(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 672 738**

(51) Int. CI.:

G06Q 10/00 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **15.04.2014 PCT/IB2014/060729**

(87) Fecha y número de publicación internacional: **15.10.2015 WO15155577**

(96) Fecha de presentación y número de la solicitud europea: **15.04.2014 E 14733316 (5)**

(97) Fecha y número de publicación de la concesión europea: **14.03.2018 EP 3129924**

(54) Título: **Sistema para comprobar la autenticidad de bienes de consumo, productos y objetos en general**

(30) Prioridad:

08.04.2014 IT PD20140096

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
15.06.2018

(73) Titular/es:

TOGNAZZO, GIORGIA (100.0%)
Via Vasco Rainer 6
35127 Padova, IT

(72) Inventor/es:

TOGNAZZO, GIORGIA

(74) Agente/Representante:

CONTRERAS PÉREZ, Yahel

ES 2 672 738 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Sistema para comprobar la autenticidad de bienes de consumo, productos y objetos en general.

Esta patente se refiere a sistemas informáticos para el control y la verificación de la autenticidad de productos y, en particular, a un nuevo sistema para el control y la verificación de la autenticidad de bienes de consumo, productos y objetos en general.

El fenómeno de los productos falsificados en general es bien conocido. Éste implica la producción de productos que son comercializados después bajo nombres falsos, respecto a, por ejemplo, el nombre de la marca, la calidad, el origen, los estándares aplicados, o similares.

Es bien conocido que la falsificación de productos provoca graves daños para las economías de todos los países productores, dado que se ponen en el mercado productos que no cumplen con las leyes aplicables, obstaculizando, en consecuencia, los mercados regulares con pérdidas de millones de euros y puestos de trabajo.

Algunos ejemplos de productos que se falsifican mucho son CDs y DVDs de audio y/o video, alimentos en general, ropa y accesorios de marca (camisas, suéteres, bolsos, abrigos, ropa interior, etc.), productos de cosmética (perfumes, etc.) y dispositivos y productos electrónicos, juguetes y productos para niños en general, gadgets y artículos promocionales para empresas (llaveros, insignias, bolígrafos, encendedores, etc.), gafas de sol, relojes, así como documentos tales como valores de diferentes tipos, incluidos billetes y documentos de identidad.

Se conoce, por lo tanto, la necesidad de crear sistemas que hagan posible la trazabilidad de cada elemento individual y la verificación de su autenticidad.

Existen actualmente diversos sistemas y dispositivos diseñados para controlar y verificar la trazabilidad de productos. Por ejemplo, existen etiquetas aplicadas al producto, adhesivas o sujetas mediante lazos o grapas, que muestran los datos del producto. Obviamente, estas etiquetas pueden falsificarse fácilmente.

Existen también etiquetas que contienen transpondedores o microchips o etiquetas RFID, que contienen información relacionada con el producto y comunican esa información a un dispositivo de lectura que los interroga emitiendo ondas de radio de baja frecuencia.

NFC (Near Field Communication) es una tecnología de comunicación entre dos dispositivos electrónicos donde la transmisión de datos se lleva a cabo simplemente acercando los dos dispositivos.

Esta tecnología también se utiliza para la transmisión de datos entre un dispositivo electrónico utilizado como lector y un transpondedor.

De manera similar a las etiquetas, incluso los transpondedores pueden ser falsificados, al igual que dispositivos electrónicos tales como teléfonos móviles o teléfonos inteligentes que utilizan los llamados sistemas operativos de "código abierto" que pueden vulnerarse fácilmente.

FR 2986357 describe un sistema conocido para identificar usuarios de un establecimiento que vende artículos ópticos, que comprende marcadores RFID conectados a las gafas y un lector RFID que detecta y lee los marcadores RFID y se comunica con un ordenador para acceder a una base de datos que contiene la información asociada a los marcadores RFID.

EP 2535850 describe un sistema conocido para zonas portuarias de carga que comprende más etiquetas RFID conectadas a objetos transportados por camiones industriales, y más lectores RFID colocados bajo tierra y que detectan las etiquetas RFID para comunicar a un ordenador la posición de los objetos en la zona portuaria de carga.

