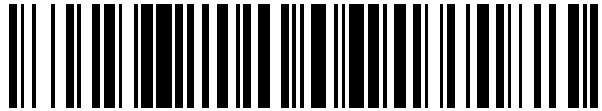


19



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 559 851**

21 Número de solicitud: 201530982

51 Int. Cl.:

**G06F 21/62** (2013.01)

**H04W 12/02** (2009.01)

12

PATENTE DE INVENCION

B1

22 Fecha de presentación:

**08.07.2015**

43 Fecha de publicación de la solicitud:

**16.02.2016**

Fecha de la concesión:

**16.11.2016**

45 Fecha de publicación de la concesión:

**23.11.2016**

73 Titular/es:

**UNIVERSITAT DE LES ILLES BALEARS (100.0%)**

**Cra. de Valldemossa, km 7.5**

**07122 Palma de Mallorca (Illes Balears) ES**

72 Inventor/es:

**ALORDA LADARIA, Bartomeu y**

**MAS YNAREJOS, Francisco**

74 Agente/Representante:

**CARVAJAL Y URQUIJO, Isabel**

54 Título: **Método y sistema de obtención de información sensible mediante dispositivo móvil**

57 Resumen:

Método de obtención de información sensible mediante dispositivo móvil, que comprende:

- capturar (302), utilizando una cámara de un dispositivo móvil (12), un código bidimensional (9) que contiene información pública (104) sin encriptar e información sensible encriptada (108) mediante una clave simétrica, donde dichos datos están ordenados según una determinada estructura interna;
- obtener la información binaria (304) del código bidimensional (9);
- obtener, a partir de dicha información binaria (304) y conociendo la estructura interna de los datos, la información pública (104) del código bidimensional (9); y
- realizar una descriptación simétrica (308) de la parte de la información binaria (304) que corresponde a la información sensible encriptada (108), obteniendo la información sensible (106).

La invención también se refiere a un producto de programa para ejecutar el método anterior, un dispositivo móvil para obtención de información sensible y un método de generación de código bidimensional con información sensible para su lectura mediante dispositivo móvil.

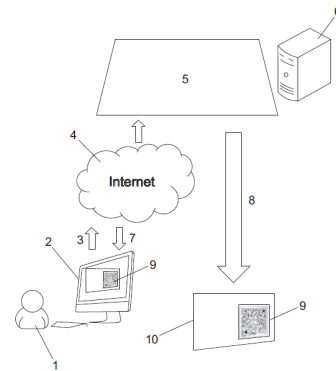


Fig. 1

ES 2 559 851 B1

**MÉTODO Y SISTEMA DE OBTENCIÓN DE INFORMACIÓN SENSIBLE MEDIANTE  
DISPOSITIVO MÓVIL**

**DESCRIPCIÓN**

5 Campo de la invención  
La presente invención se engloba dentro del campo de los sistemas de protección de datos sensibles y la ocultación de información solo disponible para lectores autorizados.

10 Antecedentes de la invención  
En la actualidad los dispositivos móviles equipados con cámara fotográfica son de uso generalizado y permiten la realización de servicios de alto valor añadido en la mayoría de los casos apoyándose en la conectividad de datos de dichos dispositivos. Por otra parte, los códigos bidimensionales son usados en múltiples soportes para la realización de la  
15 codificación/decodificación de información relativa principalmente a direcciones de páginas web o datos de contacto a modo de tarjeta de visita. Así pues, los códigos imágenes bidimensionales ofrecen la posibilidad de obtener información digital mediante el uso de las cámaras fotográficas de los dispositivos móviles para posteriormente acceder a un sistema remoto (información de un enlace a una página web) o almacenar datos descodificados en  
20 una base de datos local (actualización de la información de contactos del dispositivo móvil). Sin embargo en ningún caso se tiene control sobre quién puede obtener esos datos y no existe protección en caso de datos sensibles.

En situaciones de emergencia se producen actuaciones y decisiones que dependen de la  
25 información disponible por parte del gestor de la situación en ese momento. El acceso a información importante protegida por la ley de datos puede ser en muchos casos de vital importancia. En estos casos, el propietario de los datos no puede proporcionar dichos datos por varios motivos: no estar presente, no ser mayor de edad, no estar consciente, no hablar el idioma, dificultad para recordar/proporcionar dicha información.

30 La presente invención propone utilizar los dispositivos móviles dotados con cámara fotográfica para su uso en situaciones de emergencia o de inseguridad para la ayuda a la identificación o mejora de la actuación de los profesionales en dichas situaciones a través del tratamiento de códigos bidimensionales que contienen información protegida.

35

Descripción de la invención

La invención se refiere a una plataforma de codificación, una plataforma gestora de lectores de datos sensibles protegidos en códigos bidimensionales y un método para proteger los datos sensibles en imágenes bidimensionales. La presente invención supone una importante ayuda en situaciones de emergencia en las que no es posible contactar, no está disponible la fuente propietaria de la información o simplemente no existe cobertura de datos para la consulta de información almacenada en servidores, permitiendo obtener y disponer de la información sensible para la toma de decisiones en dichas situaciones de emergencia.

5 En la presente invención se reivindica una plataforma para la codificación de datos sensibles incorporados mediante encriptación en un código bidimensional y su aplicación para la visualización de datos susceptibles de protección y privacidad. En la presente invención se proporciona al propietario de los datos sensibles un código bidimensional, la información contenida en dicho código bidimensional siendo posible incluir tanto datos sin cifrar como datos cifrados. Los datos cifrados comprenden el conjunto de datos sensibles que su propietario protege para ser usados mediante lectores autorizados y solo en caso de extrema necesidad o de consulta por organismos autorizados. En una situación de emergencia se puede obtener con un dispositivo móvil dotado de cámara una imagen del código bidimensional. A partir de dicha imagen se obtienen los datos sin cifrar y en caso de ser un dispositivo móvil autorizado también se obtienen, aplicando un proceso de descifrado, los datos sensibles que el propietario ha considerado proteger.

