(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 569 338**

(51) Int. CI.:

G06F 21/45 (2013.01)
G06Q 10/08 (2012.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **09.05.2008 E 08750237 (3)**

(97) Fecha y número de publicación de la concesión europea: **27.01.2016 EP 2156602**

(54) Título: **Procedimiento y sistema para comprobar la autenticidad de un producto y aparato de lectura**

(30) Prioridad:

06.06.2007 DE 102007026836

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.05.2016

(73) Titular/es:

BUNDESDRUCKEREI GMBH (100.0%)
Oranienstrasse 91
10958 Berlin, DE

(72) Inventor/es:

BYSZIO, FRANK y
WIRTH, KLAUS-DIETER

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Procedimiento y sistema para comprobar la autenticidad de un producto y aparato de lectura

La invención concierne a un procedimiento para comprobar la autenticidad de un producto, en particular para la protección contra la piratería de productos, así como a un sistema correspondiente y un aparato de lectura.

Por el estado de la técnica son conocidas diversas soluciones de seguridad para proteger productos de marcas. Por ejemplo, los productos de marcas se proveen de un holograma que puede contener elementos de seguridad visibles y ocultos. Además, son conocidos también etiquetas electromagnéticas, de radiofrecuencia y acustomagnéticas para la identificación de productos de marcas. A ellas pertenecen etiquetas RFID activas y pasivas para diferentes frecuencias portadoras.

El documento WO2008/101899 A1 muestra un documento y un procedimiento para el control de acceso. A través del control de acceso debe impedirse una lectura de datos inadvertida o no autorizada. Un mecanismo de protección de este tipo se muestra también en el documento D4 KINNEGING T A F: “Documentos de viaje legibles por máquina, Informe Técnico, PKI para documentos de viaje legibles por máquina que ofrecen acceso de solo lectura ICC”, INTERNET CITATION, (Online), XP002396748, Versión 1.1, 1 de octubre de 2004.

Por el documento US 6.226.619 B1, del que parte la presente invención como estado de la técnica más próximo, se ha conocido un procedimiento para la protección contra piratería de productos, según lo cual el producto o su envase están provistos de una etiqueta que lleva un número de serie del producto. Este número de serie está almacenado también en una etiqueta RFID fijada al producto. El número de serie puede leerse con ayuda de un aparato de lectura de la etiqueta RFID y compararse con el número de serie mostrado en la etiqueta. Cuando coinciden ambos números de serie, el producto se considera como auténtico.

Una desventaja especial es en este caso que esta solución es insuficiente desde el punto de vista de la protección de datos y la protección del consumidor contra acciones de espionaje no deseadas, ya que la etiqueta RFID puede leerse por el consumidor de forma inadvertida. Sobre esta base, podrían elaborarse entonces, por ejemplo, para fines de márquetin o fines de vigilancia, perfiles de movimientos del consumidor.

Frente a esto, la presente invención se basa en el problema de crear un procedimiento mejorado para comprobar la autenticidad de un producto, así como un sistema correspondiente y un aparato de lectura. Los problemas en los que se basa la invención se resuelven respectivamente con las características de las reivindicaciones independientes. Formas de realización de la invención están indicadas en las reivindicaciones subordinadas. Según formas de realización de la invención, se crea un procedimiento para comprobar la autenticidad de un producto para la protección contra la piratería de productos con los siguientes pasos: detección de un identificador asociado al producto, introducción del identificador en un aparato de lectura, en donde el aparato de lectura presenta una interfaz para la comunicación por radio con una unidad de emisión-recepción asociada al producto, y en donde en la unidad de emisión-recepción está almacenado un valor de referencia con respecto al identificador, y autorización del aparato de lectura para un acceso a la unidad de emisión-recepción, en donde la autorización se realiza con ayuda del identificador por medio de la interfaz con respecto a la unidad de emisión-recepción y en donde el producto, al coincidir el identificador con el valor de referencia, se considera como auténtico.

Es especialmente ventajoso aquí que la comprobación de la autenticidad, es decir, la veracidad del producto, puede realizarse sólo después de la autorización previa del aparato de lectura, de modo que, por ejemplo, no puedan consultarse datos por la unidad de emisión-recepción sin que ello sea advertido por el propietario del producto. Por tanto, se garantiza la protección de los datos y puede evitarse que se establezca un perfil de movimientos del propietario del producto.

Según una forma de realización de la invención, el producto es un bien móvil como, por ejemplo, un producto de marca y/o un producto protegido por otros derechos de propiedad industrial, cuya falsificación o copia está sometida a la protección legal.

Según una forma de realización de la invención, el producto es un bien de consumo para el consumidor final (el denominado producto de consumo) o un bien de inversión. Por ejemplo, el producto puede ser una prenda de ropa, comida o su envase, un aparato electrónico como, por ejemplo, un ordenador, una pieza de máquina, una pieza de repuesto, un vehículo o una parte de vehículo, un medicamento o una bebida de alta calidad.

Por medio de la aplicación de formas de realización del procedimiento según la invención, un consumidor final potencial del producto puede, por ejemplo, cerciorarse de su autenticidad antes de la compra del producto. Además, puede facilitarse también, por ejemplo, a intermediarios, cadenas comerciales y similares, que quisieran ofrecer un producto de este tipo al consumidor final, seguridad con respecto a la autenticidad de los productos ofrecidos por ellos.

Según una forma de realización de la invención, una característica de identificación está dispuesta en el producto o

su envase, por ejemplo en forma de una etiqueta. La detección del identificador puede realizarse visualmente por un usuario y/u ópticamente con ayuda de un sensor del aparato de lectura.

Por ejemplo, puede imprimirse en texto claro un número de serie del producto, u otra indicación que identifica de forma inequívoca el producto, sobre una etiqueta que se encuentra en el producto. El número de serie puede leerse por un usuario en la etiqueta y, por ejemplo, introducirse manualmente en el aparato de lectura por medio de un teclado. Alternativamente, la detección del identificador puede realizarse automáticamente por la característica de identificación, en particular con ayuda de un sensor óptico del aparato de lectura. Esto es particularmente ventajoso cuando el identificador no está indicado en texto claro de manera legible para un usuario sobre la característica de identificación, en particular cuando la característica de identificación es un código de barras, un holograma, una memoria óptica o similares.

Según una forma de realización de la invención, el aparato de lectura envía el identificador a la unidad de emisión-recepción. Ésta compara el identificador con un valor de referencia. Al coincidir el identificador con el valor de referencia, la unidad de emisión-recepción señaliza la autenticidad del producto. En caso contrario, la unidad de emisión-recepción no emite ninguna señal. Por tanto, en esta forma de realización un acceso del aparato de lectura a la unidad de emisión-recepción es sólo posible cuando el aparato de lectura transmite a la unidad de emisión-recepción un identificador adecuado con el que se proporciona la autorización del aparato de lectura.

Según una forma de realización de la invención, el aparato de lectura envía un comando de acceso a la unidad de emisión-recepción. El comando de acceso es total o parcialmente codificado con ayuda del identificador o un código derivada del mismo, por ejemplo después de un procedimiento de codificación simétrica. En este caso, la autorización del aparato de lectura con respecto a la unidad de emisión-recepción se proporciona cuando la unidad de emisión-recepción puede descodificar el comando de acceso con ayuda del valor de referencia almacenado en la unidad de emisión-recepción.

