(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 534 931**

(51) Int. CI.:

G06Q 10/08 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **19.05.2009 E 09749853 (9)**

(97) Fecha y número de publicación de la concesión europea: **14.01.2015 EP 2283456**

(54) Título: **Procedimiento y dispositivo para identificar objetos**

(30) Prioridad:

20.05.2008 DE 102008001880

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
30.04.2015

(73) Titular/es:

SECURECODE LTD (100.0%)
Königsberger Str. 15
91083 Baiersdorf, DE

(72) Inventor/es:

KAULARTZ, MARKUS;
REISER, OLIVER;
ZICH, MICHAEL;
BAUER, SIMON y
KOBSDAJ, DANIEL

(74) Agente/Representante:

TORO GORDILLO, Francisco Javier

DESCRIPCIÓN

Procedimiento y dispositivo para identificar objetos

La presente invención se refiere a un procedimiento y a un dispositivo para identificar objetos y para verificar la autenticidad de los objetos identificados y, en particular, para identificar de manera segura frente a falsificaciones fármacos y/o medicamentos y para verificar la identificación por parte de un consumidor.

Para la identificación de mercancías como, por ejemplo, medicamentos, prendas de ropa, soportes de sonido o similares se han desarrollado diferentes procedimientos para ofrecer a fabricantes, distribuidores, autoridades aduaneras, consumidores, etc. la posibilidad de verificar la autenticidad de las mercancías. Mediante estos procedimientos, por ejemplo, se debe posibilitar al consumidor verificar la autenticidad de las mercancías adquiridas para, de este modo, protegerse frente a copias, especialmente frente a fármacos y/o medicamentos falsificados que posiblemente no tienen los efectos deseados o incluso tienen efectos perjudiciales.

En el documento DE 43 41 880 A1 se describe para ello un sistema de control para objetos con soportes de datos en los que se pueden almacenar datos como código de identificación, y con aparatos externos para el registro de datos y para el procesamiento de datos basado en ordenador que se puede utilizar para la protección frente a una imitación y reproducción no autorizadas de artículos. El sistema de control verifica datos específicos del fabricante que están almacenados como código de identificación en el soporte de datos como, por ejemplo, un chip RFID. El soporte de datos está colocado en el artículo a proteger. Sin embargo, chips RFID conocidos de este tipo no son seguros frente a falsificaciones, ya que es posible una falsificación o reproducción de soportes de datos correspondientes así como una reprogramación o destrucción del soporte de datos mediante métodos conocidos. La posibilidad de manipulación de los soportes de datos limita considerablemente la fiabilidad de un sistema de control correspondiente. Además, para la verificación de la autenticidad del código de identificación es necesario un aparato especial con el que se lee el soporte de datos. Estos aparatos no existen regularmente, en particular para el consumidor, debido a la diversidad de los diferentes soportes de datos y objetos, de modo que no existe una verificación sencilla y segura de artículos precisamente para el consumidor.

En el documento EP 0 889 448 B1 se describe un procedimiento en el que los objetos se proveen de una etiqueta en la que está aplicado un patrón irreproducible. El patrón irreproducible se genera a este respecto a partir de la descripción del objeto. La verificación de la etiqueta se realiza en este procedimiento mediante un palpado con un aparato especial. Sin embargo, aparatos correspondientes no existen en el sitio de los consumidores, y la posibilidad de verificación de las etiquetas no existe por este motivo precisamente para consumidores. Además, aparatos especiales de este tipo para la verificación no se pueden manejar de manera sencilla de modo que se producen inevitablemente errores en la verificación por parte de personas inexpertas tales como el consumidor que afectan adicionalmente a la fiabilidad del procedimiento correspondiente.

En el documento US 2006/0053025 A1 se describe un procedimiento para identificar y autenticar un producto con el fin de detectar falsificaciones. Este procedimiento comprende en particular las etapas de procedimiento: generar datos de identificación originales relativos al producto, encriptar estos datos de identificación originales para generar a partir de los mismos datos de identificación encriptados, almacenar los datos de identificación originales y los datos de identificación encriptados asociados en un sistema de base de datos e identificar el producto con los datos de identificación encriptados mientras que se envasa.

La invención se basa por tanto en el objetivo de proponer un procedimiento y un dispositivo para identificar objetos y para verificar la autenticidad de objetos identificados de manera correspondiente que ofrezca una seguridad muy alta y sea fácil de manejar.

Según la invención, este objetivo se consigue mediante un procedimiento para identificar un objeto según la reivindicación 1, un procedimiento para verificar la autenticidad de un objeto según la reivindicación 4, un dispositivo para identificar un objeto según la reivindicación 7 y un dispositivo para verificar la autenticidad de un objeto según la reivindicación 9. Formas de realización de la presente invención se definen en las reivindicaciones dependientes.

Un procedimiento para identificar un objeto, que tiene al menos una identificación de objeto, con un código de objeto que se utiliza para la verificación de la autenticidad del objeto, tiene las etapas: generar un código de sistema aleatorio unívoco que consiste en una primera y una segunda parte de código de sistema, generándose la primera parte de código de sistema a partir de una primera reserva de caracteres mediante un primer procedimiento aleatorio y la segunda parte de código de sistema a partir de una segunda reserva de caracteres mediante un segundo procedimiento aleatorio, y almacenar el código de sistema junto con al menos una primera información específica de objeto en una primera memoria de datos, encriptándose la primera parte de código de sistema mediante un primer procedimiento de encriptación y la segunda parte de código de sistema mediante un segundo procedimiento de encriptación antes del almacenamiento; generar una clave de encriptación aleatoria a partir de una tercera reserva de caracteres mediante un tercer procedimiento aleatorio, generar una identificación de asignación unívoca mediante un procedimiento de asignación, y almacenar la clave de encriptación, la identificación de asignación y al menos una segunda información específica de objeto en una segunda memoria de datos; generar el código de

objeto que consiste al menos en la primera parte de código de sistema y la identificación de asignación, encriptar el código de sistema mediante un tercer procedimiento de encriptación, encriptar la identificación de objeto mediante un cuarto procedimiento de encriptación, y almacenar el código de sistema encriptado junto con la identificación de objeto encriptada en una tercera memoria de datos; y colocar el código de objeto en el objeto.

Según un aspecto de la presente invención se propone que el procedimiento comprenda además que para el código de sistema almacenado se almacena adicionalmente una información de activación en la primera memoria de datos que identifica si el código de sistema es activo o inactivo, pudiendo verificarse el código de sistema sólo tras una activación. La seguridad de la identificación del objeto se mejora adicionalmente de manera ventajosa por que la identificación del objeto se activa sólo antes de la venta del objeto al consumidor y, con ello, se recubre una cadena de suministro insegura desde el fabricante hasta el consumidor.

Según un aspecto adicional de la presente invención se propone que el código de objeto se divida en una primera y una segunda parte de código de objeto. Además, se propone que la segunda parte de código de objeto se coloque en el objeto de modo que no se puede ver desde fuera y que la primera parte de código de objeto se coloque por fuera en el objeto. Se propone a este respecto que la primera parte de código de objeto se coloque por debajo de una protección visual. De este modo, de manera conveniente se puede aumentar adicionalmente la seguridad y la fiabilidad de la identificación del objeto.

Un procedimiento para verificar la autenticidad de un objeto con un código de objeto, que tiene al menos una identificación de objeto que está caracterizada con uno de los procedimientos propuestos para identificar objetos según la presente invención, tiene las etapas: transmitir el código de objeto mediante un medio de transmisión y recibir el código de objeto transmitido mediante un dispositivo de verificación, dividir el código de objeto en al menos una primera parte de código de sistema y una identificación de asignación, encriptar la primera parte de código de sistema con un primer procedimiento de encriptación, comparar la primera parte de código de sistema encriptada con las primeras partes de código de sistema que están almacenadas en la primera memoria de datos y, si la primera parte de código de sistema encriptada se encuentra en la primera memoria de datos, desencriptar una segunda parte de código de sistema almacenada en la primera memoria de datos con un segundo procedimiento de encriptación, unir las partes de código de sistema primera y segunda de modo que se obtiene un código de sistema, comparar la identificación de asignación con identificaciones de asignación que están almacenadas en la segunda memoria de datos y, si se encuentra una identificación de asignación que coincide, encriptar el código de sistema mediante un tercer procedimiento de encriptación, comparar el código de sistema encriptado con códigos de sistema encriptados que están almacenados en la tercera memoria de datos y, si se encuentra un código de sistema encriptado que coincide, desencriptar una identificación de objeto encriptada asignada mediante un cuarto procedimiento de encriptación, e visualizar una identificación de objeto desencriptada para comparar la identificación de objeto visualizada con la identificación de objeto en el objeto. El procedimiento permite por tanto una verificación especialmente sencilla y fiable de la identificación.

Según un aspecto adicional del procedimiento anteriormente mencionado se propone que el procedimiento, en el que el código de sistema está almacenado en la primera memoria de datos con una información de activación adicional que indica si el código de sistema es activo o inactivo, tenga una etapa en la que se activa la información de activación de uno de los códigos de sistema. Este aspecto del procedimiento es especialmente conveniente para cerrar la cadena de suministro insegura entre el fabricante y el consumidor.

Según aspectos adicionales de la invención, el medio de transmisión es Internet o una red de telefonía móvil. Además se almacenan datos específicos de consulta, que se generan en la verificación del código de objeto, en una cuarta memoria de datos. En función del respectivo medio de transmisión se propone a este respecto de manera conveniente que los datos específicos de consulta comprendan, en el caso de una entrada del código por Internet, al menos una indicación de tiempo, la dirección IP, el proveedor de servicios de Internet y el número de intentos de entrada así como, en caso de una entrada del código por SMS; al menos una indicación de tiempo, el número de teléfono móvil y el número de marcaje SMS. Esto es ventajoso, ya que los medios de transmisión propuestos son muy extendidos y, con ello, accesibles para casi cualquier consumidor. El almacenamiento de datos específicos de consulta es ventajoso además, por ejemplo, para verificar cuándo, cómo y por parte de quién se verificó por primera vez un código de objeto.

Un dispositivo para identificar un objeto con un código de objeto y un dispositivo para verificar un código de objeto de un objeto tienen dispositivos que están diseñados para realizar las etapas de los procedimientos de la presente invención. Además, la presente invención propone un programa informático que, cuando se ejecuta en un ordenador, controla éste de modo que realiza el procedimiento según la presente invención, así como un soporte de datos en el que está almacenado el programa informático.

En un aspecto adicional de la presente invención se propone un objeto que está identificado con un código de objeto que se generó con el procedimiento según la invención.