US 2009/0289775 describe un sistema conocido para identificar productos, que comprende unas etiquetas RFID conectadas a los artículos, un lector RFID que lee el código de las etiquetas RFID y se comunica con un terminal configurado para mostrar en una pantalla información almacenada en una base de datos y relativa a los artículos. US 2010/0127871 describe un sistema conocido para identificar productos enviados que comprende unas etiquetas RFID conectadas a los productos y un lector RFID que lee las etiquetas RFID y se comunica con un servidor que envía al lector RFID información de los productos.

US 2005/0064867 describe un sistema conocido para compartir información, que comprende una etiqueta RFID conectada a un cartel y un terminal móvil que lee la etiqueta RFID y se comunica con un servidor que envía la información del cartel a otro terminal móvil.

Los sistemas del tipo conocido descritos en las patentes mencionadas anteriormente FR 2986357, EP 2535850, US 2009/0289775, US 2010/0127871 y US 2005/0064867 no permiten verificar la autenticidad de un producto.

La solicitud de patente WO 2008/060242 describe un sistema conocido para protección de derechos de autor de software que comprende una etiqueta RFID conectada a un paquete de software y que contiene una clave de licencia. Además, el sistema comprende un lector RFID (integrado en la placa base del ordenador) que interroga a la etiqueta RFID para recibir la clave de licencia, para que el ordenador pueda extraer la información para instalar el software.

El sistema descrito en WO 2008/060242 no es intrínsecamente seguro, ya que, si un infractor obtiene la clave de licencia, éste puede reproducir ilegalmente el software sin posibilidad de verificar la autenticidad del producto.

Para superar los inconvenientes mencionados anteriormente, se ha diseñado y desarrollado un nuevo tipo de sistema para el control y la verificación de la autenticidad de bienes de consumo, productos y artículos en general.

El objetivo principal de la presente invención es posibilitar el control y la verificación de la autenticidad de cualquier tipo de producto, en tiempo real y por cualquier persona, ya que utiliza tecnología de fácil acceso.

El sistema también puede aplicarse para verificar un solo elemento.

Otro objetivo de la presente invención es garantizar la seguridad, haciendo que el sistema sea resistente a violaciones y copias.

Estos y otros fines, directos y complementarios, se consiguen mediante el nuevo sistema para el control y la verificación de la autenticidad de bienes de consumo, productos y artículos en general. El nuevo sistema utiliza NFC (Near Field Communication) y tecnología RFID, donde la transmisión de datos es bidireccional, es decir, hay un intercambio de datos desde el dispositivo a uno o más transpondedores, pero también desde esos uno o más transpondedores al dispositivo.

El nuevo sistema también incluye por lo menos un servidor de soporte para la aplicación en el dispositivo de lectura, es decir, por ejemplo, un teléfono móvil, para evitar violaciones del sistema.

La presente invención tiene las siguientes ventajas: compacto tamaño y grosor, alta flexibilidad, total impermeabilidad, bajos costes de producción, y facilidad de gestión, haciendo que la invención sea accesible para una amplia gama de usuarios, que pueden utilizarla para fines comerciales o personales y privados.

El nuevo sistema es particularmente eficaz cuando se aplica como un sistema de control para orden público que, durante controles de rutina en tiendas, mercadillos, aduanas, almacenes, etc., puede determinar la autenticidad del producto y toda la información sobre cumplimiento y origen, y en el que tales controles pueden realizarse de manera segura, en tiempo real, sin pérdida de tiempo.

El nuevo sistema es utilizado de manera efectiva y fácil por cualquier operador sin necesidad de preparación y entrenamiento especial ya que el operador debe utilizar un dispositivo de lectura, por ejemplo, un teléfono móvil, y no tiene que hacer nada más que colocar el dispositivo cerca del artículo/producto a examinar.

El resultado de la verificación, positiva o negativa, llega al dispositivo de lectura de manera automática y sin errores.

El nuevo sistema también se utiliza de manera efectiva por cualquier comprador o consumidor en el momento de la selección, compra o consumo del producto por medio de una aplicación de software instalada en el dispositivo o terminal electrónico en su posesión, tal como un teléfono inteligente, tableta, o similar. El sistema implica la instalación de un software especial para cada uno de los sistemas operativos utilizados actualmente, tales como "Android", "I-phone", etc.