Después de una autorización del aparato de lectura de este tipo, la unidad de emisión-recepción transmite el valor de referencia al aparato de lectura, de modo que el aparato de lectura pueda comprobar el identificador con ayuda del valor de referencia. Preferiblemente, el valor de referencia se codifica también antes de su transmisión desde la unidad de emisión-recepción hasta el aparato de lectura, por ejemplo con el mismo código simétrico con el que se ha codificado también el comando de acceso a través del aparato de lectura.

Según una forma de realización de la invención, la fiabilidad de la comprobación de la autenticidad se incrementa adicionalmente por que la unidad de emisión-recepción se debe autentificar frente al aparato de lectura o a una tarjeta inteligente asociada al aparato de lectura con ayuda de un procedimiento criptográfico. Alternativa o adicionalmente, el aparato de lectura o la tarjeta inteligente asociada al aparato de lectura debe autentificarse también frente a la unidad de emisión-recepción. La autentificación puede realizarse respectivamente con ayuda de un código simétrico o un par de códigos asimétricos, por ejemplo con un procedimiento de reto-respuesta.

Según una forma de realización de la invención, la fiabilidad de la comprobación de la autenticidad se incrementa por que la unidad de emisión-recepción está configurada para transmitir una firma del valor de referencia al aparato de lectura. Por ejemplo, el valor de referencia se firma digitalmente con ayuda del código privado del fabricante del producto o de una cadena de producción que oferta el producto. La firma del valor de referencia se comprueba por el aparato de lectura con ayuda del correspondiente código público. Este código público puede estar almacenado en el aparato de lectura. El aparato de lectura puede disponer también de una interfaz como, por ejemplo, una interfaz de red, en particular una interfaz de internet, para consultar el código público necesario desde un servidor de registro.

Según una forma de realización de la invención, después de la autorización y, eventualmente, de la autentificación y/o comprobación de la firma, pueden leerse por medio del aparato de lectura datos relativos al producto procedentes de la unidad de emisión-recepción. Estos datos relativos al producto pueden ser indicaciones con respecto a la utilizabilidad, la manipulación, el mantenimiento o similares. En particular, los datos relativos al producto pueden contener una fecha de caducidad.

Según una forma de realización de la invención, los datos relativos al producto contienen datos ambientales relevantes para el producto como, por ejemplo, datos de temperatura. Por ejemplo, para la utilizabilidad de un medicamento, junto con su fecha de caducidad, puede ser relevante también si el medicamento, después de su producción, se ha conservado durante el transporte y el almacenamiento en una zona de temperatura especificada. Por ejemplo, para diferentes medicamentos es necesario que estos se enfríen permanentemente. Para comprobar la utilizabilidad, por ejemplo, de un medicamento, tales datos ambientales relevantes para el producto se leen por el aparato de lectura en la memoria.

En un aspecto adicional, la invención concierne a un sistema para comprobar la autenticidad de un producto con una característica de identificación asociada al producto o asociable por personalización, mediante la cual se puede detectar ópticamente un identificador, y con una unidad de emisión-recepción que está configurada para la comunicación por radio con un aparato de lectura, en donde en la unidad de emisión-recepción se almacena o es almacenable un valor de referencia con respecto al identificador, y en donde la unidad de emisión-recepción

presenta medios para la autorización del aparato de lectura a un acceso a la unidad de emisión-recepción, de modo que la comprobación de la autenticidad del producto pueda realizarse con ayuda del identificador y del valor de referencia solamente después de la autorización.

Por tanto, el sistema puede suministrarse, por ejemplo al fabricante del producto, con una característica de identificación aún no personalizada y/o una unidad de emisión-recepción aún no personalizada, en cuyo caso la colocación del sistema en el producto y la personalización específica del producto – por ejemplo, por asignación de un número de serie – se realizan por el fabricante del producto. No obstante, la personalización puede realizarse también por parte del fabricante del sistema según la invención cuando se facilita a éste por el fabricante del producto la información de personalización como, por ejemplo, los números de serie.

Según una forma de realización de la invención, la unidad de emisión-recepción es un transpondedor, en particular un transpondedor RFID. Un transpondedor RFID se designa también como etiqueta RFID, chip RFID, tag RFID, label RFID o radioetiqueta. El transpondedor RFID tiene una interfaz de radio a través de la cual pueden hacerse disponibles por medio de ondas de radio los datos almacenados en el transpondedor RFID. A frecuencias bajas esto sucede inductivamente por medio de un campo cercano y a frecuencias más elevadas esto se realiza por medio de un campo lejano electromagnético. El transpondedor RFID contiene preferiblemente un microchip y una antena que están alojados en un soporte o carcasa o están impresos sobre un sustrato. El transpondedor RFID puede estar configurado de manera pasiva o activa, en cuyo último caso dispone de una fuente de energía como, por ejemplo, una batería.

En un aspecto adicional, la invención concierne a un aparato de lectura para una unidad de emisión-recepción asociada a un producto, con medios para introducir un identificador que está asociado al producto, una interfaz para la comunicación por radio con la unidad de emisión-recepción y medios para autorizar un acceso del aparato de lectura a la unidad de emisión-recepción con ayuda del identificador.

En lo que sigue, se explican con más detalle formas de realización de la invención con referencia a los dibujos. Muestran:

La figura 1, un diagrama de bloques de una forma de realización de un sistema según la invención y de un aparato de lectura según la invención,

La figura 2, otra forma de realización de un sistema según según la invención y de un aparato de lectura según la invención,

La figura 3, un diagrama de flujo de una forma de realización de un procedimiento según la invención,

La figura 4, un diagrama de bloques de otra forma de realización de un sistema según la invención y de un aparato de lectura según la invención, y

La figura 5, un diagrama de flujo de una forma de realización adicional de un procedimiento según la invención.

Los elementos de las figuras que se corresponden uno con otro están marcados con los mismos símbolos de referencia.

La figura 1 muestra un producto 100. El producto 100 puede ser un bien móvil como, por ejemplo un bien de consumo, en particular una prenda de ropa, una bebida, un producto electrónico o una máquina, un aparato, un componente de máquina o aparato, una pieza de repuesto, un medicamento o similares. En particular, el producto 100 puede ser un producto protegido por uno o varios derechos de propiedad industrial, en particular un producto de marcha cuya imitación no permitida puede llevar a un daño económico considerable y/o a un riesgo para la seguridad o una amenaza para la salud.

El producto 100 debe protegerse frente a copias e imitaciones no permitidas, en particular contra la denominada piratería de productos, para lo cual se le provee de un sistema según la invención para comprobar la veracidad, es decir, la autenticidad del producto.

Para ello, el producto 100 lleva asociado un identificador. El identificador puede ser una marcación con ayuda de la cual el producto pueda identificarse de manera inequívoca, por ejemplo un número de serie o un número de serie en combinación con un número de fabricante. En particular, el identificador puede ser un denominado Identificador Globalmente Único (GUID).

El identificador puede colocarse con ayuda de una característica de identificación directamente en el producto 100 o su envase. Por ejemplo, se encuentra en o sobre el producto 100 una etiqueta 102 sobre la cual se ha impreso en texto claro el identificador (“ID de producto”). La etiqueta 102 está configurada, por ejemplo, de tal manera que no pueda retirarse del producto 100 sin ser destruida. La etiqueta 102 puede llevar también un holograma o una memoria óptica, en la cual pueda leerse a maquina la ID del producto con ayuda de un sensor óptico.