Formas de realización preferidas de la invención se explican a continuación meramente a modo de ejemplo y sin ninguna limitación mediante los dibujos adjuntos en los que:

La Figura 1 es un diagrama de desarrollo de una forma de realización del procedimiento según la invención;

La Figura 2 es una representación de desarrollo detallada para la generación del código de sistema de un ejemplo de realización de la forma de realización según la figura 1;

La Figura 3 muestra una representación de desarrollo detallada para la generación de las claves de encriptación según un ejemplo de realización de la forma de realización según la figura 1;

La Figura 4 muestra una representación de desarrollo detallada para la generación del código de objeto según un ejemplo de realización de la forma de realización según la figura 1;

La Figura 5A muestra un objeto con una primera parte de código de objeto colocada por fuera por debajo de una protección visual y una segunda parte de código de objeto que no se puede ver desde fuera;

La Figura 5B muestra el objeto según la figura 5A en el que se ha retirado la protección visual de la primera parte de código de objeto y se puede ver la segunda parte de código de objeto mediante una apertura del objeto.

La Figura 5C muestra un desarrollo esquemático de una verificación del código de objeto del objeto según la figura 5B por parte de un consumidor utilizando el procedimiento según la figura 1;

La Figura 6 muestra una representación esquemática de una forma de realización del dispositivo para identificar objetos; y

La Figura 7 muestra una representación esquemática de una forma de realización del dispositivo para la verificación de un código de objeto.

Un ejemplo de realización de un dispositivo para identificar un objeto se representa en la figura 6. El dispositivo 600 comprende un dispositivo de generación de código de sistema 610 que genera un código de sistema aleatorio unívoco y lo entrega a un primer dispositivo de almacenamiento de datos 620 para su almacenamiento en una memoria de datos 625, un dispositivo de generación de clave de encriptación 630 que genera una clave de encriptación aleatoria y la entrega a un segundo dispositivo de almacenamiento de datos 640 para su almacenamiento en una memoria de datos 645, un dispositivo de generación de código de objeto 650 que genera un código de objeto y lo entrega a un tercer dispositivo de almacenamiento de datos 660 para su almacenamiento en una memoria de datos 665, y un dispositivo de colocación de código de objeto 670 que coloca el código de objeto generado por el dispositivo de generación de código de objeto 650 en un objeto. El código de sistema generado por el dispositivo de generación de código de sistema 610 y la clave de encriptación generada por el dispositivo de generación de clave de encriptación 630 se entregan además al dispositivo de generación de código de objeto 650.

Preferiblemente, los dispositivos de almacenamiento de datos 620, 640 y 660 y las memorias de datos 625, 645 y 665 están realizados físicamente separados para mejorar la seguridad, en un ejemplo de realización simplificado, las memorias de datos 625, 645 y 665 también están integradas en los dispositivos de almacenamiento de datos 620, 640 y 660 correspondientes. Además, las memorias de datos 625, 645 y 665 están realizadas preferiblemente como memorias de datos físicamente separadas para garantizar un máximo de seguridad. En un ejemplo de realización que no pertenece a la invención, las memorias de datos 625, 645 y 665 están reunidas conjuntamente en una memoria de datos para simplificar el dispositivo 600. Para el experto en la técnica es evidente que también se reúnen en cada caso dos de las memorias de datos en una memoria de datos y que se puede utilizar una memoria de datos independiente adicional para la tercera de las memorias de datos.

En el ejemplo de realización de un procedimiento según la figura 1 se genera en la etapa 105 el código de sistema, en la etapa 110 la clave de encriptación y en la etapa 115 el código de objeto. Los ejemplos de realización en las figuras 2, 3 y 4 muestran en cada caso en detalle la generación de los códigos o claves individuales. En la figura 1 se representan las memorias de datos 625, 645 y 665 de manera simplificada como memoria de datos 120.

La generación del código de sistema se representa de manera detallada en la figura 2. A modo de ejemplo se describe en este caso la generación de un código de sistema con una longitud de 128 caracteres, formándose el código de sistema a partir de una primera parte de código de sistema 215 que comprende los diez primeros caracteres del código de sistema y una segunda parte de código de sistema 245 que comprende los 118 caracteres restantes del código de sistema. Para el experto en la técnica es evidente que se pueden utilizar de manera adecuada otras longitudes de carácter cualesquiera como, por ejemplo, 64, 256, 512 caracteres para el código de sistema y para las respectivas partes de código de sistema 215, 245. Mediante el dispositivo de generación de código de sistema 610 se genera a partir de una primera reserva de caracteres 200 la primera parte de código de sistema 215 con una longitud de diez caracteres aplicando un primer procedimiento aleatorio 205. La primera reserva de caracteres 200 comprende a este respecto, por ejemplo, un número de caracteres que se seleccionan a partir de una reserva de caracteres global que está disponible para el procedimiento o para el dispositivo. En la forma de realización descrita en este caso, toda la reserva de caracteres comprende las letras mayúsculas A a Z y los números 0 a 9 pero no comprende caracteres especiales. La primera reserva de caracteres 200 se reduce en

este ejemplo de realización en caracteres y números como, por ejemplo, Z y 2 para garantizar la univocidad de la primera parte de código de sistema 215. El primer procedimiento aleatorio 205 es cualquier procedimiento conocido por el estado de la técnica en el que se selecciona de manera aleatoria, es decir, de manera que no se puede predecir, un número de caracteres a partir de una reserva de caracteres previamente establecida. A modo de ejemplo se genera en este caso mediante el dispositivo de generación de código de sistema 610 la secuencia de caracteres “F37E4A1BD8” como primera parte de código de sistema 215. Esta primera parte de código de sistema 215 se encripta en la etapa 220 aplicando un procedimiento de encriptación conocido en el estado de la técnica de modo que se obtiene una primera parte de código de sistema encriptada 225. Preferiblemente, en este ejemplo de realización se utiliza una función Hash criptográfica como, por ejemplo, el algoritmo de resumen de mensaje 5 (de forma breve: MD5, *Message-Digest Algorithm*) o el algoritmo Hash seguro (de forma breve: SHA, *Secure Hash Algorithm*) como procedimiento de encriptación.

Además, el dispositivo de generación de código de sistema 610 genera en la etapa 240 una segunda parte de código de sistema 245 a partir de una segunda reserva de caracteres 230 mediante un segundo procedimiento aleatorio 235. La segunda reserva de caracteres 230 comprende preferiblemente toda la reserva de caracteres anteriormente descrita. El segundo procedimiento aleatorio 235 es igualmente cualquier procedimiento aleatorio con las mismas propiedades tal como ya se describieron anteriormente, preferiblemente, el segundo procedimiento aleatorio 235 es idéntico al primer procedimiento aleatorio 205. La segunda parte de código de sistema 245 así generada con una longitud de 118 caracteres se encripta mediante un segundo procedimiento de encriptación en la etapa 250. Preferiblemente, en este ejemplo de realización se aplica un procedimiento de encriptación simétrico como, por ejemplo, la Advanced Encryption Standard (Norma de Cifrado Avanzado, de forma breve, AES) o la Data Encryption Standard (Norma de Cifrado de Datos, de forma breve: DES) que utiliza la primera parte de código de sistema 215 como clave para la encriptación. El resultado de la etapa 250 es una segunda parte de código de sistema encriptada 255.

La primera parte de código de sistema encriptada 225 y la segunda parte de código de sistema encriptada 255 se almacenan en la etapa 265 junto con una primera información 260 específica de objeto mediante el primer dispositivo de almacenamiento de datos 620 en la memoria de datos 625 de modo que la primera parte de código de sistema encriptada 225, la segunda parte de código de sistema encriptada 255 y la primera información 260 específica de objeto están asignadas unas a otras. La primera información 260 específica de objeto comprende en este ejemplo de realización preferiblemente un número de unidad de producción que identifica un número de objetos de una producción y la fecha actual.

La primera parte de código de sistema 215 y la segunda parte de código de sistema 245 forman el código de sistema cuando ambas partes de código de sistema se combinan entre sí. Según la forma de realización representada en la figura 2, el código de sistema no se forma de modo que está disponible para su uso en etapas adicionales del procedimiento sino que el código de sistema se forma en cada caso en una etapa individual en la que es necesario mediante una combinación de la primera parte de código de sistema 215 con la segunda parte de código de sistema 245 para esta etapa individual. La combinación es a este respecto una sucesión de la primera parte de código de sistema y de la segunda parte de código de sistema de modo que forman un código de sistema con una longitud correspondiente. Para el experto en la técnica es evidente que el código de sistema se puede tener preparado como tal mediante una etapa adicional correspondiente para su uso en el procedimiento adicional.

Además, en un ejemplo de realización se almacena adicionalmente una información de activación, no mostrada en la figura 2, mediante el dispositivo de almacenamiento de datos 620 en la memoria de datos 120 que, estando asignada a una primera parte de código de sistema 215 encriptada, indica si ésta está bloqueada o libre. Esta información de activación se debe activar antes de la verificación de un código de objeto mediante una etapa de activación que se describe más en detalle más abajo para poder verificar el código de objeto.

El procedimiento de la figura 1 genera en una etapa adicional 110 una clave de encriptación 315 y una identificación de asignación 330. La generación de la clave de encriptación 315 y la identificación de asignación 330 se representa de manera detallada en la figura 3 según un ejemplo de realización. La clave de encriptación 315 se genera en la etapa 310 mediante el dispositivo de generación de clave de encriptación 630 aplicando un tercer procedimiento aleatorio 305 a partir de una tercera reserva de caracteres 300. La tercera reserva de caracteres 300 comprende, por ejemplo, toda la reserva de caracteres anteriormente mencionada y adicionalmente todas las letras minúsculas y caracteres especiales. De manera conveniente, el tercer procedimiento aleatorio 305 es idéntico al primer procedimiento aleatorio 205 y al segundo procedimiento aleatorio 235, pudiendo también emplearse otros procedimientos aleatorios conocidos. La clave de encriptación 315 tiene preferiblemente una longitud de caracteres entre 200 y 500 caracteres y es variable, es decir, la longitud de caracteres cambia en intervalos de tiempo previamente determinados. La clave de encriptación tiene en el ejemplo de realización preferido en este caso una longitud de 256 caracteres.

Además, en la etapa 325 se genera una identificación de asignación 330 aplicando un procedimiento de asignación 320 fijado. Un procedimiento de asignación 320 preferido, por ejemplo, calcula el número de los días que existen entre una fecha de referencia y la fecha de encriptación y lo emite como la identificación de asignación 330. Además es posible una encriptación de la identificación de asignación 330 mediante el procedimiento de asignación 320. En

el ejemplo de realización preferido en este caso se encripta la identificación de asignación 330 aplicando un procedimiento de encriptación sencillo en el que cada carácter individual se codifica. Si, por ejemplo, entre la fecha de referencia y la fecha de encriptación existen 121 días, entonces el número de los días se divide en primer lugar mediante el procedimiento de asignación 320 en dos partes como, por ejemplo, 1 como primera parte y 21 como segunda parte. A continuación, la primera parte y la segunda parte se convierten aplicando una norma de conversión como, por ejemplo, 1=A, 2=B, 3=C,…, 21=U, …, 26=Z, 27=A,…, 52=Z, 53=A, etc., en las letras “A” para la primera parte y “U” para la segunda parte, por lo que resulta la combinación de letras “AU” como identificación de asignación 330 uniendo la primera parte y la segunda parte.