De esta manera, cualquier consumidor o comprador puede verificar la autenticidad de un producto en cualquier momento, antes o después de la compra.

En sus partes principales, el nuevo sistema comprende:

- uno o más microchips operativos con un sistema de lectura RFID - NFC, adhesivo o no, de plástico o papel o material genéticamente compuesto, rígido o flexible, con varias medidas posibles, capaz de ejecutar programas o cálculos matemáticos, y que contiene por lo menos un código alfanumérico código, aplicándose, incorporándose o de otro modo conectándose este uno o más microchips a un producto a rastrear o a su envoltorio o embalaje;

- por lo menos un lector o dispositivo de lectura que contiene por lo menos un circuito de transmisión y recepción de datos;
- por lo menos un servidor central para la recepción, transmisión, procesamiento y almacenamiento de datos.

Este lector o dispositivo de lectura en particular se comunica preferiblemente a través de un módulo NFC y/o GSM y/o UMTS y/o Internet o similar. En la realización preferida, este lector, a su vez, comprende un dispositivo electrónico tal como un teléfono móvil, teléfono inteligente o tableta, equipado con un dispositivo NFC y por lo menos una aplicación de software dedicada o "*App*".

Esta aplicación de software o "*App*" puede descargarse preferiblemente desde un sitio web autorizado por uno o más productores de artículos/productos a verificar. Esto impide el uso de software no genuino, es decir, copias falsas realizadas por falsificadores, lo que garantiza la certeza de las certificaciones, y en el que la aplicación de software contiene en la misma todos los parámetros correctos y autorizados para conectarse a ese servidor sin posibilidad de ser vistos por terceros no autorizados.

Este software también puede instalarse en el lector a través de una conexión por cable directa a un terminal que contiene el software de aplicación autorizado, encontrándose este terminal, por ejemplo, dentro de la tienda oficial y certificada en la que se encuentra el producto/artículo.

Este microchip se produce por medio de un sistema de producción de circuitos integrados, o puede conectarse o integrarse en el producto.

A continuación, se da una descripción del funcionamiento del nuevo sistema.

El microchip FC-RFID, tal como se ha mencionado, insertado o aplicado al producto a rastrear y colocado en el mismo es un programa para generar un código de identificación alfanumérico único.

Cuando el lector o dispositivo de lectura electrónica, tal como un teléfono móvil con el software de aplicación habilitado, consulta el microchip mediante tecnología NFC, el microchip envía un código de identificación único, que podría ser, por ejemplo, de 64 o 128 bits.

El dispositivo de lectura, lector, teléfono móvil o similar recibe el código de identificación único y lo envía al servidor FTP a través de una conexión a una red local o global (Internet) o comunicación GSM o similar.

El servidor FTP, equipado con un sistema de control de cálculo y alfanumérico, recibe el código de identificación único, lo procesa con uno o más algoritmos específicos que generan un nuevo código, o código de retorno, el cual se envía después al dispositivo de lectura.

El dispositivo de lectura, a su vez, lo envía al microchip aplicado al producto a rastrear a través de comunicación NFC.

El microchip reconstruye el (los) algoritmo(s) para procesar el código de retorno e información del servidor, y devuelve un código final de éxito con la respuesta al dispositivo. De lo contrario, si el código de retorno recibido desde el servidor no se considera válido, el microchip envía un código final de fallo con la respuesta al dispositivo de lectura.

Este código de retorno sólo puede ser reconocido por el microchip que generó el código de identificación único inicial, ya que está vinculado al mismo a través del sistema de algoritmos.

Este intercambio de códigos ocurre en tiempo real.

El microchip de tecnología NFC - RFID está equipado, de este modo, con un sistema de comunicación bidireccional, que posibilita la transmisión y recepción de datos y la capacidad para computar y/o ejecutar el software dedicado. El microchip también es legible por medio de tecnología NFC que, en combinación con el sistema de control de código comprobado, hace que el sistema sea seguro.

El dispositivo de lectura y la aplicación de software no conocen los algoritmos, lo que evita el riesgo de una violación del sistema de información del dispositivo. De hecho, los teléfonos inteligentes generalmente utilizan sistemas operativos "Android" que están sometidos fácilmente a ataques externos que podrían copiar estos algoritmos.