El producto 100 lleva asociada además una unidad de emisión-recepción, es decir, un transpondedor 104. El transpondedor 104 está configurado para la comunicación inalámbrica por radio con un aparato de lectura 106. Por ejemplo, el transpondedor 104 puede ser un transpondedor RFID, en particular una denominada etiqueta RFID.

El transpondedor 104 tiene una interfaz de radio 108 para la comunicación con una interfaz de radio 110 correspondiente del aparato de lectura 106. El transpondedor 104 dispone, además, de un circuito de mando lógico 112 como, por ejemplo, un microprocesador para la ejecución de instrucciones de programa. Además, el transpondedor 104 tiene una memoria electrónica para almacenar un valor de referencia 114 con respecto al identificador.

El aparato de lectura 106 tiene una interfaz 116 para la introducción del identificador en el aparato de lectura 106. La interfaz 116 puede ser, por ejemplo, un teclado a través del cual un usuario pueda introducir manualmente en el aparato de lectura 106 el identificador previamente leído en la etiqueta 102. La interfaz 116 puede presentar también un sensor para la detección automática del identificador de la etiqueta 102 y para su introducción en el aparato de lectura 106.

El aparato de lectura 106 dispone, además, de un procesador 118 para la ejecución de instrucciones de programa 120, así como una unidad de visualización 122.

Para comprobar la autenticidad del producto 100 se procede de la siguiente manera: En primer lugar, se detecta el identificador de la etiqueta 102 visualmente por un usuario o a máquina con un sensor de la interfaz 116 y se le introduce en el aparato de lectura 106. Por medio de la ejecución de las instrucciones de programa 120 se activa la interfaz de radio 110 del aparato de lectura 106, de modo que una señal 124 sea transmitida de la interfaz de radio 110 a la interfaz de radio 108 del transpondedor 104. Con la señal 124 se transmite del aparato de lectura 106 al transpondedor 104 el identificador que se ha introducido previamente por medio de la interfaz 116.

El transpondedor 104 evalúa la señal 124 recibida del aparato de lectura 106, para lo cual, con ayuda del circuito de mando lógico 112, se realiza una comprobación de coincidencia del identificador recibido con la señal 124 y del valor de referencia 114. Cuando se presenta esta coincidencia, entonces el aparto de lectura 106 se considera como autorizado frente al transpondedor 104. Simultáneamente, se sigue de la coincidencia del identificador y del valor de referencia 114 que el producto 100 es auténtico. La autenticidad del producto se señaliza por el transpondedor 104 frente al aparato de lectura 106 por medio de la emisión de una señal 126 desde la interfaz de radio 108 de dicho transpondedor. Debido a la recepción de la señal 126, el aparato de lectura 106 emite en su unidad de visualización 122 un correspondiente mensaje para el usuario, según lo cual el producto es auténtico.

Por el contrario, cuando el identificador recibido por el transpondedor 104 con la señal 124 no coincide con el valor de referencia 114, el aparato de lectura 106 no se considera como autorizado para acceder al transpondedor 104. En este caso, el transpondedor 104 no emite ninguna señal en respuesta a la señal 124.

Por tanto, en este caso es especialmente ventajoso que sea posible una reacción del transpondedor 104 solamente después de la autorización del aparato de lectura 106, presuponiendo la autorización del aparato de lectura 106 que se detecta, por ejemplo visual u ópticamente, el identificador de la etiqueta 102. Dado que esto no puede realizarse de forma inadvertida por el propietario del producto 100, se evita así que se establezca un perfil de movimientos del propietario del producto 100 con ayuda del transpondedor 104.

En una forma de realización de la invención, la etiqueta 102 está dispuesta de modo que ésta no pueda detectarse visual u ópticamente sin dificultades en el estado de uso del producto 100. Por ejemplo, la etiqueta 102 está fijada en el interior de una prenda de ropa.

El transpondedor 104 está unido de forma mecánica preferiblemente con el producto 100 o su envase de modo que aquél no pueda retirarse sin destrucción o apenas pueda retirarse del producto 100 o su envase.

La figura 2 muestra otra forma de realización de un sistema según la invención para comprobar la autenticidad del producto 100. En la forma de realización de la figura 2, las instrucciones de programa 120 contienen una componente criptográfica 128, por ejemplo para una codificación y descodificación con ayuda de un código simétrico. El circuito de mando lógico 112 del transpondedor 104 está configurado también en esta forma de realización como procesador que, entre otras cosas, sirve para ejecutar una correspondiente componente criptográfica 130.

Para comprobar la autenticidad del producto 100 se procede aquí, por ejemplo, de la siguiente manera: Después de la detección del identificador de la etiqueta 102 y su introducción a través de la interfaz 116 del aparato de lectura 106, el procesador 118 genera, por la ejecución de las instrucciones de programa 120, un comando que se transmite como señal 124 al transpondedor 104. El comando 124 es un comando de acceso al transpondedor 104 para leer el valor de referencia 114 del transpondedor 104.

Para que el transpondedor 104 haga posible una comprobación de la autorización del aparato de lectura, se codifica

el comando 124. Para ello, el comando se codifica, por medio de la componente criptográfica 128, con el identificador o un código derivado de éste, con ayuda de un procedimiento de codificación simétrica, antes de la transmisión al transpondedor 104. Con la recepción de la señal 124 por el transpondedor 104 se inicia la componente criptográfica 130 para descodificar como código simétrico el comando recibido con la señal 124 con ayuda del valor de referencia 114. Sólo cuando se logra esta descodificación, es decir, cuando el valor de referencia 114 casa con el identificador detectado de la etiqueta 102, el transpondedor 104 emite la señal 126, con la cual el valor de referencia 114 se transmite desde el transpondedor 104 hasta el aparato de lectura 106. Preferiblemente, el valor de referencia 114 se transmite codificado, para lo cual, por ejemplo, el valor de referencia 114 se codifica con el identificador como código simétrico por medio de la componente criptográfica 130.

Por tanto, tras la recepción de la señal 126 y, eventualmente, la descodificación por medio de la componente criptográfica 128, el valor de referencia 114 se presenta en el aparato de lectura 106, de modo que este valor pueda compararse con el identificador por el aparato de lectura 106. Cuando coinciden el identificador y el valor de referencia 114, el aparato de lectura 106 emite en su unidad de visualización 122 un correspondiente mensaje que indica la autenticidad del producto 100.

Es también especialmente ventajoso aquí de nuevo que un acceso del aparato de lectura 106 al transpondedor presuponga la autorización del mismo, concibiéndose ésta cuando previamente se ha detectado un identificador de la etiqueta 102 y se le ha introducido en el aparato de lectura 106, cuyo identificador casa con el valor de referencia 114 almacenado en el transpondedor 104, dado que sólo en este caso se logra la descodificación del comando recibido con la señal 124 por la componente criptográfica 130 del transpondedor 104.

La figura 3 muestra un diagrama de flujo correspondiente. En el paso 200 se detecta visualmente por un usuario u ópticamente a máquina el identificador, es decir, por ejemplo una ID de producto singular, en el producto o su envase y se le introduce manual o automáticamente en el aparato de lectura.