La plataforma gestora de lectores contempla la autorización de aplicaciones lectoras y usuarios autorizados a la lectura de los datos protegidos mediante un sistema de activación que comprende un servidor que actúa como agente de verificación de los usuarios autorizados, una aplicación que realiza la petición de activación para proceder a la lectura de datos protegidos en los códigos bidimensionales y un mecanismo de encriptación asimétrica que permita la actualización de datos de las aplicaciones lectoras permitiendo el proceso de activación de las mismas, indicando fecha de caducidad de la autorización e intercambio de estadísticas de lecturas realizadas, mejorando de esta forma la gestión de los lectores autorizados. El mecanismo de encriptación asimétrica permite la actualización de las claves simétricas entre la plataforma y las aplicaciones lectoras autorizadas permitiendo incrementar la seguridad de todo el conjunto mediante la variación de las claves de codificación de datos.

35

Un primer aspecto de la presente invención se refiere a un método de obtención de información sensible mediante dispositivo móvil. El método comprende al menos las siguientes etapas:

- 5           - Capturar, utilizando una cámara de un dispositivo móvil, un código bidimensional que contiene información pública sin encriptar e información sensible encriptada mediante una clave simétrica, donde dichos datos están ordenados según una determinada estructura interna.
- Obtener la información binaria del código bidimensional.
- 10          - Obtener, a partir de dicha información binaria y conociendo la estructura interna de los datos, la información pública del código bidimensional.
- Realizar una descriptación simétrica de la parte de la información binaria que corresponde a la información sensible encriptada, obteniendo la información sensible.

15 El método puede además comprender la etapa de mostrar en la pantalla del dispositivo móvil la información pública y la información sensible obtenidas.

Un segundo aspecto de la presente invención se refiera a un dispositivo móvil para obtención de información sensible, que comprende una cámara y una aplicación lectora de códigos bidimensionales instalada en el dispositivo móvil. La aplicación lectora de códigos bidimensionales está configurada para:

- 20           - Capturar, utilizando la cámara del dispositivo móvil, un código bidimensional que contiene información pública sin encriptar e información sensible encriptada mediante una clave simétrica, donde dichos datos están ordenados según una determinada estructura interna.
- 25           - Obtener la información binaria del código bidimensional.
- Obtener, a partir de dicha información binaria y conociendo la estructura interna de los datos, la información pública del código bidimensional.
- Realizar una descriptación simétrica de la parte de la información binaria que corresponde a la información sensible encriptada, obteniendo la información sensible.

30 La aplicación lectora de códigos bidimensionales puede estar además configurada para mostrar en la pantalla del dispositivo móvil la información pública y la información sensible obtenidas.

35 En una realización preferida la aplicación lectora de códigos bidimensionales ha sido

previamente activada mediante intercambio de datos con encriptación asimétrica con una plataforma gestora, a partir de los cuales la aplicación recibe la clave simétrica de lectura del código bidimensional, la estructura interna de los datos y la fecha de caducidad de la activación.

5

Un tercer aspecto de la presente invención se refiere a un producto de programa que comprende medios de instrucciones de programa para llevar a cabo el método definido anteriormente cuando el programa se ejecuta en un dispositivo móvil. El producto de programa está preferiblemente almacenado en un medio de soporte de programas, tales como un pendrive, un CD, un DVD o un disco duro.

10

Un cuarto aspecto de la presente invención se refiere a un método de generación de código bidimensional con información sensible para su lectura mediante dispositivo móvil, que comprende las siguientes etapas:

15

- Recibir una unidad de procesamiento de datos una serie de datos desglosados en información pública y en información sensible que se quiere proteger.

- Encriptar la información sensible mediante una clave simétrica, obteniendo una información sensible encriptada.

20

- Generar un código bidimensional que contiene la información pública sin encriptar y la información sensible encriptada.

Los datos son preferentemente introducidos por un usuario en un formulario web y son recibidos por un servidor web, el cual envía al usuario el código bidimensional generado.

25

#### Breve descripción de los dibujos

A continuación se pasa a describir de manera muy breve una serie de dibujos que ayudan a comprender mejor la invención y que se relacionan expresamente con una realización de dicha invención que se presenta como un ejemplo no limitativo de ésta.

30

La Figura 1 muestra un diagrama de bloques de la plataforma generadora del código bidimensional.

La Figura 2 muestra un diagrama de bloques de la plataforma gestora de los lectores autorizados para leer el código bidimensional.

35

La Figura 3 muestra el esquema funcional del proceso de generación del código bidimensional con la información protegida ofrecida por el titular de dicha información.

5 La Figura 4 muestra el esquema funcional del proceso de activación de la aplicación lectora instalada en los lectores autorizados.

La Figura 5 muestra el esquema del proceso de lectura de la información protegida por parte de los lectores autorizados y activados previamente.

#### 10 Descripción detallada de la invención

La presente invención se refiere a una plataforma que permite la encriptación de datos sensibles mediante códigos bidimensionales y su posterior lectura y utilización. Los datos sensibles pueden ser de diferente índole, por ejemplo datos médicos.

15 La **Figura 1** representa un esquema funcional de la plataforma generadora del código bidimensional. Un usuario 1 (por ejemplo, un turista a punto de partir de viaje a una región de su país o a otro país) introduce en un formulario web, utilizando un dispositivo electrónico 2 (un ordenador, una PDA, un *smartphone*, etc.) una serie de datos 3 que se envían a través de Internet 4 a un servicio web/API 5 gestionado por un servidor web 6. Los datos 3 se  
20 desglosan en datos públicos o de carácter general y unos datos privados o confidenciales (como por ejemplo, información médica del usuario) que el usuario 1 quiere proteger.

La plataforma generadora o servidor web 6 se encarga de generar un código bidimensional (en particular, un código QR) que contiene información sin encriptar (los datos públicos) e  
25 información encriptada (los datos privados, confidenciales). Los datos públicos y privados se disponen bien de forma consecutiva o bien mezclados, de acuerdo a una determinada estructura que no sigue ningún patrón que permita indicar dónde empiezan los datos públicos y dónde empiezan los datos privados, con el objeto de no establecer pautas que permitan la obtención de información para la rotura de la protección de codificación de los  
30 datos privados. El código bidimensional 9 generado se envía al usuario, bien de forma digital 7 por parte del propio servidor web 6 al propio dispositivo electrónico 2 para que el usuario 1 lo imprima, o mediante un envío físico 8 mediante el que el usuario recibe un soporte físico 10 (e.g. una tarjeta o carnet) con el código bidimensional 9 imprimido en él. La plataforma generadora no almacena ninguna información que el usuario ha remitido para crear el  
35 código bidimensional, el cual una vez generado y enviado de vuelta al usuario tampoco es

almacenado en el servidor.