Con el fin de limitar todavía más el riesgo de una violación del sistema, puede añadirse también una etapa de transmisión de datos adicional entre el microchip aplicado al artículo y el servidor.

Para impedir vulneraciones del algoritmo contenido en el servidor, el servidor, a su vez, está conectado a una tarjeta protegida externa de manera que el dispositivo de lectura y el servidor funcionan esencialmente como transceptores de datos entre el microchip NFC-RFID y la tarjeta de procesamiento conectada al servidor.

Este sistema puede ser utilizado, por lo tanto, por cualquier persona que esté en posesión de un dispositivo electrónico con tecnología NFC y con el software de aplicación instalado y habilitado. Además, este sistema permite a las autoridades verificar rápidamente los productos en cualquier momento y en cualquier lugar.

En otra realización, particularmente útil para su uso por parte de fuerzas del orden público o personal dedicado a la verificación de productos, el lector y el servidor están conectados por cable e incluso integrados en un único dispositivo, tal como un ordenador portátil.

El desarrollo del software del microchip y/o el servidor puede incluir el historial del producto tal como, por ejemplo, datos relacionados con su producción, trazabilidad, estado de importación, etc.

Por ejemplo, los datos introducidos en el microchip en el momento de la producción pueden enviarse y almacenarse en el servidor el cual, a su vez, divide los productos por lotes de producción, fecha de producción, país de producción, y los datos que identifican el producto en sí, lo que permite un mejor seguimiento.

El lector o dispositivo de lectura incluye, además de la tecnología NFC, incluso una tarjeta SFM para transmisión de datos a través de SMS y/o a través de una conexión de INTERNET o similar (UMTS, GSM, GPRS, etc.).

El servidor puede estar ubicado en cualquier lugar, pero preferiblemente en un centro designado con un soporte técnico apropiado.

Los dibujos adjuntos, figuras 1 y 2, muestran, a modo de ejemplo no limitativo, el funcionamiento del nuevo sistema.

El nuevo sistema comprende por lo menos un microchip (1), con un sistema de lectura RFID - NFC aplicado a un producto (10) cuya autenticidad debe comprobarse. El microchip (1) contiene un código de identificación único (11), por ejemplo, un código alfanumérico de 64 o 128 bits.

En el ejemplo de la figura 1, el sistema también comprende por lo menos un lector o dispositivo de lectura (2), que puede ser, por ejemplo, un dispositivo de lectura dedicado o un teléfono inteligente, tableta u otro dispositivo electrónico normal que, a su vez, funcione con tecnología NFC y pueda comunicarse con tecnología GSM, UMTS o GPRS, o mediante conexión a una red local o global (Internet). Este dispositivo de lectura (2) también comprende preferiblemente por lo menos una tarjeta SIM de identificación.

En el dispositivo de lectura hay instalada por lo menos una aplicación de software dedicada o "*App*" que permite un funcionamiento del sistema sin problemas.

El nuevo sistema también incluye por lo menos un servidor FTP centralizado (3) para la recepción, transmisión, procesamiento, y almacenamiento de datos.

Para verificar la autenticidad del producto (10), el usuario debe acercar el dispositivo de lectura (2) al microchip (1), es decir, cerca del producto (10) sobre el que está aplicado el microchip, y debe activar la aplicación de software instalada en el dispositivo de lectura (2).

El microchip (1) es interrogado (21) entonces y, como respuesta, envía el código de identificación (11) al dispositivo de lectura (2).

El dispositivo de lectura (2) recibe el código de identificación único (11) y lo envía, a través de una conexión a una red local o global (Internet), o comunicación GSM o similar, al servidor FTP (3).

El servidor FTP (3), equipado con un sistema de control alfanumérico, recibe el código de identificación único (11), lo procesa con uno o más algoritmos específicos que generan un nuevo código, o código de retorno (31), el cual se envía al dispositivo de lectura (2).

El dispositivo de lectura (2), a su vez, a través de comunicación NFC, lo envía al microchip (1) aplicado en el producto a rastrear (10).

El microchip (1) reconstruye el (los) algoritmo(s) para reconocer el código de retorno (31) y el servidor (3) y, si es reconocido, envía un código final de éxito o fallo (12) al dispositivo de lectura (2).