En la etapa 340 se almacenan la clave de encriptación 315 y la identificación de asignación 330 junto con una segunda información 335 específica de objeto mediante el segundo dispositivo de almacenamiento de datos 640 en la memoria de datos 120. La segunda información 335 específica de objeto comprende a este respecto preferiblemente el número de unidad de producción y la fecha actual.

La generación del código de objeto 405 se realiza en la etapa 115 en la figura 1 que se representa de manera detallada según un ejemplo de realización en la figura 4. En la etapa 400 se genera mediante el dispositivo de generación de código de objeto 650 un código de objeto 405 que consiste al menos en la primera parte de código de sistema 215 y la identificación de asignación 330. Preferiblemente, la primera parte de código de sistema 215 y la identificación de asignación 330 se unen, resultando en el ejemplo descrito en este caso de la primera parte de código de sistema 215 anteriormente descrita con diez caracteres y la identificación de asignación 330 con dos caracteres el código de objeto 405 “F37E4A1BD8AU” con 12 caracteres.

Además, mediante el dispositivo de generación de código de objeto 650 se encripta el código de sistema que consiste en la primera parte de código de sistema 215 y la segunda parte de código de sistema 245 en la etapa 410 mediante un tercer procedimiento de encriptación de modo que se obtiene un código de sistema 415 encriptado. El tercer procedimiento de encriptación es un procedimiento de encriptación conocido en el estado de la técnica, preferiblemente un procedimiento de encriptación asimétrico como, por ejemplo, el algoritmo RSA, que utiliza la clave de encriptación 315 como clave. El procedimiento de encriptación asimétrico no se utiliza en la forma de realización descrita en este caso como procedimiento clásico de clave pública sino como una encriptación unidireccional, ya que el procedimiento utiliza la clave de encriptación 315 como clave pública sin proporcionar una clave adicional como clave privada para la encriptación.

El dispositivo de generación de código de objeto 650 encripta además en la etapa 425 una identificación de objeto 420 mediante un cuarto procedimiento de encriptación. El cuarto procedimiento de encriptación es cualquier procedimiento de encriptación conocido, en este caso se utiliza a modo de ejemplo un procedimiento de encriptación simétrico como, por ejemplo, la Advanced Encryption Standard (de forma breve: AES) o la Data Encryption Standard (de forma breve: DES), que utiliza como clave el código de sistema que consiste en la primera parte de código de sistema 215 y la segunda parte de código de sistema 245. La identificación de objeto 420 comprende en este ejemplo de realización preferiblemente el nombre del producto, la unidad de producción y/o la especificación del producto o la indicación del contenido exacto del producto que se debe dotar del código de objeto. El resultado de la etapa 425 es una identificación de objeto 430 encriptada.

En la etapa 440 se almacenan el código de sistema 415 encriptado de la etapa 410 y la identificación de objeto 430 encriptada de la etapa 425 mediante el tercer dispositivo de almacenamiento de datos 660 en la memoria de datos 120.

El código de objeto 405 se coloca en la etapa 125 mostrada en la figura 1 mediante el dispositivo de colocación de código de objeto 670 en el objeto para el que se generó el código de objeto 405. El objeto se fabricó a este respecto mediante la producción con el número de unidad de producción correspondiente y se dotó de la identificación de objeto 420 correspondiente. El código de objeto 405 se coloca a este respecto de tal manera en el objeto que, por ejemplo se puede leer y, por tanto, se puede verificar a continuación por parte de un consumidor.

En un ejemplo de realización adicional, el código de objeto se divide en una primera parte de código de objeto y una segunda parte de código de objeto. La división así como las longitudes de carácter de la primera y la segunda parte de código de objeto se pueden elegir a este respecto de cualquier manera. En el ejemplo de realización preferido en este caso, la primera parte de código de objeto se corresponde con dos terceras partes y la segunda parte de código de objeto se corresponde con una tercera parte del código de objeto 405. En el caso de una división del código de objeto 405 tal como se describió en el ejemplo anterior, la primera parte de código de objeto es “F37E4A1B” y la segunda parte de código de objeto es “D8AU”. Para el experto en la técnica es evidente que también son posibles otras divisiones como, por ejemplo, una cuarta parte y tres cuartas partes para las respectivas partes de código de objeto.

Para el experto en la técnica es evidente, por tanto, que la seguridad del procedimiento se consigue por que una desencriptación de la identificación de objeto 420 de la memoria de datos 645 y la asignación del código de objeto a la identificación de objeto sólo son posibles cuando son conocidos los procedimientos de encriptación utilizados así como las claves utilizadas para ello que, sin embargo, sólo existen como información encriptada en las memorias de

datos 625 y 645. Sólo en la memoria de datos 635 existen informaciones no encriptadas que consisten en la clave de encriptación 315, la identificación de asignación 330 y los segundos datos 335 específicos de objeto que, sin embargo, en sí aún no son suficientes para desencriptar las informaciones encriptadas en las memorias de datos 625 o 645 o para establecer una asignación del código de objeto a la identificación de objeto. Por tanto, también en caso de conocerse informaciones a partir de una de las memorias de datos 625, 635 o 645 no es posible restablecer todas las informaciones encriptadas, en particular la identificación de objeto y la asignación del código de objeto a la identificación de objeto.

Con referencia a la figura 5A y la figura 5B se describe ahora cómo el código de objeto 405 está colocado en el objeto 500. La primera parte de código de objeto y la segunda parte de código de objeto, que existieron según el ejemplo de realización anteriormente descrito mediante una división a partir del código de objeto 405, se colocan en un ejemplo de realización preferido en diferentes posiciones en el objeto 500. La primera parte de código de objeto 520 está colocada a este respecto de modo que se puede ver desde fuera en el propio objeto 500 o sobre el embalaje del objeto, lo que no se puede ver en la figura 5A. La segunda parte de código de objeto 530 está colocada de modo que no se puede ver desde fuera sobre el objeto 500, por ejemplo, en el lado interior del embalaje del objeto o sobre el producto embalado. La primera parte de código de objeto 520 está colocada en el ejemplo de realización representado en la figura 5A por debajo de una protección visual 510 como, por ejemplo, un campo de rascado, debiendo destruirse la protección visual 510 para que se vea la primera parte de código de objeto 520. Además, según la figura 5B, la segunda parte de código de objeto 530 se puede ver, por ejemplo, cuando se haya abierto el embalaje del objeto.

Un dispositivo para verificar un código de objeto se representa según un ejemplo de realización en la figura 7. El dispositivo 700 comprende un dispositivo de recepción 720 que recibe el código de objeto del objeto que se transmite mediante un medio de transmisión 710 y lo transmite a un dispositivo de verificación 740 mediante el que se verifica este código de objeto. El resultado de la verificación se visualiza mediante un dispositivo de visualización 790. El dispositivo de verificación 740 comprende un dispositivo de división de código de objeto 750 que divide el código de objeto y lo entrega a un primer dispositivo de comparación 760 y a un segundo dispositivo de comparación 770 para su procesamiento adicional. El primer dispositivo de comparación 760 procesa la parte entregada del código de objeto y compara el resultado de este procesamiento con datos de una memoria de datos 765, leyendo el primer dispositivo de comparación 760, en caso de encontrar una entrada que coincide con la parte procesada del código de objeto en la memoria de datos 765, datos de la memoria de datos 765 que están asignados a la entrada que coincide. Los datos leídos se tienen preparados por el primer dispositivo de comparación 760 en el dispositivo de verificación 740 para su procesamiento adicional. El segundo dispositivo de comparación 770 compara la otra parte entregada del código de objeto con datos en una memoria de datos 775 y, en caso de encontrar una entrada que coincide en la memoria de datos 775, lee datos asignados a esta entrada de la memoria de datos 775. Los datos leídos se procesan adicionalmente mediante el segundo dispositivo de comparación 770 y se tienen preparados en el dispositivo de verificación 740. Un tercer dispositivo de comparación 780 recibe los datos que se tienen preparados en el dispositivo de verificación 740, y procesa estos datos, comparándose los datos procesados con datos que están almacenados en una memoria de datos 785. En caso de encontrar una entrada que coincide en la memoria de datos 785, datos asignados a esta entrada se leen mediante el tercer dispositivo de comparación 780 y se entregan como resultado de la verificación del código de objeto al dispositivo de visualización 790.

En un ejemplo de realización, la o las memorias de datos 765, 775 y 785 es o son idénticas a la o las memorias de datos 625, 645 y 665 correspondientes de la figura 6. En otro ejemplo de realización, en el que las memorias de datos de la figura 7 y las memorias de datos de la figura 6 no son idénticas, al menos los datos, que están almacenados en cada caso en las memorias de datos 765, 775, 785 de la figura 7, son idénticos a los datos que están almacenados en las memorias de datos 625, 645 y 665 correspondientes de la figura 6. Además, el dispositivo 700 comprende en un ejemplo de realización un dispositivo de activación 730 que almacena una información de activación en la memoria de datos 765.

A continuación se describe una forma de realización del procedimiento para verificar un código de objeto con referencia a la figura 1. En la figura 1 se representan las memorias de datos 765, 775 y 785 de manera simplificada como memoria de datos 120. El código de objeto que se generó con el procedimiento anteriormente descrito y que está colocado en un objeto se entrega en la etapa 130 al medio de transmisión 710 para su verificación. El medio de transmisión 710 transmite el código de objeto al dispositivo de recepción 720. El dispositivo de recepción 720 transmite el código de objeto recibido entonces al dispositivo de verificación 740. El medio de transmisión 710 es Internet o una red de telefonía móvil. En un ejemplo de realización especialmente preferido, tanto Internet como la red de telefonía móvil se pueden utilizar de manera alternativa como medio de transmisión 710 para la transmisión del código de objeto al dispositivo de verificación 740. A este respecto, el dispositivo de recepción 720 es preferiblemente una página web 560, cuando el medio de transmisión 710 es Internet, y un mensaje corto 550 como, por ejemplo, el servicio de mensajería corta (SMS) conocido por el estado de la técnica, cuando el medio de transmisión 710 es la red de telefonía móvil. El código de objeto recibido por el dispositivo de recepción 720 se entrega a continuación en la etapa 135 al dispositivo de verificación 740 para su verificación.

