
105
103
109
121
112
215
119
211
213
209
213
115
117
221
603
114
601

Fig. 2


209
Clave estática
301
223
219
Clave dinámica
Clave secreta
225
Ruido de sistema
221
UPI
227
305
Ruido físico
207
Clave física

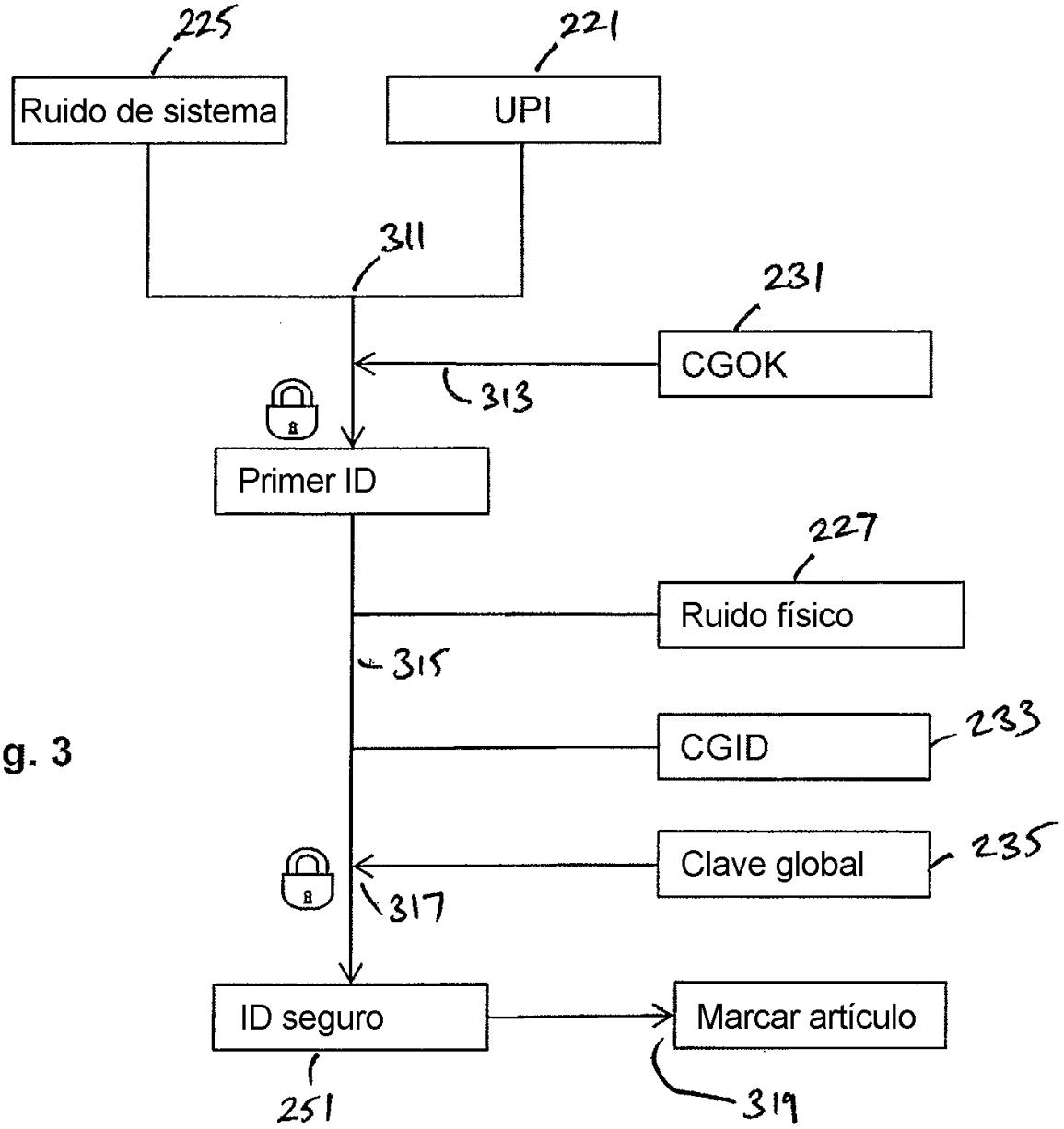

225
Ruido de sistema
221
UPI
311
231
CGOK
313
Primer ID
227
Ruido físico
315
CGID
233
Clave global
235
317
ID seguro
Marcar artículo
251
319