El código final (12) aparece, por ejemplo, en una pantalla (21) del dispositivo de lectura (2) o se emite un pitido o mensaje de voz. Por el contrario, en el ejemplo de la figura 2, el dispositivo de lectura (2) y el servidor (3) están conectados entre sí por cable o incluso integrados en un único dispositivo, tal como un ordenador portátil. Esta solución es particularmente útil porque permite utilizar el dispositivo de lectura (2) eficazmente incluso en ausencia de cobertura de red, ya sea por cable o inalámbrica, dado que está conectado directamente al servidor (3) para el procesamiento de los códigos. Estas especificaciones, son suficientes para que la persona experta realice y utilice la invención y, por consiguiente, en la aplicación práctica puede haber variaciones sin perjuicio del contenido del concepto innovador.

Por lo tanto, con referencia a la descripción anterior y a los dibujos adjuntos, se adjuntan las siguientes reivindicaciones.

REIVINDICACIONES

1. Sistema para el control y la verificación de la autenticidad de bienes de consumo, productos y artículos en general (10), que comprende por lo menos un microchip (1) con tecnología de comunicación NFC, adecuado para ser aplicado a un artículo/producto/embalaje (10), teniendo dicho microchip (1) la capacidad de ejecutar software y conteniendo por lo menos un código de identificación (11), y por lo menos un dispositivo de lectura (2), adecuado para comunicarse con dicho microchip (1), por lo menos un servidor (3) para el procesamiento, comunicación y almacenamiento de datos y en el que dicho dispositivo de lectura (2) es adecuado para intercambiar uno o más códigos de identificación (11, 31) en ambas direcciones entre dicho microchip (1) y dicho servidor (3), en el que dicho microchip (1) implementa el control de dichos códigos (11, 31) y envía un código final de identificación (12) a dicho dispositivo de lectura (2) relativo a la identificación exitosa o fallida, y en el que:

- dicho microchip (1) está destinado a ser aplicado a dicho artículo/producto/embalaje (10) para ser comprobado durante la producción del propio artículo/producto/embalaje (1);
- dicho dispositivo de lectura (2) es adecuado para interrogar a dicho microchip (1) que, como respuesta, envía por lo menos dicho código de identificación (11);
- dicho dispositivo de lectura (2) es adecuado para enviar dicho código de identificación (11) a dicho servidor (3);
- dicho servidor (3) es adecuado para procesar dicho código de identificación (11) recibido por dicho dispositivo de lectura (2) por medio de uno o más algoritmos dedicados, generando un código de retorno (31), que lo envía a dicho dispositivo de lectura (2);
- dicho dispositivo de lectura (2) es adecuado para enviar dicho código de retorno (31) recibido desde dicho servidor (3) a dicho microchip (1); caracterizado por el hecho de que

  - dicho microchip (1) es adecuado para procesar dicho código de retorno (31) recibido desde dicho dispositivo de lectura (2) con uno o más algoritmos y enviar una respuesta de reconocimiento o no reconocimiento a dicho dispositivo de lectura (2);
  siendo reconocido el código de retorno (31) solamente por dicho microchip (1) que generó el código de identificación único inicial (11), estando vinculado el código de retorno (31) al código de identificación (11) a través del sistema de algoritmos.

2. Sistema de acuerdo con la reivindicación 1, caracterizado por el hecho de que dicho lector (2) está asociado a un teléfono móvil, teléfono inteligente, tableta u otro dispositivo electrónico con tecnología NFC que comprende por lo menos un circuito de recepción y transmisión de datos por medio de por lo menos un módulo NFC y/o GSM y/o UMTS y/o Internet o similar, con el cual se comunica con dicho servidor (3).

3. Sistema de acuerdo con la reivindicación 1, caracterizado por el hecho de dicho lector (2) está conectado por cable o de manera inalámbrica a dicho servidor (3).

4. Sistema de acuerdo con la reivindicación 3, caracterizado por el hecho de dicho lector (2) y dicho servidor (3) están integrados en un único dispositivo, ya sea portátil o no portátil.