En la etapa 135, el código de objeto se divide mediante el dispositivo de división de código de objeto 750 en al menos una primera parte de código de sistema y una identificación de asignación. En el ejemplo descrito en este

caso, en el que el código de objeto consiste en 12 caracteres, correspondiéndose los diez primeros caracteres con la primera parte de código de sistema y los dos últimos caracteres con la identificación de asignación, el código de objeto se divide en una primera parte de código de sistema con diez caracteres y una identificación de asignación con dos caracteres. La primera parte de código de sistema se encripta además en el primer dispositivo de comparación 760 mediante el primer procedimiento de encriptación elegido tal como se describió anteriormente. A continuación, esta primera parte de código de sistema encriptada se compara con primeras partes de código de sistema encriptadas que están almacenadas en la memoria de datos 120. Cuando se encuentra una primera parte de código de sistema encriptada almacenada en la memoria de datos 120 que coincide con la primera parte de código de sistema encriptada del código de objeto a verificar, entonces se leen mediante el primer dispositivo de comparación 760 los datos asignados almacenados en la memoria de datos 120. Estos datos almacenados comprenden en el ejemplo de realización preferido en este caso una segunda parte de código de sistema encriptada y una primera información específica de objeto. La segunda parte de código de sistema encriptada se desencripta mediante el primer dispositivo de comparación 760 aplicando el segundo procedimiento de encriptación que es idéntico al procedimiento de encriptación simétrico anteriormente elegido y la primera parte de código de sistema como clave de modo que se obtiene una segunda parte de código de sistema. Además, en un ejemplo de realización, la primera parte de código de sistema y la segunda parte de código de sistema desencriptada se unen de modo que se obtiene un código de sistema. La primera parte de código de sistema y la segunda parte de código de sistema, la primera información específica de objeto y, si está formado, el código de sistema se tienen preparados en el dispositivo de verificación 740 para su uso adicional en otros dispositivos del dispositivo de verificación 740. Adicionalmente, en un ejemplo de realización, los datos leídos y/o un mensaje, que identifica que se ha encontrado una coincidencia en la memoria de datos 120, se entregan al dispositivo de visualización 790 para su visualización. Si mediante el primer dispositivo de comparación 760 en la memoria de datos 120 no se encuentra una primera parte de código de sistema encriptada que coincide, se entrega un mensaje de error 145 al dispositivo de visualización 790 que identifica que no se ha podido encontrar una coincidencia. En este caso se finaliza el procedimiento y el dispositivo de visualización 790 visualiza el mensaje de error 145.

En caso de que mediante el primer dispositivo de comparación 760 en la memoria de datos 120 se haya encontrado una primera parte de código de sistema encriptada que coincide, el procedimiento se continúa entregando la identificación de asignación obtenida mediante una división en el dispositivo de división de código de objeto 750 al segundo dispositivo de comparación 770. El segundo dispositivo de comparación 770 compara la identificación de asignación entregada con identificaciones de asignación que están almacenadas en la memoria de datos 120. En caso de que se encuentre una identificación de asignación que coincide en la memoria de datos 120 se leen mediante el segundo dispositivo de comparación 770 los datos asignados a esta identificación de asignación como, por ejemplo, una clave de encriptación y una segunda información específica de objeto que se tienen preparadas para su procesamiento adicional en el dispositivo de verificación 740. Los datos leídos y/o un mensaje adecuado, que indica que datos se encontraron en la memoria de datos 120 y están proporcionados para su procesamiento adicional en el dispositivo de verificación 740, se entregan al dispositivo de visualización 790 para su visualización. En caso de que en la memoria de datos 120 no se haya podido encontrar una identificación de asignación que coincide, se envía al dispositivo de visualización 790 un mensaje de error 145 correspondiente que identifica que la identificación de asignación no se encontró por el segundo dispositivo de comparación 770 en la memoria de datos 120. En este caso, el procedimiento se finaliza y el dispositivo de visualización 790 visualiza el mensaje de error 145.

En caso de que mediante el segundo dispositivo de comparación 770 se haya encontrado una coincidencia en la memoria de datos 120, el procedimiento se continúa mediante el tercer dispositivo de comparación 780. El tercer dispositivo de comparación 780 encripta con la clave de encriptación mediante una aplicación de un tercer procedimiento de encriptación el código de sistema proporcionado en el dispositivo de verificación 740 que está formado a partir de la primera parte de código de sistema y la segunda parte de código de sistema. El tercer procedimiento de encriptación es a este respecto idéntico al tercer procedimiento de encriptación anteriormente descrito. El código de sistema así encriptado se compara con códigos de sistema encriptados en la memoria de datos 120. Si a este respecto se encuentra en la memoria de datos 120 un código de sistema encriptado que coincide, entonces se leen mediante el tercer dispositivo de comparación 780 los datos asignados a este código de sistema encriptado como, por ejemplo, en este caso una identificación de objeto encriptada. La identificación de objeto encriptada se desencripta mediante una aplicación del cuarto procedimiento de desencriptación anteriormente descrito mediante el tercer dispositivo de comparación 780 con los códigos de sistema proporcionados en el dispositivo de verificación 740 como clave. La identificación de objeto desencriptada y/o un mensaje adecuado que indica que en la memoria de datos 120 se encontró un código de sistema encriptado que coincide se transmiten al dispositivo de visualización 790 para visualizarse por el dispositivo de visualización 790. Si en la memoria de datos 120 no se encuentra una coincidencia, entonces se envía un mensaje de error 145 al dispositivo de visualización 790 que identifica que el código de sistema no se encontró en la memoria de datos 120. En este caso se finaliza el procedimiento y el dispositivo de visualización 790 visualiza el mensaje de error 145.

El dispositivo de visualización 790 visualiza los datos y/o mensajes recibidos por los dispositivos de comparación primero, segundo y tercero. Por ejemplo, en un ejemplo de realización preferido se visualiza el mensaje de error 145 que indica que no existe el código de objeto entregado, lo que permite concluir que existe una entrada errónea del código de objeto o una falsificación del objeto. En caso de que se haya encontrado el código de objeto, es decir, en caso de que se hayan encontrado el primer código de sistema en la memoria de datos 120, la identificación de

asignación en la memoria de datos 120 y datos que coinciden en la memoria de datos 120, la identificación de objeto 180 desencriptada se visualiza mediante el dispositivo de visualización 790.

A continuación se describe mediante las figuras 5A, 5B y 5C la verificación de un código de objeto utilizando el procedimiento anteriormente descrito por parte de un consumidor. El consumidor adquiere, por ejemplo, de un comerciante, un objeto 500 que está dotado de un código de objeto que se generó con un procedimiento para identificar un objeto según la presente invención. Mediante una destrucción de la protección visual 510 se puede ver la primera parte de código de objeto 520 “F37E4A1B”. La segunda parte de código de objeto 530 “D8AU” se puede ver mediante una apertura del envase del objeto 500. El consumidor une ahora las dos partes de código de objeto de modo que se obtiene el código de objeto “F37E4A1BD8AU”. Este código de objeto se transmite por parte del consumidor al dispositivo de verificación 740 mediante el medio de transmisión 710. En la figura 5C se representa una página web 540 que funciona como dispositivo de recepción 720 cuando el medio de transmisión 710 es Internet. En la página web 540 existe un campo de entrada 541 en el que el consumidor introduce el código de objeto. La transmisión del código de objeto introducido al dispositivo de verificación 740 se realiza mediante una confirmación del interruptor funcional 542 proporcionado en la página web 540. El dispositivo de verificación 740 verifica a continuación el código de objeto transmitido en la etapa 135 tal como se describió anteriormente. El resultado de la etapa 135 se transmite al dispositivo de visualización 790. Cuando el medio de transmisión 710 es Internet, el dispositivo de visualización 790 visualiza el resultado preferiblemente como una página web 560 en la que se visualiza la identificación de objeto 561 para el código de objeto verificado. Además, el dispositivo de visualización 790 también puede visualizar el código de objeto introducido, por ejemplo, para su control. Cuando la etapa 135 no se realiza con éxito, entonces el dispositivo de visualización 790 visualiza en la página web 560 el mensaje de error 145 que indica que no se ha encontrado el código de objeto. El consumidor compara ahora en una etapa 580 si la identificación de objeto 561 transmitida coincide con la identificación de objeto en el objeto 500. Si estas dos identificaciones de objeto son idénticas, entonces el objeto es auténtico según el procedimiento.

Según un ejemplo de realización adicional que se describe ahora con referencia a la figura 5C, el consumidor introduce el código de objeto del objeto 500 en un mensaje corto SMS 550 cuando se utiliza la red de telefonía móvil como medio de transmisión 710. El mensaje corto SMS 550 contiene el número 551 del dispositivo de verificación así como el código de objeto a verificar como texto de mensaje 552. El mensaje corto SMS 550 se transmite al dispositivo de verificación 740 accionando el botón “enviar” 553 en el aparato del consumidor como, por ejemplo, un teléfono móvil que usa la red de telefonía móvil. El dispositivo de verificación 740 verifica el código de objeto realizando la etapa 135. El resultado de la verificación se envía mediante un SMS de respuesta 570 a través de la red de telefonía móvil al aparato del consumidor. El SMS de respuesta contiene, en el caso de una verificación con éxito, como texto de respuesta 572, por ejemplo, el código de objeto para el control y la identificación de objeto. En caso de una verificación sin éxito, el texto de respuesta 572 contiene el mensaje 145. El consumidor compara ahora en una etapa 580 si la identificación de objeto transmitida en el texto de respuesta 572 coincide con la identificación de objeto en el objeto 500. Si estas dos identificaciones de objeto son idénticas, el objeto es auténtico según el procedimiento.

Según un ejemplo de realización preferido, el dispositivo de visualización 790 visualiza la identificación de objeto como una página web 580, cuando el medio de transmisión es Internet, y como un mensaje corto de respuesta 570 cuando el medio de transmisión es una red de telefonía móvil, tal como se representa en cada caso en la figura 5C. La identificación de objeto visualizada se puede comparar ahora con la identificación colocada sobre el objeto para determinar la autenticidad del objeto. El objeto está autenticado cuando la identificación de objeto visualizada y la identificación de objeto colocada son idénticas.

En un ejemplo de realización preferido del procedimiento según la figura 1, el código de sistema está dotado en la memoria de datos 120 de una información de activación que indica si está activado el código de objeto. Tras la verificación del código de objeto en la etapa 135 se verifica adicionalmente en la etapa 160 si el código de objeto verificado también está liberado. La consulta de un código de objeto desactivado conduce a este respecto a un mensaje 165 correspondiente en el dispositivo de visualización 790. Si se determina en la verificación en la etapa 160 que el código de objeto está liberado, entonces éste se transmite para su visualización 150 al dispositivo de visualización 790.

Preferiblemente, el código de objeto y, con ello, también el código de sistema así como el código de objeto se desactiva por estándar en la generación de la primera parte de código de sistema en la etapa 110. El código de sistema se activa mediante una etapa 155 que se debe realizar antes de una verificación en la etapa 135. A este respecto, el código de objeto se activa mediante una entrada de la primera parte de código de sistema en el dispositivo de activación 730 cuando en la memoria de datos 765 se encuentra una primera parte de código de sistema que coincide que aún no está activada. En caso de que se encuentre una primera parte de código de sistema no activada que coincide se activa la información de activación para la primera parte de código de sistema y el código de objeto está liberado por tanto para una verificación. Además se envía un mensaje adecuado que indica que se ha activado el código de objeto al dispositivo de visualización 790. En caso contrario se visualiza un mensaje correspondiente mediante el dispositivo de visualización 790 que identifica que la primera parte de código de sistema introducida no existe en la memoria de datos 765 o que la primera parte de código de sistema introducida se encontró en la memoria de datos 765 pero ya está activada.