Fig. 3

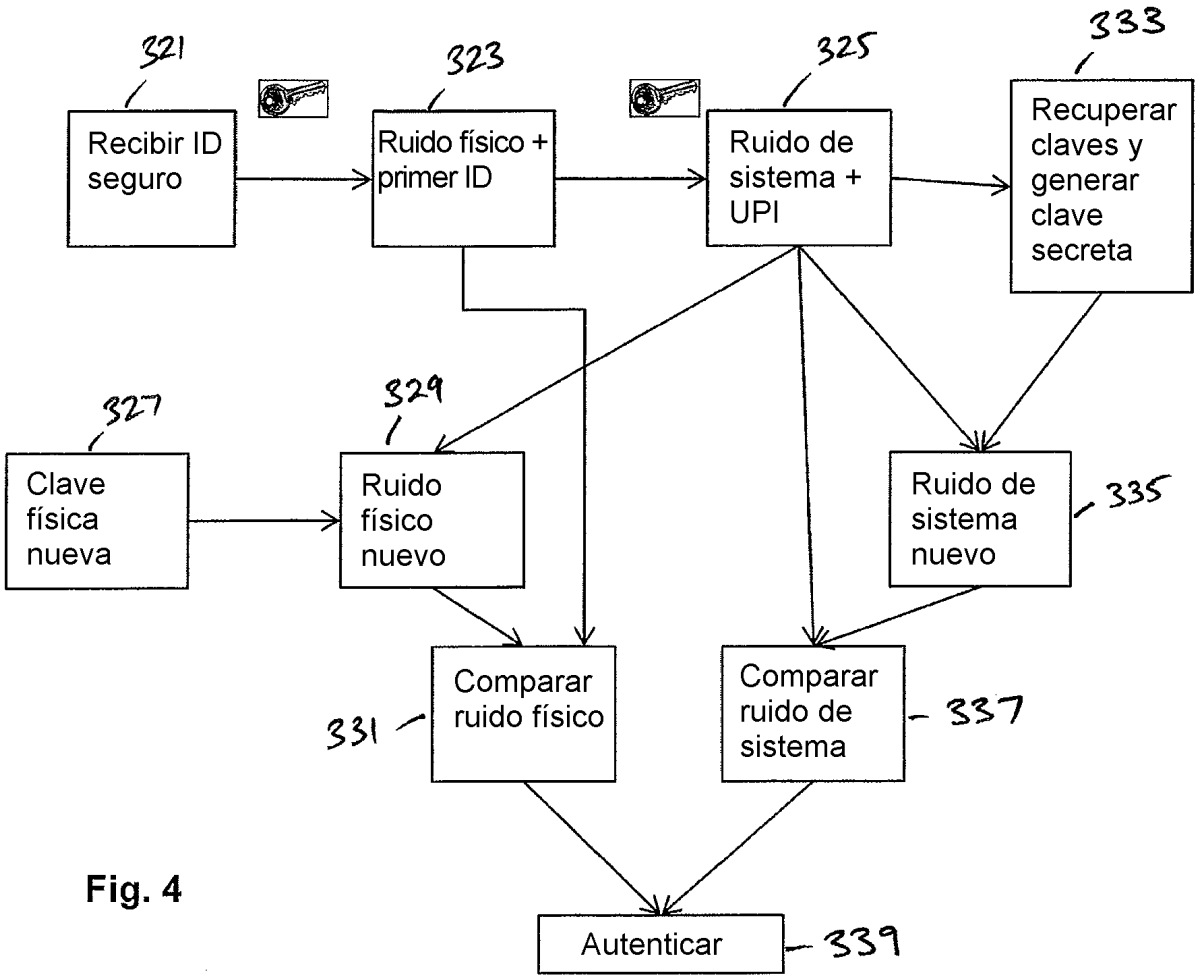

321
Recibir ID seguro
323
Ruido físico + primer ID
325
Ruido de sistema + UPI
333
Recuperar claves y generar clave secreta
327
Clave física nueva
329
Ruido físico nuevo
Ruido de sistema nuevo
335
331
Comparar ruido físico
Comparar ruido de sistema
337
Autenticar
339