En el paso 202 se autoriza el aparato de lectura con ayuda del identificador frente al transpondedor, que, por ejemplo, está configurado como una etiqueta RFID. Para ello, el aparato de lectura transmite en texto claro el identificador detectado en el paso 200 a la etiqueta RFID, de modo que la etiqueta RFID pueda comprobar la coincidencia del identificador con un valor de referencia almacenado en la etiqueta RFID. Alternativamente, el aparato de lectura envía un comando de acceso codificado a la etiqueta RFID, cuyo comando de acceso está codificado con un código simétrico, siendo el código simétrico el identificador o un código derivado de éste. La comprobación de la autorización del aparato de lectura puede realizarse entonces por medio de la etiqueta RFID a través de un intento de descodificación del comando de acceso con ayuda del valor de referencia almacenado en la etiqueta RFID.

La comprobación de la coincidencia del identificador y del valor de referencia se realiza en el paso 204, cuyo paso se realiza por una comparación directa del identificador con el valor de referencia o por un intento de descodificación, como se explica anteriormente. Cuando resulta una coincidencia entre el identificador y el valor de referencia, entonces, en el paso 206, se emite una señal desde la etiqueta RFID y/o el aparato de lectura, según la cual el producto es auténtico. En caso contrario, la etiqueta RFID no proporciona el valor de referencia al aparato de lectura o no reacciona de ninguna forma al intento de acceso del aparato de lectura, de donde se sigue que el producto no es auténtico (paso 208).

La figura 4 muestra un diagrama de bloques de una forma de realización adicional de un sistema según la invención y de un aparato de lectura 106 según la invención. En esta forma de realización, el transpondedor 104 está configurado para la autentificación frente al aparato de lectura 106 o frente a una tarjeta inteligente 132 asociada al aparato de lectura 106. La autentificación del transpondedor 104 puede realizarse con ayuda de un procedimiento criptográfico simétrico o asimétrico, por ejemplo para comprobar la autenticidad del transpondedor 104 por medio de un procedimiento de reto-respuesta.

En la forma de realización aquí considerada, el aparato de lectura 106 puede presentar una interfaz 134 de tarjeta inteligente para la tarjeta inteligente 132, en la que está almacenada una clave maestra 136. La tarjeta inteligente 132 está asociada a un usuario autorizado del aparato de lectura 106.

El aparato de lectura 106 puede presentar además un interfaz de red 138 para comunicarse a través de una red 140, como, por ejemplo, Internet, con un servidor de registro, es decir, un denominado directorio 142.

El transpondedor 104 tiene en la forma de realización aquí considerada al menos una memoria electrónica 144 en la que están almacenados el valor de referencia 114 y, opcionalmente, otros datos. En este caso, puede tratarse de un par de códigos asimétricos que consta de un código público 146 y un código privado 148. Este par de códigos puede estar asociado a un fabricante del producto 100. Al menos el código privado 148 está almacenado en una zona especialmente protegida de la memoria electrónica 144, de modo que, en principio, no puede leerse.

Junto al valor de referencia 114, una firma electrónica 150 del valor de referencia 114 puede estar almacenada en la memoria electrónica 144. La firma electrónica 150 se obtiene por la codificación del valor de referencia o de un valor

hash obtenido del valor de referencia 114 con el código privado 148.

Además, en la memoria electrónica 144 pueden almacenarse datos relativos al producto como, por ejemplo, una fecha de caducidad 152 del producto 100. Además, pueden almacenarse también informaciones ambientales relevantes para el producto en la memoria electrónica 144, como, por ejemplo, valores de temperatura 154. Los valores de temperatura pueden detectarse con ayuda de un sensor de temperatura 156 del transpondedor 104 a intervalos temporales regulares o irregulares durante el transporte y/o el almacenamiento del producto 100 y archivarse en la memoria 144 según su transcurso temporal. Eso es especialmente relevante cuando el producto 100 es un bien perecedero, como, por ejemplo, un alimento o un medicamento, que deba refrigerarse continuamente.

Para comprobar la autenticidad del producto 100 se procede, por ejemplo, de la siguiente manera: En primer lugar, como en las formas de realización de las figuras 1 y 2, se detecta un identificador de la etiqueta 102 y se le introduce por medio de la interfaz 116 en el aparato de lectura 106. El aparato de lectura 106 lee en la tarjeta inteligente 132 la clave maestra 136 por medio de la interfaz 134 de tarjeta inteligente y genera un código simétrico a partir de la clave maestra 136 y el identificador. Gracias a la ejecución de las instrucciones de programa 120 se genera un comando de acceso 124 y se le codifica con ayuda del código simétrico por medio de la componente criptográfica 128.

Para autentificar el transpondedor 104 por medio de un procedimiento de reto-respuesta sobre la base del par de códigos asimétricos 146, 148, el aparato de lectura 106 puede generar además un número aleatorio y codificar éste con ayuda del código público 146. El código público 146 puede almacenarse en el aparato de lectura 106. Alternativamente, el aparato de lectura 106, por medio de su interfaz de red 138, puede interrogar al código público 146 del servidor de registro 142, para lo cual dirige al servidor de registro 142 una solicitud de banco de datos 158 con, por ejemplo, la indicación del fabricante del producto 100.

El número aleatorio codificado con el código público 146 se transmite al transpondedor 104 como parte del comando de acceso tras la codificación simétrica del comando de acceso como señal 124. Con ayuda del valor de referencia 114 y la componente criptográfica 130 se cancela allí la codificación simétrica del comando de acceso. El número aleatorio del comando de acceso codificado con el código público 146 se descodifica con ayuda del código privado 148.

El transpondedor 104 transmite entonces la señal 126 al aparato de lectura 106 como respuesta a la señal 124, transmitiéndose el número aleatorio descodificado junto con la señal 126. Asimismo, la señal 126 puede codificarse, preferiblemente con ayuda del mismo código simétrico con el que se ha codificado el comando de acceso de la señal 124.

El aparato de lectura 106 compara entonces el número aleatorio originariamente generado con el número aleatorio recibido del transpondedor 104. Si coinciden ambos números aleatorios, el transpondedor 104 se considera entonces como auténtico. Además, el aparato de lectura 106 se considera entonces también como autorizado para el acceso al transpondedor 104, dado que, en caso contrario, habría fallado la descodificación con ayuda del valor de referencia 114 por medio de la componente criptográfica 130, de modo que la señal 126 no habría podido transmitirse.

El aparato de lectura 106 puede emitir por medio de su unidad de visualización 122 un mensaje según el cual el producto es auténtico.

Para una fiabilidad todavía más elevada de la comprobación de la autenticidad puede procederse además de la siguiente manera: Tras la autorización del aparato de lectura y de la autentificación del transpondedor 104, el aparato de lectura 106 envía otro comando de acceso al transpondedor 104 para leer el valor de referencia 114 y su firma 150. La comunicación correspondiente entre el aparato de lectura 106 y el transpondedor 104 puede realizarse nuevamente de forma protegida con ayuda de una codificación simétrica.

El aparato de lectura 106 comprueba entonces la firma 150. Sólo cuando la comprobación de la firma 150 es exitosa y después de que se hayan producido tanto la autorización del aparato de lectura como la autentificación del transpondedor 104, el aparato de lectura 106 emite hacia la unidad de visualización 122, en esta forma de realización un mensaje según el cual el producto 100 es auténtico.