La **Figura 2** representa un esquema de la plataforma gestora de lectores autorizados para leer el código bidimensional 9 previamente creado por la plataforma generadora. Los usuarios 11 de esta plataforma gestora serían por ejemplo los integrantes de los diferentes servicios de emergencias (médicos, policías, etc.), los cuales utilizan un dispositivo móvil 12 (por ejemplo, un *smartphone* o una tableta electrónica) con una cámara fotográfica y una aplicación lectora del código bidimensional, a través del cual el usuario 11 puede leer la información contenida en el código bidimensional 9 que está impreso en el soporte físico 10. Para ello el usuario 11 enfoca 13 la cámara del dispositivo móvil 12 al código bidimensional 9, hace una foto del mismo y la aplicación lectora instalada en el dispositivo móvil 12 será capaz de obtener los datos encriptados del código sin necesidad de disponer de conectividad de datos. Para el acceso a la información sensible y el correcto tratamiento de los datos leídos por la aplicación lectora, la ordenación y estructura interna de los datos públicos y privados dentro del código bidimensional es conocida por la propia aplicación lectora. El proceso de activación de la aplicación proporciona mediante comunicación cifrada la información necesaria tanto de la estructura interna de la información sensible, como las claves para su lectura, así como la fecha de validez de la activación. Por tanto, el proceso de activación de la aplicación se debe realizar con anterioridad a la realización de capturas de códigos bidimensionales mediante el uso de algún mecanismo de conexión de datos con la plataforma gestora de lectores (wifi, 3G).

En este punto es necesario recordar que el código bidimensional integra dos niveles de datos: datos en abierto y datos encriptados. La selección del nivel de protección de los datos introducidos por el usuario en la plataforma generadora la realiza el mismo usuario en el proceso de generación. Los datos en abierto serán accesibles mediante una aplicación lectora general de imágenes bidimensionales con salida de texto. En este caso el usuario lector podrá identificar el texto en abierto que serán caracteres coherentes, del texto cifrado que aparecerá como una secuencia aleatoria de caracteres sin sentido. Los datos encriptados solo serán accesibles mediante la aplicación lectora específica previo proceso de activación o autorización.

El proceso de activación de las aplicaciones lectoras específicas se basa en la autorización por parte de la plataforma gestora de cada organismo oficial involucrado en tareas de emergencias (agentes de seguridad, sanidad, bomberos, etc.). Cada organismo oficial

puede gestionar las autorizaciones de las aplicaciones lectoras específicas que usarán sus agentes.

El proceso de activación consistirá en un intercambio de datos 17 entre una plataforma gestora de lectores 20, gestionado por un servidor 16, y las aplicaciones lectoras de los dispositivos móviles 12. Este intercambio de datos se realiza mediante comunicación de datos con encriptación asimétrica. El registro de la aplicación lectora y su desbloqueo para realizar el proceso de obtención de datos encriptados se realiza de la siguiente forma:

1. La aplicación lectora específica se instala en el dispositivo móvil 12 del agente.
2. La aplicación lectora específica pide código de identificación del agente. Dicho código deberá ser proporcionado por el organismo oficial al cual el agente está adscrito.
3. La aplicación lectora específica comunica dicho código a la plataforma gestora 20 que una vez validada la identificación sin duplicidades se realizará el intercambio de datos 17 para proceder al desbloqueo y actualización de la aplicación. Dicho intercambio actualiza tanto la clave simétrica de lectura como la fecha máxima de la autorización, así como información relativa al formato de los datos.

Una vez activada la aplicación, se muestra en la pantalla del dispositivo móvil 12 la información contenida en el código bidimensional 9, tanto los datos públicos como los datos confidenciales debidamente descifrados. De esta forma, si la persona poseedora del soporte físico 10 con el código bidimensional 9 impreso tuviera por ejemplo algún accidente, los servicios de emergencias serían capaces de leer la información encriptada (datos médicos relevantes incluyendo grupo sanguíneo, medicamentos o principios activos a los que es alérgico, etc.) utilizando un dispositivo móvil 12 lector para así poder asistirle con rapidez. Parte importante de la presente invención radica en que el código QR contiene los dos tipos de información, la pública y la encriptada (no se requiere conexión de datos para el acceso a la información), y que ésta última sólo puede ser visualizada por usuarios (e.g. médicos, policías) previamente autorizados.

La **Figura 3** representa un esquema del proceso de generación 100 de la imagen bidimensional con información protegida. En un primer paso 102 el propietario de la información sensible se conecta a la plataforma generadora del código bidimensional. Como se ha indicado previamente en la descripción de la Figura 1, en una realización particular el usuario 1 rellena un formulario web con información pública 104 (información no sensible) y



con información sensible 106 (información privada). A continuación la información sensible 106 se encripta mediante encriptación simétrica con una clave que será establecida para todos los usuarios y que deberá estar relacionada con la clave de la aplicación lectora, obteniendo información sensible encriptada 108. Posteriormente se genera el código bidimensional 110 sin almacenar los datos sensibles en la plataforma generadora. El propietario finalmente recibe 112 el código bidimensional generado, bien en formato digital para que lo imprima o en formato ya impreso.

La **Figura 4** muestra un esquema del proceso de activación 200 de la aplicación lectora del código bidimensional (app lectora) instalada en el dispositivo móvil 12. La plataforma gestora 20 de la app lectora está gestionada por diferentes organismos autorizados. Un agente autorizado se encarga de acceder a la plataforma gestora 20, descargar e instalar 202 la app lectora específica en el dispositivo móvil 12 para proceder a su activación o desbloqueo junto con el identificador del agente autorizado. A continuación se lleva a cabo la activación 204 de la aplicación lectora. Para ello la app lectora pide el identificador para su activación. La app lectora se comunica entonces con la plataforma gestora 20 y recibe una clave lectora y una fecha de caducidad de la activación. La aplicación lectora queda activa 206 hasta la fecha de caducidad. La app lectora es activada para descifrar la información cifrada contenida en el código bidimensional 9.