En ejemplos de realización adicionales del procedimiento según la figura 1 se almacenan datos específicos de consulta en una memoria de datos adicional que no se representa. Estos datos específicos de consulta comprenden en la transmisión del código de objeto a través de Internet preferiblemente una indicación de tiempo que indica cuándo se ha transmitido el código de objeto, la dirección IP que indica el origen de la transmisión, el proveedor de servicios de Internet y el número de intentos de entrada. En caso de usar una red de telefonía móvil como dispositivo de transmisión 710, los datos específicos de consulta comprenden preferiblemente una indicación de tiempo, el número de teléfono móvil de la persona que realiza la consulta y el número de marcaje SMS. El número de marcaje SMS es, por ejemplo, un denominado número abreviado SMS. Sin embargo, en algunas redes de telefonía móvil, el número de marcaje SMS también puede ser un número largo SMS correspondiente. Formatos adicionales de números de marcaje SMS son posibles en función de la red de telefonía móvil. Para el experto en la técnica es evidente que se pueden almacenar datos adicionales específicos de consulta y que dicha memoria de datos adicional también es idéntica a las memorias de datos anteriormente descritas.

Ejemplos de realización preferidos adicionales de la presente invención comprenden en la verificación de un código de objeto transmitido una consulta de los datos específicos de consulta para determinar si el código de objeto ya se consultó. Adicionalmente, en estos ejemplos de realización, en el caso de una consulta por primera vez del código de objeto, una identificación de consulta y una palabra clave de consulta se generan y se almacenan como datos específicos de consulta en una memoria de datos de consulta que no está representada. La identificación de consulta y la palabra clave de consulta, por ejemplo, se visualizan al consumidor mediante el dispositivo de visualización 790 que verifica por primera vez un determinado código de objeto, es decir, el código de objeto aún no se ha consultado o verificado previamente. En el caso de intentos de consulta adicionales de este código de objeto, que ya se consultó una vez, se transmite adicionalmente la identificación de consulta y la palabra clave de consulta por parte del consumidor para garantizar que sólo el consumidor que ha consultado por primera vez el código de objeto puede realizar consultas adicionales con éxito para este código de objeto. Otros consumidores que no disponen de la identificación de consulta correspondiente y de la palabra clave de consulta para este código de objeto o no pueden consultar con éxito el código de objeto o reciben un mensaje correspondiente que indica que ya se ha verificado por primera vez el código de objeto.

El procedimiento según la invención se realiza preferiblemente como programa informático en un ordenador y controla éste. El ordenador comprende a este respecto cualquier dispositivo de procesamiento de datos incluyendo ordenadores de sobremesa, arquitecturas de cliente-servidor u otros sistemas informáticos conectados por red, siempre que estén preparados de manera correspondiente y sean adecuados para realizar el procedimiento.

REIVINDICACIONES

1. Procedimiento para identificar un objeto (500), que está dotado al menos de una identificación de objeto (420), mediante un código de objeto (405) que se utiliza para la verificación de la autenticidad del objeto (500), que comprende las etapas:

a) generar (105) un código de sistema aleatorio unívoco que consiste en unas partes de código de sistema primera y segunda (215, 245), generándose la primera parte de código de sistema (215) a partir de una primera reserva de caracteres (200) mediante un primer procedimiento aleatorio (205) y la segunda parte de código de sistema (245) a partir de una segunda reserva de caracteres (230) mediante un segundo procedimiento aleatorio (235), y almacenar (265) el código de sistema junto con al menos una primera información (260) específica de objeto en una primera memoria de datos (625), encriptándose la primera parte de código de sistema (215) mediante un primer procedimiento de encriptación (220) y la segunda parte de código de sistema (245) mediante un segundo procedimiento de encriptación (250) que utiliza la primera parte de código de sistema (215) como clave, antes del almacenamiento;
b) generar (110, 310) una clave de encriptación (315) aleatoria a partir de una tercera reserva de caracteres (300) mediante un tercer procedimiento aleatorio (305), generar (325) una identificación de asignación (330) unívoca mediante un procedimiento de asignación (320) y almacenar (340) la clave de encriptación (315), la identificación de asignación (330) y al menos una segunda información (335) específica de objeto en una segunda memoria de datos (635);
c1) generar (115, 400) el código de objeto (405) que consiste al menos en la primera parte de código de sistema (215) y la identificación de asignación (330);
c2) encriptar (410) el código de sistema mediante un tercer procedimiento de encriptación que utiliza la clave de encriptación (315) como clave, encriptar (425) la identificación de objeto (420) mediante un cuarto procedimiento de encriptación que utiliza el código de sistema como clave, y almacenar (435) el código de sistema (415) encriptado junto con la identificación de objeto (430) encriptada en una tercera memoria de datos (645);
d) colocar (125) el código de objeto (405) en el objeto (500);

proporcionando el procedimiento una cuarta memoria de datos en la que se almacenan datos específicos de consulta generados en la verificación de la autenticidad del objeto (500),
estando las memorias de datos (625, 635, 645) físicamente separadas unas de otras.

2. Procedimiento según la reivindicación 1, almacenándose para el código de sistema almacenado en la etapa a) adicionalmente una información de activación en la primera memoria de datos (625) (155) que identifica si el código de sistema está activo o inactivo, pudiendo verificarse el código de sistema sólo tras una activación; y/o dividiéndose el código de objeto (405) en unas partes de código de objeto primera y segunda (520, 530).

3. Procedimiento según la reivindicación 2, estando la segunda parte de código de objeto (530) colocada de tal manera en el objeto (500) que no se puede ver desde fuera, y estando la primera parte de código de objeto (520) colocada por fuera en el objeto (500); y estando colocada preferiblemente la primera parte de código de objeto (520) por debajo de una protección visual (510).

4. Procedimiento para verificar la autenticidad de un objeto (500) que está dotado al menos de una identificación de objeto (420) mediante un código de objeto (405), estando el código de objeto (405) generado según una de las reivindicaciones anteriores, que comprende las etapas:

e) transmitir el código de objeto (405) mediante un medio de transmisión, recibir el código de objeto (405) transmitido mediante un dispositivo de verificación y almacenar datos específicos de consulta en una cuarta memoria de datos que se generan en la verificación de la autenticidad del código de objeto (405);
f) dividir el código de objeto (405) en al menos una primera parte de código de sistema (215) y una identificación de asignación (330);
g) encriptar la primera parte de código de sistema (215) con un primer procedimiento de encriptación, comparar la primera parte de código de sistema encriptada (225) con las primeras partes de código de sistema que están almacenadas en la primera memoria de datos (625) y, si la primera parte de código de sistema encriptada (225) se encuentra en la primera memoria de datos (625), desencriptar una segunda parte de código de sistema (255) almacenada en la primera memoria de datos (625) con un segundo procedimiento de encriptación que utiliza la primera parte de código de sistema (215) como clave, unir las partes de código de sistema primera y segunda (215, 245) de modo que se obtiene un código de sistema;
h) comparar la identificación de asignación (330) con identificaciones de asignación que están almacenadas en la segunda memoria de datos (635) y, si se encuentra una identificación de asignación que coincide, encriptar el código de sistema mediante un tercer procedimiento de encriptación que utiliza una clave de encriptación (315) almacenada junto con la identificación de asignación (330) en la segunda memoria de datos (635);
i) comparar el código de sistema (415) encriptado con códigos de sistema encriptados que están almacenados en la tercera memoria de datos (645) y, si se encuentra un código de sistema encriptado que coincide, desencriptar una identificación de objeto (430) encriptada asignada mediante un cuarto procedimiento de encriptación que utiliza el código de sistema como clave; y

j) visualizar (150) una identificación de objeto desencriptada para comparar la identificación de objeto visualizada con la identificación de objeto (420) en el objeto (500),

estando las memorias de datos (625, 635, 645) físicamente separadas unas de otras.

5. Procedimiento según la reivindicación 4, en el que el código de sistema está almacenado en la primera memoria de datos (625) con una información de activación adicional que indica si el código de sistema está activo o inactivo, teniendo el procedimiento una etapa adicional que se realiza antes de la etapa e) en la que se activa la información de activación de uno de los códigos de sistema (155), y/o siendo el medio de transmisión Internet o una red de telefonía móvil.

6. Procedimiento según una de las reivindicaciones 4 o 5, comprendiendo los datos específicos de consulta, en el caso de una entrada del código por Internet, al menos una indicación de tiempo, la dirección IP, el proveedor de servicios de Internet y el número de intentos de entrada; y/o comprendiendo los datos específicos de consulta, en el caso de una entrada del código por SMS, al menos una indicación de tiempo, el número de teléfono móvil y el número de marcaje SMS.

7. Dispositivo (600) para identificar un objeto (500), que está dotado al menos de una identificación de objeto (420), mediante un código de objeto (405) que se utiliza para la verificación de la autenticidad del objeto (500), que comprende:

un dispositivo de generación de código de sistema (610) que está diseñado para generar un código de sistema aleatorio unívoco que consiste en unas partes de código de sistema primera y segunda (215, 245), generándose la primera parte de código de sistema (215) a partir de una primera reserva de caracteres (200) mediante un primer procedimiento aleatorio (205) y la segunda parte de código de sistema (245) a partir de una segunda reserva de caracteres (230) mediante un segundo procedimiento aleatorio (235); un primer dispositivo de almacenamiento de datos (620; 625) que está diseñado para almacenar el código de sistema generado por el dispositivo de generación de código de sistema (610) junto con al menos una primera información (260) específica de objeto, encriptándose la primera parte de código de sistema (215) mediante un primer procedimiento de encriptación y la segunda parte de código de sistema (245) mediante un segundo procedimiento de encriptación que utiliza la primera parte de código de sistema (215) como clave, antes del almacenamiento;
un dispositivo de generación de clave de encriptación (630) que está diseñado para generar una clave de encriptación (315) aleatoria a partir de una tercera reserva de caracteres (300) mediante un tercer procedimiento aleatorio (305) y una identificación de asignación (330) unívoca mediante un procedimiento de asignación (320);
un segundo dispositivo de almacenamiento de datos (640) que está diseñado para almacenar la clave de encriptación (315) generada, la identificación de asignación (330) y al menos una segunda información (335) específica de objeto;
un dispositivo de generación de código de objeto (650) que está diseñado para generar un código de objeto (405) que consiste al menos en la primera parte de código de sistema (215) y la identificación de asignación (330);
un tercer dispositivo de almacenamiento de datos (660) que está diseñado para almacenar el código de sistema (415) encriptado mediante un tercer procedimiento de encriptación que utiliza la clave de encriptación (315) como clave junto con la identificación de objeto (420) que está encriptada mediante un cuarto procedimiento de encriptación que utiliza el código de sistema como clave;
un dispositivo de colocación de código de objeto (670) que está diseñado para colocar el código de objeto (405) en el objeto (500); y
un cuarto dispositivo de almacenamiento de datos que está diseñado para almacenar datos específicos de consulta que se generan en la verificación de la autenticidad del objeto (500),
estando los dispositivos de almacenamiento de datos (620, 640, 660) físicamente separados unos de otros.