Alternativamente, la autentificación del transpondedor 104 puede realizarse también frente a la tarjeta inteligente 132, por ejemplo con un denominado procedimiento de verificación tarjeta a tarjeta. Además, puede preverse también que la autentificación sea mutua, es decir que se deba autentificar también el aparato de lectura 106 o la tarjeta inteligente 132 frente al transpondedor 104, lo que de nuevo puede realizarse con la asistencia de un procedimiento de reto-respuesta y con ayuda de un código asimétrico o simétrico.

Solamente después de que se termine con éxito la comprobación de la autenticidad del producto, el aparato de lectura 106 puede dirigir un comando de acceso adicional al transpondedor 104 para leer en la memoria 144 la fecha de caducidad 152 y/o los valores de temperatura 154. Estos se evalúan entonces por las instrucciones de programa

120 y/o se emiten por medio de la unidad de visualización 122. De esta forma, puede comprobarse si el producto 100 es aún utilizable.

La figura 5 muestra un diagrama de flujo correspondiente. En el paso 300 se detecta el identificador de manera correspondiente al paso 200 de la forma de realización de la figura 3 y se le introduce en el aparato de lectura. En el paso 302 se realiza la autorización del aparato de lectura con ayuda del identificador frente a la etiqueta RFID. Esto puede realizarse directamente utilizando el identificador como código simétrico o con ayuda de un código simétrico generado a partir del identificador y una clave maestra y que corresponde al valor de referencia almacenado en la etiqueta RFID.

En el paso 304 se autentifica la etiqueta RFID frente al aparato de lectura o la tarjeta inteligente asociada al aparato de lectura, por ejemplo con ayuda de un procedimiento de reto-respuesta. Opcionalmente, en el paso 306 se autentifica también el aparato de lectura o la tarjeta inteligente frente a la etiqueta RFID. Además, puede realizarse una comprobación de firma en el paso 308, para lo cual el aparato de lectura, tras su autorización, accede a la etiqueta RFID y obtiene de allí la firma del valor de referencia.

En el paso 310 se realiza una comprobación de coincidencia del identificador, es decir, de la ID del producto, con el valor de referencia leído por el aparato de lectura en la etiqueta RFID. Cuando existe una coincidencia, entonces en el paso 312 se emite desde el aparato de lectura una señal, según la cual el producto es auténtico. A continuación, por medio del aparato de lectura, pueden leerse, procesarse o visualizarse datos de producto adicionales e informaciones ambientales relevantes para el producto contenidos en la etiqueta RFID.

En caso de que la comprobación en el paso 310 no proporcione ninguna coincidencia, el producto no es auténtico, lo que puede señalizarse por medio de la emisión de una señal correspondiente por el aparato de lectura (paso 316).

Lista de símbolos de referencia

100	Producto
102	Etiqueta
104	Transpondedor
106	Aparato de lectura
108	Interfaz de radio
110	Interfaz de radio
112	Circuito de mando lógico
114	Valor de referencia
116	Interfaz
118	Procesador
120	Instrucciones de programa
122	Unidad de visualización
124	Señal
126	Señal
128	Componente criptográfica
130	Componente criptográfica
132	Tarjeta inteligente
134	Interfaz de tarjeta inteligente
136	Clave maestra
138	Interfaz de red
140	Red

142 Servidor de registro

144 Memoria electrónica

146 Código público

148 Código privado

150 Firma

152 Fecha de caducidad

154 Valores de temperatura

156 Sensor de temperatura

REIVINDICACIONES

1. Procedimiento para comprobar la autenticidad de un producto (100) a fin de protegerlo contra la piratería de productos, que comprende los siguientes pasos:

- detección de un identificador asociado al producto,

- introducción del identificador en un aparato de lectura (106), en donde el aparato de lectura presenta una interfaz (110) para comunicación por radio con una unidad de emisión-recepción (104) asociada al producto, y en donde en la unidad de emisión-recepción está almacenado un valor de referencia (114) con respecto al identificador,

- autorización del aparato de lectura para acceder a la unidad de emisión-recepción, en donde la autorización frente a la unidad de emisión-recepción se realiza con ayuda del identificador por medio de la interfaz (110),

en el que el producto se considera como auténtico cuando el identificador coincide con el valor de referencia,

en el que la detección del identificador se realiza con ayuda de un sensor óptico (116),

en el que el aparato de lectura, para su autorización frente a la unidad de emisión-recepción, envía el identificador a la unidad de emisión-recepción por medio de la interfaz (110) y la unidad de emisión-recepción comprueba el identificador con ayuda del valor de referencia, y en el que, en caso de coincidencia del identificador con el valor de referencia, el aparato de lectura se considera como autorizado, de modo que la unidad de emisión-recepción señaliza a continuación la autenticidad del producto frente al aparato de lectura, y en el que la unidad de emisión-recepción, en caso contrario, no emite ninguna señal.

2. Procedimiento según la reivindicación 1, en el que el aparato de lectura, para su autorización

- frente a la unidad de emisión-recepción, envía el identificador a la unidad de emisión-recepción por medio de la interfaz (110) y la unidad de emisión-recepción comprueba el identificador con ayuda del valor de referencia, y en donde, en caso de coincidencia del identificador con el valor de referencia, el aparato de lectura se considera como autorizado, de modo que la unidad de emisión-recepción señaliza a continuación la autenticidad del producto frente al aparato de lectura, y/o

- envía un comando de acceso a la unidad de emisión-recepción por medio de la interfaz (110), en donde el comando de acceso se codifica con ayuda del identificador, y en donde la autorización se realiza cuando el comando de acceso codificado puede descodificarse por la unidad de emisión-recepción con ayuda del valor de referencia,

en el que, tras la autorización del aparato de lectura, la unidad de emisión-recepción transmite el valor de referencia (114) al aparato de lectura, en el que se comprueba el identificador con ayuda del valor de referencia.

3. Procedimiento según la reivindicación 1 o 2, en el que, tras la constatación de la autenticidad del producto, se lean por el aparato de lectura datos (152, 154) relativos al producto en una memoria (144) de la unidad de emisión-recepción, en donde los datos relativos al producto contienen datos ambientales (154) relevantes para el producto y en donde los datos ambientales relevantes para el producto contienen datos de temperatura que se han detectado con ayuda de un sensor (156) y se han almacenado en la memoria de la unidad de emisión-recepción.

4. Procedimiento según cualquiera de las reivindicaciones anteriores, en el que el producto es un envase, un bien de consumo o un bien de inversión, en particular una prenda de ropa, un alimento, un aparato electrónico, un componente de máquina, una pieza de repuesto, un vehículo o componente de vehículo, un medicamento o una botella de bebida.