La **Figura 5** muestra un esquema del proceso de lectura 300 de la información protegida en el código bidimensional 9. El dispositivo móvil 12 que tiene instalada una app activada debidamente autorizada, hace una foto 302 del código bidimensional 9. A continuación se obtiene 304 la información binaria del código bidimensional 9, a partir de la cual la aplicación lectora obtiene la información pública 106 no sensible y realiza una descifrado simétrica 308, utilizando la clave lectora recibida, de la información cifrada incluida en el código bidimensional 9, obteniendo la información sensible 106. La información pública 104 obtenida puede ser leída 312 por cualquier lector de códigos bidimensionales, al no estar encriptada. Sin embargo, la información sensible 106 obtenida únicamente es accesible mediante la aplicación lectora específica siempre que esta esté desbloqueada mediante la identificación del agente autorizado. Tanto la información sensible 106 como la información pública 104 se muestra 314 en la pantalla del dispositivo móvil 12 y el agente autorizado accede entonces a dicha información.

## REIVINDICACIONES

1. Método de obtención de información sensible mediante dispositivo móvil, caracterizado por que comprende:

- 5           - generar un código bidimensional (9) que contiene información pública (104) sin encriptar e información sensible encriptada (108) mediante una clave simétrica, donde dichos datos están ordenados según una determinada estructura interna;
- activar (206) una aplicación lectora de códigos bidimensionales instalada en un dispositivo móvil (12) mediante intercambio de datos (17) con encriptación asimétrica con  
10 una plataforma gestora (20), a partir de los cuales la aplicación lectora recibe la clave simétrica de lectura del código bidimensional (9) y su estructura interna de datos;
- capturar (302), utilizando una cámara del dispositivo móvil (12), el código bidimensional (9) previamente generado;
- obtener la información binaria (304) del código bidimensional (9);
- 15           - obtener, a partir de dicha información binaria (304) y conociendo la estructura interna de los datos, la información pública (104) del código bidimensional (9); y
- realizar una desencriptación simétrica (308) de la parte de la información binaria (304) que corresponde a la información sensible encriptada (108), obteniendo la información sensible (106).

20

2. Método según la reivindicación 1, caracterizado por que comprende mostrar (314) en la pantalla del dispositivo móvil (12) la información pública (104) y la información sensible (106) obtenidas.

25

3. Método según cualquiera de las reivindicaciones anteriores, caracterizado por que la generación del código bidimensional (9) comprende:

- recibir una unidad de procesamiento de datos una serie de datos (3) desglosados en información pública (104) y en información sensible (106) que se quiere proteger;
- encriptar la información sensible (106) mediante la clave simétrica, obteniendo una  
30 información sensible encriptada (108); y
- generar (110) el código bidimensional que contiene la información pública (104) sin encriptar y la información sensible encriptada (108).

35

4. Método según la reivindicación 3, caracterizado por que los datos (3) son introducidos (102) por un usuario (1) en un formulario web y son recibidos por una plataforma generadora (6), la cual envía al usuario (1) el código bidimensional generado.

5. Sistema de obtención de información sensible mediante dispositivo móvil, caracterizado por que comprende:

5 una plataforma generadora (6) configurada para generar un código bidimensional (9) que contiene información pública (104) sin encriptar e información sensible encriptada (108) mediante una clave simétrica, donde dichos datos están ordenados según una determinada estructura interna;

10 una plataforma gestora (20) configurada para activar (206) una aplicación lectora de códigos bidimensionales instalada en un dispositivo móvil (12) mediante intercambio de datos (17) con encriptación asimétrica con el dispositivo móvil (12), a partir de los cuales la aplicación lectora recibe la clave simétrica de lectura del código bidimensional (9) y su estructura interna de datos; y

15 un dispositivo móvil (12) con una cámara y la aplicación lectora de códigos bidimensionales instalada en el dispositivo móvil (12), donde la aplicación lectora de códigos bidimensionales está configurada para:

- capturar (302), utilizando la cámara del dispositivo móvil (12), el código bidimensional (9) previamente generado por la plataforma generadora (6);

- obtener la información binaria (304) del código bidimensional (9);

20 - obtener, a partir de dicha información binaria (304) y conociendo la estructura interna de los datos, la información pública (104) del código bidimensional (9); y

- realizar una desencriptación simétrica (308) de la parte de la información binaria (304) que corresponde a la información sensible encriptada (108), obteniendo la información sensible (106).

25 6. Sistema según la reivindicación 5, caracterizado por que la aplicación lectora de códigos bidimensionales está configurada para mostrar (314) en la pantalla del dispositivo móvil (12) la información pública (104) y la información sensible (106) obtenidas.

30 7. Sistema según cualquiera de las reivindicaciones 5 a 6, caracterizado por que el intercambio de datos (17) entre la plataforma gestora (20) y la aplicación lectora de códigos bidimensionales incluye la fecha de caducidad de la activación.

35 8. Sistema según cualquiera de las reivindicaciones 5 a 7, caracterizado por que la plataforma generadora (6) es un servidor web.