8. Dispositivo (600) según la reivindicación 7, que comprende además:

un dispositivo de división que está diseñado para dividir el código de objeto (405) en unas partes de código de objeto primera y segunda (520, 530).

9. Dispositivo (700) para verificar la autenticidad de un objeto (500), que está dotado al menos de una identificación de objeto (420), mediante un código de objeto (405), habiéndose generado el código de objeto (405) según un dispositivo según una de las reivindicaciones 7 u 8, que comprende:

un dispositivo de recepción (720) que está diseñado para recibir el código de objeto (405) que se transmite mediante al menos un medio de transmisión (710);
un dispositivo de verificación (740) que está diseñado para desencriptar el código de objeto (405) introducido en el dispositivo de entrada y posibilitar la desencriptación del código de objeto (405) introducido, que comprende:

un dispositivo de división de código de objeto (750) que está diseñado para dividir el código de objeto (405) introducido al menos en una primera parte de código de sistema (215) y una identificación de asignación

(330);
un primer dispositivo de comparación (760) que está diseñado para encriptar la primera parte de código de sistema (215) con un primer procedimiento de encriptación y comparar la primera parte de código de sistema encriptada (225) con las primeras partes de código de sistema que están almacenadas en el primer dispositivo de almacenamiento de datos (620) y, si la primera parte de código de sistema encriptada (225) se encuentra en el primer dispositivo de almacenamiento de datos (620), desencriptar una segunda parte de código de sistema (255) almacenada en el primer dispositivo de almacenamiento de datos (620) con un segundo procedimiento de encriptación que utiliza la primera parte de código de sistema (215) como clave y unir las partes de código de sistema primera y segunda (215, 245) de modo que se obtiene un código de sistema;
un segundo dispositivo de comparación (770) que está diseñado para comparar la identificación de comparación (330) con identificaciones de asignación que están almacenadas en el segundo dispositivo de almacenamiento (640) y, si se encuentra una identificación de asignación que coincide, encriptar el código de sistema mediante un tercer procedimiento de encriptación que utiliza como clave una clave de encriptación (315) almacenada junto con la identificación de asignación (330) en la segunda memoria de datos (635; 775);
un tercer dispositivo de comparación (780) que está diseñado para comparar el código de sistema (415) encriptado con códigos de sistema encriptados que están almacenados en el tercer dispositivo de almacenamiento de datos (660) y, si se encuentra un código de sistema (415) encriptado que coincide, desencriptar una identificación de objeto (430) encriptada asignada mediante un cuarto procedimiento de encriptación que utiliza como clave la primera parte de código de sistema (215);
un dispositivo de visualización (790) que visualiza la identificación de objeto (420) desencriptada por el dispositivo de verificación (740); y
un cuarto dispositivo de almacenamiento de datos que está diseñado para almacenar datos específicos de consulta que se generan en la verificación de la autenticidad del código de objeto (405),
estando los dispositivos de almacenamiento de datos (620, 640, 660) físicamente separados unos de otros.

10. Dispositivo (700) según la reivindicación 9, que comprende además:

un dispositivo de activación (730) que está diseñado para activar un código de sistema almacenado como inactivo en el primer dispositivo de almacenamiento de datos (620); y/o siendo el medio de transmisión (710) Internet o una red de telefonía móvil.

11. Dispositivo (700) según la reivindicación 10, almacenando el cuarto dispositivo de almacenamiento de datos, en el caso de una entrada del código de objeto (405) por Internet, al menos una indicación de tiempo, la dirección IP, el proveedor de servicios de Internet y el número de intentos de entrada.

12. Dispositivo (700) según la reivindicación 10, almacenando el cuarto dispositivo de almacenamiento de datos, en el caso de una entrada del código de objeto (405) por SMS, al menos una indicación de tiempo, el número de teléfono móvil y el número de marcaje SMS.

13. Objeto (500) que está identificado con un código de objeto (405) que se ha generado con el procedimiento según una de las reivindicaciones 1 a 3.

14. Programa informático que, cuando se ejecuta en un ordenador, controla éste de modo que realiza el procedimiento según una de las reivindicaciones 1 a 6.

15. Soporte de datos en el que está almacenado de modo que se puede leer por máquina un programa informático según la reivindicación 14.

Fig. 1

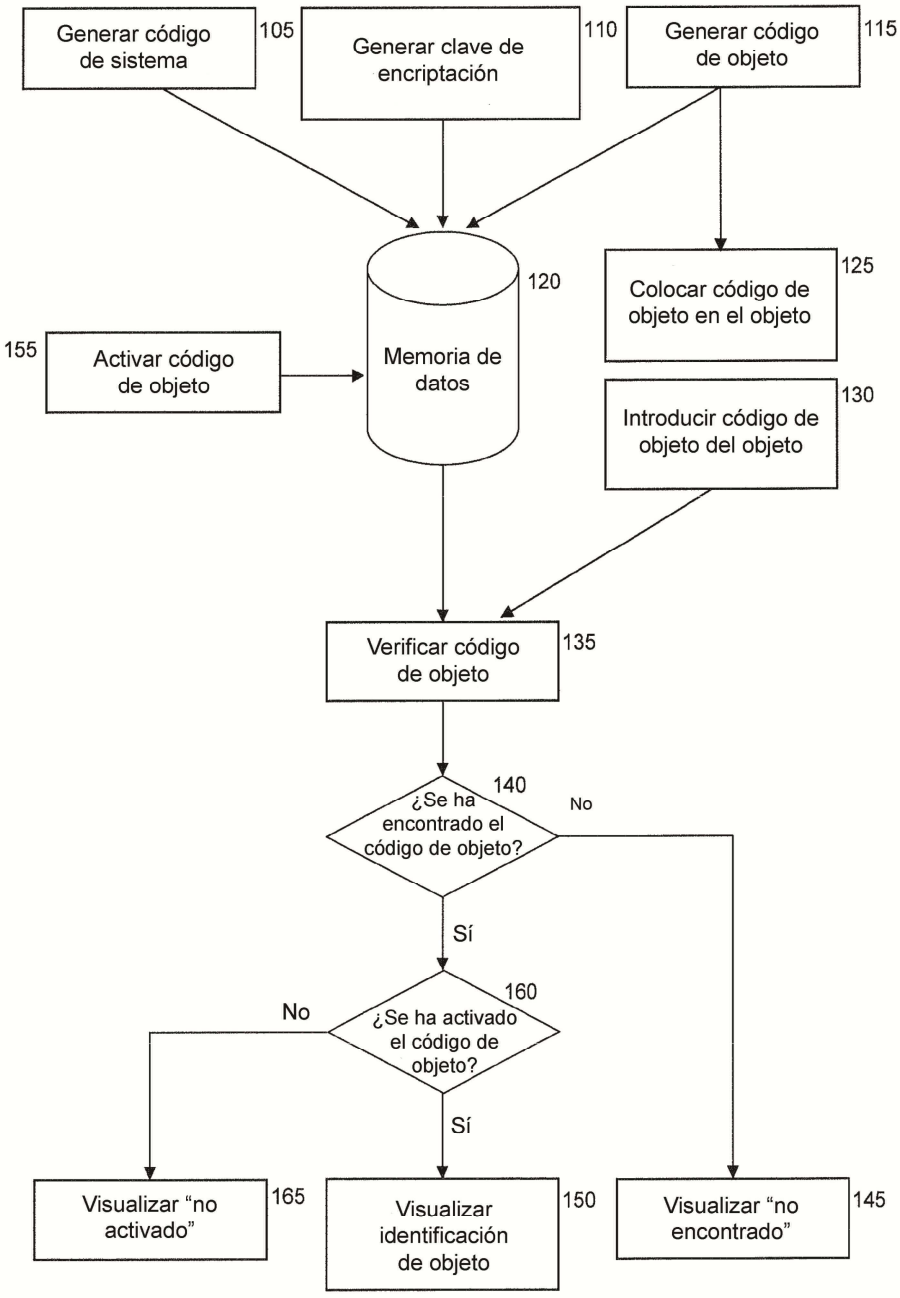

Generar código de sistema
105
Generar clave de encriptación
110
Generar código de objeto
115
120
Memoria de datos
155
Activar código de objeto
Colocar código de objeto en el objeto
125
Introducir código de objeto del objeto
130
Verificar código de objeto
135
¿Se ha encontrado el código de objeto?
140
No
Sí
¿Se ha activado el código de objeto?
160
No
Sí
Visualizar "no activado"
165
Visualizar identificación de objeto
150
Visualizar "no encontrado"
145

Fig. 2

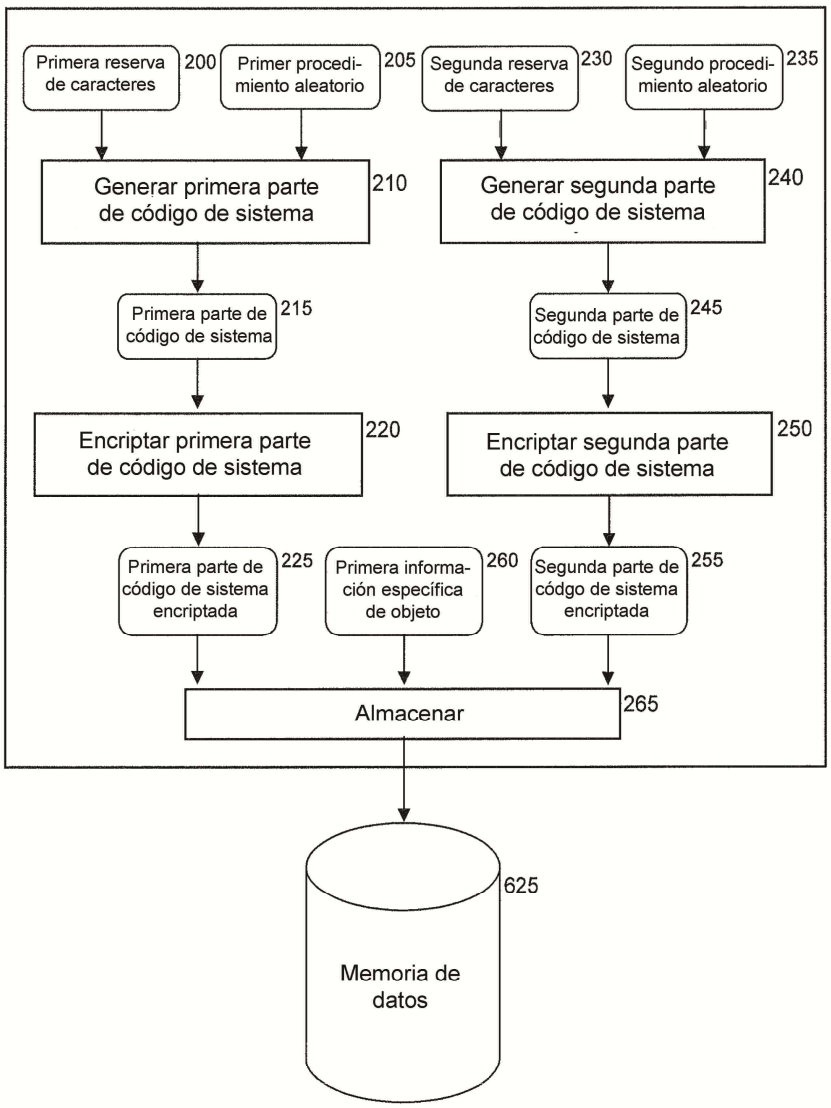

Primera reserva de caracteres
200
Primer procedimiento aleatorio
205
Segunda reserva de caracteres
230
Segundo procedimiento aleatorio
235
Generar primera parte de código de sistema
210
Generar segunda parte de código de sistema
240
Primera parte de código de sistema
215
Segunda parte de código de sistema
245
Encriptar primera parte de código de sistema
220
Encriptar segunda parte de código de sistema
250
Primera parte de código de sistema encriptada
225
Primera información específica de objeto
260
Segunda parte de código de sistema encriptada
255
Almacenar
265
Memoria de datos
625