5. Sistema de acuerdo con cualquiera de las reivindicaciones anteriores, caracterizado por el hecho de que dicho microchip (1) reconstruye el (los) algoritmo(s) para reconocer dicho código de retorno (31) y dicho servidor (3), y cuando se reconoce, envía un código final (12) de nuevo a dicho dispositivo de lectura (2) comunicando el reconocimiento con éxito o fallo del artículo en cuestión.

6. Sistema de acuerdo con cualquiera de las reivindicaciones anteriores, caracterizado por el hecho de que dicho dispositivo de lectura (2) comprende por lo menos una aplicación de software dedicado o "*App*" para la transmisión de datos desde/hacia dicho microchip (1) y desde/hacia dicho servidor (3), el que dicha aplicación de software se instala en dicho dispositivo de lectura (2) a través de una conexión por cable o inalámbrica a un terminal autorizado local o remoto.

7. Sistema de acuerdo con cualquiera de las reivindicaciones anteriores, caracterizado por el hecho de que dicho servidor (3) es de tipo FTP centralizado para la recepción, transmisión, procesamiento y almacenamiento de datos.

8. Sistema de acuerdo con cualquiera de las reivindicaciones anteriores, caracterizado por el hecho de que dicho intercambio de códigos (11, 31, 12) se produce en tiempo real.

9. Sistema de acuerdo con cualquiera de las reivindicaciones anteriores, caracterizado por el hecho de que dicho microchip (1) y dicho servidor (3) son adecuados cada uno para transmitir mutuamente dos o más de dichos códigos (11, 31) por medio de dicho dispositivo de lectura (2).

10. Sistema de acuerdo con cualquiera de las reivindicaciones anteriores, caracterizado por el hecho de que comprende una tarjeta protegida externa conectada a dicho servidor (3), y en el que dicho servidor (3) transmite dichos códigos (11) recibidos desde dicho dispositivo de lectura (2), y en el que dicha tarjeta es adecuada para generar dicho código de retorno (31) que envía a dicho servidor (3)