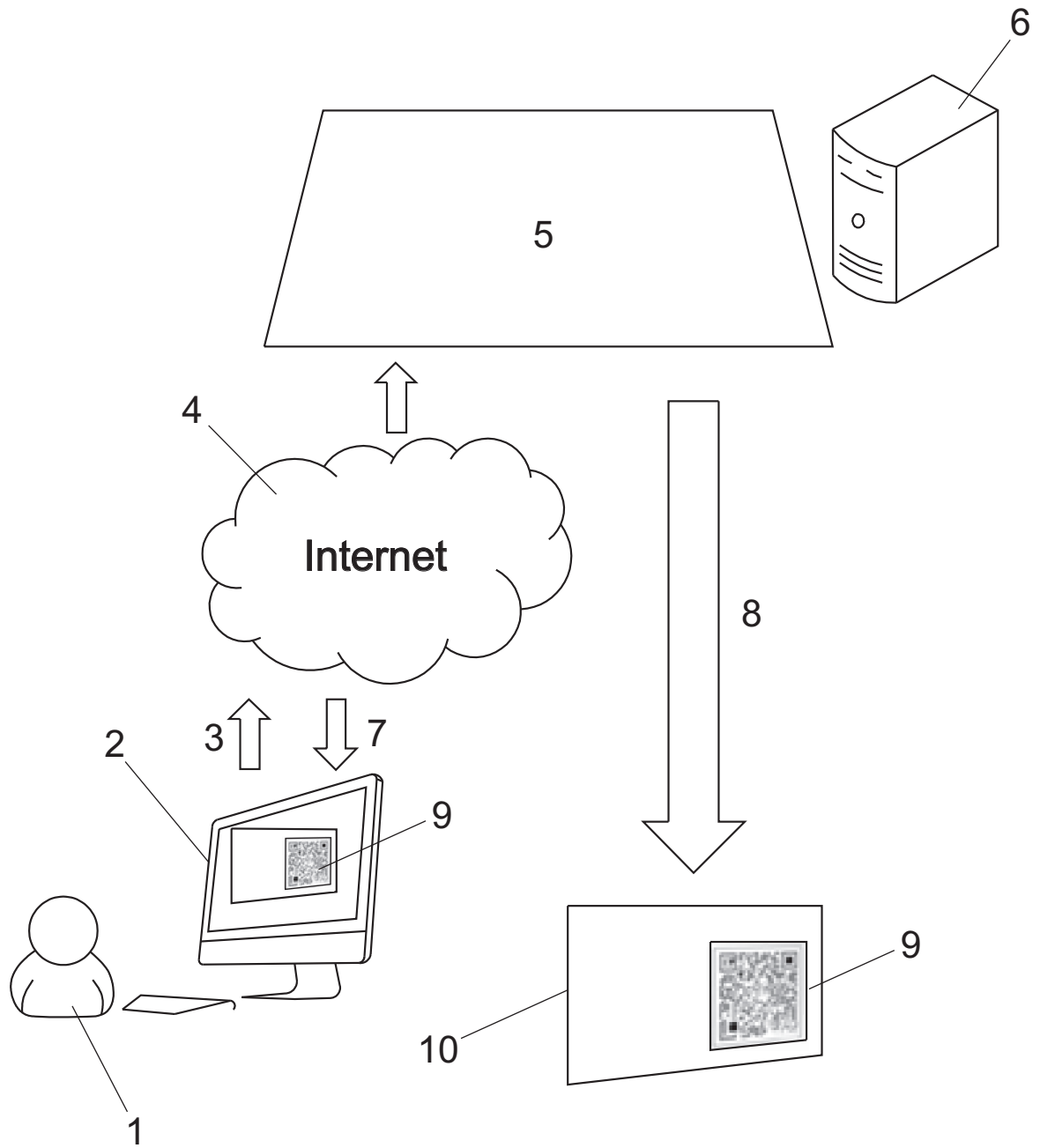


Fig. 1

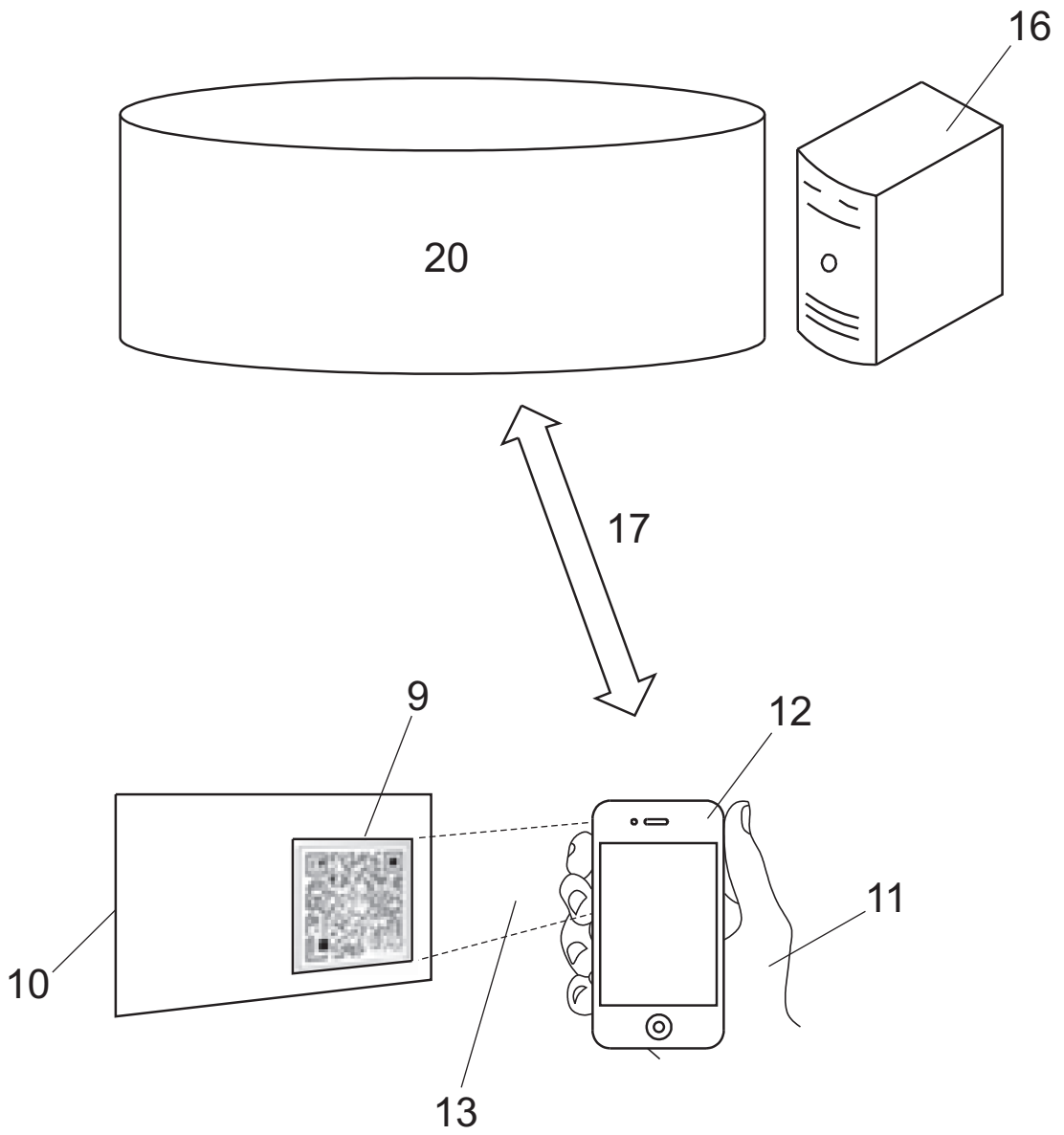


Fig. 2