Fig. 4

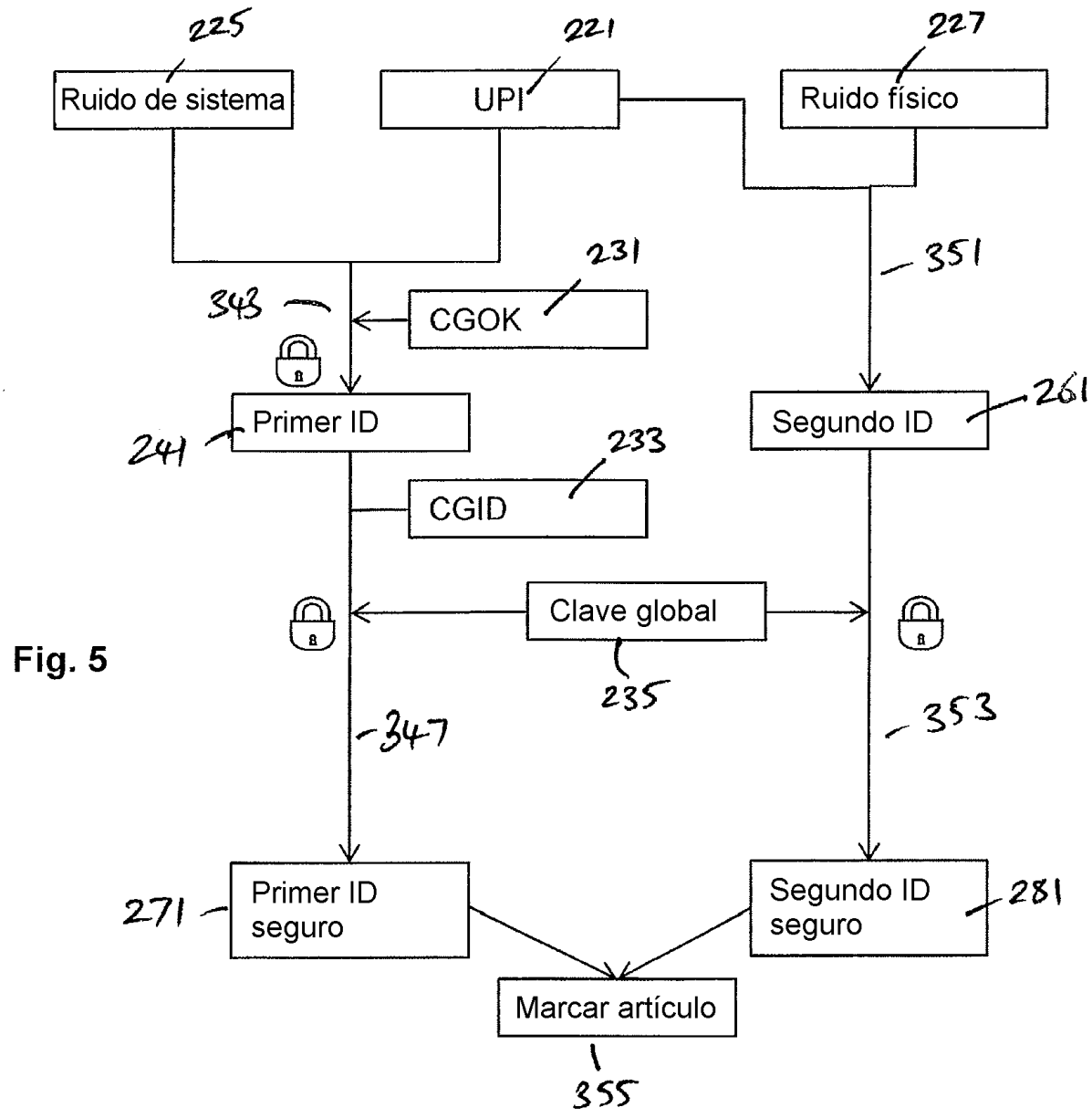

225
Ruido de sistema
221
UPI
227
Ruido físico
231
CGOK
343
351
241
Primer ID
261
Segundo ID
233
CGID
Clave global
235
347
353
271
Primer ID seguro
Segundo ID seguro
281
Marcar artículo
355