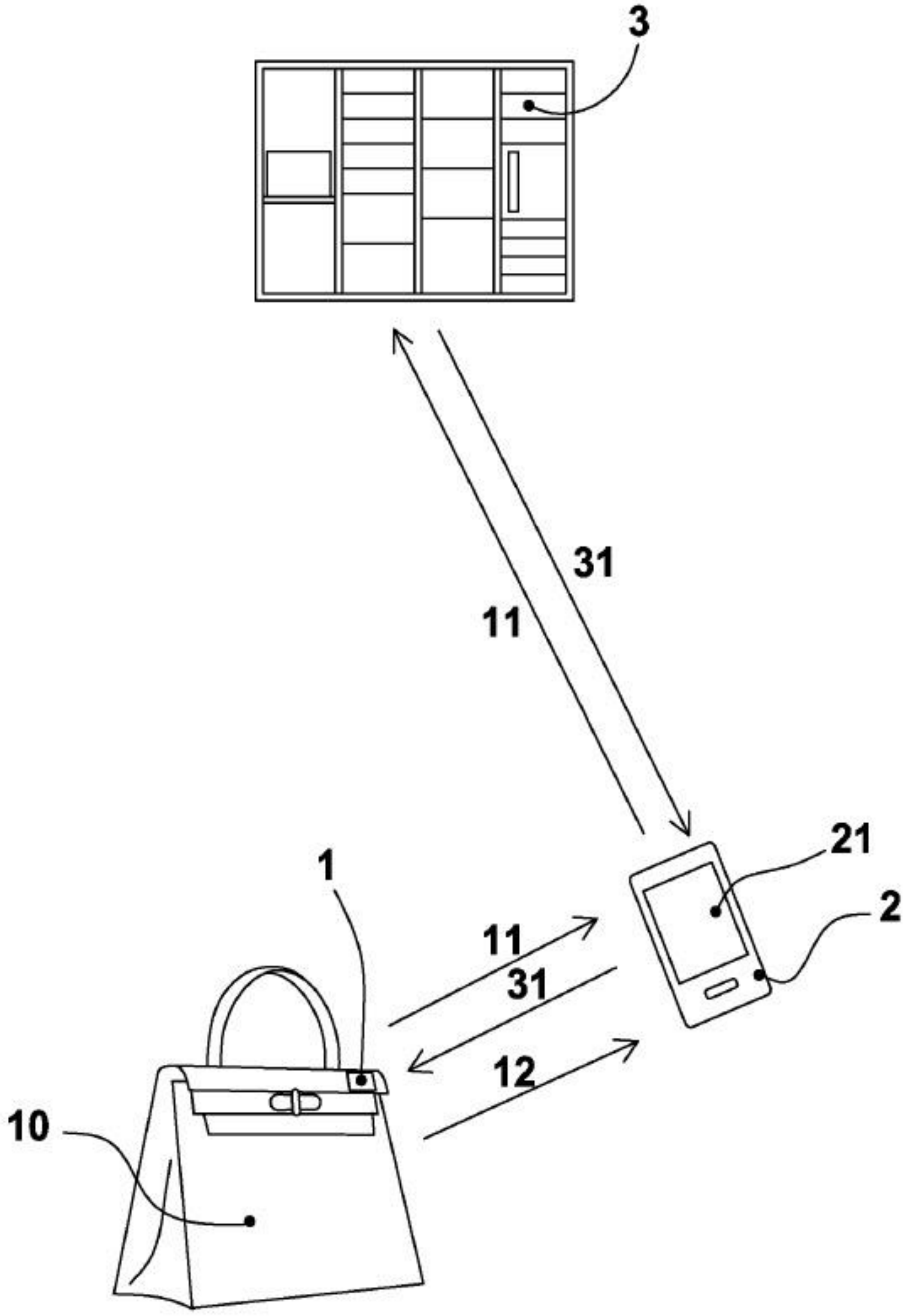

Fig. 1

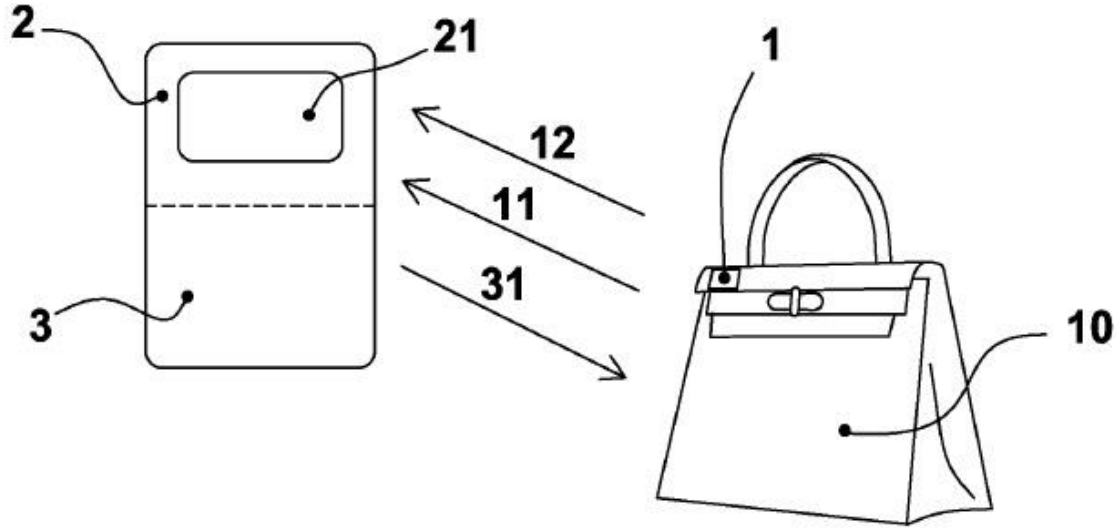

Fig. 2

REFERENCIAS CITADAS EN LA DESCRIPCIÓN

Esta lista de referencias citadas por el solicitante es únicamente para la comodidad del lector. No forma parte del documento de la patente europea. A pesar del cuidado tenido en la recopilación de las referencias, no se pueden excluir errores u omisiones y la EPO niega toda responsabilidad en este sentido.

Documentos de patentes citados en la descripción

- FR 2986357 **[0011] [0015]**
- EP 2535850 A **[0012] [0015]**
- US 20090289775 A **[0013] [0015]**
- US 20100127871 A **[0013] [0015]**
- US 20050064867 A **[0014] [0015]**
- WO 2008060242 A **[0016] [0017]**