Fig. 3

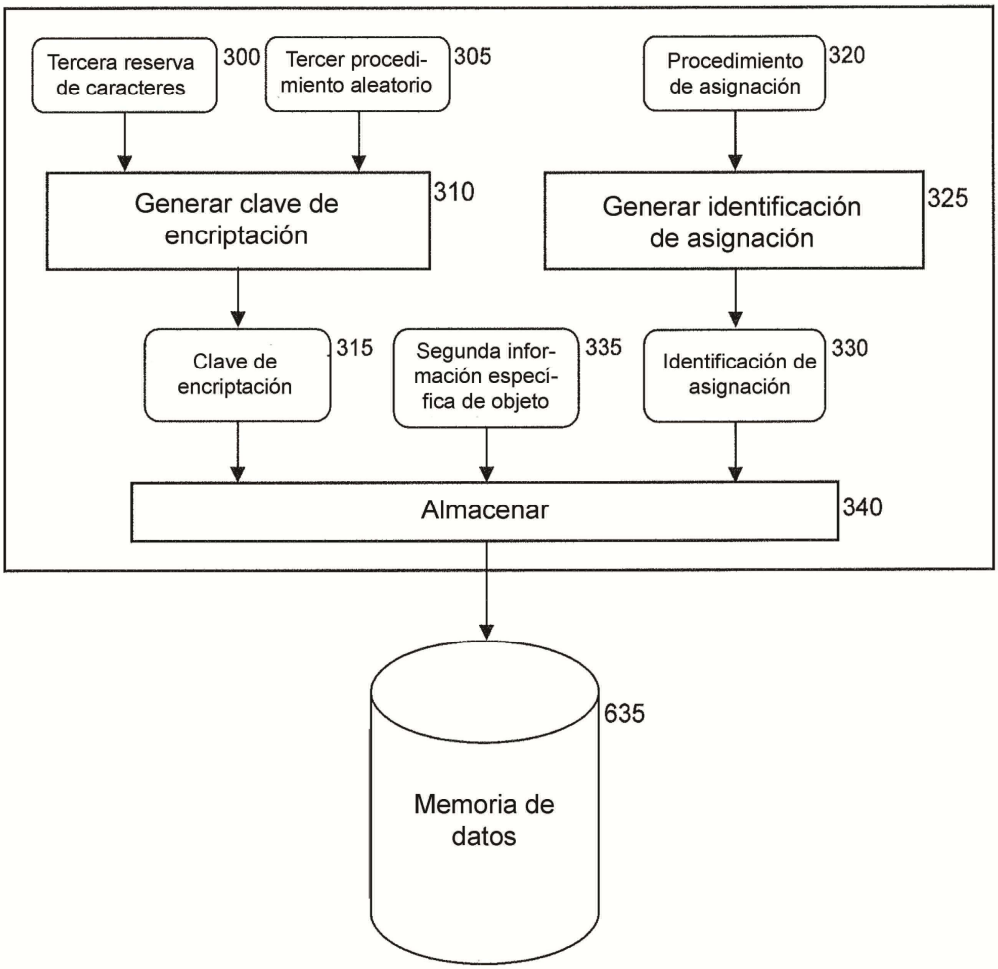

Tercera reserva de caracteres
300
Tercer procedimiento aleatorio
305
Procedimiento de asignación
320
Generar clave de encriptación
310
Generar identificación de asignación
325
Clave de encriptación
315
Segunda información específica de objeto
335
Identificación de asignación
330
Almacenar
340
635
Memoria de datos

Fig. 4

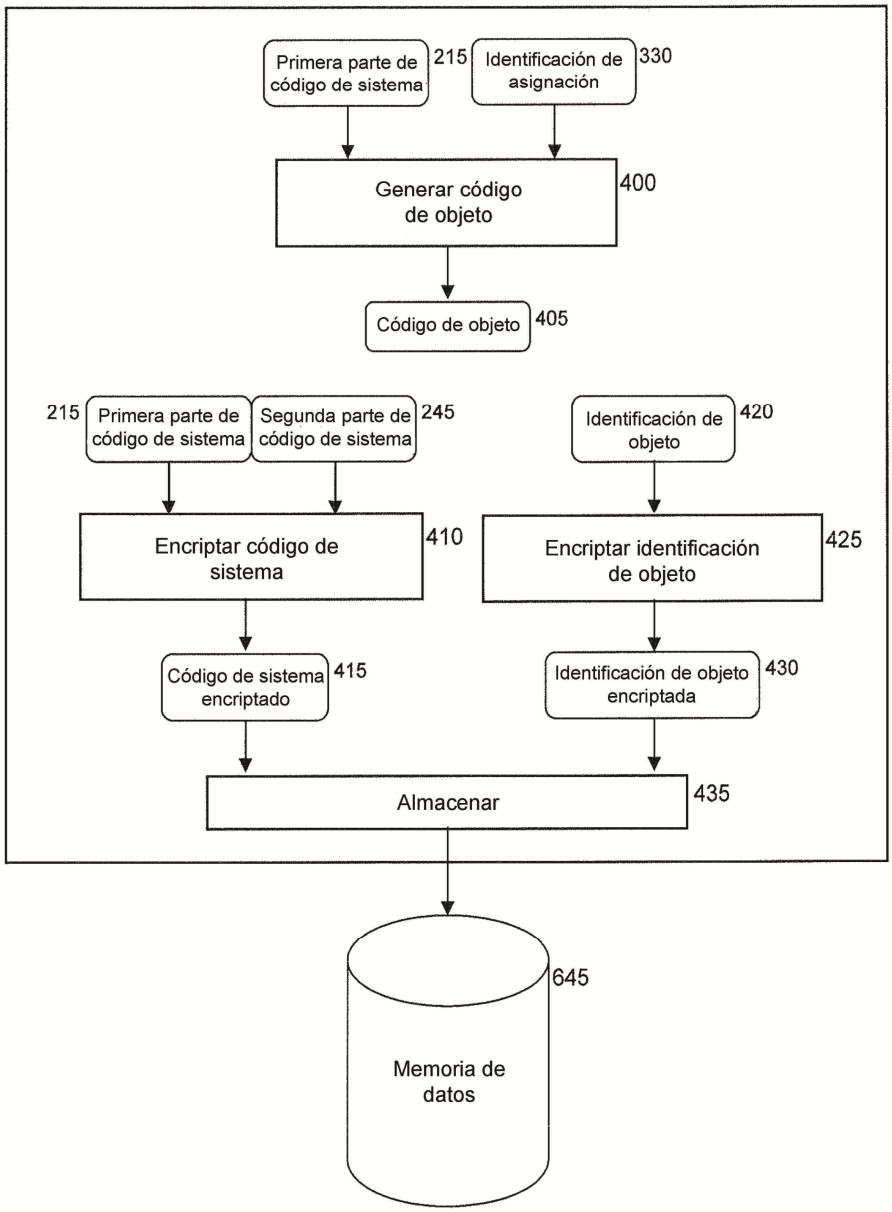
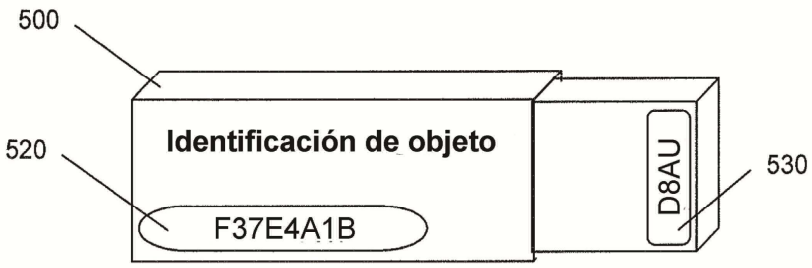

Primera parte de código de sistema
215
Identificación de asignación
330
Generar código de objeto
400
Código de objeto
405
215
Primera parte de código de sistema
Segunda parte de código de sistema
245
Identificación de objeto
420
Encriptar código de sistema
410
Encriptar identificación de objeto
425
Código de sistema encriptado
415
Identificación de objeto encriptada
430
Almacenar
435
645
Memoria de datos