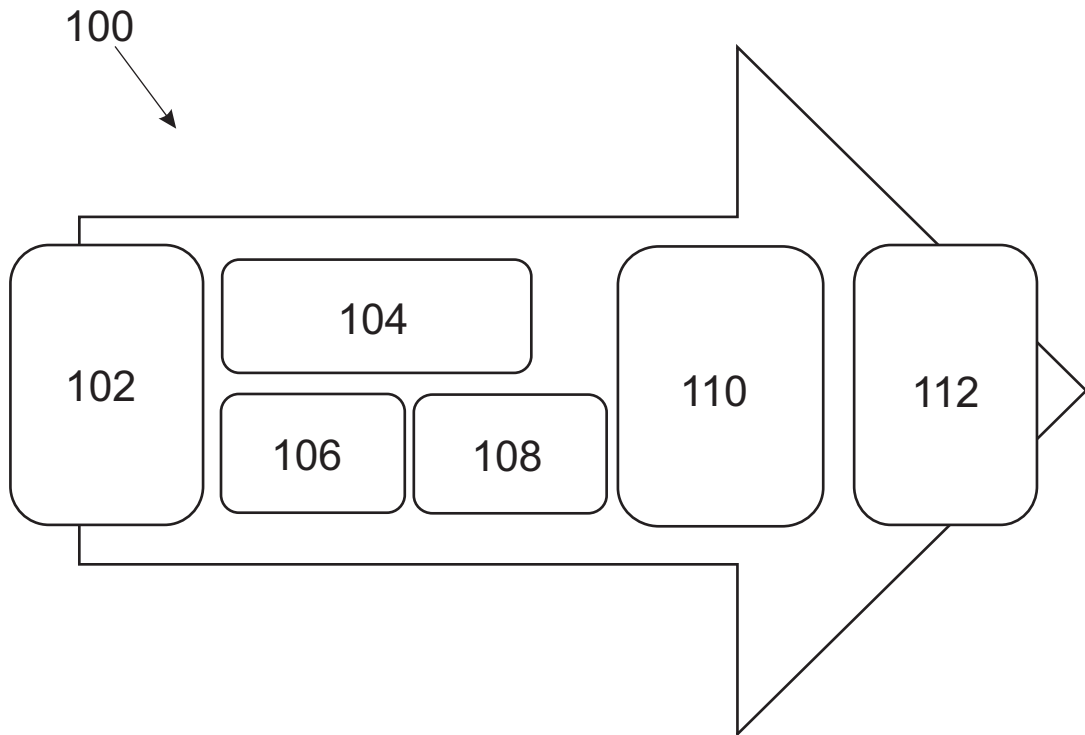


Fig. 3

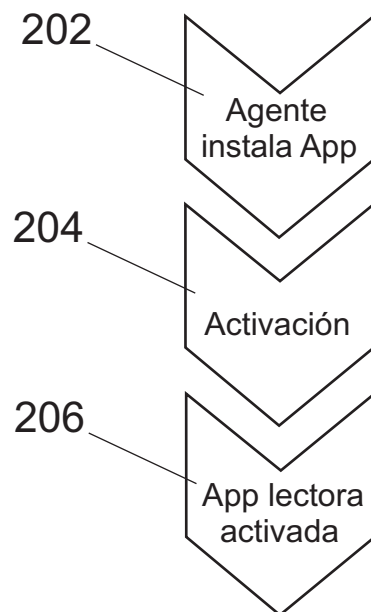
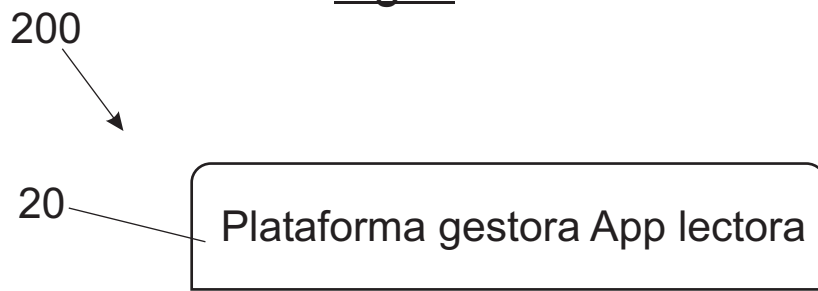