5. Sistema para comprobar la autenticidad de un producto (100) a fin de protegerlo contra la piratería, que comprende:

- un característica de identificación (102) asociada al producto o asociable por personalización, en la que puede ser detectado un identificador,

- una unidad de emisión-recepción (104) que está configurada para la comunicación por radio con un aparato de lectura (106), en donde en la unidad de emisión-recepción está almacenado o puede almacenarse un valor de referencia (114) con respecto al identificador, y en donde la unidad de emisión-recepción presenta medios (112, 130) para autorizar al aparato de lectura a acceder a la unidad de emisión-recepción, de modo que la comprobación de la autenticidad del producto con ayuda del identificador y del valor de referencia puede realizarse solamente después de la autorización,

en el que la unidad de emisión-recepción está configurada para la recepción del identificador proveniente del aparato de lectura, en el que el aparato de lectura se considera como autorizado cuando el identificador coincide con el valor de referencia, de modo que la unidad de emisión-recepción señaliza seguidamente la autenticidad del producto

frente al aparato de lectura, en el que la unidad de emisión-recepción, en caso contrario, no emite ninguna señal, y en el que el sistema comprende también un sensor óptico para detectar el identificador.

6. Sistema según la reivindicación 5, en el que la unidad de emisión-recepción está configurada para recibir del aparato de lectura un comando de acceso codificado con ayuda del identificador, considerándose el aparato de lectura como autorizado cuando la unidad de emisión-recepción pueda descodificar el comando de acceso con ayuda del valor de referencia.

7. Sistema según la reivindicación 6, en el que la unidad de emisión-recepción está configurada de modo que, tras la autorización del aparato de lectura, se transmite el valor de referencia al aparato de lectura, en el que se comprueba el identificador con ayuda del valor de referencia, de manera que el aparato de lectura señaliza la autenticidad del producto en caso de coincidencia del identificador con el valor de referencia.

8. Sistema según cualquiera de las reivindicaciones 5 a 7, en el que la unidad de emisión-recepción está configurada para realizar la operación de autentificación con ayuda de un procedimiento criptográfico frente al aparato de lectura o a una tarjeta inteligente (132) asociada al aparato de lectura.

9. Sistema según cualquiera de las reivindicaciones 5 a 8, en el que la unidad de emisión-recepción está configurada para transmitir una firma (150) del valor de referencia al aparato de lectura.

10. Sistema según cualquiera de las reivindicaciones 5 a 9, en el que la unidad de emisión-recepción presenta una memoria (144) para almacenar datos (152, 154) relativos al producto, y en el que la unidad de emisión-recepción está configurada para transmitir al aparato de lectura, tras su autorización, los datos relativos al producto.

11. Sistema según cualquiera de las reivindicaciones 5 a 11, en el que la unidad de emisión-recepción es un transpondedor, en particular un transpondedor RFID.

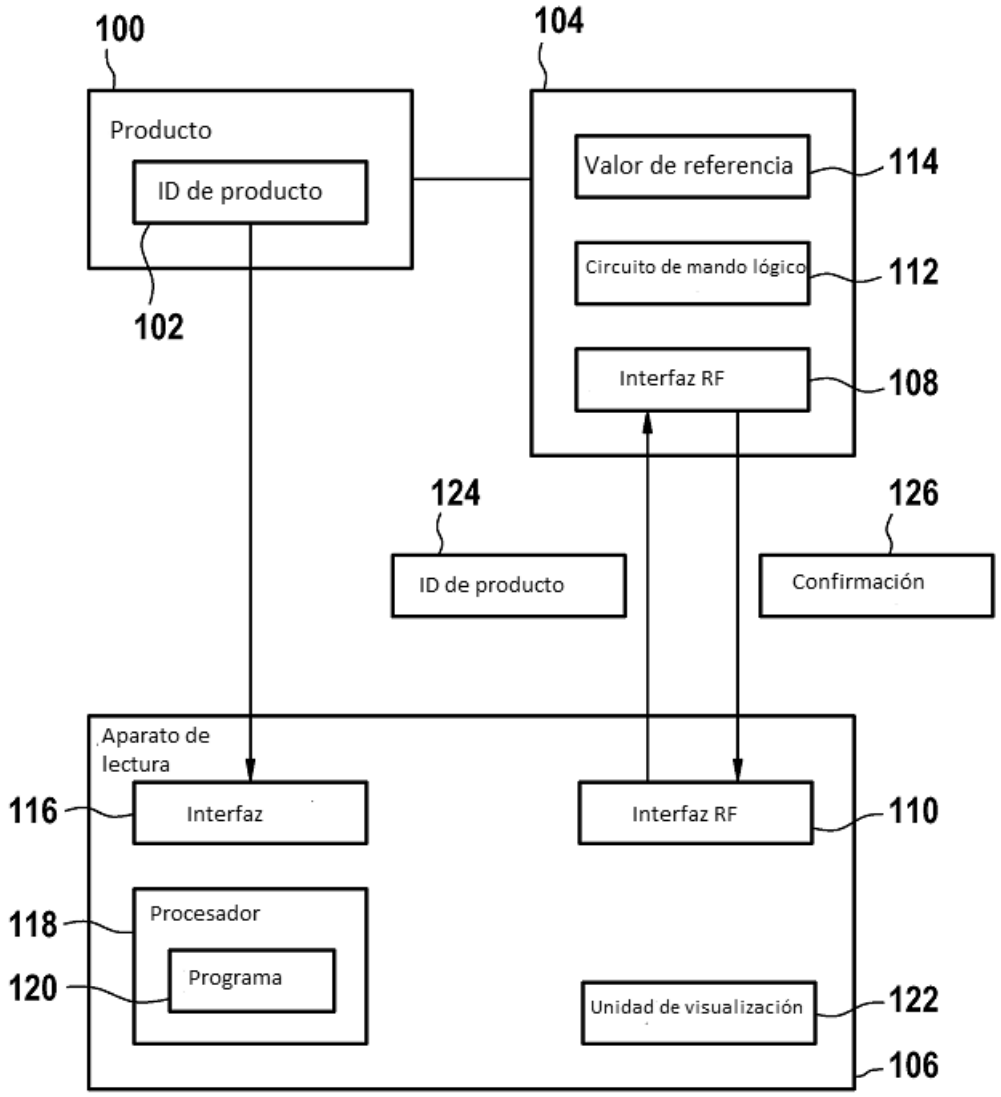
100
Producto
ID de producto
102
104
Valor de referencia
114
Circuito de mando lógico
112
Interfaz RF
108
124
ID de producto
126
Confirmación
Aparato de lectura
116
Interfaz
Interfaz RF
110
118
Procesador
120
Programa
Unidad de visualización
122
106