Fig. 5A

Fig. 5B



Código de objeto = F37E4A1BD8AU

Fig. 5C

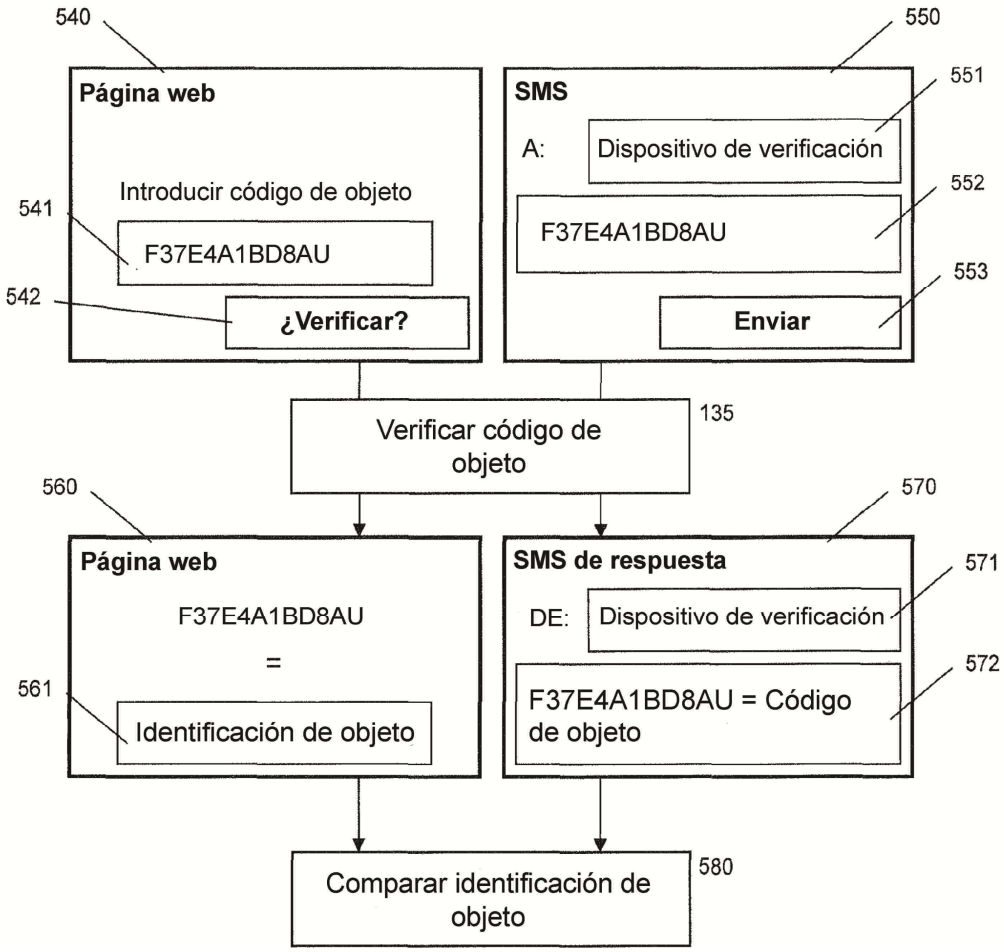

540
Página web
Introducir código de objeto
541
F37E4A1BD8AU
542
¿Verificar?
550
SMS
551
A:
Dispositivo de verificación
552
F37E4A1BD8AU
553
Enviar
Verificar código de objeto
135
560
Página web
F37E4A1BD8AU
=
561
Identificación de objeto
570
SMS de respuesta
571
DE:
Dispositivo de verificación
572
F37E4A1BD8AU = Código de objeto
Comparar identificación de objeto
580

Fig. 6

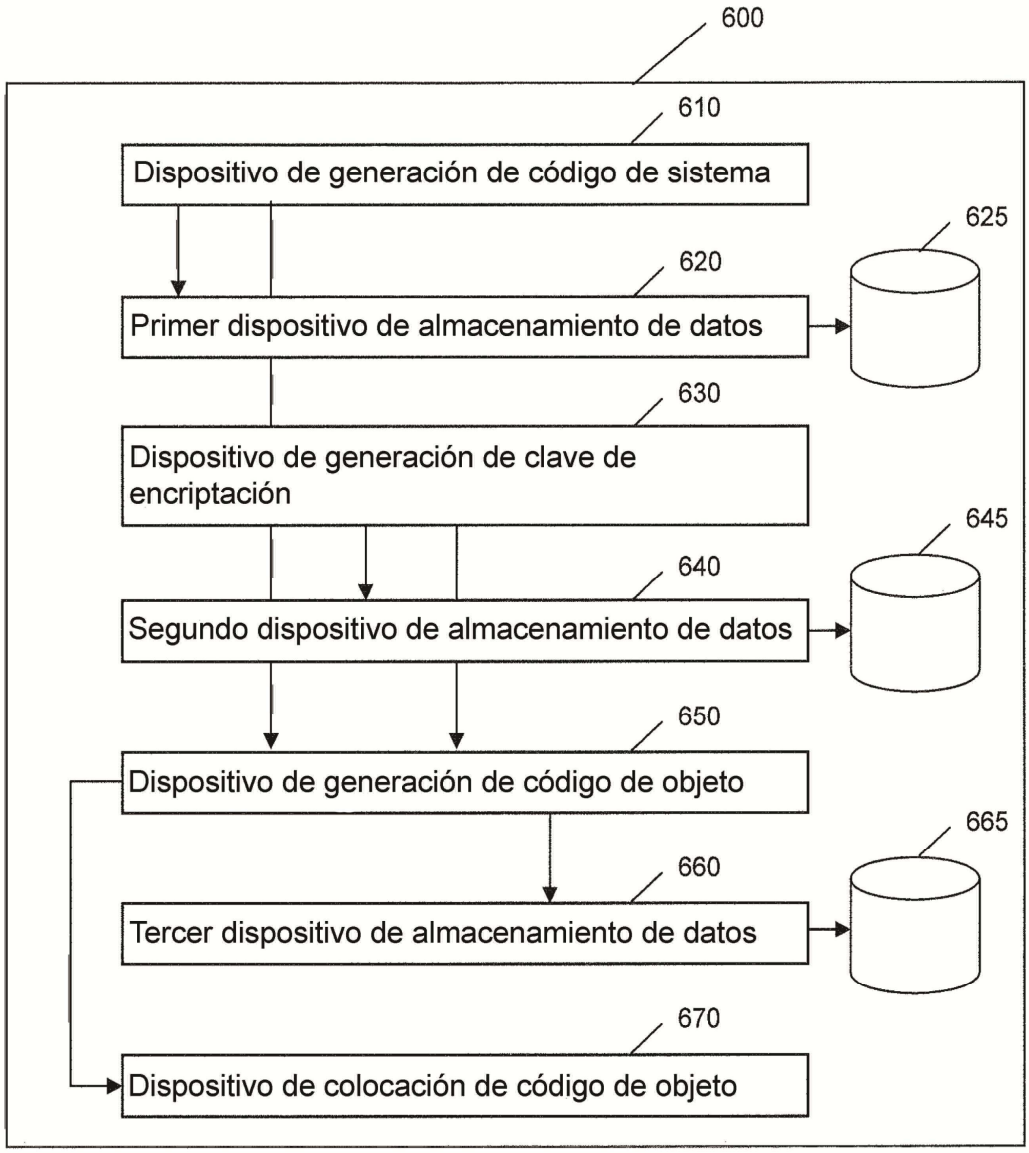
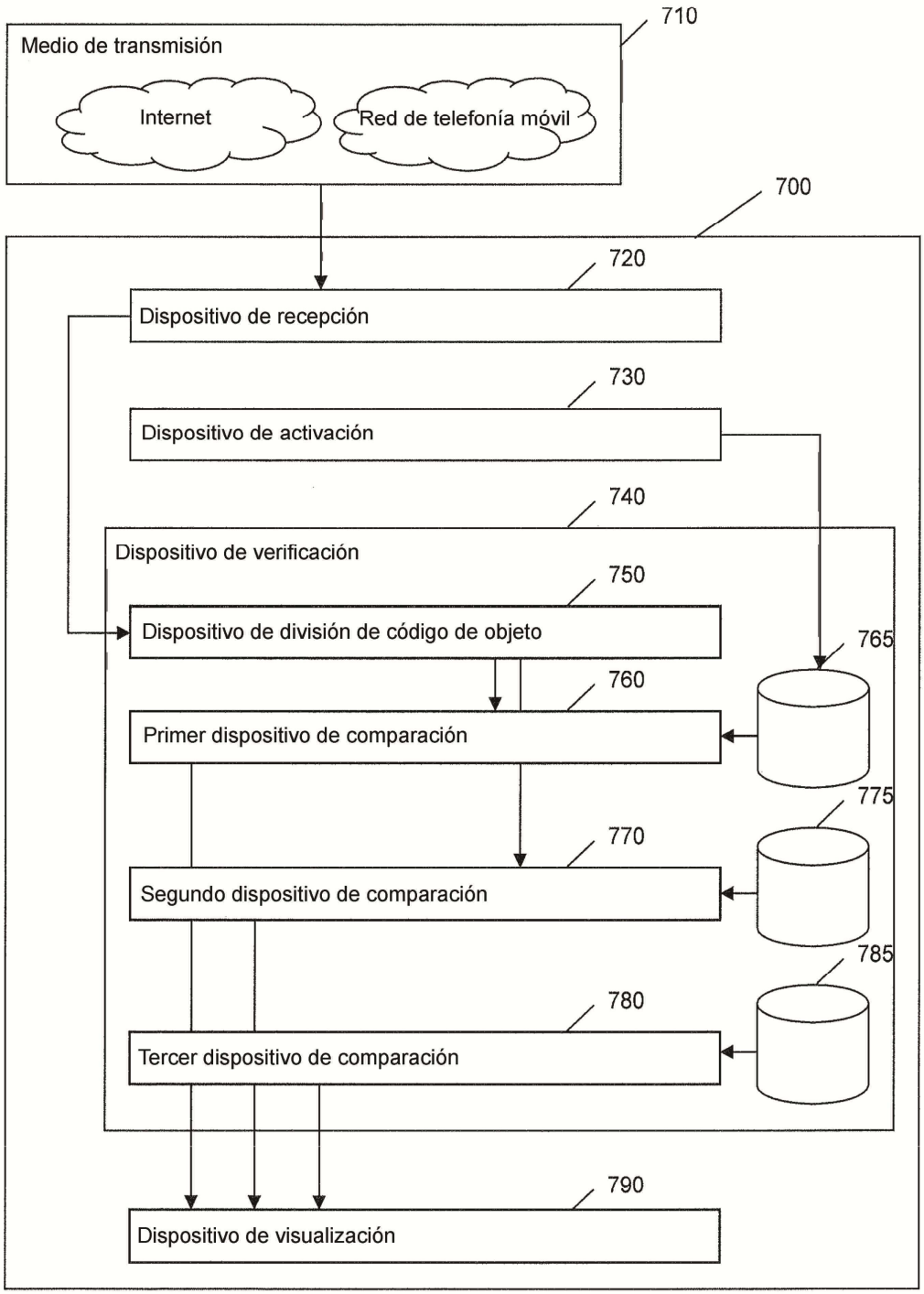

600
610
Dispositivo de generación de código de sistema
625
620
Primer dispositivo de almacenamiento de datos
630
Dispositivo de generación de clave de encriptación
645
640
Segundo dispositivo de almacenamiento de datos
650
Dispositivo de generación de código de objeto
665
660
Tercer dispositivo de almacenamiento de datos
670
Dispositivo de colocación de código de objeto

Fig. 7


710
Medio de transmisión
Internet
Red de telefonía móvil
700
720
Dispositivo de recepción
730
Dispositivo de activación
740
Dispositivo de verificación
750
Dispositivo de división de código de objeto
765
760
Primer dispositivo de comparación
775
770
Segundo dispositivo de comparación
785
780
Tercer dispositivo de comparación
790
Dispositivo de visualización

REFERENCIAS CITADAS EN LA DESCRIPCIÓN

Esta lista de referencias citadas por el solicitante es para conveniencia del lector. No forma parte del documento de la Patente Europea. Aunque se ha tenido mucho cuidado en la compilación de las referencias, no pueden excluirse errores u omisiones y la EPO declina responsabilidades por este asunto.

Documentos de patentes citadas en la descripción

* DE 4341880 A1 **[0003]**
* EP 0889448 B1 **[0004]**
* US 20060053025 A1 **[0005]**