Fig. 4

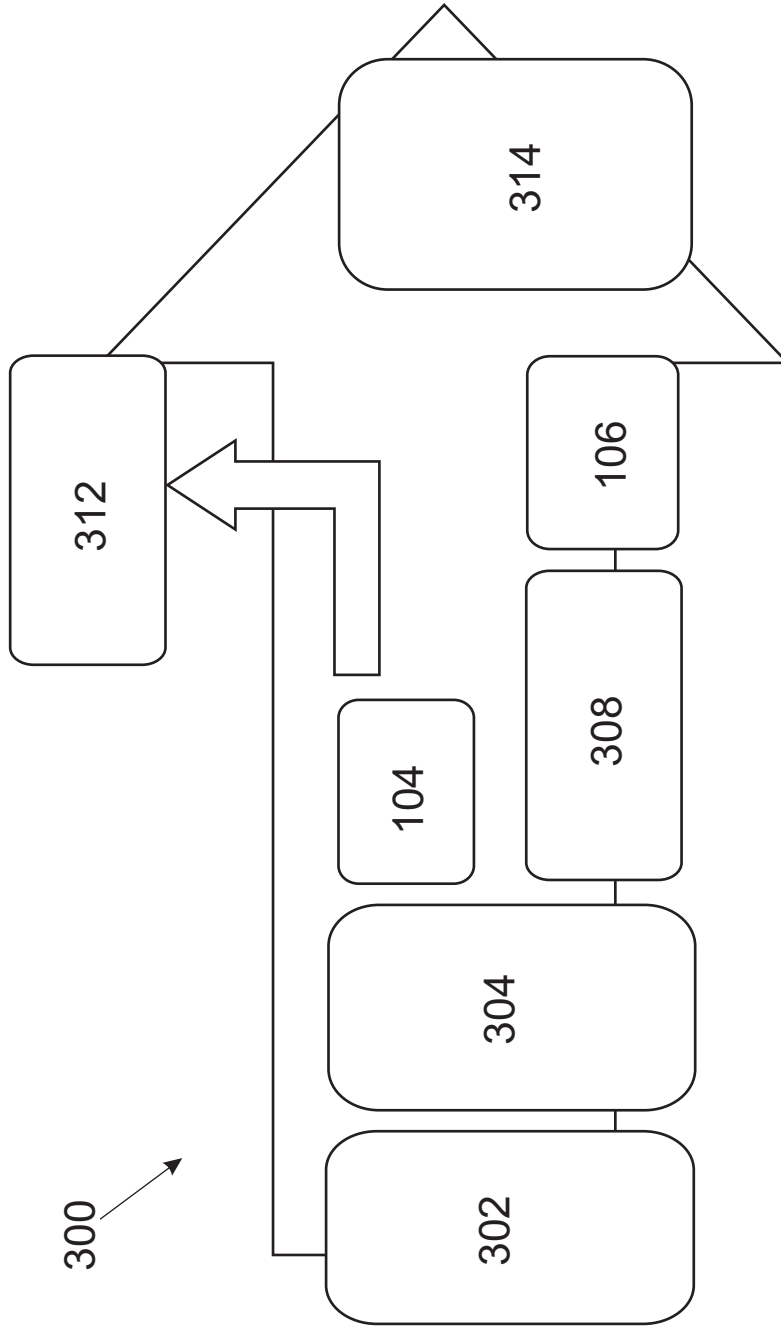


Fig. 5



OFICINA ESPAÑOLA  
DE PATENTES Y MARCAS

ESPAÑA

②① N.º solicitud: 201530982

②② Fecha de presentación de la solicitud: 08.07.2015

③② Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

⑤① Int. Cl.: **G06F21/62** (2013.01)  
**H04W12/02** (2009.01)

DOCUMENTOS RELEVANTES

Categoría	⑤⑥ Documentos citados	Reivindicaciones afectadas
X	US 2013159699 A1 (TORKKEL JUHA) 20.06.2013, página 3, líneas 26-29; página 10, línea 17 – página 11, línea 22; página 12, línea 5 – página 13, línea 6; página 14, líneas 14-29; página 15, líneas 8-31; página 16, líneas 15-16; página 16, líneas 20-22.	1-8
A	US 2012209749 A1 (HAMMAD AYMAN et al.) 16.08.2012, párrafo [0075].	7
A	US 2015040199 A1 (SURACE DOMENICO et al.) 05.02.2015, párrafos [0042-0044],[0079-0119].	7

Categoría de los documentos citados

X: de particular relevancia

Y: de particular relevancia combinado con otro/s de la misma categoría

A: refleja el estado de la técnica

O: referido a divulgación no escrita

P: publicado entre la fecha de prioridad y la de presentación de la solicitud

E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

**El presente informe ha sido realizado**

para todas las reivindicaciones

para las reivindicaciones nº:

Fecha de realización del informe  
08.02.2016

Examinador  
M. L. Álvarez Moreno

Página  
1/5



Documentación mínima buscada (sistema de clasificación seguido de los símbolos de clasificación)

G06F, H04W

Bases de datos electrónicas consultadas durante la búsqueda (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)

INVENES, EPODOC, WPI

Fecha de Realización de la Opinión Escrita: 08.02.2016

**Declaración**

<b>Novedad (Art. 6.1 LP 11/1986)</b>	Reivindicaciones 1-8	<b>SI</b>
	Reivindicaciones	<b>NO</b>
<b>Actividad inventiva (Art. 8.1 LP11/1986)</b>	Reivindicaciones	<b>SI</b>
	Reivindicaciones 1-8	<b>NO</b>

Se considera que la solicitud cumple con el requisito de aplicación industrial. Este requisito fue evaluado durante la fase de examen formal y técnico de la solicitud (Artículo 31.2 Ley 11/1986).

**Base de la Opinión.-**

La presente opinión se ha realizado sobre la base de la solicitud de patente tal y como se publica.

**1. Documentos considerados.-**

A continuación se relacionan los documentos pertenecientes al estado de la técnica tomados en consideración para la realización de esta opinión.

Documento	Número Publicación o Identificación	Fecha Publicación
D01	US 2013159699 A1 (TORKKEL JUHA)	20.06.2013
D02	US 2012209749 A1 (HAMMAD AYMAN et al.)	16.08.2012
D03	US 2015040199 A1 (SURACE DOMENICO et al.)	05.02.2015

**2. Declaración motivada según los artículos 29.6 y 29.7 del Reglamento de ejecución de la Ley 11/1986, de 20 de marzo, de Patentes sobre la novedad y la actividad inventiva; citas y explicaciones en apoyo de esta declaración****Reivindicación independiente de método 1**

El documento D01 muestra un método para, mediante la cámara de un teléfono móvil, obtener información tanto pública como privada contenida en una etiqueta de código bidimensional. Para analizar el documento se va a utilizar la misma terminología usada en la redacción de las reivindicaciones. El método divulgado en D01 comprende las siguientes etapas:

- generar un código bidimensional que contiene información sin encriptar e información encriptada mediante una clave asimétrica, donde dichos datos están ordenados según una determinada estructura interna; (página 10, línea 17 - página 11, línea 22; página 12, líneas 5-10; página 14, líneas 14-29)
- activar una aplicación lectora de códigos bidimensionales instalada en un dispositivo móvil mediante intercambio de datos con una plataforma, a partir de los cuales la aplicación lectora recibe la clave de lectura del código bidimensional y su estructura interna de datos (página 3, líneas 26-29; página 15, líneas 29-31; página 16, líneas 15-16 y 20-22);
- capturar, utilizando una cámara del dispositivo móvil, el código bidimensional previamente generado (página 15, líneas 8-10);
- obtener la información binaria del código bidimensional (página 15, líneas 10-12);
- obtener, a partir de dicha información binaria y conociendo la estructura interna de los datos, la información pública del código bidimensional; y (página 15, líneas 10-11; 20-26)
- realizar una descriptación asimétrica de la parte de la información binaria que corresponde a la información encriptada, obteniendo la información sensible (página 15, líneas 10-26)

Se identifican dos diferencias entre el método mostrado en el documento D01 y el de la reivindicación 1. La primera de ellas consiste en que D01 no especifica que el modo de obtención de la clave sea mediante intercambio de datos con encriptación asimétrica pero sí indica (página 3, líneas 26-29; página 12, línea 30 - página 13, línea 6) que el terminal recibe dicha clave de forma directa o indirecta a través de la red y desde el sistema informático que almacena toda la información.

La utilización de comunicaciones seguras para proteger intercambios de información es de uso habitual en las comunicaciones informáticas. En la reivindicación no se identifican características adicionales relacionadas con dicho intercambio cifrado que pudieran contribuir a conferir actividad inventiva. La segunda diferencia consiste en la utilización de distintos tipos de encriptación para el cifrado de los datos en el código bidimensional. D01 utiliza asimétrica y la reivindicación simétrica. La encriptación requiere en ambos casos (simétrico o asimétrico) la utilización de claves previamente conocidas por el dispositivo móvil. En la reivindicación no se identifican características adicionales relacionadas con dicho cifrado simétrico que pudieran contribuir a conferir actividad inventiva.

La reivindicación 1 no cumple el requisito de actividad inventiva según el artículo 8 de la Ley de Patentes.

**Reivindicación dependiente de método 2**

El dispositivo del documento D01 muestra la información en la pantalla (página 16, líneas 26 y 28; página 17, líneas 2-3 y 8-9).

La reivindicación 2 no cumple el requisito de actividad inventiva según el artículo 8 de la Ley de Patentes.

**Reivindicación dependiente de método 3**

La generación del código bidimensional comprende (página 14, líneas 14-29):

- recibir una serie de datos desglosados en información pública y en información que se quiere proteger;
- encriptar la información sensible mediante la clave, obteniendo una información encriptada; y
- generar el código bidimensional que contiene la información pública sin encriptar y la información encriptada.

La reivindicación 3 no cumple el requisito de actividad inventiva según el artículo 8 de la Ley de Patentes.

**Reivindicación dependiente de método 4**

En el documento D01 (página 13, línea 22 - página 14, línea 13) se indica que a la plataforma generadora se le facilitan los datos necesarios para generar el código. Aunque de forma preferente el código se imprime en una etiqueta, el servidor dispone de medios para enviar códigos bidimensionales al usuario (página 21, líneas 20-31). La reivindicación 4 no define características técnicas particulares relacionadas ni con la comunicación de datos ni con el envío de los códigos que puedan contribuir a conferir actividad inventiva.

La reivindicación 4 no cumple el requisito de actividad inventiva según el artículo 8 de la Ley de Patentes.

**Reivindicación independiente de sistema 5**

Se aplican los mismos argumentos indicados al analizar la reivindicación 1. El documento D01 muestra un sistema que dispone de los medios apropiados para realizar las mismas acciones que se definen en la reivindicación 5. Medios para generar un código bidimensional que contiene información sin encriptar e información encriptada mediante una clave, donde dichos datos están ordenados según una determinada estructura interna; medios para activar una aplicación lectora de códigos bidimensionales instalada en un dispositivo móvil, a partir de los cuales la aplicación lectora recibe la clave de lectura del código bidimensional y su estructura interna de datos; y un dispositivo móvil con una cámara y la aplicación lectora de códigos bidimensionales instalada en el dispositivo móvil, donde la aplicación lectora de códigos bidimensionales está configurada para:

- capturar, utilizando la cámara del dispositivo móvil, el código bidimensional previamente generado;
- obtener la información binaria del código bidimensional;
- obtener, a partir de dicha información binaria y conociendo la estructura interna de los datos, la información pública del código bidimensional; y
- realizar una desencriptación de la parte de la información binaria que corresponde a la información encriptada, obteniendo dicha información.

La reivindicación 5 no cumple el requisito de actividad inventiva según el artículo 8 de la Ley de Patentes.

**Reivindicación dependiente de sistema 6**

Se aplican los mismos argumentos que al analizar la reivindicación 2.

La reivindicación 6 no cumple el requisito de actividad inventiva según el artículo 8 de la Ley de Patentes.

**Reivindicación dependiente de sistema 7**

La utilización de fechas de expiración o caducidad es de uso habitual en plataformas informáticas, ya sea como periodos de validez de claves de cifrado (p.ej. claves de un solo uso) o como periodos de validez relacionados con autorizaciones de uso de aplicaciones y/o servicios específicos (D02 párrafo 0075; D03 párrafos 0042-0044; 0079-0119).

La reivindicación no define características particulares relacionadas ni con el intercambio de datos entre la plataforma gestora y la aplicación lectora de códigos bidimensionales sobre la fecha de caducidad de la activación, ni sobre la utilización de dicha fecha de caducidad que puedan contribuir a conferir actividad inventiva.

La reivindicación 7 no cumple el requisito de actividad inventiva según el artículo 8 de la Ley de Patentes.

**Reivindicación dependiente de sistema 8**

Los medios generadores del código en D01 se corresponden con un sistema informático conectado en red (página 3, líneas 26-29). La reivindicación no identifica características particulares del servidor web que puedan contribuir a conferir actividad inventiva.

La reivindicación 8 no cumple el requisito de actividad inventiva según el artículo 8 de la Ley de Patentes.