Fig. 1

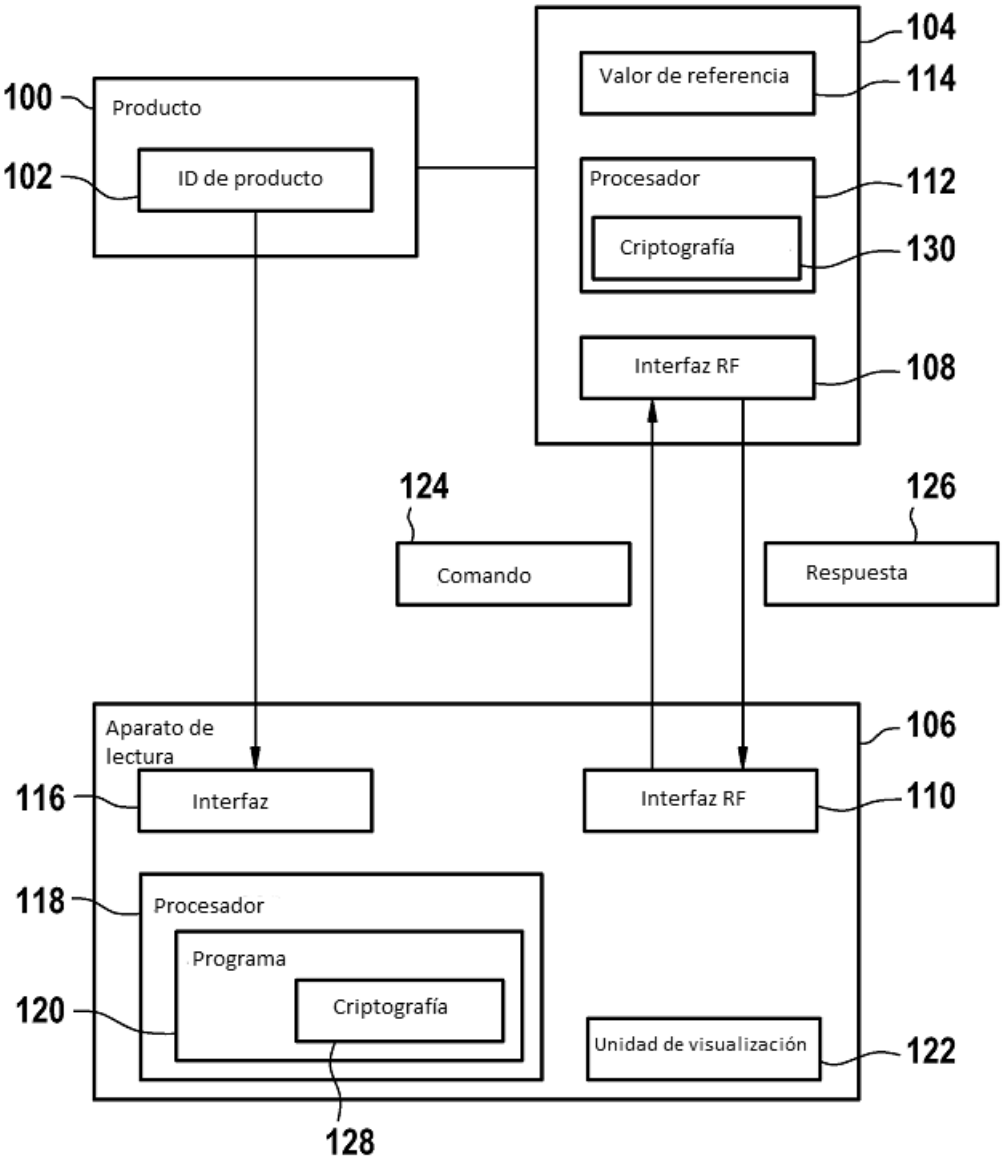
100
Producto
102
ID de producto
104
Valor de referencia
114
Procesador
112
Criptografía
130
Interfaz RF
108
124
Comando
126
Respuesta
Aparato de lectura
106
116
Interfaz
Interfaz RF
110
118
Procesador
Programa
120
Criptografía
Unidad de visualización
122
128

Fig. 2

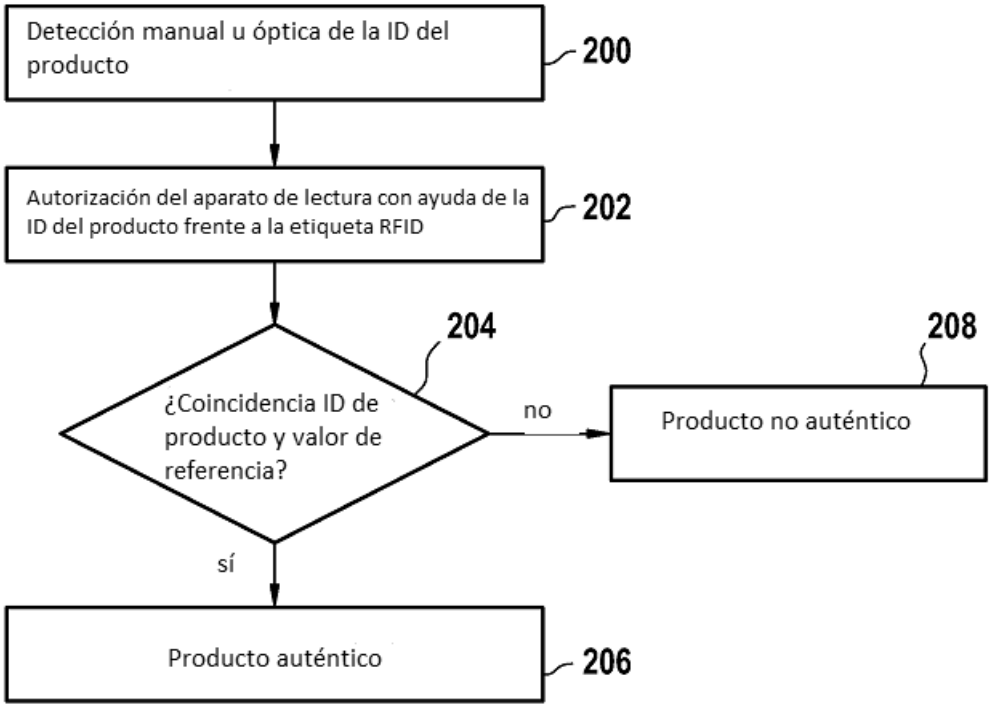
Detección manual u óptica de la ID del producto
200
Autorización del aparato de lectura con ayuda de la ID del producto frente a la etiqueta RFID
202
204
¿Coincidencia ID de producto y valor de referencia?
no
208
Producto no auténtico
sí
Producto auténtico
206