Fig. 5

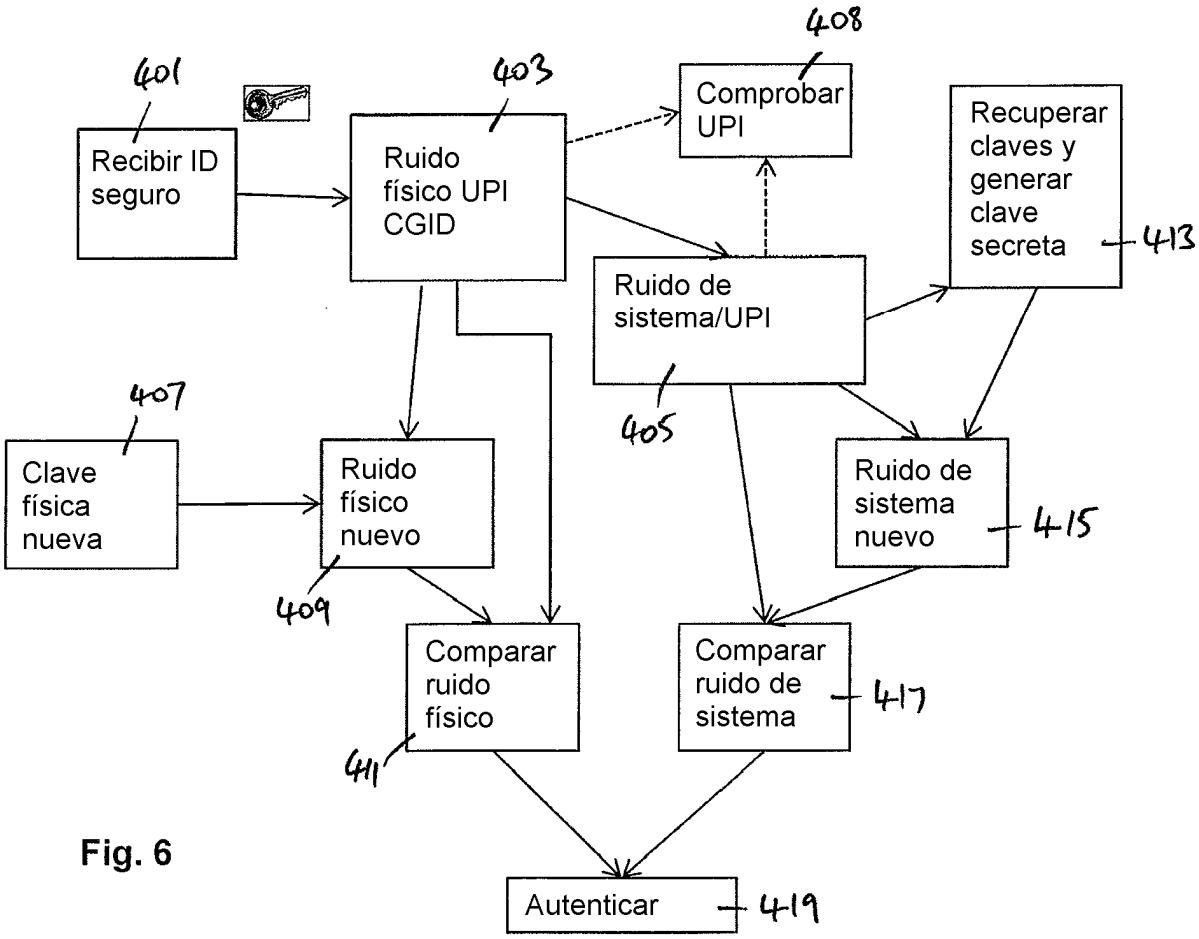

401
Recibir ID seguro
403
Ruido físico UPI CGID
408
Comprobar UPI
Recuperar claves y generar clave secreta
413
Ruido de sistema/UPI
405
407
Clave física nueva
Ruido físico nuevo
409
Ruido de sistema nuevo
415
Comparar ruido físico
411
Comparar ruido de sistema
417
Autenticar
419

Fig. 6