Fig. 3

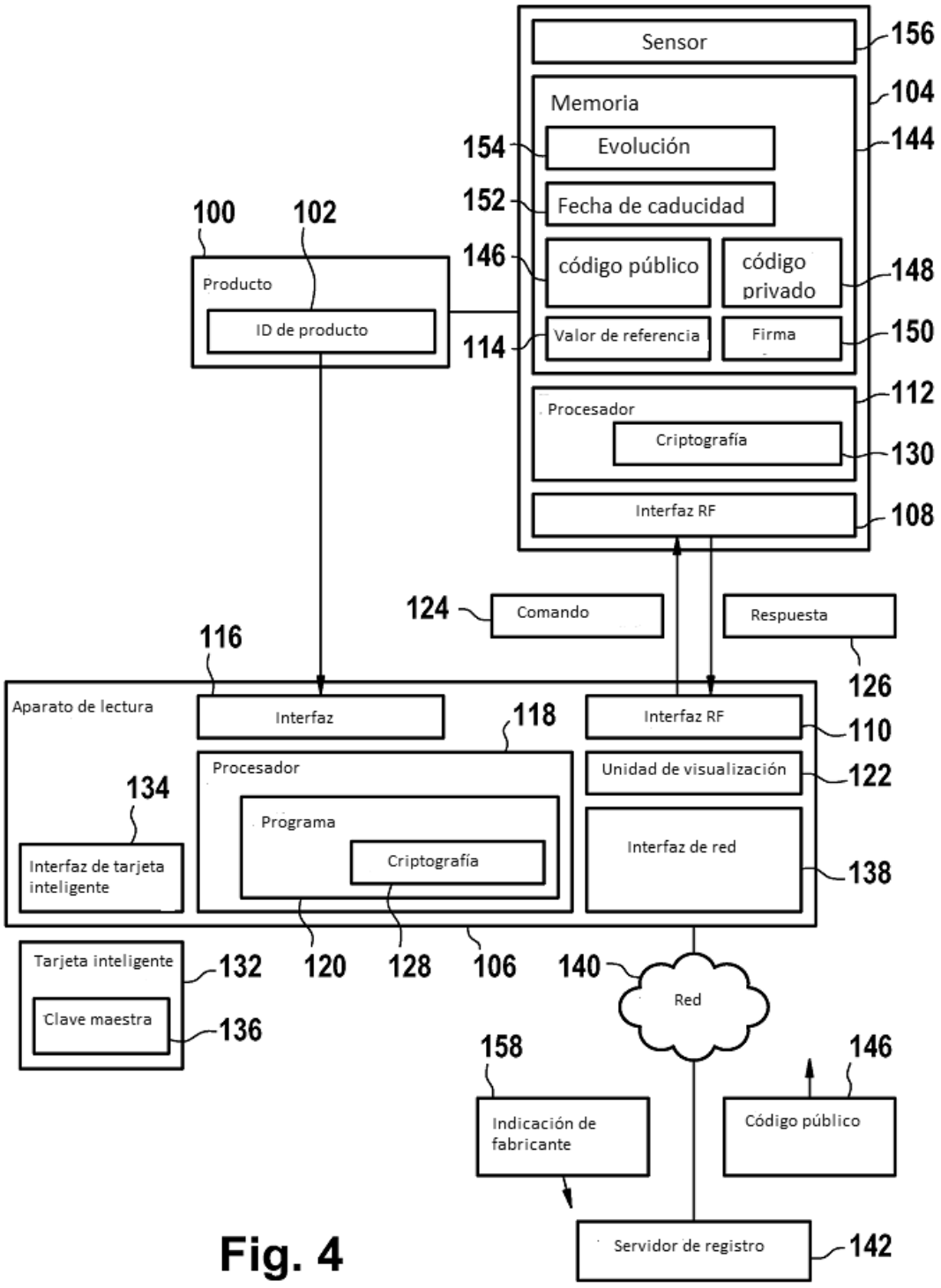
Sensor
156
Memoria
104
154
Evolución
144
152
Fecha de caducidad
100
102
146
código público
código privado
148
Producto
ID de producto
114
Valor de referencia
Firma
150
Procesador
112
Criptografía
130
Interfaz RF
108
124
Comando
Respuesta
126
116
Aparato de lectura
Interfaz
118
Interfaz RF
110
Procesador
Unidad de visualización
122
134
Programa
Interfaz de tarjeta inteligente
Criptografía
Interfaz de red
138
Tarjeta inteligente
132
120
128
106
140
Red
Clave maestra
136
158
146
Indicación de fabricante
Código público
Servidor de registro
142

Fig. 4

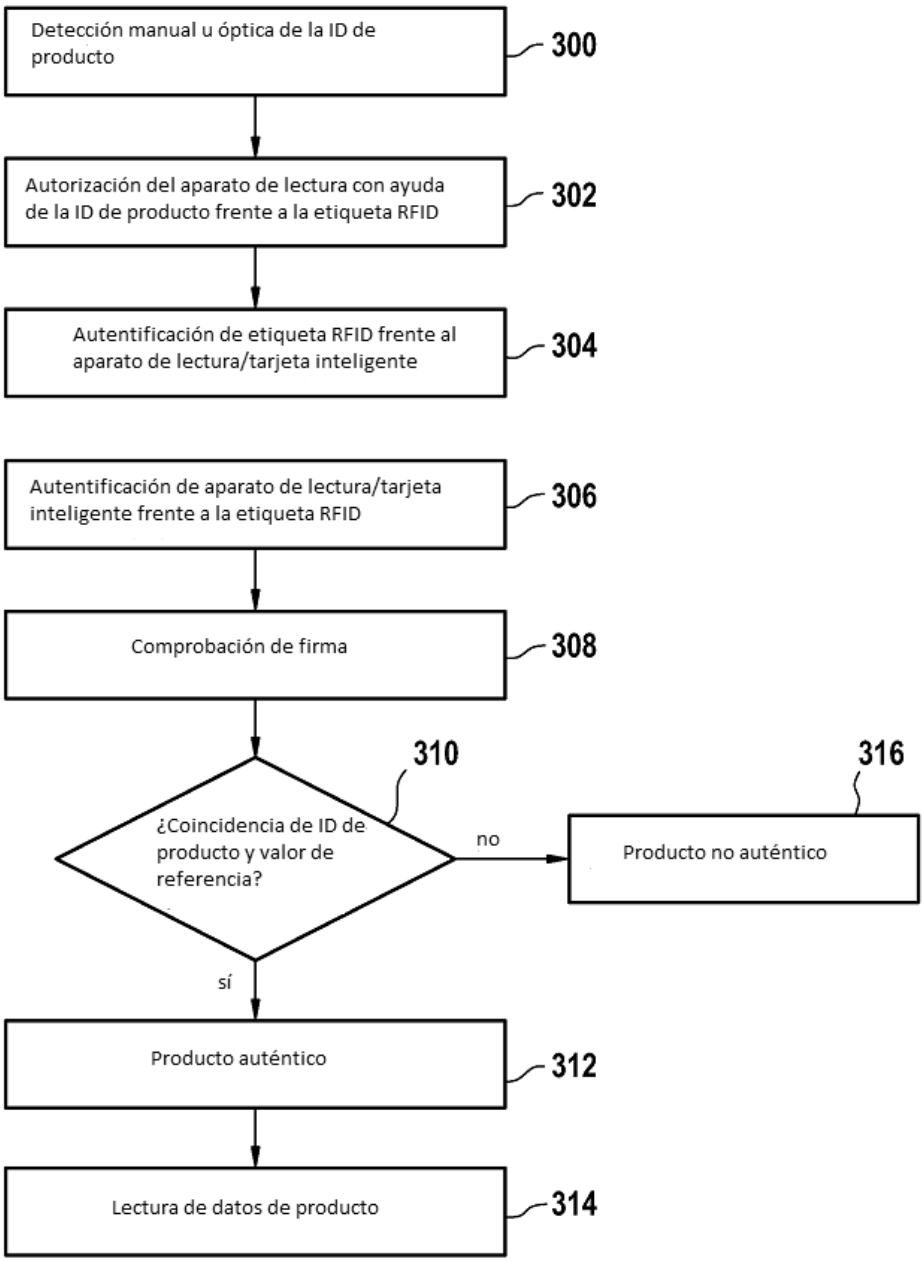
Detección manual u óptica de la ID de producto
300
Autorización del aparato de lectura con ayuda de la ID de producto frente a la etiqueta RFID
302
Autentificación de etiqueta RFID frente al aparato de lectura/tarjeta inteligente
304
Autentificación de aparato de lectura/tarjeta inteligente frente a la etiqueta RFID
306
Comprobación de firma
308
310
¿Coincidencia de ID de producto y valor de referencia?
no
316
Producto no auténtico
sí
Producto auténtico
312
Lectura de datos de producto
314

Fig. 5